



사용자 가이드

AWS 복원력 허브



AWS 복원력 허브: 사용자 가이드

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 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 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

AWS Resilience Hub란 무엇인가요?	1
AWS Resilience Hub – 복원력 관리	1
AWS Resilience Hub 작동 방식	2
AWS Resilience Hub – 복원력 테스트	4
AWS Resilience Hub 개념	5
복원력	6
Recovery Point Objective(RPO)	6
Recovery Time Objective(RTO)	6
예상 워크로드 복구 시간 목표	6
예상 워크로드 복구 시점 목표	6
Application	6
애플리케이션 구성 요소	6
애플리케이션 규정 준수 상태	7
드리프트 감지	7
복원력 평가	8
복원력 점수	8
중단 유형	8
AWS FIS 실험	8
SOP	9
AWS Resilience Hub 페르소나	9
지원되는 AWS Resilience Hub 리소스	10
AWS Resilience Hub 및 myApplications	14
자세히 알아보기	15
시작	16
사전 조건	16
애플리케이션 추가	17
애플리케이션을 추가하여 시작하기	18
애플리케이션 리소스 관리	18
애플리케이션에 리소스 AWS Resilience Hub 추가	19
RTO 및 RPO 설정	23
예약된 평가 및 드리프트 알림 설정	24
권한 설정	26
애플리케이션 구성 파라미터 구성	27
애플리케이션에 태그 추가	27

검토 및 게시	28
평가 실행	28
사용 AWS Resilience Hub	30
AWS Resilience Hub 요약	30
애플리케이션 상태	31
리소스 유형별 상위 인프라 권장 사항	31
인프라 권장 사항	32
구현되지 않은 운영 권장 사항	32
경보 권장 사항	32
SOP 권장 사항	33
AWS FIS 실험 권장 사항	33
드리프트가 있는 애플리케이션	33
복원력 점수	34
복원력 점수에 대한 하위 10개 애플리케이션	34
정책별 애플리케이션 상태	34
AWS Resilience Hub 대시보드	35
애플리케이션 상태	35
시간 경과에 따른 애플리케이션 복원력 점수	35
구현된 경보	36
구현된 실험	36
애플리케이션 관리	36
애플리케이션 요약 보기	39
애플리케이션 리소스 편집	41
애플리케이션 구성 요소 관리	49
새 애플리케이션 버전 게시	56
애플리케이션 버전 보기	57
애플리케이션 리소스 보기	58
애플리케이션 삭제	59
애플리케이션 구성 파라미터	59
복원력 정책 관리	60
복원력 정책 생성	62
복원력 정책의 세부 정보에 액세스	65
에서 복원력 평가 관리 AWS Resilience Hub	66
에서 복원력 평가 실행 AWS Resilience Hub	66
평가 보고서 검토	67
복원력 평가 삭제	76

복원력 위젯에서 복원력 평가 관리	76
복원력 위젯에서 복원력 평가 실행	77
복원력 위젯에서 평가 요약 검토	78
경보 관리	79
운영 권장 사항에서 경보 생성	80
경보 보기	82
표준 운영 절차 관리	85
AWS Resilience Hub 권장 사항을 기반으로 SOP 구축	87
사용자 지정 SSM 문서 생성	88
기본값 대신 사용자 정의 SSM 문서 사용	88
SOP 테스트	89
표준 운영 절차 보기	89
AWS Fault Injection Service 실험 관리	91
실험 시작, 생성 및 실행 AWS FIS	91
AWS FIS 실험 보기	94
AWS Fault Injection Service 실험 실패/상태 확인	96
복원력 점수 이해	99
애플리케이션의 복원력 점수에 액세스	100
복원력 점수 계산	102
권장 사항을 애플리케이션에 통합	111
AWS CloudFormation 템플릿 수정	114
AWS Resilience Hub APIs 사용하여 애플리케이션 설명 및 관리	118
애플리케이션 준비	118
애플리케이션 만들기	118
복원력 정책 생성	119
애플리케이션 리소스 가져오기 및 가져오기 상태 모니터링	120
애플리케이션을 게시하고 복원력 정책을 할당합니다.	122
애플리케이션 실행 및 분석	124
복원력 평가 실행 및 모니터링	124
복원력 정책 생성	127
애플리케이션 수정	142
리소스를 수동으로 추가합니다.	142
리소스를 단일 애플리케이션 구성 요소로 그룹화	144
AppComponent에서 리소스 제외하기	145
보안	147
데이터 보호	147

저장된 데이터 암호화	148
전송 중 암호화	148
ID 및 액세스 관리	149
대상	149
ID를 통한 인증	150
정책을 사용하여 액세스 관리	153
AWS Resilience Hub와 IAM의 작동 방식	155
IAM 역할 및 권한 설정	167
문제 해결	168
AWS Resilience Hub 액세스 권한 참조	170
AWS 관리형 정책	184
AWS Resilience Hub 페르소나 및 IAM 권한 참조	194
로 Terraform 상태 파일 가져오기 AWS Resilience Hub	197
Amazon EKS 클러스터에 대한 AWS Resilience Hub 액세스 활성화	201
Amazon SNS 주제에 AWS Resilience Hub 게시하도록 활성화	213
AWS Resilience Hub 권장 사항을 포함하거나 제외할 수 있는 권한 제한	214
인프라 보안	215
AWS 서비스에 대한 복원력 검사	216
Amazon Elastic File System	217
파일 시스템 유형	217
파일 시스템 백업	217
데이터 복제	217
Amazon Relational Database Service 및 Amazon Aurora	217
단일 AZ 배포	217
다중 AZ 배포	217
백업	218
리전 간 장애 조치	218
더 빠른 리전 내 장애 조치	218
Amazon Simple Storage Service(S3)	219
버전 관리	219
예약된 백업	219
데이터 복제	219
Amazon DynamoDB	220
예약된 백업	220
글로벌 테이블	220
Amazon Elastic Compute Cloud	220

상태 저장 인스턴스	220
Auto Scaling 그룹	221
Amazon EC2 플릿	221
Amazon EBS	221
예약된 백업	221
데이터 백업 및 복제	222
AWS Lambda	222
고객 Amazon VPC 액세스	222
Dead Letter Queue(DLQ)	222
Amazon Elastic Kubernetes 서비스	222
다중 AZ 배포	223
배포와 ReplicaSet 비교	223
배포 유지 관리	223
Amazon Simple Notification Service	223
주제 구독	224
Amazon Simple Queue Service	224
Dead Letter Queue(DLQ)	224
Amazon Elastic Container Service	224
다중 AZ 배포	224
Elastic Load Balancing	224
다중 AZ 배포	224
Amazon API Gateway	225
리전 간 배포	225
프라이빗 API 다중 AZ 배포	225
Amazon DocumentDB	225
다중 AZ 배포	225
탄력적 클러스터 및 다중 AZ 배포	225
탄력적 클러스터 및 수동 스냅샷	225
NAT 게이트웨이	226
다중 AZ 배포	226
Amazon Route 53	226
다중 AZ 배포	226
Amazon Application Recovery Controller(ARC)	226
다중 AZ 배포	226
Amazon FSx for Windows File Server	227
파일 시스템 유형	227

파일 시스템 백업	227
데이터 복제	227
AWS Step Functions	227
버전 관리 및 별칭	227
리전 간 배포	228
Amazon ElastiCache (Redis OSS)	228
단일 AZ 배포	228
단일 AZ 배포	228
리전 간 장애 조치	228
백업	228
더 빠른 리전 내 장애 조치	229
다른 서비스와 함께 사용	230
AWS CloudFormation	230
AWS Resilience Hub 및 AWS CloudFormation 템플릿	230
에 대해 자세히 알아보기 AWS CloudFormation	231
AWS CloudTrail	231
AWS Systems Manager	231
AWS Trusted Advisor	232
문서 기록	235
AWS 용어집	265
.....	cclxvi

AWS Resilience Hub란 무엇인가요?

AWS Resilience Hub 는에서 애플리케이션의 복원력 태세를 관리하고 개선할 수 있는 중앙 위치입니다. AWS를 AWS Resilience Hub 사용하면 복원력 목표를 정의하고, 이러한 목표에 대한 복원력 태세를 평가하고, AWS Well-Architected Framework를 기반으로 개선을 위한 권장 사항을 구현할 수 있습니다. 또한 AWS Resilience Hub내에서 애플리케이션에 대한 실제 중단을 모방하여 종속성을 더 잘 이해하고 잠재적 약점을 발견하는 실험을 생성하고 실행할 AWS Fault Injection Service 수 있습니다.는 복원력을 지속적으로 강화하는 데 필요한 모든 AWS 서비스와 도구를 중앙에 AWS Resilience Hub 제공합니다. AWS Resilience Hub 는 다른 서비스와 협력하여 권장 사항을 제공하고 애플리케이션 리소스를 관리하는 데 도움이 됩니다. 자세한 내용은 [다른 서비스와 함께 사용](#) 단원을 참조하십시오.

다음 테이블에는 모든 관련 복원력 서비스의 설명서 링크가 나와 있습니다.

관련 AWS 복원력 서비스 및 참조

AWS 복원력 서비스	설명서 링크
AWS Elastic Disaster Recovery	Elastic Disaster Recovery란 무엇입니까?
AWS Backup	정의 AWS Backup
Amazon Application Recovery Controller(ARC) (ARC)	Amazon Application Recovery Controller(ARC)란 무엇입니까?

주제

- [AWS Resilience Hub – 복원력 관리](#)
- [AWS Resilience Hub – 복원력 테스트](#)
- [AWS Resilience Hub 개념](#)
- [AWS Resilience Hub 페르소나](#)
- [AWS Resilience Hub 지원되는 리소스](#)
- [AWS Resilience Hub 및 myApplications](#)

AWS Resilience Hub – 복원력 관리

AWS Resilience Hub 는 AWS 애플리케이션의 복원력을 정의, 검증 및 추적할 수 있는 중앙 위치를 제공합니다. AWS Resilience Hub 는 애플리케이션을 중단으로부터 보호하고 복구 비용을 절감하여

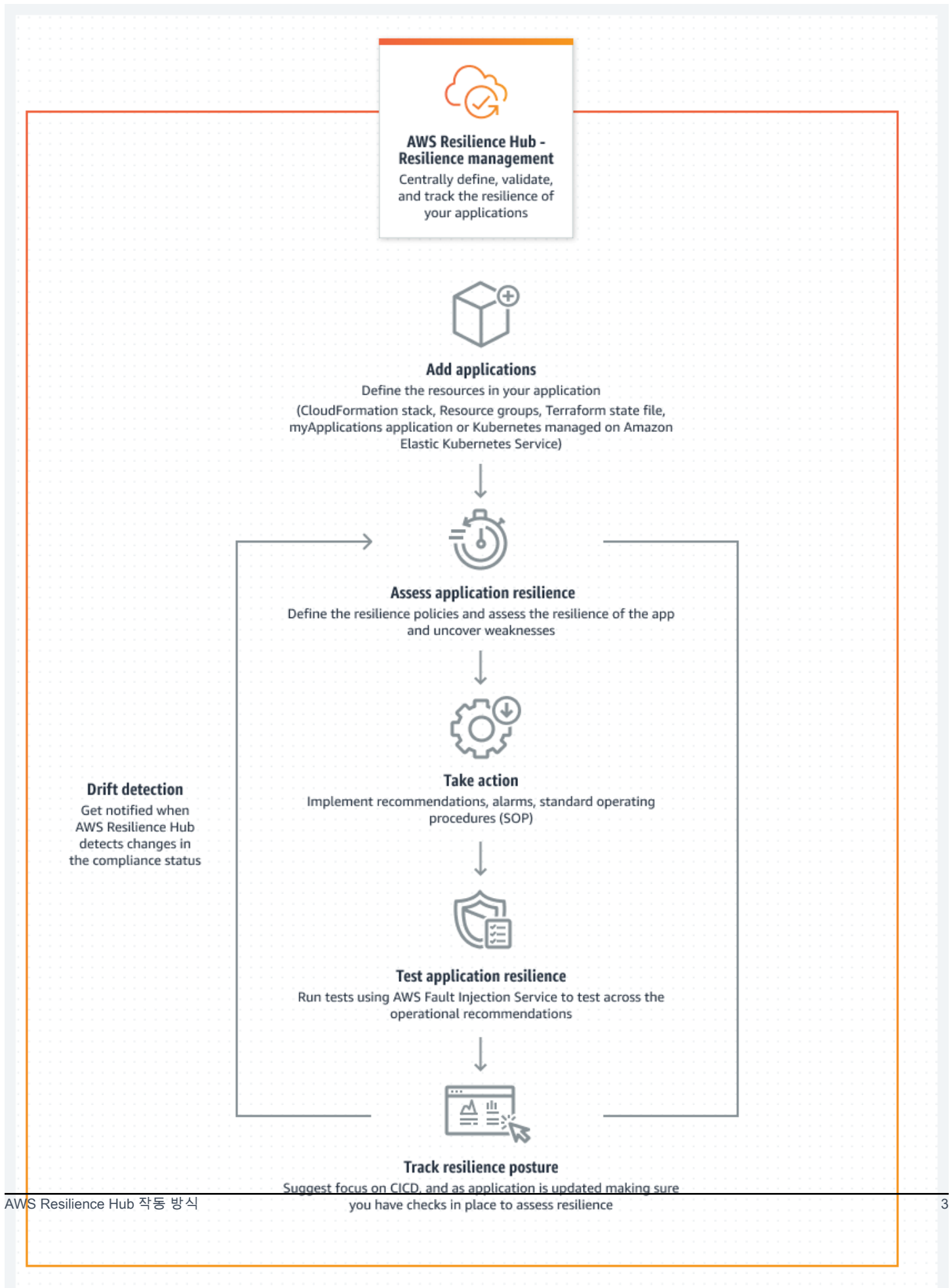
비즈니스 연속성을 최적화하여 규정 준수 및 규제 요구 사항을 충족할 수 있도록 지원합니다. AWS Resilience Hub 를 사용하여 다음을 수행할 수 있습니다.

- 인프라를 분석하고 애플리케이션 복원력을 개선하기 위한 권장 사항을 얻습니다. 권장 사항은 애플리케이션 복원력 개선을 위한 아키텍처 지침 외에도 복원력 정책을 충족하고, 통합 및 전달(CI/CD) 파이프라인에서 애플리케이션과 함께 배포하고 실행할 수 있는 테스트, 경보 및 표준 운영 절차(SOP)를 구현하기 위한 코드를 제공합니다.
- 다양한 조건에서 Recovery Time Objective(RTO) 및 Recovery Point Objective(RPO) 목표를 평가합니다.
- 복구 비용을 줄이면서 비즈니스 연속성을 최적화합니다.
- 프로덕션 환경에서 문제가 발생하기 전에 문제를 식별하고 해결합니다.

애플리케이션을 프로덕션에 배포한 후 CI/CD 파이프라인 AWS Resilience Hub 에를 추가하여 프로덕션으로 릴리스되기 전에 모든 빌드를 검증할 수 있습니다.

AWS Resilience Hub 작동 방식

다음 다이어그램은 AWS Resilience Hub 작동 방식에 대한 개략적인 개요를 제공합니다.



설명

AWS CloudFormation 스택, Terraform 상태 파일 AWS Resource Groups, Amazon Elastic Kubernetes Service 클러스터에서 리소스를 가져와 애플리케이션을 설명하거나 myApplications에 이미 정의된 애플리케이션 중에서 선택할 수 있습니다.

정의

애플리케이션의 복원력 정책을 정의합니다. 이러한 정책에는 애플리케이션, 인프라, 가용 영역 및 리전 중단에 대한 RTO 및 RPO 목표가 포함됩니다. 이러한 목표는 애플리케이션이 복원력 정책을 충족하는지 여부를 추정하는 데 사용됩니다.

평가

애플리케이션을 설명하고 애플리케이션에 복원력 정책을 추가한 후 복원력 평가를 실행합니다. AWS Resilience Hub 평가는 Well-Architected Framework의 모범 사례를 AWS 사용하여 애플리케이션의 구성 요소를 분석하고 잠재적 복원력 약점을 찾아냅니다. 이러한 약점은 불완전한 인프라 설정, 잘못된 구성 또는 추가 구성 개선이 필요한 상황으로 인해 발생할 수 있습니다. 복원력을 개선하려면 평가 보고서의 권장 사항에 따라 애플리케이션 및 복원력 정책을 업데이트하세요. 권장 사항에는 구성 요소, 경보, 테스트 및 복구 SOP가 포함됩니다. 그런 다음 다른 평가를 실행하고 결과를 이전 보고서와 비교하여 복원력이 얼마나 향상되는지 확인할 수 있습니다. 예상 워크로드 RTO와 예상 워크로드 RPO가 RTO 및 RPO 목표를 충족할 때까지 이 프로세스를 반복하세요.

Validate

테스트를 실행하여 AWS 리소스의 복원력과 애플리케이션, 인프라, 가용 영역 및 AWS 리전 인시던트에서 복구하는 데 걸리는 시간을 측정합니다. 복원력을 측정하기 위해 이러한 테스트는 AWS 리소스 중단을 시뮬레이션합니다. 운영 중단의 예로는 네트워크 사용 불가 오류, 장애 조치, 중지된 프로세스, Amazon RDS 부팅 복구, 가용 영역 문제 등이 있습니다.

보기 및 추적

AWS 애플리케이션을 프로덕션 환경에 배포한 후 AWS Resilience Hub 를 사용하여 애플리케이션의 복원력 상태를 계속 추적할 수 있습니다. 중단이 발생하면 운영자에서 중단을 보고 연결된 복구 프로세스를 AWS Resilience Hub 시작할 수 있습니다.

AWS Resilience Hub – 복원력 테스트

AWS Resilience Hub 는 와의 향상된 통합을 지원합니다 AWS FIS. 이 통합을 통해 AWS Resilience Hub 는 평가 중인 애플리케이션의 특정 컨텍스트를 기반으로 AWS FIS 작업 및 시나리오를 사용하여 맞춤형 권장 사항을 제공할 수 있습니다. 권장 실험을 실행하거나 AWS FIS 서비스를 사용하여 자체 테스트를 수행하면 애플리케이션의 복원력 점수를 개선하는 데 직접적으로 도움이 됩니다.

이러한 AWS FIS 작업 및 시나리오는 중단 이벤트를 생성하여 애플리케이션의 복원력 태세를 테스트 하므로 애플리케이션이 응답하는 방식을 관찰할 수 있습니다.는 중단을 유발하는 다양한 사전 구축된 시나리오와 다양한 작업을 AWS FIS 제공합니다. 또한 프로덕션 환경에서 실험을 실행하는 데 필요한 제어 장치 및 가드레일도 포함되어 있습니다. 제어 장치 및 가드레일에는 특정 조건이 충족될 경우 자동 롤백을 수행하거나 실험을 중단하는 옵션이 포함되어 있습니다. 를 사용하여 [AWS Resilience Hub 콘솔](#)에서 실험 AWS FIS 을 실행하려면 [the section called “사전 조건”](#) 섹션에 정의된 사전 조건을 완료 합니다.

다음 표에는 탐색 창에서 사용할 수 있는 모든 AWS FIS 옵션과 AWS Resilience Hub 콘솔에서 테스트 사용을 AWS FIS 시작하는 절차가 포함된 관련 AWS FIS 설명서 링크가 나와 있습니다.

AWS FIS 탐색 메뉴 옵션 및 참조

AWS FIS 탐색 메뉴 옵션	AWS FIS 설명서
복원력 테스트	실험 템플릿 만들기
시나리오 라이브러리	AWS FIS 라이브러리
실험 템플릿	에 대한 실험 템플릿 AWS FIS

다음 표에는 복원력 테스트 섹션의 드롭다운 메뉴에서 사용할 수 있는 모든 AWS FIS 옵션과 콘솔에서 AWS FIS 테스트 사용을 시작하는 절차가 포함된 관련 AWS FIS 설명서 링크가 나열되어 있습니다 AWS Resilience Hub .

AWS FIS 드롭다운 메뉴 옵션 및 참조

AWS FIS 드롭다운 메뉴 옵션	AWS FIS 설명서
실험 템플릿 만들기	실험 템플릿 만들기
시나리오에서 실험 생성	시나리오 사용

AWS Resilience Hub 개념

이러한 개념은 애플리케이션 복원력을 개선하고 애플리케이션 중단을 방지하는 데 도움이 되는 AWS Resilience Hub의 접근 방식을 더 잘 이해하는 데 도움이 될 수 있습니다.

복원력

지정된 시간 내에 가용성을 유지하고 소프트웨어 및 운영 중단으로부터 복구할 수 있는 능력.

Recovery Point Objective(RPO)

마지막 데이터 복구 시점 이후 허용되는 최대 시간입니다. 이에 따라 마지막 복구 시점과 서비스 중단 사이에 허용되는 데이터 손실로 간주되는 범위가 결정됩니다.

Recovery Time Objective(RTO)

서비스 중단과 서비스 복원 사이의 허용 가능한 지연 시간입니다. 이는 서비스를 이용할 수 없을 때 허용 가능한 기간으로 간주되는 기간을 결정합니다.

예상 워크로드 복구 시간 목표

예상 워크로드 복구 시간 목표(예상 워크로드 RTO)는 가져온 애플리케이션 정의를 기반으로 애플리케이션이 충족한 다음 평가를 실행할 것으로 예상되는 RTO입니다.

예상 워크로드 복구 시점 목표

예상 워크로드 복구 시점 목표(예상 워크로드 RPO)는 가져온 애플리케이션 정의를 기반으로 애플리케이션이 충족한 다음 평가를 실행할 것으로 예상되는 RPO입니다.

Application

AWS Resilience Hub 애플리케이션은 복원력 태세를 관리하기 위해 지속적으로 모니터링 및 평가되는 AWS 지원되는 리소스 모음입니다.

애플리케이션 구성 요소

단일 단위로 작동하고 실패하는 관련 AWS 리소스 그룹입니다. 예를 들어 기본 데이터베이스와 복제 데이터베이스가 있는 경우 두 데이터베이스 모두 동일한 애플리케이션 구성 요소(AppComponent)에 속합니다.

AWS Resilience Hub 는 어떤 AWS 리소스가 어떤 유형의 AppComponent에 속할 수 있는지 결정합니다. 예를 들어 DBInstance은 `AWS::ResilienceHub::DatabaseAppComponent`에 속할 수 있지만 `AWS::ResilienceHub::ComputeAppComponent`에는 속하지 않을 수 있습니다.

애플리케이션 규정 준수 상태

AWS Resilience Hub 는 애플리케이션에 대해 다음과 같은 규정 준수 상태 유형을 보고합니다.

정책 충족

애플리케이션이 정책에 정의된 RTO 및 RPO 목표를 충족하는 것으로 추정됩니다. 모든 구성 요소가 정의된 정책 목표를 충족합니다. 예를 들어 AWS 리전 간 중단에 대해 24시간의 RTO 및 RPO 목표를 선택했습니다. 백업이 폴백 리전에 복사되는 것을 AWS Resilience Hub 확인할 수 있습니다. 백업 표준 운영 절차(SOP)에서 복구를 유지하고 이를 테스트하고 시간을 정해야 합니다. 이는 운영 권장 사항에 있으며 전체 복원력 점수의 일부입니다.

정책 위반

애플리케이션이 정책에 정의된 RTO 및 RPO 목표를 충족하는 것으로 추정할 수 없습니다. 하나 이상의 AppComponent가 정책 목표를 충족하지 않습니다. 예를 들어 AWS 리전 간 중단에 대해 24시간의 RTO 및 RPO 목표를 선택했지만 데이터베이스 구성에는 글로벌 복제 및 백업 복사본과 같은 리전 간 복구 방법이 포함되지 않습니다.

평가되지 않음

애플리케이션은 평가가 필요합니다. 현재는 평가 또는 추적되지 않습니다.

변경 사항 감지됨

새로 게시된 애플리케이션 버전 중 아직 평가되지 않은 버전이 있습니다.

드리프트 감지

AWS Resilience Hub 는 애플리케이션에 대한 평가를 실행하는 동안 드리프트 알림을 실행하여 AppComponent 구성의 변경 사항이 애플리케이션의 규정 준수 상태에 영향을 미쳤는지 확인합니다. 또한 애플리케이션의 입력 소스 내에서 리소스 추가 또는 삭제와 같은 변경 사항을 확인하고 감지하며 이에 대해 알립니다. 비교를 위해 애플리케이션 구성 요소가 정책을 충족한 이전 평가를 AWS Resilience Hub 사용합니다.는 다음 유형의 드리프트를 AWS Resilience Hub 감지합니다.

- 애플리케이션 정책 드리프트 -이 드리프트 유형은 이전 평가에서 정책을 준수했지만 현재 평가를 준수하지 못한 모든 AppComponent를 식별합니다.
- 애플리케이션 리소스 드리프트 -이 드리프트 유형은 현재 애플리케이션 버전의 모든 드리프트된 리소스를 식별합니다.

복원력 평가

AWS Resilience Hub 는 격차 및 잠재적 해결 방법 목록을 사용하여 선택한 정책의 효과를 측정하여 재해를 복구하고 계속합니다. 정책에 따른 각 애플리케이션 구성 요소 또는 애플리케이션 규정 준수 상태를 평가합니다. 이 보고서에는 비용 최적화 권장 사항 및 잠재적 문제에 대한 참조가 포함됩니다.

복원력 점수

AWS Resilience Hub 는 애플리케이션이 애플리케이션의 복원력 정책, 경보, 표준 운영 절차(SOPs) 및 테스트를 충족하기 위한 권장 사항을 얼마나 잘 따르는지 나타내는 점수를 생성합니다.

중단 유형

AWS Resilience Hub 는 다음과 같은 유형의 중단에 대한 복원력을 평가하는 데 도움이 됩니다.

애플리케이션

인프라는 정상이지만 애플리케이션 또는 소프트웨어 스택이 필요에 따라 작동하지 않습니다. 이는 새 코드 배포, 구성 변경, 데이터 손상 또는 다운스트림 의존성 오작동 이후에 발생할 수 있습니다.

클라우드 인프라

운영 중단으로 인해 클라우드 인프라가 예상대로 작동하지 않습니다. 하나 이상의 구성 요소의 로컬 오류로 인해 운영 중단이 발생할 수 있습니다. 대부분의 경우 이러한 유형의 운영 중단은 결함이 있는 구성 요소를 재부팅하거나 재할용하거나 다시 로드하면 해결됩니다.

클라우드 인프라 AZ 중단

하나 이상의 가용 영역을 사용할 수 없습니다. 이러한 유형의 중단은 다른 가용 영역으로 전환하여 해결할 수 있습니다.

클라우드 인프라 리전 사고

하나 이상의 리전을 사용할 수 없습니다. 이러한 유형의 사고는 다른 AWS 리전으로 전환하여 해결할 수 있습니다.

AWS FIS 실험

AWS Resilience Hub 에서는 AWS FIS 작업을 사용하여 다양한 유형의 중단에 대한 애플리케이션 복원력을 확인하는 실험을 권장합니다. 이러한 중단에는 애플리케이션, 인프라, 가용 영역(AZ) 또는 애플리케이션 구성 요소 AWS 리전 인시던트가 포함됩니다.

이러한 실험을 통해 다음을 지원합니다.

- 오류를 주입합니다.
- 경보가 운영 중단을 감지할 수 있는지 확인합니다.
- 복구 절차 또는 표준 운영 절차(SOP)가 제대로 작동하여 운영 중단으로부터 애플리케이션을 복구하는지 확인합니다.

SOP 테스트는 예상 워크로드 RTO와 예상 워크로드 RPO를 측정합니다. 다양한 애플리케이션 구성을 테스트하고 출력 RTO와 RPO가 정책에 정의된 목표를 충족하는지 측정할 수 있습니다.

SOP

표준 운영 절차(SOP)는 운영 중단 또는 경보 발생 시 애플리케이션을 효율적으로 복구하도록 설계된 일련의 규범적 단계입니다. 애플리케이션 평가를 기반으로 SOPs 세트를 AWS Resilience Hub 권장하며, 적시에 복구할 수 있도록 중단 전에 SOPs를 준비, 테스트 및 측정하는 것이 좋습니다.

AWS Resilience Hub 페르소나

엔터프라이즈 애플리케이션을 구축하려면 인프라, 비즈니스 연속성, 애플리케이션 소유자 및 애플리케이션 모니터링을 담당하는 기타 이해관계자와 같은 다양한 교차 기능 팀의 협업이 필요합니다. 팀마다 다른 페르소나에서 애플리케이션을 구축하고 관리하는 데 기여하며 AWS Resilience Hub, 각 페르소나는 역할과 책임이 다릅니다. 다양한 페르소나에 권한을 부여하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [the section called “AWS Resilience Hub 페르소나 및 IAM 권한 참조”](#).

에서 애플리케이션 생성 및 평가 실행을 시작하려면 다음 페르소나를 생성하는 AWS Resilience Hub 것이 좋습니다.

- 인프라 애플리케이션 관리자 -이 페르소나가 있는 사용자는 인프라 및 애플리케이션 리소스를 설정, 구성 및 유지 관리하여 애플리케이션의 신뢰성과 보안을 보장할 책임이 있습니다. 이들의 책임은 다음과 같습니다.
 - 애플리케이션이 정기적으로 배포 및 업데이트되도록 보장
 - 시스템 성능 모니터링
 - 문제 해결
 - 백업 및 재해 복구 계획 구현
- 비즈니스 연속성 관리자 -이 페르소나가 있는 사용자는 애플리케이션 정책을 지시하고 애플리케이션의 비즈니스 중요도를 결정할 책임이 있습니다. 이들의 책임은 다음과 같습니다.

- 정책 설정 시 주요 의사 결정
- 비즈니스 중요도 평가
- 중요한 애플리케이션에 리소스 할당
- 위험 평가 및 관리
- 애플리케이션 소유자 -이 페르소나가 있는 사용자는 가용성과 신뢰성이 높은 애플리케이션을 보장할 책임이 있습니다. 이들의 책임은 다음과 같습니다.
 - 애플리케이션 성능을 측정 및 모니터링하고 병목 현상을 식별하기 위한 주요 성능 식별자 정의
 - 여러 이해관계자를 위한 교육 구성
 - 다음 문서가 up-to-date 상태인지 확인합니다.
 - 애플리케이션 아키텍처
 - 배포 프로세스
 - 구성 모니터링
 - 성능 최적화 기법
- 읽기 전용 액세스 -이 페르소나가 있는 사용자는 읽기 전용 권한으로 제한됩니다. 이들의 책임에는 복원력 점수, 운영 권장 사항 및 복원력 권장 사항을 모니터링하여 애플리케이션의 성능 및 상태에 대한 가시성과 감독을 유지하는 것이 포함됩니다. 또한 애플리케이션이 조직의 목표를 충족하는지 확인하기 위해 문제, 추세 및 개선 영역을 식별할 책임도 있습니다.

AWS Resilience Hub 지원되는 리소스

중단 시 애플리케이션 성능에 영향을 미치는 리소스는 `AWS::RDS::DBInstance` 및와 같은 AWS Resilience Hub 최상위 리소스에서 완벽하게 지원됩니다 `AWS::RDS::DBCluster`.

가 평가에 지원되는 모든 서비스의 리소스를 포함하는 AWS Resilience Hub 데 필요한 권한에 대한 자세한 내용은 섹션을 참조하세요 [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#).

AWS Resilience Hub 는 다음 AWS 서비스의 리소스를 지원합니다.

- 컴퓨팅
 - Amazon Elastic Compute Cloud(Amazon EC2)

Note

AWS Resilience Hub 는 Amazon EC2 리소스에 액세스하기 위한 이전 Amazon 리소스 이름(ARN) 형식을 지원하지 않습니다. 새 ARN 형식은 AWS 계정 ID를 사용하고 클러스터의

리소스에 태그를 지정하는 향상된 기능을 활성화하며 클러스터에서 실행되는 서비스 및 작업의 비용도 추적합니다.

- 이전 형식(사용되지 않음) - `arn:aws:ec2:<region>::instance/<instance-id>`
- 새 형식 - `arn:aws:ec2:<region>:<account-id>:instance/<instance-id>`
새 ARN 형식에 대한 자세한 내용은 [Amazon ECS 배포를 새 ARN 및 리소스 ID 형식으로 마이그레이션을 참조하세요](#).

- AWS Lambda
- Amazon Elastic Kubernetes Service(Amazon EKS)
- Amazon Elastic Container Service(Amazon ECS)
- AWS Step Functions
- 데이터베이스
 - Amazon Relational Database Service(Amazon RDS)
 - Amazon DynamoDB
 - Amazon DocumentDB
 - Amazon ElastiCache
- 네트워킹 및 콘텐츠 전송
 - Amazon Route 53
 - Elastic Load Balancing
 - Network Address Translation(NAT)
- 스토리지
 - Amazon Elastic Block Store(Amazon EBS)
 - Amazon Elastic File System(Amazon EFS)
 - Amazon Simple Storage Service(S3)
 - Amazon FSx for Windows File Server
- 기타
 - Amazon API Gateway
 - Amazon Application Recovery Controller(ARC)(Amazon ARC)
 - Amazon Simple Notification Service
 - Amazon Simple Queue Service
 - AWS Auto Scaling

- AWS Backup
- AWS 탄력적 재해 복구

Note

- AWS Resilience Hub 는 각 리소스의 지원되는 인스턴스를 볼 수 있도록 하여 애플리케이션 리소스에 대한 추가적인 투명성을 제공합니다. 또한는 평가 프로세스 중에 리소스 인스턴스를 검색하는 동안 각 리소스의 고유한 인스턴스를 식별하여 보다 정확한 복원력 권장 사항을 AWS Resilience Hub 제공합니다. 애플리케이션에 리소스 인스턴스를 추가하는 것에 대한 자세한 내용은 [AWS Resilience Hub 애플리케이션 리소스 편집](#) 단원을 참조하세요.
- AWS Resilience Hub 는에서 Amazon EKS 및 Amazon ECS를 지원합니다 AWS Fargate.
- AWS Resilience Hub 는 다음 서비스의 일부로 AWS Backup 리소스 평가를 지원합니다.
 - Amazon EBS
 - Amazon EFS
 - Amazon S3
 - Amazon Aurora Global Database
 - Amazon DynamoDB
 - Amazon RDS 서비스
 - Amazon FSx for Windows File Server
- 의 Amazon ARC는 Amazon DynamoDB 글로벌, Elastic Load Balancing, Amazon RDS 및 AWS Auto Scaling 그룹만 AWS Resilience Hub 평가합니다.
- 에서 리전 간 리소스를 평가 AWS Resilience Hub 하려면 단일 애플리케이션 구성 요소에서 리소스를 그룹화합니다. 각 AWS Resilience Hub 애플리케이션 구성 요소에서 지원하는 리소스 및 그룹화 리소스에 대한 자세한 내용은 [애플리케이션 구성 요소에서 리소스 그룹화](#) 단원을 참조하세요.
- 현재는 Amazon EKS 클러스터 AWS Resilience Hub 가 있거나 애플리케이션이 옵트인 활성화 리전에서 생성된 경우 Amazon EKS 클러스터에 대한 리전 간 평가를 지원하지 않습니다 AWS .
- 현재는 다음 Kubernetes 리소스 유형만 AWS Resilience Hub 평가합니다.
 - 배포
 - ReplicaSets

- 포드

AWS Resilience Hub 는 다음 유형의 리소스를 무시합니다.

- 예상 워크로드 RTO 또는 예상 워크로드 RPO에 영향을 주지 않는 리소스 –
AWS::RDS::DBParameterGroup와 같이 예상 워크로드 RTO 또는 예상 워크로드 RPO에 영향을 주지 않는 리소스는 AWS Resilience Hub에서 무시됩니다.
- 최상위가 아닌 리소스 -는 최상위 리소스의 속성을 쿼리하여 다른 속성을 도출할 수 있으므로 최상위 리소스 AWS Resilience Hub 만 가져옵니다. 예를 들어, AWS::ApiGateway::RestApi와 AWS::ApiGatewayV2::Api는 Amazon API Gateway에서 지원되는 리소스입니다. 하지만 AWS::ApiGatewayV2::Stage는 최상위 리소스가 아닙니다. 따라서에서 가져오지 않습니다 AWS Resilience Hub.

 Note

지원되지 않는 리소스

- AWS Resource Groups (Amazon Route 53 RecordSets 및 API-GW HTTP) 및 Amazon Aurora Global 리소스를 사용하여 여러 리소스를 식별할 수 없습니다. 평가의 일환으로 이러한 리소스를 분석하려면 애플리케이션에 리소스를 수동으로 추가해야 합니다. 그러나 평가를 위해 Amazon Aurora Global 리소스를 추가할 때는 Amazon RDS 인스턴스의 Application Component로 그룹화해야 합니다. 리소스 편집에 대한 자세한 내용은 [the section called “애플리케이션 리소스 편집”](#) 단원을 참조하세요.
- 이러한 리소스는 애플리케이션 복구에 영향을 미칠 수 있지만 AWS Resilience Hub 현재에서 완전히 지원되지는 않습니다. AWS Resilience Hub 는 애플리케이션이 AWS CloudFormation 스택, Terraform 상태 파일 AWS Resource Groups또는 myApplications 애플리케이션으로 지원되는 경우 지원되지 않는 리소스에 대해 사용자에게 경고하기 위해 노력합니다.
- 애플리케이션 리소스를 로 가져오는 과정에서 AWS Resilience Hub 일부 리소스는 무시될 수 있습니다. 리소스를 무시하면 리소스를 전혀 가져올 수 없습니다. 그러나 지원되지 않음으로 표시된 리소스는 현재와 호환되지 AWS Resilience Hub 않지만 향후 지원될 수 있으므로 평가를 위해 애플리케이션에 포함될 수 있습니다. 또한 AWS Resilience Hub 에서 지원하지 않는 특정 리소스는 무시할 수 있습니다 AWS Resource Groups. 에서 지원하는 리소스에 대한

자세한 내용은 및 태그 편집기와 함께 사용할 수 있는 리소스 유형을 AWS Resource Groups 참조하세요. [AWS Resource Groups](#)

AWS Resilience Hub 및 myApplications

myApplications 대시보드의 복원력 위젯은 애플리케이션 복원력을 평가하고 모니터링하는 프로세스를 간소화합니다. 이를 통해 AWS Resilience Hub 콘솔에서 수동으로 다시 생성할 필요 없이 myApplications에 정의된 애플리케이션의 복원력을 빠르게 평가할 수 있습니다. 이 통합 접근 방식은 myApplications의 애플리케이션 관리 기능과의 복원력 평가 기능을 결합하여 두 플랫폼의 강점을 활용할 수 있도록 합니다. 복원력 위젯은 애플리케이션 정의와 복원력 평가 기능을 결합하여 워크플로를 간소화하여 관련 정보에 액세스하고 중앙 위치에서 복원력을 강화하기 위한 조치를 취할 수 있습니다. 복원력 위젯에서 애플리케이션을 평가하면 다음을 AWS Resilience Hub 수행합니다.

- 에서 선택한 애플리케이션을 생성합니다 AWS Resilience Hub.
- 모델과 연결된 리소스를 자동으로 검색하고 매핑합니다.
- 복구 시간 목표(RTO) 및 복구 시점 목표(RPO)에 대해 미리 정의된 값을 사용하여 새 복원력 정책을 생성하고 할당합니다. 이는 RTO의 경우 4시간, RPO의 경우 1시간입니다. 평가를 생성한 후 복원력 정책을 수정하거나 AWS Resilience Hub 콘솔에서 다른 정책을 할당할 수 있습니다. 복원력 정책 업데이트 및 다른 정책 연결에 대한 자세한 내용은 섹션을 참조하세요 [복원력 정책 관리](#).
- 복원력 정책에 정의된 RTO 및 RPO를 기준으로 애플리케이션의 복원력을 평가하여 애플리케이션 아키텍처 개선이 필요한 영역을 식별합니다. 장애 시나리오에는 가용 영역 장애, 리전 중단 및 기타 잠재적 중단이 포함됩니다.
- 초기 평가 후 애플리케이션의 리소스 및 구성 변경 사항을 지속적으로 모니터링하여 변경 사항이 애플리케이션의 복원력에 영향을 미치는 경우 알림 또는 업데이트를 제공합니다.

Note

평가를 시작하기 전에를 사용하여 평가 실행과 관련된 잠재적 비용을 평가하는 것이 좋습니다 AWS Resilience Hub. 자세한 요금 정보는 [AWS Resilience Hub 요금](#)을 참조하세요.

애플리케이션을 평가한 후 로 이동을 선택하여 위젯 AWS Resilience Hub 에서의 전체 기능에 액세스 AWS Resilience Hub 하여 AWS Resilience Hub 콘솔에서 애플리케이션 세부 정보를 볼 수 있습니다.

myApplications의 애플리케이션을에 포함하는 프로세스는 다음 규칙 및 제약 조건에 따라 관리 AWS Resilience Hub 됩니다.

- 의 애플리케이션에는 하나의 myApplications 애플리케이션만 연결할 수 있습니다 AWS Resilience Hub. 즉, myApplications 대시보드의 복원력 위젯에서 평가를 AWS Resilience Hub 실행하거나 콘솔에서 애플리케이션을 설명하는 동안 [myApplications 애플리케이션 사용](#) 절차를 완료하여 myApplications 애플리케이션을 애플리케이션에 연결할 수 있습니다 AWS Resilience Hub .
- myApplications 환경과 동일한 AWS 리전 및 AWS 계정 경계 내에 있는 myApplications 애플리케이션만 포함, 평가 및 볼 수 있습니다. 다른 AWS 리전 또는 별도의 AWS 계정으로 생성된 애플리케이션은이 위젯을 통해 표시되거나 액세스할 수 없습니다.
- myApplications 대시보드에서만 리소스를 추가, 제거 및 업데이트할 수 있습니다. myApplications 대시보드에서 애플리케이션 리소스를 수정할 때 리소스 변경 사항을 AWS Resilience Hub 보려면 다시 가져와야 합니다 AWS Resilience Hub.

자세히 알아보기

myApplications 대시보드에서 애플리케이션 및 리소스를 관리하는 방법에 대한 자세한 내용은 AWS Console Home 설명서의 다음 주제를 참조하세요.

- [myApplications는 무엇에 있나요 AWS?](#)
- [myApplications에서 첫 번째 애플리케이션 생성](#)
- [리소스 관리](#)
- [복원력 위젯](#)

에서 애플리케이션 설명 및 평가 실행에 대한 자세한 내용은 다음 주제를 AWS Resilience Hub참조하세요.

- [Resiliency 위젯에서 기존 myApplications 애플리케이션에 대한 복원력 평가를 처음으로 실행하려면](#)
- [Resiliency 위젯에서 기존 myApplications 애플리케이션에 대한 복원력 평가를 다시 실행하려면](#)
- [복원력 위젯에서 평가 요약 검토](#)

시작

이 섹션에서는 사용을 시작하는 방법을 설명합니다 AWS Resilience Hub. 여기에는 계정에 대한 AWS Identity and Access Management (IAM) 권한 생성이 포함됩니다.

주제

- [사전 조건](#)
- [예 애플리케이션 추가 AWS Resilience Hub](#)

사전 조건

를 사용하려면 먼저 다음 사전 조건을 완료해야 AWS Resilience Hub합니다.

- AWS 계정 - 내에서 사용할 각 AWS 계정 유형(primary/secondary/resource 계정)에 대해 하나 이상의 계정을 생성합니다 AWS Resilience Hub. AWS 계정 생성 및 관리에 대한 자세한 내용은 다음을 참조하세요.
 - 처음 AWS 사용자 - [시작하기: 처음 AWS 사용자이신가요?](#)
 - AWS 계정 관리 - <https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html>
- AWS Identity and Access Management (IAM) 권한 - AWS 계정을 생성한 후 생성한 각 계정에 필요한 역할과 IAM 권한을 구성해야 합니다. 예를 들어 애플리케이션 리소스에 액세스하기 위해 AWS 계정을 생성한 경우 새 역할을 설정하고가 계정에서 애플리케이션 리소스에 액세스하는 AWS Resilience Hub 데 필요한 IAM 권한을 구성해야 합니다. IAM 권한에 대한 자세한 내용은 [the section called “AWS Resilience Hub와 IAM의 작동 방식”](#)을 참조하시고, 역할에 정책을 추가하는 방법에 대한 자세한 내용은 [the section called “JSON 파일을 사용하여 신뢰 정책 정의”](#)를 참조하세요.

사용자, 그룹 및 역할에 IAM 권한을 빠르게 추가하려면 AWS 관리형 정책()을 사용하면 됩니다[the section called “AWS 관리형 정책”](#). AWS 관리형 정책을 사용하면 정책을 직접 작성하는 AWS 계정 것보다에서 사용할 수 있는 일반적인 사용 사례를 다루는 것이 더 쉽습니다.는 관리형 정책에 추가 권한을 AWS Resilience Hub AWS 추가하여 다른 AWS 서비스에 대한 지원을 확장하고 새 기능을 포함합니다. 따라서:

- 기존 고객이고 애플리케이션이 평가 내에서 최신 개선 사항을 사용하도록 하려면 애플리케이션의 새 버전을 게시한 다음 새 평가를 실행해야 합니다. 자세한 정보는 다음의 주제를 참조하세요.
 - [the section called “새 애플리케이션 버전 게시”](#)
 - [the section called “에서 복원력 평가 실행 AWS Resilience Hub”](#)

- AWS 관리형 정책을 사용하여 사용자, 그룹 및 역할에 적절한 IAM 권한을 할당하지 않는 경우 이러한 권한을 수동으로 구성해야 합니다. AWS 관리형 정책에 대한 자세한 내용은 섹션을 참조하세요 [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#).

에 애플리케이션 추가 AWS Resilience Hub

AWS Resilience Hub 는 소프트웨어 개발 수명 주기에 통합되는 복원력 평가 및 검증을 제공합니다. 다음을 AWS Resilience Hub 통해 AWS 애플리케이션을 사전에 준비하고 중단으로부터 보호할 수 있습니다.

- 복원력 약점 발견.
- 목표 Recovery Point Objective(RPO) 및 Recovery Time Objective(RTO)를 충족할 수 있는지 추정합니다.
- 프로덕션에 출시되기 전에 문제를 해결합니다.

이 섹션에서는 애플리케이션 추가 방법을 소개합니다. 기존 myApplications 애플리케이션, AWS CloudFormation 스택 또는에서 리소스를 수집하고 적절한 복원력 정책을 AWS Resource Groups 생성합니다. 애플리케이션을 설명한 후 애플리케이션에 게시 AWS Resilience Hub하고 애플리케이션의 복원력에 대한 평가 보고서를 생성할 수 있습니다. 그런 다음 평가의 권장 사항을 사용하여 복원력을 개선할 수 있습니다. 다른 평가를 실행하고 결과를 비교한 다음 예상 워크로드 RTO와 예상 워크로드 RPO가 RTO 및 RPO 목표를 달성할 때까지 반복할 수 있습니다.

주제

- [애플리케이션을 추가하여 시작하기](#)
- [이 애플리케이션을 관리하는 방법 선택](#)
- [리소스 컬렉션 추가](#)
- [RTO 및 RPO 설정](#)
- [예약된 평가 및 드리프트 알림 설정](#)
- [권한 설정](#)
- [애플리케이션 구성 파라미터 구성](#)
- [태그 추가](#)
- [애플리케이션 검토 및 게시 AWS Resilience Hub](#)
- [애플리케이션 평가 AWS Resilience Hub 실행](#)

애플리케이션을 추가하여 시작하기

AWS 애플리케이션의 세부 정보를 설명하고 보고서를 실행하여 복원력을 평가 AWS Resilience Hub 하여 시작합니다.

시작하려면 AWS Resilience Hub 홈 페이지의 시작하기에서 애플리케이션 추가를 선택합니다.

관련 비용 및 결제에 대한 자세한 내용은 [AWS Resilience Hub 요금](#)을 AWS Resilience Hub참조하세요.

애플리케이션의 세부 정보를 AWS Resilience Hub에서 설명하세요.

이 섹션에서는 기존 AWS 애플리케이션의 세부 정보를 설명하는 방법을 보여줍니다 AWS Resilience Hub.

애플리케이션 세부 정보 설명하려면

1. 애플리케이션 이름을 입력합니다.
2. (선택 사항) 애플리케이션에 대한 설명을 입력합니다.

다음

[이 애플리케이션을 관리하는 방법 선택](#)

이 애플리케이션을 관리하는 방법 선택

AWS CloudFormation 스택, AWS Resource Groups myApplications 애플리케이션 및 Terraform 상태 파일 외에도 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 있는 리소스를 추가할 수 있습니다. 즉, AWS Resilience Hub를 사용하면 Amazon EKS 클러스터에 있는 리소스를 선택적 리소스로 추가할 수 있습니다. 이 섹션에서는 애플리케이션 리소스의 위치를 결정하는 데 도움이 되는 다음과 같은 옵션을 제공합니다.

- 리소스 컬렉션 - 리소스 컬렉션 중 하나에서 리소스를 검색하려면 이 옵션을 선택합니다. 리소스 컬렉션에는 AWS CloudFormation 스택, AWS Resource Groups myApplications 애플리케이션 및 Terraform 상태 파일이 포함됩니다.

이 옵션을 선택하는 경우 [the section called “리소스 컬렉션 추가”](#)의 절차 중 하나를 완료해야 합니다.

- EKS 전용 - Amazon EKS 클러스터 내 네임스페이스에서 리소스를 검색하려면 이 옵션을 선택합니다.

이 옵션을 선택하는 경우 [the section called “EKS 클러스터를 추가합니다.”](#)의 절차를 완료해야 합니다.

- 리소스 컬렉션 및 EKS - AWS CloudFormation 스택, AWS Resource Groups Terraform 상태 파일 및 Amazon EKS 클러스터에서 리소스를 검색하려면 이 옵션을 선택합니다.

이 옵션을 선택하는 경우 [the section called “리소스 컬렉션 추가”](#)의 절차 중 하나를 완료한 다음 [the section called “EKS 클러스터를 추가합니다.”](#)의 절차를 완료하세요.

Note

애플리케이션당 지원되는 리소스 수에 대한 자세한 내용은 [Service Quotas](#)를 참조하세요.

다음

[리소스 컬렉션 추가](#)

리소스 컬렉션 추가

이 섹션에서는 애플리케이션 구조의 기반을 형성하는 데 사용할 수 있는 다음 옵션에 대해 설명합니다.

- [리소스 컬렉션 추가](#)
- [EKS 클러스터를 추가합니다.](#)

리소스 컬렉션 추가

이 섹션에서는 애플리케이션 구조의 기반을 형성하는 데 사용하는 다음 방법에 대해 설명합니다.

- [AWS CloudFormation 스택 사용](#)
- [사용 AWS Resource Groups](#)
- [myApplications 애플리케이션 사용](#)
- [Terraform 상태 파일 사용](#)

AWS CloudFormation 스택 사용

설명하려는 애플리케이션에서 사용할 리소스가 포함된 AWS CloudFormation 스택을 선택합니다. 스택은 애플리케이션을 설명하는 데 AWS 계정 사용하는에서 가져오거나 다른 계정 또는 리전에서 가져올 수 있습니다.

애플리케이션 구조의 기반을 형성하는 리소스를 검색하려면

1. CloudFormation 스택을 선택하여 스택 기반 리소스를 검색합니다.
2. AWS 계정 및 리전과 연결된 스택 선택 드롭다운 목록에서 스택을 선택합니다.

다른 리전 AWS 계정, 다른 리전 또는 둘 다에 있는 스택을 사용하려면 AWS 리전 외부에 스택 추가 옆에 있는 오른쪽 화살표를 선택하고 스택 ARN 입력 상자에 스택의 Amazon 리소스 이름 (ARN)을 입력한 다음 스택 ARN 추가를 선택합니다. ARN에 대한 자세한 내용은 AWS 일반 참조의 [Amazon 리소스 이름\(ARN\)](#)을 참조하십시오.

사용 AWS Resource Groups

설명하려는 애플리케이션에서 사용할 리소스가 AWS Resource Groups 포함된를 선택합니다.

애플리케이션 구조의 기반을 형성하는 리소스를 검색하려면

1. 리소스 그룹을 선택하여 리소스 AWS Resource Groups 가 포함된를 검색합니다.
2. 리소스 그룹 선택 드롭다운 목록에서 리소스를 선택합니다.

다른 AWS 계정리전, 다른 리전 또는 둘 다에 AWS Resource Groups 있는를 사용하려면 리소스 그룹 ARN: 옆에 있는 오른쪽 화살표를 선택하고 리소스 그룹 ARN AWS Resource Groups 입력 상자의 Amazon 리소스 이름(ARN)을 입력한 다음 리소스 그룹 ARN 추가를 선택합니다. ARN에 대한 자세한 내용은 AWS 일반 참조의 [Amazon 리소스 이름\(ARN\)](#)을 참조하십시오.

myApplications 애플리케이션 사용

에 포함할 myApplications 애플리케이션 선택 AWS Resilience Hub

에 myApplications 애플리케이션을 포함하려면 AWS Resilience Hub

1. myApplications 선택합니다.
2. 애플리케이션 선택 드롭다운 목록에서 애플리케이션을 선택합니다.

Terraform 상태 파일 사용

설명하려는 애플리케이션에서 사용할 Amazon S3 버킷 리소스가 포함된 Terraform 상태 파일을 선택합니다. Terraform 상태 파일의 위치로 이동하거나 다른 지역에 있는 액세스 권한이 있는 Terraform 상태 파일에 대한 링크를 제공할 수 있습니다.

Note

AWS Resilience Hub 는 Terraform 상태 파일 버전 0.12 이상을 지원합니다.

애플리케이션 구조의 기반을 형성하는 리소스를 검색하려면

1. Terraform 상태 파일을 선택하여 S3 버킷 리소스를 검색하세요.
2. 상태 파일 선택:: 섹션에서 S3 찾아보기를 선택하여 Terraform 상태 파일의 위치로 이동합니다.

다른 리전에 있는 Terraform 상태 파일을 사용하려면 S3 URI 필드에 Terraform 상태 파일의 위치에 대한 링크를 제공하고 S3 URL 추가를 선택합니다.

Terraform 상태 파일의 한도는 4메가바이트 (MB) 입니다.

3. S3에서 아카이브 선택 대화 상자의 버킷 섹션에서 Amazon Simple Storage Service 버킷을 선택합니다.
4. 객체 섹션에서 키를 선택하고 선택(Choose)을 선택합니다.

EKS 클러스터를 추가합니다.

이 섹션에서는 Amazon EKS 클러스터를 사용하여 애플리케이션 구조의 기반을 형성하는 방법을 설명합니다.

Note

Amazon EKS 클러스터에 연결하려면 Amazon EKS 권한과 추가 IAM 역할이 있어야 합니다. 클러스터에 연결하기 위한 단일 계정 및 교차 계정 Amazon EKS 권한과 추가 IAM 역할을 추가하는 방법에 대한 자세한 내용은 다음 주제를 참조하세요.

- [AWS Resilience Hub 액세스 권한 참조](#)
- [the section called “Amazon EKS 클러스터에 대한 AWS Resilience Hub 액세스 활성화”](#)

설명하는 애플리케이션에서 사용하려는 리소스가 포함된 Amazon EKS 클러스터와 네임스페이스를 선택하세요. Amazon EKS 클러스터는 애플리케이션을 설명하는 데 AWS 계정 사용하는에서 가져오거나 다른 계정 또는 다른 리전에서 가져올 수 있습니다.

Note

가 Amazon EKS 클러스터를 평가 AWS Resilience Hub 하려면 EKS 클러스터 및 네임스페이스 섹션의 각 Amazon EKS 클러스터에 관련 네임스페이스를 수동으로 추가해야 합니다. 네임스페이스 이름은 Amazon EKS 클러스터의 네임스페이스 이름과 정확히 일치해야 합니다.

Amazon EKS 클러스터를 추가하려면

1. EKS 클러스터 섹션을 선택하고 및 AWS 계정 리전과 연결된 EKS 클러스터 선택 드롭다운 목록에서 Amazon EKS 클러스터를 선택합니다.
2. 다른 리전 AWS 계정, 다른 리전 또는 둘 다에 있는 Amazon EKS 클러스터를 사용하려면 다른 계정 또는 리전 내에 EKS 클러스터 추가 옆에 있는 오른쪽 화살표를 선택하고 EKS ARN 입력 상자에 Amazon EKS 클러스터의 Amazon 리소스 이름(ARN)을 입력한 다음 EKS ARN 추가를 선택합니다. ARN에 대한 자세한 내용은 AWS 일반 참조의 [Amazon 리소스 이름\(ARN\)](#)을 참조하십시오.

지역 간 Amazon Elastic Kubernetes Service 클러스터에 액세스할 수 있는 권한을 추가하는 방법에 대한 자세한 내용은 [the section called “Amazon EKS 클러스터에 대한 AWS Resilience Hub 액세스 활성화”](#) 단원을 참조하세요.

선택한 Amazon EKS 클러스터에서 네임스페이스를 추가하려면

1. 네임스페이스 추가 섹션의 EKS 클러스터 및 네임스페이스 테이블에서 Amazon EKS 클러스터 이름 왼쪽에 있는 라디오 버튼을 선택한 다음 네임스페이스 업데이트를 선택합니다.

다음과 같이 Amazon EKS 클러스터를 식별할 수 있습니다.

- EKS 클러스터 이름 - 선택한 Amazon EKS 클러스터의 이름을 나타냅니다.
- 네임스페이스 수 - Amazon EKS 클러스터에서 선택한 네임스페이스의 수를 나타냅니다.
- 상태 - AWS Resilience Hub 가 애플리케이션에 선택한 Amazon EKS 클러스터의 네임스페이스를 포함했는지 여부를 나타냅니다. 다음 옵션을 사용하여 상태를 식별할 수 있습니다.
 - 네임스페이스 필요 - Amazon EKS 클러스터의 네임스페이스를 포함하지 않았음을 나타냅니다.

- 네임스페이스 추가됨 - Amazon EKS 클러스터의 네임스페이스를 하나 이상 포함했음을 나타냅니다.
2. 네임스페이스를 추가하려면 네임스페이스 업데이트 대화 상자에서 새 네임스페이스 추가를 선택합니다.

네임스페이스 업데이트 대화 상자에는 Amazon EKS 클러스터에서 선택한 모든 네임스페이스가 편집 가능한 옵션으로 표시됩니다.

3. 네임스페이스 업데이트 대화 상자에는 다음과 같은 편집 옵션이 있습니다.
 - 새 네임스페이스를 추가하려면 새 네임스페이스 추가를 선택한 다음 네임스페이스 상자에 네임스페이스 이름을 입력합니다.

네임스페이스 이름은 Amazon EKS 클러스터의 네임스페이스 이름과 정확히 일치해야 합니다.

- 네임스페이스를 제거하려면 네임스페이스 옆에 있는 제거를 선택합니다.
- 선택한 네임스페이스를 모든 Amazon EKS 클러스터에 적용하려면 모든 EKS 클러스터에 네임스페이스 적용을 선택합니다.

이 옵션을 선택하면 다른 Amazon EKS 클러스터에서 이전에 선택한 네임스페이스가 현재 선택한 네임스페이스로 재정의됩니다.

4. 업데이트된 네임스페이스를 애플리케이션에 포함시키려면 업데이트 를 선택합니다.

다음

[RTO 및 RPO 설정](#)

RTO 및 RPO 설정

자체 RTO/RPO 목표를 사용하여 새 복원력 정책을 정의하거나 사전 정의된 RTO/RPO 목표가 있는 기존 복원력 정책을 선택할 수 있습니다. 기존 복구 정책 중 하나를 사용하려면 기존 정책 선택 옵션을 선택하고 옵션 항목 드롭다운 목록에서 기존 대상 애플리케이션을 선택합니다.

고유한 RTO/RPO 목표를 정의하려면

1. 새 복원력 정책 생성 옵션을 선택합니다.
2. 정책 이름 입력 상자(이름 아래)에 복원력 정책의 이름을 입력합니다.

이 필드에는 자동 생성된 이름이 미리 채워져 있습니다. 동일한를 사용하거나 다른 이름을 제공할 수 있습니다.

3. (선택 사항) 설명 상자에 복원력 정책에 대한 설명을 입력합니다.
4. RTO/RPO 목표 섹션에서 RTO/RPO를 정의합니다.

Note

- 애플리케이션의 기본 RTO 및 RPO가 미리 채워져 있습니다. RTO와 RPO는 지금 또는 애플리케이션을 평가한 후에 변경할 수 있습니다.
- AWS Resilience Hub 를 사용하면 복원력 정책의 RTO 및 RPO 필드에 값 0을 입력할 수 있습니다. 하지만 애플리케이션을 평가하는 동안 가능한 가장 낮은 평가 결과는 거의 0에 가깝습니다. 따라서 RTO 및 RPO 필드에 값을 0으로 입력하면 예상 워크로드 RTO와 예상 워크로드 RPO 결과가 0에 가까워지고 애플리케이션의 규정 준수 상태가 정책 위반으로 설정됩니다.

5. 인프라 및 AZ의 RTO/RPO를 정의하려면 오른쪽 화살표를 선택하여 인프라 RTO 및 RPO 섹션을 확장하세요.
6. RTO/RPO 대상에서 상자에 숫자 값을 입력한 다음 RTO와 RPO 모두에 대해 값이 나타내는 시간 단위를 선택합니다.

인프라 RTO 및 RPO 섹션의 인프라 및 가용 영역에 대해 이러한 항목을 반복합니다.

7. (선택 사항) 다중 리전 애플리케이션이 있고 리전 RTO 및 RPO를 정의하려면 리전 - 선택 사항을 클릭합니다.

RTO 및 RPO에서 상자에 숫자 값을 입력한 다음 RTO와 RPO 모두에 대해 값이 나타내는 시간 단위를 선택합니다.

다음

[the section called “예약된 평가 및 드리프트 알림 설정”](#)

예약된 평가 및 드리프트 알림 설정

AWS Resilience Hub 를 사용하면 예약된 평가 및 드리프트 알림을 설정하여 매일 애플리케이션을 평가하고 드리프트가 감지될 때 알림을 받을 수 있습니다.

드리프트 알림을 설정하려면

1. 매일 애플리케이션을 평가하려면 매일 자동 평가를 클릭합니다.

이 옵션이 켜져 있는 경우 일일 평가 일정은 다음과 같은 경우에만 시작됩니다.

- 애플리케이션이 처음으로 수동으로 성공적으로 평가됩니다.
- 애플리케이션은 적절한 IAM 역할로 구성되어 있습니다.
- 애플리케이션이 현재 IAM 사용자 권한으로 구성된 경우
AWSResilienceHubAssessmentExecutionPolicy에서 적절한 절차를 사용하는

[the section called “AWS Resilience Hub와 IAM의 작동 방식”](#) 역할을 생성해야 합니다.

2. 가 복원력 정책에서 드리프트를 AWS Resilience Hub 감지하거나 리소스가 드리프트되었을 때 알림을 받으려면 애플리케이션이 드리프트할 때 알림 받기를 켭니다.

이 옵션이 켜져 있는 경우, 드리프트 알림을 수신하려면 Amazon Simple Notification Service(SNS) 주제를 지정해야 합니다. Amazon SNS 주제를 제공하려면 SNS 주제 제공 섹션에서 SNS 주제 선택 옵션을 선택하고 SNS 주제 선택 드롭다운 목록에서 Amazon SNS 주제를 선택합니다.

Note

- AWS Resilience Hub 가 Amazon SNS 주제에 알림을 게시하도록 하려면 Amazon SNS 주제를 적절한 권한으로 구성해야 합니다. 권한 설정에 대한 자세한 정보는 [the section called “Amazon SNS 주제에 AWS Resilience Hub 게시하도록 활성화”](#) 단원을 참조하세요.
- 일일 평가는 실행 할당량에 영향을 미칠 수 있습니다. 할당량에 대한 자세한 내용은 AWS 일반 참조의 [AWS Resilience Hub 엔드포인트 및 할당량](#)을 참조하세요.

다른 AWS 계정 리전이나 다른 리전 또는 둘 다에 있는 Amazon SNS 주제를 사용하려면 SNS 주제 ARN 입력을 선택하고 SNS 주제 제공 상자에 Amazon SNS 주제의 Amazon 리소스 이름(ARN)을 입력합니다. ARN에 대한 자세한 내용은 AWS 일반 참조의 [Amazon 리소스 이름\(ARN\)](#)을 참조하십시오.

다음

[권한 설정](#)

권한 설정

AWS Resilience Hub 를 사용하면 기본 계정 및 보조 계정이 리소스를 검색하고 평가하는 데 필요한 권한을 구성할 수 있습니다. 하지만 절차를 개별적으로 실행하여 각 계정에 대한 권한을 구성해야 합니다.

IAM 역할 및 IAM 권한을 구성하려면

1. 현재 계정의 리소스에 액세스하는 데 사용할 기존 IAM 역할을 선택하려면 IAM 역할 선택 드롭다운 목록에서 IAM 역할을 선택합니다.

Note

교차 계정 설정의 경우 IAM 역할 ARNs)을 지정하지 않으면 AWS Resilience Hub 는 모든 계정에 대해 IAM 역할 선택 드롭다운 목록에서 선택한 IAM 역할을 사용합니다.

계정에 연결된 기존 IAM 역할이 없는 경우 다음 옵션 중 하나를 사용하여 IAM 역할을 생성할 수 있습니다.

- AWS IAM 콘솔 -이 옵션을 선택하는 경우 IAM 콘솔에서 AWS Resilience Hub 역할을 생성하려는 절차를 완료해야 합니다.
 - AWS CLI -이 옵션을 선택하면 AWS CLI의 모든 단계를 완료해야 합니다.
 - CloudFormation 템플릿 - 이 옵션을 선택하는 경우 계정 유형(기본 계정 또는 보조 계정)에 따라 적절한 AWS CloudFormation 템플릿을 사용하여 역할을 생성해야 합니다.
2. 오른쪽 화살표를 선택하여 교차 계정에서 IAM 역할 추가 - 선택 섹션을 확장합니다.
 3. 교차 계정에서 IAM 역할을 선택하려면 IAM 역할 ARN 입력 상자에 IAM 역할의 ARN을 입력합니다. 입력하는 IAM 역할의 ARN이 현재 계정에 속하지 않는지 확인하세요.
 4. 현재의 IAM 사용자를 사용하여 애플리케이션 리소스를 검색하려면 오른쪽 화살표를 선택하여 현재 IAM 사용자 권한 사용 섹션을 확장하고 AWS Resilience Hub내에서 필요한 기능을 활성화하려면 권한을 수동으로 구성해야 한다는 점을 이해합니다를 선택합니다.

이 옵션을 선택하면 일부 AWS Resilience Hub 기능(예: 드리프트 알림)이 예상대로 작동하지 않을 수 있으며 새 애플리케이션을 생성하기 위해 제공한 입력은 무시됩니다.

다음

[애플리케이션 구성 파라미터 구성](#)

애플리케이션 구성 파라미터 구성

이 섹션에서는를 사용하여 리전 간 장애 조치 지원에 대한 세부 정보를 제공할 수 있습니다 AWS Elastic Disaster Recovery. AWS Resilience Hub 는이 정보를 사용하여 복원력 권장 사항을 제공합니다.

애플리케이션 구성 파라미터에 대한 자세한 내용은 [애플리케이션 구성 파라미터](#) 단원을 참조하세요.

애플리케이션 구성 파라미터를 추가하려면 (선택 사항)

1. 애플리케이션 구성 파라미터 섹션을 확장하려면 오른쪽 화살표를 선택합니다.
2. 계정 ID 상자에 장애 조치 계정 ID를 입력합니다. 기본적으로이 필드에는 사용되는 계정 ID로 미리 채워져 있으며 AWS Resilience Hub, 이를 변경할 수 있습니다.
3. 지역 드롭다운 목록에서 장애 조치 지역을 선택합니다.

Note

이 기능을 비활성화하려면 드롭다운 목록에서 “—”를 선택합니다.

다음

[태그 추가](#)

태그 추가

AWS 리소스에 태그 또는 레이블을 할당하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적합니다.

(선택 사항) 애플리케이션에 태그를 추가하려면 하나 이상의 태그를 애플리케이션에 연결하려는 경우 새 태그 추가를 선택합니다. 태그에 대한 자세한 내용은 AWS 일반 참조 안내서의 [리소스 태깅 \(Tagging resources\)](#)을 참조하세요.

애플리케이션 추가를 선택하여 애플리케이션을 생성합니다.

다음

[애플리케이션 검토 및 게시 AWS Resilience Hub](#)

애플리케이션 검토 및 게시 AWS Resilience Hub

애플리케이션을 생성한 후에도 애플리케이션을 검토하고 리소스를 편집할 수 있습니다. 작업을 마치면 게시를 선택하여 애플리케이션을 게시합니다.

Note

AWS Resilience Hub는 백그라운드에서 애플리케이션 리소스를 스캔하고 보다 효율적인 방식으로 그룹화하여 평가의 정확도를 개선할 수 있는지 확인합니다. 가 관련 AppComponents로 그룹화할 수 있는 리소스를 AWS Resilience Hub 식별하면 애플리케이션 페이지의 애플리케이션 구조 탭에 리소스 그룹화 권장 사항 정보 알림이 표시되고 권장 사항 검토를 선택하여 검토할 수 있습니다. 자세한 내용은 [the section called “AWS Resilience Hub 리소스 그룹화 권장 사항”](#) 단원을 참조하십시오.

애플리케이션 검토 및 리소스 편집에 대한 자세한 내용은 다음을 참조하세요.

- [the section called “애플리케이션 요약 보기”](#)
- [the section called “애플리케이션 리소스 편집”](#)

다음

[애플리케이션 평가 AWS Resilience Hub 실행](#)

애플리케이션 평가 AWS Resilience Hub 실행

게시한 애플리케이션은 요약 페이지에 나열됩니다.

AWS Resilience Hub 애플리케이션을 게시하면 복원력 평가를 실행할 수 있는 애플리케이션 요약 페이지로 리디렉션됩니다. 이 평가는 애플리케이션에 연결된 복원력 정책을 기준으로 애플리케이션 구성을 평가합니다. 애플리케이션이 복원력 정책의 목표를 기준으로 어떻게 측정되는지를 보여주는 평가 보고서가 생성됩니다.

복원력 평가를 실행하려면

1. 애플리케이션 요약 페이지에서 복원력 평가를 선택합니다.

2. 복원력 평가 실행 대화 상자에서 보고서의 고유한 이름을 입력하거나 이름 보고 상자에 생성된 이름을 사용합니다.
3. Run(실행)을 선택합니다.
4. 평가 보고서가 생성되었다는 알림을 받은 후 평가 탭과 평가를 선택하여 보고서를 확인하세요.
5. 검토 탭을 선택하면 애플리케이션의 평가 보고서를 볼 수 있습니다.

사용 AWS Resilience Hub

AWS Resilience Hub 를 사용하면 애플리케이션의 복원력을 개선하고 애플리케이션 중단 시 복구 시간을 AWS 줄일 수 있습니다.

주제:

- [AWS Resilience Hub 요약](#)
- [AWS Resilience Hub 대시보드](#)
- [AWS Resilience Hub 애플리케이션 설명 및 관리](#)
- [복원력 정책 관리](#)
- [에서 복원력 평가 실행 및 관리 AWS Resilience Hub](#)
- [복원력 위젯에서 복원력 평가 실행 및 관리](#)
- [경보 관리](#)
- [표준 운영 절차 관리](#)
- [AWS Fault Injection Service 실험 관리](#)
- [복원력 점수 이해](#)
- [를 사용하여 애플리케이션에 운영 권장 사항 통합 AWS CloudFormation](#)

AWS Resilience Hub 요약

AWS Resilience Hub 는 여러 AWS 서비스 및 리소스에서 애플리케이션의 복원력을 at-a-glance 볼 수 있는 차트 및 그래프가 포함된 시각적 요약을 제공합니다. 이 포괄적이고 간결한 시각적 요약을 통해 잠재적인 복원력 격차를 신속하게 식별하고, 작업의 우선순위를 지정하고, 중단으로부터 복구할 수 있는 애플리케이션 기능을 개선하는 데 따른 진행 상황을 추적할 수 있습니다. 내보내기를 선택하고 지표를 처음 내보내는 경우는 액세스하려는 리전에서 새 Amazon S3 버킷을 AWS Resilience Hub 생성합니다 AWS Resilience Hub. 이 Amazon S3 버킷은 처음 생성되며 성공적으로 완료되면 내보낸 지표를 저장하는 데 사용됩니다. 내보낸 데이터를 Amazon S3에 저장하는 경우 추가 요금이 부과됩니다. 이러한 요금에 대한 자세한 내용은 [Amazon S3 요금](#)을 참조하십시오.

위젯의 차트와 그래프는 다음을 이해하는 데 도움이 됩니다.

- 애플리케이션의 전체 복원력 점수 및 현재 운영 상태에 대한 개요입니다.

- 설정된 정책을 준수하지 않거나 권장 구성에서 드리프트된 애플리케이션을 강조 표시하여 정책 위반 또는 모범 사례 이탈 가능성. 또한 우선 순위를 지정하고 해결할 수 있는 특정 영역도 강조 표시됩니다.
- 즉각적인 주의가 필요한 중요한 리소스 또는 애플리케이션.
- 경보 구현, AWS Fault Injection Service (AWS FIS) 실험 수행, 표준 운영 절차 수립과 같은 복원력 관행을 강화하기 위한 권장 사항입니다. 이러한 권장 사항은 시간이 지남에 따라 추적되므로 구현 진행 상황을 모니터링하고 애플리케이션의 전반적인 복원력 상태에 미치는 영향을 측정할 수 있습니다.

위젯

- [애플리케이션 상태](#)
- [리소스 유형별 상위 인프라 권장 사항](#)
- [인프라 권장 사항](#)
- [구현되지 않은 운영 권장 사항](#)
- [경보 권장 사항](#)
- [SOP 권장 사항](#)
- [AWS FIS 실험 권장 사항](#)
- [드리프트가 있는 애플리케이션](#)
- [복원력 점수](#)
- [복원력 점수에 대한 하위 10개 애플리케이션](#)
- [정책별 애플리케이션 상태](#)

애플리케이션 상태

이 위젯은 애플리케이션이 복원력 정책을 준수하는지 여부를 나타냅니다. 팝업에서 애플리케이션 수 옆에 있는 숫자를 선택하면 애플리케이션 창에서 연결된 모든 애플리케이션을 볼 수 있습니다. 생성한 모든 애플리케이션을 보려면 애플리케이션 보기를 선택합니다. 에서 애플리케이션 관리에 대한 자세한 내용은 섹션을 AWS Resilience Hub참조하세요 [AWS Resilience Hub 애플리케이션 요약 보기](#).

리소스 유형별 상위 인프라 권장 사항

이 위젯은 복원력을 개선하기 위해 마지막으로 성공한 평가에서 제공된 리소스의 각 AWS 리소스 유형에 대한 인프라 권장 사항 수를 표시합니다. 세부 정보 위로 마우스를 가져가거나 세부 정보로 이동하

여 세부 정보를 식별할 수 있습니다. 생성한 모든 애플리케이션을 보려면 애플리케이션 보기를 선택합니다. 인프라 권장 사항에 대한 자세한 내용은 섹션을 참조하세요 [복원력 권장 사항 검토](#).

인프라 권장 사항

이 위젯에는 복원력을 개선하기 위해 마지막으로 성공한 평가에서 제공된 인프라 권장 사항의 최대 수가 있는 최대 10개의 애플리케이션이 나열됩니다. 생성한 모든 애플리케이션을 보려면 애플리케이션 보기를 선택합니다. 인프라 권장 사항에 대한 자세한 내용은 섹션을 참조하세요 [복원력 권장 사항 검토](#).

다음을 사용하여 세부 정보를 식별할 수 있습니다.

- 애플리케이션 이름 - 애플리케이션을 정의할 때 제공한 애플리케이션의 이름입니다 AWS Resilience Hub.
- 개수 - 마지막으로 성공한 평가 AWS Resilience Hub 에서가 제공한 인프라 권장 사항 수를 나타냅니다. 평가 보고서에 제공된 모든 인프라 권장 사항을 보려면 번호를 선택합니다.
- 마지막 평가 - 애플리케이션이 마지막으로 성공적으로 평가된 날짜와 시간을 나타냅니다.

구현되지 않은 운영 권장 사항

이 위젯에는 복원력 태세를 개선하기 위해 마지막으로 성공한 평가에서 구현되지 않은 운영 권장 사항의 최대 수가 제공된 최대 10개의 애플리케이션이 나열됩니다. 생성한 모든 애플리케이션을 보려면 애플리케이션 보기를 선택합니다. 운영 권장 사항에 대한 자세한 내용은 섹션을 참조하세요 [운영 권장 사항 검토](#).

다음을 사용하여 세부 정보를 식별할 수 있습니다.

- 애플리케이션 이름 - 애플리케이션을 정의할 때 제공한 애플리케이션의 이름입니다 AWS Resilience Hub.
- 개수 - 마지막으로 성공한 평가 AWS Resilience Hub 에서가 제공한 운영 권장 사항 수를 나타냅니다. 평가 보고서에서 구현되지 않은 운영 권장 사항을 모두 보려면 번호를 선택합니다.
- 마지막 평가 시간 - 애플리케이션이 마지막으로 성공적으로 평가된 날짜와 시간을 나타냅니다.

경보 권장 사항

이 위젯에는 선택한 기간 동안 복원력을 개선하기 위해 제공되는 모든 Amazon CloudWatch 경보 권장 사항이 나열됩니다. 다양한 범주(구현됨, 구현되지 않음, 제외됨)는 애플리케이션에서 구현 상태를 나타냅니다. 각 범주를 마우스로 가리키거나 해당 범주로 이동하여 각 범주에 대한 Amazon CloudWatch

경보 권장 사항 수를 볼 수 있습니다. 생성한 모든 애플리케이션을 보려면 애플리케이션 보기를 선택합니다. 경보 권장 사항에 대한 자세한 내용은 섹션을 참조하세요 [운영 권장 사항 검토](#).

SOP 권장 사항

이 위젯에는 선택한 기간 동안 복원력을 개선하기 위해 제공되는 모든 표준 운영 절차(SOP) 권장 사항이 나열되어 있습니다. 다양한 범주(구현됨, 구현되지 않음, 제외됨)는 애플리케이션에서 구현 상태를 나타냅니다. 각 범주를 마우스로 가리키거나 해당 범주로 이동하여 각 범주에 대한 SOP 권장 사항 수를 볼 수 있습니다. 생성한 모든 애플리케이션을 보려면 애플리케이션 보기를 선택합니다. 운영 권장 사항에 대한 자세한 내용은 섹션을 참조하세요 [운영 권장 사항 검토](#).

AWS FIS 실험 권장 사항

이 위젯에는 선택한 기간 동안 복원력 태세를 개선하기 위해 제공되는 모든 AWS FIS 실험 권장 사항이 나열됩니다. 다양한 범주(구현됨, 구현되지 않음, 부분 구현됨, 제외됨)는 애플리케이션에서 구현 상태를 나타냅니다. 각 범주를 마우스로 가리키거나 범주로 이동하여 범주별 AWS FIS 실험 권장 사항 수를 볼 수 있습니다. 생성한 모든 애플리케이션을 보려면 애플리케이션 보기를 선택합니다. AWS FIS 실험 권장 사항에 대한 자세한 내용은 섹션을 참조하세요 [표준 운영 절차 관리](#).

드리프트가 있는 애플리케이션

이 위젯은 마지막으로 성공한 평가에서 이전 규정 준수 상태에서 드리프트한 모든 애플리케이션을 나열합니다. 생성한 모든 애플리케이션을 보려면 애플리케이션 보기를 선택합니다. 의 애플리케이션 관리에 대한 자세한 내용은 섹션을 AWS Resilience Hub참조하세요 [AWS Resilience Hub 애플리케이션 요약 보기](#).

다음을 사용하여 세부 정보를 식별할 수 있습니다.

- 애플리케이션 이름 - 애플리케이션을 정의할 때 제공한 애플리케이션의 이름입니다 AWS Resilience Hub.
- 정책 드리프트 - 이전 평가에서 정책을 준수했지만 현재 평가를 준수하지 못한 모든 애플리케이션 구성 요소를 보려면 애플리케이션 이름 옆에 있는 번호를 선택합니다.
- 리소스 드리프트 - 아래 번호를 선택하면 최신 가져오기에서 구성에서 변경된 모든 리소스를 볼 수 있습니다.

복원력 점수

이 위젯은 최대 5개의 애플리케이션에 대해 선택한 기간 동안 애플리케이션의 복원력 점수 추세를 표시합니다. 애플리케이션 이름과 연결된 선 위로 마우스를 가져가거나 애플리케이션으로 이동한 다음 애플리케이션 이름을 선택하여 애플리케이션 요약을 보면서 애플리케이션의 복원력 점수를 볼 수 있습니다. 생성한 모든 애플리케이션을 보려면 애플리케이션 보기를 선택합니다. 복원력 점수에 대한 자세한 내용은 섹션을 참조하세요 [복원력 점수 이해](#).

복원력 점수에 대한 하위 10개 애플리케이션

이 위젯은 가장 최근 평가에서 복원력이 가장 낮은 최대 10개의 애플리케이션을 나열하여 복원력을 개선하기 위해 즉각적인 주의가 필요한 애플리케이션을 강조합니다. 생성한 모든 애플리케이션을 보려면 애플리케이션 보기를 선택합니다. 복원력 점수에 대한 자세한 내용은 섹션을 참조하세요 [복원력 점수 이해](#).

다음을 사용하여 세부 정보를 식별할 수 있습니다.

- 애플리케이션 이름 - 애플리케이션을 정의할 때 제공한 애플리케이션의 이름입니다 AWS Resilience Hub.
- 복원력 점수 - 평가를 실행한 후 애플리케이션에 AWS Resilience Hub 대해에서 결정한 전체 복원력 점수입니다.
- 마지막 평가 시간 - 애플리케이션이 마지막으로 성공적으로 평가된 날짜와 시간을 나타냅니다.

정책별 애플리케이션 상태

이 위젯에는 모든 정책과 위반, 충족 또는 아직 평가되지 않은 애플리케이션 수가 나열됩니다. 생성한 모든 정책을 보려면 정책 보기를 선택합니다. 복원력 점수에 대한 자세한 내용은 섹션을 참조하세요 [복원력 정책 관리](#).

다음을 사용하여 세부 정보를 식별할 수 있습니다.

- 정책 이름 - 정의 중에 제공한 정책 이름을 나타냅니다 AWS Resilience Hub.
- 유형 - 애플리케이션에 연결된 정책 유형(탄력성 정책)을 나타냅니다.
- 정책 이름 - 복원력 정책에 정의된 RTO 및 RPO 대상을 위반한 애플리케이션 수를 나타냅니다.
- 충족된 앱 - 복원력 정책을 준수하는 애플리케이션 수를 나타냅니다.
- 평가되지 않은 앱 - 복원력 정책에 대해 아직 평가되지 않은 애플리케이션 수를 나타냅니다.

- 복원력 점수 - 평가를 실행한 후 애플리케이션에 AWS Resilience Hub 대해에서 결정한 전체 복원력 점수입니다.
- 마지막 평가 시간 - 애플리케이션이 마지막으로 성공적으로 평가된 날짜와 시간을 나타냅니다.

AWS Resilience Hub 대시보드

대시보드는 애플리케이션 포트폴리오의 복원력 상태를 포괄적으로 보여줍니다. 대시보드는 복원력 이벤트(예: 사용할 수 없는 데이터베이스 또는 복원력 검증 실패), 알림 및 CloudWatch 및 AWS Fault Injection Service ()와 같은 서비스의 인사이트를 집계하고 구성합니다AWS FIS.

또한 대시보드는 평가된 각 애플리케이션에 대한 복원력 점수를 생성합니다. 이 점수는 권장 복원력 정책, 경보, 복구 표준 운영 절차(SOPs) 및 테스트를 기준으로 평가할 때 애플리케이션이 얼마나 잘 작동하는지 나타냅니다. 이 점수를 사용하여 시간 경과에 따른 복원력 개선을 측정할 수 있습니다.

AWS Resilience Hub 대시보드를 보려면 탐색 메뉴에서 대시보드를 선택합니다. 대시보드 페이지에는 다음 섹션이 표시됩니다.

애플리케이션 상태

애플리케이션 상태는 애플리케이션이 연결된 복원력 정책을 준수하는지 여부를 나타냅니다. 또한 평가가 완료된 후 상태는 애플리케이션의 입력 소스가 수정되었는지 여부도 나타냅니다. 다음 각 상태 아래의 숫자를 선택하여 애플리케이션 페이지에서 동일한 상태를 공유하는 모든 애플리케이션을 봅니다.

- 정책의 애플리케이션 - 연결된 복원력 정책을 준수하는 모든 애플리케이션을 나타냅니다.
- 애플리케이션 위반 정책 - 연결된 복원력 정책을 준수하지 않는 모든 애플리케이션을 나타냅니다.
- 평가되지 않은 애플리케이션 - 규정 준수가 아직 평가되거나 추적되지 않은 모든 애플리케이션을 나타냅니다.
- 드리프트된 애플리케이션 - 복원력 정책에서 드리프트되었거나 리소스가 드리프트된 모든 애플리케이션을 나타냅니다.

시간 경과에 따른 애플리케이션 복원력 점수

시간 경과에 따른 애플리케이션 복원력 점수를 사용하면 지난 30일 동안의 애플리케이션 복원력 그래프를 볼 수 있습니다. 드롭다운 메뉴에 10개의 애플리케이션이 나열될 수 있지만 한 번에 최대 4개의 애플리케이션 그래프 AWS Resilience Hub 만 표시합니다. 복원력 점수에 대한 자세한 내용은 섹션을 참조하세요 [복원력 점수 이해](#).

Note

AWS Resilience Hub 는 예약된 평가를 동시에 실행하지 않습니다. 따라서 애플리케이션의 일일 평가를 보려면 나중에 시간에 따른 복원력 점수 그래프로 돌아가야 할 수도 있습니다.

AWS Resilience Hub 또한 Amazon CloudWatch를 사용하여 이러한 그래프를 생성합니다. CloudWatch에서 지표 보기(View metrics in CloudWatch)를 선택하여 CloudWatch 대시보드에서 애플리케이션 복원력에 대한 보다 세부적인 정보를 생성하고 확인합니다. CloudWatch에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 [대시보드 사용\(Using dashboards\)](#)을 참조하세요.

구현된 경보

이 섹션에서는 Amazon CloudWatch에서 모든 애플리케이션을 모니터링하기 위해 설정한 모든 경보를 나열합니다. 자세한 내용은 섹션을 참조하세요 [경보 보기](#).

구현된 실험

이 단원에서는 모든 애플리케이션에서 구현한 모든 오류 주입 실험을 나열합니다. 자세한 내용은 [AWS FIS 실험 보기](#) 단원을 참조하십시오.

AWS Resilience Hub 애플리케이션 설명 및 관리

AWS Resilience Hub 애플리케이션은 AWS 애플리케이션 중단을 방지하고 복구하도록 구성된 AWS 리소스 모음입니다.

AWS Resilience Hub 애플리케이션을 설명하려면 애플리케이션 이름, 하나 이상의 AWS CloudFormation 스택의 리소스 및 적절한 복원력 정책을 제공합니다. 기존 AWS Resilience Hub 애플리케이션을 템플릿으로 사용하여 애플리케이션을 설명할 수도 있습니다.

AWS Resilience Hub 애플리케이션을 설명한 후에는 복원력 평가를 실행할 수 있도록 애플리케이션을 게시해야 합니다. 그런 다음 평가의 권장 사항을 사용하여 다른 평가를 실행하고 결과를 비교한 다음 예상 워크로드 RTO와 예상 워크로드 RPO가 RTO 및 RPO 목표를 충족할 때까지 프로세스를 반복하여 복원력을 개선할 수 있습니다.

애플리케이션 페이지를 보려면 탐색 창에서 애플리케이션을 선택합니다. 애플리케이션 페이지에서 다음을 통해 애플리케이션을 식별할 수 있습니다.

- 이름 - 애플리케이션을 정의할 때 제공한 애플리케이션의 이름입니다 AWS Resilience Hub.

- 설명 - AWS Resilience Hub에서 애플리케이션을 정의할 때 제공한 애플리케이션에 대한 설명입니다.
- 규정 준수 상태 - 애플리케이션 상태를 평가됨, 평가되지 않음, 정책 위반 또는 변경 감지됨으로 AWS Resilience Hub 설정합니다.
- 평가됨 - 애플리케이션을 AWS Resilience Hub 평가했습니다.
- 평가되지 않음 - 애플리케이션을 평가하지 AWS Resilience Hub 않았습니다.
- 정책 위반 - 애플리케이션이 복구 시간 목표(RTO) 및 복구 시점 목표(RPO)에 대한 복원력 정책의 목표를 충족하지 못했다 AWS Resilience Hub 고 판단했습니다. 애플리케이션의 복원력을 재평가 AWS Resilience Hub 하기 전에에서 제공하는 권장 사항을 검토하고 사용합니다. 권장 사항에 대한 자세한 내용은 [예 애플리케이션 추가 AWS Resilience Hub](#) 단원을 참조하세요.
- 변경 사항 감지 - 애플리케이션과 연결된 복원력 정책에 대한 변경 사항을 감지 AWS Resilience Hub 했습니다. 애플리케이션이 복원력 정책의 목표를 충족하는지 확인하려면 AWS Resilience Hub 에 대한 애플리케이션을 재평가해야 합니다.
- 예정된 평가 - 리소스 유형은 애플리케이션의 구성 요소 리소스를 식별합니다. 예정된 평가에 대한 자세한 내용은 [애플리케이션 복원력](#) 단원을 참조하세요.
- 활성화됨 - 애플리케이션이 AWS Resilience Hub에 의해 매일 자동으로 평가됨을 나타냅니다.
- 비활성화됨 - 애플리케이션이에 의해 매일 자동으로 평가되지 AWS Resilience Hub 않으며 애플리케이션을 수동으로 평가해야 함을 나타냅니다.
- 드리프트 상태 - 애플리케이션이 이전에 성공한 평가에서 드리프트되었는지 여부를 나타내며 다음 상태 중 하나를 설정합니다.
- 드리프트됨 - 이전의 성공적인 평가에서 복원력 정책을 준수했던 애플리케이션이 이제 복원력 정책을 위반하여 애플리케이션이 위험에 처해 있음을 나타냅니다. 또한 현재 애플리케이션 버전에 포함된 입력 소스 내의 리소스가 추가 또는 제거되었는지 여부도 나타냅니다.
- 드리프트 안됨 - 애플리케이션이 여전히 정책에 정의된 RTO 및 RPO 목표를 충족하는 것으로 추정됨을 나타냅니다. 또한 현재 애플리케이션 버전에 포함된 입력 소스 내의 리소스가 추가되거나 제거되지 않았음을 나타냅니다.
- 예상 워크로드 RTO - 애플리케이션의 가능한 최대 예상 워크로드 RTO를 나타냅니다. 이 값은 마지막으로 성공적으로 평가한 모든 중단 유형의 최대 예상 워크로드 RTO입니다.
- 예상 워크로드 RPO - 애플리케이션의 가능한 최대 예상 워크로드 RPO를 나타냅니다. 이 값은 마지막으로 성공적으로 평가한 모든 중단 유형의 최대 예상 워크로드 RTO입니다.
- 마지막 평가 시간 - 애플리케이션이 마지막으로 성공적으로 평가된 날짜와 시간을 나타냅니다.
- 생성 시간 - 애플리케이션이 생성된 날짜 및 시간입니다.

- ARN – 애플리케이션의 Amazon 리소스 이름(ARN)입니다. ARN에 대한 자세한 내용은 AWS 일반 참조의 [Amazon 리소스 이름\(ARN\)](#)을 참조하십시오.

Note

AWS Resilience Hub 는 이미지 리포지토리에 Amazon ECR을 사용하는 경우에만 리전 간 Amazon ECS 리소스의 복원력을 완전히 평가할 수 있습니다.

또한 애플리케이션 페이지에서 다음 옵션 중 하나를 사용하여 애플리케이션 목록을 필터링할 수도 있습니다.

- 애플리케이션 찾기 - 애플리케이션 이름을 입력하여 애플리케이션 이름을 기준으로 결과를 필터링합니다.
- 마지막 평가 시간을 날짜 및 시간 범위로 필터링 - 이 필터를 적용하려면 달력 아이콘을 선택하고 다음 옵션 중 하나를 선택하여 시간 범위와 일치하는 결과를 기준으로 필터링합니다.
- 상대 범위 - 사용 가능한 옵션 중 하나를 선택하고 적용을 선택합니다.

사용자 지정 범위 옵션을 선택하는 경우 기간 입력 상자에 기간을 입력하고 시간 단위 드롭다운 목록에서 적절한 시간 단위를 선택한 다음 적용을 선택합니다.

- 절대 범위 - 날짜 및 시간 범위를 지정하려면 시작 시간과 종료 시간을 제공한 다음 적용을 선택합니다.

다음 주제에서는 AWS Resilience Hub 애플리케이션을 설명하는 다양한 접근 방식과 이를 관리하는 방법을 보여줍니다.

주제

- [AWS Resilience Hub 애플리케이션 요약 보기](#)
- [AWS Resilience Hub 애플리케이션 리소스 편집](#)
- [애플리케이션 구성 요소 관리](#)
- [새 AWS Resilience Hub 애플리케이션 버전 게시](#)
- [모든 AWS Resilience Hub 애플리케이션 버전 보기](#)
- [AWS Resilience Hub 애플리케이션의 리소스 보기](#)
- [AWS Resilience Hub 애플리케이션 삭제](#)
- [애플리케이션 구성 파라미터](#)

AWS Resilience Hub 애플리케이션 요약 보기

AWS Resilience Hub 콘솔의 애플리케이션 요약 페이지에서는 애플리케이션 정보 및 복원력 상태에 대한 개요를 제공합니다.

애플리케이션 요약을 보려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 보려는 애플리케이션의 이름을 선택합니다.

애플리케이션 요약 페이지에는 다음 섹션이 포함되어 있습니다.

주제

- [평가 요약](#)
- [요약](#)
- [애플리케이션 복원력](#)
- [구현된 경보](#)
- [구현된 실험](#)

평가 요약

이 섹션에서는 마지막으로 성공한 평가에 대한 요약을 제공하고 중요한 권장 사항을 실행 가능한 인사이트로 강조합니다. Amazon Bedrock 생성형 AI 기능을 AWS Resilience Hub 사용하여 사용자가 제공하는 가장 중요한 복원력 권장 사항에 집중할 수 있도록 지원합니다. AWS Resilience Hub. 중요한 항목에 집중하면 애플리케이션의 복원력을 개선하는 가장 중요한 권장 사항에 집중할 수 있습니다. 권장 사항을 선택하여 요약을 보고 세부 정보 보기를 선택하여 평가 보고서의 관련 섹션에서 권장 사항에 대한 자세한 내용을 봅니다. 평가 보고서 검토에 대한 자세한 내용은 섹션을 참조하세요 [the section called “평가 보고서 검토”](#).

Note

- 이 평가 요약은 미국 동부(버지니아 북부) 리전에서만 사용할 수 있습니다.
- Amazon Bedrock의 대규모 언어 모델(LLMs)에서 생성된 평가 요약은 제안 사항일 뿐입니다. 생성형 AI 기술의 현재 수준은 완벽하지 않으며 LLMs 실행할 수 없습니다. 드물긴 하지만 편

향과 잘못된 답변이 필요합니다. LLM의 출력을 사용하기 전에 평가 요약의 각 권장 사항을 검토합니다.

요약

이 섹션에서는 다음 섹션에서 선택한 애플리케이션에 대한 요약을 제공합니다.

- 애플리케이션 정보 - 이 섹션에서는 선택한 애플리케이션에 대한 다음 정보를 제공합니다.
 - 애플리케이션 상태 - 애플리케이션의 상태를 나타냅니다.
 - 설명 - 애플리케이션에 대한 설명입니다.
 - 버전 - 현재 평가된 애플리케이션 버전을 나타냅니다.
 - 복원력 정책 - 애플리케이션이 연결된 복원력 정책을 나타냅니다. 복원력 정책에 대한 자세한 내용은 [복원력 정책 관리](#) 단원을 참조하세요.
- 애플리케이션 드리프트 - 이 섹션에서는 선택한 애플리케이션에 대한 평가를 실행하여 복원력 정책을 준수하는지 확인하는 동안 감지된 드리프트를 강조 표시합니다. 또한 애플리케이션 버전이 마지막으로 게시된 이후 리소스가 추가 또는 제거되었는지도 확인합니다. 이 섹션에는 다음 정보가 표시됩니다.
 - 정책 드리프트 - 이전 평가에서 정책을 준수했지만 현재 평가를 준수하지 못한 모든 애플리케이션 구성 요소를 보려면 아래 번호를 선택합니다.
 - 리소스 드리프트 - 아래 번호를 선택하여 최신 평가에서 드리프트된 모든 리소스를 봅니다.

애플리케이션 복원력

복원력 점수 섹션에 표시된 지표는 애플리케이션의 최신 복원력 평가에서 가져온 것입니다.

복원력 점수

복원력 점수는 잠재적 중단에 대처하기 위한 준비 상태를 수치화하는 데 도움이 됩니다. 이 점수는 애플리케이션이 애플리케이션의 복원력 정책, 경보, 표준 운영 절차(SOP) 및 테스트를 충족하기 위한 AWS Resilience Hub 권장 사항을 얼마나 잘 준수했는지를 반영합니다.

애플리케이션이 달성할 수 있는 최대 복원력 점수는 100%입니다. 점수는 미리 정의된 기간 동안 실행되는 모든 권장 테스트를 나타냅니다. 이는 테스트에서 올바른 경보가 시작되고 경보가 올바른 SOP를 시작함을 나타냅니다.

예를 들어,가 하나의 경보와 하나의 SOP로 하나의 테스트를 AWS Resilience Hub 권장한다고 가정해 보겠습니다. 테스트가 실행되면 경보가 관련 SOP를 시작한 다음 성공적으로 실행됩니다. 복원력 점수에 대한 자세한 내용은 [복원력 점수 이해](#) 단원을 참조하세요.

구현된 경보

애플리케이션 요약 구현된 경보 섹션에는 애플리케이션을 모니터링하기 위해 Amazon CloudWatch에서 설정한 경보가 나열됩니다. 경보에 대한 자세한 내용은 [경보 관리](#) 단원을 참조하세요.

구현된 실험

애플리케이션 요약 오류 삽입 실험 섹션에는 오류 삽입 실험 목록이 표시됩니다. 오류 삽입 실험에 대한 자세한 내용은 [AWS Fault Injection Service 실험 관리](#) 단원을 참조하세요.

AWS Resilience Hub 애플리케이션 리소스 편집

정확하고 유용한 복원력 평가를 받으려면 애플리케이션 설명이 업데이트되고 실제 AWS 애플리케이션 및 리소스와 일치하는지 확인합니다. 평가 보고서, 검증 및 권장 사항은 나열된 리소스를 기반으로 합니다. AWS 애플리케이션에서 리소스를 추가하거나 제거하는 경우 이러한 변경 사항에 반영해야 합니다 AWS Resilience Hub.

AWS Resilience Hub 는 애플리케이션 소스에 대한 투명성을 제공합니다. 애플리케이션에서 리소스와 애플리케이션 소스를 식별하고 편집할 수 있습니다.

Note

리소스를 편집하면 애플리케이션의 AWS Resilience Hub 참조만 수정됩니다. 실제 리소스는 변경되지 않습니다.

누락된 리소스를 추가하거나, 기존 리소스를 수정하거나, 필요하지 않은 리소스를 제거할 수 있습니다. 리소스는 논리적 애플리케이션 구성 요소(AppComponents)로 그룹화됩니다. 애플리케이션 구조를 더 잘 반영하도록 AppComponent를 편집할 수 있습니다.

애플리케이션의 초안 버전을 편집하고 변경 사항을 새(릴리스) 버전에 게시하여 애플리케이션 리소스에 추가하거나 업데이트합니다.는 복원력 평가를 실행하기 위해 애플리케이션의 릴리스 버전(업데이트된 리소스 포함)을 AWS Resilience Hub 사용합니다.

애플리케이션의 복원력을 평가하려면

1. 탐색 창에서 애플리케이션을 선택합니다.

2. 애플리케이션 페이지에서 편집하려는 애플리케이션 이름을 선택합니다.
3. 작업 메뉴에서 복원력 평가를 선택합니다.
4. 복원력 평가 실행 대화 상자에서 보고서의 고유한 이름을 입력하거나 이름 보고 상자에 생성된 이름을 사용합니다.
5. Run(실행)을 선택합니다.
6. 평가 보고서가 생성되었다는 알림을 받은 후 평가 탭과 평가를 선택하여 보고서를 확인하세요.
7. 검토 탭을 선택하면 애플리케이션의 평가 보고서를 볼 수 있습니다.

예약된 평가를 활성화하려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 예약된 평가를 활성화할 애플리케이션을 선택합니다.
3. 매일 자동 평가를 켭니다.

예약된 평가를 비활성화하려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 예약된 평가를 활성화할 애플리케이션을 선택합니다.
3. 매일 자동 평가를 끕니다.

Note

예약된 평가를 비활성화하면 드리프트 알림이 비활성화됩니다.

4. 끄기를 선택합니다.

애플리케이션에 대해 드리프트 알림을 활성화하려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 드리프트 알림을 활성화할 애플리케이션을 선택하거나 드리프트 알림 설정을 편집합니다.
3. 다음 옵션 중 하나를 선택하여 드리프트 알림을 편집할 수 있습니다.
 - 작업에서 드리프트 알림 활성화를 선택합니다.
 - 애플리케이션 드리프트 섹션에서 알림 활성화를 선택합니다.

4. 의 단계를 완료한 [예약된 평가 및 드리프트 알림 설정](#)다음 이 절차로 돌아갑니다.
5. 활성화를 선택합니다.

드리프트 알림을 활성화하면 예약된 평가도 활성화됩니다.

애플리케이션의 드리프트 알림을 편집하려면

 Note

이 절차는 예약된 평가(일일 자동 평가 활성화) 및 드리프트 알림을 활성화한 경우에 적용됩니다.

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 드리프트 알림을 활성화할 애플리케이션을 선택하거나 드리프트 알림 설정을 편집합니다.
3. 다음 옵션 중 하나를 선택하여 드리프트 알림을 편집할 수 있습니다.
 - 작업에서 드리프트 알림 편집을 선택합니다.
 - 애플리케이션 드리프트 섹션에서 알림 편집을 선택합니다.
4. 의 단계를 완료한 [예약된 평가 및 드리프트 알림 설정](#)다음 이 절차로 돌아갑니다.
5. 저장(Save)을 선택합니다.

애플리케이션의 보안 권한을 업데이트하려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 보안 권한을 업데이트하려는 애플리케이션을 선택합니다.
3. 작업에서 권한 업데이트를 선택합니다.
4. 보안 권한을 업데이트하려면 [권한 설정](#)의 단계를 완료한 다음 이 절차로 돌아갑니다.
5. 저장 및 업데이트를 선택합니다.

애플리케이션에 복원력 정책을 연결하려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 편집하려는 애플리케이션 이름을 선택합니다.

3. 작업 메뉴에서 복원력 정책 연결을 선택합니다.
4. 정책 연결 대화 상자의 복원력 정책 선택 드롭다운 목록에서 복원력 정책을 선택합니다.
5. 연결을 선택합니다.

애플리케이션의 입력 소스, 리소스 및 AppComponent를 편집하려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 편집하려는 애플리케이션 이름을 선택합니다.
3. 애플리케이션 구조 탭을 선택합니다.
4. 버전 앞의 더하기 기호 +를 선택한 다음 초안 상태의 애플리케이션 버전을 선택합니다.
5. 애플리케이션의 입력 소스, 리소스 및 AppComponent를 편집하려면 다음 절차의 단계를 완료하세요.

애플리케이션의 입력 소스를 편집하려면

1. 애플리케이션의 입력 소스를 편집하려면 입력 소스 탭을 선택합니다.

입력 소스 섹션에는 애플리케이션 리소스의 모든 입력 소스가 나열됩니다. 다음과 같은 방법으로 입력 소스를 식별할 수 있습니다.

- 소스 이름 – 입력 소스의 이름입니다. 소스 이름을 선택하여 각 애플리케이션에서 세부 정보를 봅니다. 수동으로 추가한 입력 소스의 경우 링크를 사용할 수 없습니다. 예를 들어 AWS CloudFormation 스택에서 가져온 소스 이름을 선택하면 콘솔의 스택 세부 정보 페이지로 AWS CloudFormation 리디렉션됩니다.
- 소스 ARN – 입력 소스의 Amazon 리소스 이름(ARN)입니다. ARN을 선택하여 각 애플리케이션에서 세부 정보를 확인합니다. 수동으로 추가한 입력 소스의 경우 링크를 사용할 수 없습니다. 예를 들어 AWS CloudFormation 스택에서 가져온 ARN을 선택하면 AWS CloudFormation 콘솔의 스택 세부 정보 페이지로 리디렉션됩니다.
- 소스 유형 – 입력 소스의 유형입니다. 입력 소스에는 Amazon EKS 클러스터, AWS CloudFormation 스택, myApplications 애플리케이션 AWS Resource Groups, Terraform 상태 파일 및 수동으로 추가된 리소스가 포함됩니다.
- 연결된 리소스 – 입력 소스와 연결된 리소스의 수입입니다. 숫자를 선택하면 리소스 탭에서 입력 소스의 모든 관련 리소스를 볼 수 있습니다.

2. 애플리케이션에 입력 소스를 추가하려면 입력 소스 섹션에서 입력 소스 추가를 선택합니다. 입력 소스 추가에 대한 자세한 내용은 [the section called “애플리케이션에 리소스 AWS Resilience Hub 추가”](#) 단원을 참조하세요.
3. 입력 소스를 편집하려면 입력 소스를 선택하고 작업에서 다음 옵션 중 하나를 선택합니다.
 - 입력 소스 다시 가져오기(최대 5개) – 선택한 입력 소스를 최대 5개까지 다시 가져옵니다.
 - 입력 소스 삭제 – 선택한 입력 소스를 삭제합니다.

애플리케이션을 게시하려면 애플리케이션에 최소 하나 이상의 입력 소스가 있어야 합니다. 입력 소스를 모두 삭제하면 새 버전 게시가 비활성화됩니다.

애플리케이션의 리소스를 편집하려면

1. 애플리케이션의 리소스를 편집하려면 리소스 탭을 선택합니다.

Note

미평가 리소스 목록을 보려면 미평가 리소스 보기를 선택합니다.

리소스 섹션에는 애플리케이션 설명의 템플릿으로 사용하기로 선택한 애플리케이션의 리소스가 나열됩니다. 검색 환경을 개선하기 위해 AWS Resilience Hub 는 여러 검색 기준에 따라 리소스를 그룹화했습니다. 이러한 검색 기준에는 AppComponent 유형, 지원되지 않는 리소스, 제외된 리소스가 포함됩니다. 리소스 테이블의 검색 기준에 따라 리소스를 필터링하려면 각 검색 기준 아래의 숫자를 선택합니다.

다음은 통해 리소스를 식별할 수 있습니다.

- 논리적 ID - 논리적 ID는 AWS CloudFormation 스택, Terraform 상태 파일, 수동으로 추가된 애플리케이션, myApplications 애플리케이션 또는의 리소스를 식별하는 데 사용되는 이름입니다 AWS Resource Groups.

Note

- Terraform을 사용하면 다양한 리소스 유형에 동일한 이름을 사용할 수 있습니다. 따라서 동일한 이름을 공유하는 리소스의 경우 논리적 ID 끝에 “- 리소스 유형”이 표시됩니다.

- 모든 애플리케이션 리소스의 인스턴스를 보려면 논리적 ID 앞에 있는 더하기(+) 기호를 선택합니다. 애플리케이션 리소스의 모든 인스턴스를 보려면 각 리소스의 논리적 ID 앞에 있는 더하기(+) 기호를 선택합니다.

지원되는 리소스에 대한 자세한 내용은 [the section called “지원되는 AWS Resilience Hub 리소스”](#) 단원을 참조하세요.

- 리소스 유형 - 리소스 유형은 애플리케이션의 구성 요소 리소스를 식별합니다. 예를 들면 AWS::EC2::Instance는 Amazon EC2 인스턴스를 선언합니다. AppComponent 리소스 그룹화에 대한 자세한 내용은 [애플리케이션 구성 요소에서 리소스 그룹화](#) 단원을 참조하세요.
- 소스 이름 - 입력 소스의 이름입니다. 소스 이름을 선택하여 각 애플리케이션에서 세부 정보를 봅니다. 수동으로 추가한 입력 소스의 경우 링크를 사용할 수 없습니다. 예를 들어 AWS CloudFormation 스택에서 가져온 소스 이름을 선택하면의 스택 세부 정보 페이지로 리디렉션됩니다 AWS CloudFormation.
- 소스 유형 - 입력 소스의 유형입니다. 입력 소스에는 AWS CloudFormation 스택, myApplications 애플리케이션 AWS Resource Groups, Terraform 상태 파일 및 수동으로 추가된 리소스가 포함됩니다.

Note

Amazon EKS 클러스터를 편집하려면 AWS Resilience Hub 애플리케이션 절차의 입력 소스 편집의 단계를 완료합니다.

- 소스 스택 - 리소스가 포함된 AWS CloudFormation 스택입니다. 이 열은 선택한 애플리케이션 구조 유형에 따라 달라집니다.
- 물리적 ID - Amazon EC2 인스턴스 ID 또는 S3 버킷 이름 같은 해당 리소스에 대해 실제 할당된 식별자입니다.
- 포함 - AWS Resilience Hub 이 해당 리소스를 애플리케이션에 포함하는지 여부를 나타냅니다.
- 평가 가능 - AWS Resilience Hub 가 리소스의 복원력을 평가할 것인지 여부를 나타냅니다.
- AppComponents - 애플리케이션 구조가 검색될 때 리소스에 할당된 AWS Resilience Hub 구성 요소입니다.
- 이름 - 애플리케이션 리소스의 이름입니다
- 계정 - 물리적 리소스를 소유한 AWS 계정입니다.

2. 목록에 없는 리소스를 찾으려면 검색 상자에 리소스 논리 ID를 입력합니다.

3. 애플리케이션에서 리소스를 제거하려면 리소스를 선택한 다음 작업에서 리소스 제외를 선택합니다.
4. 애플리케이션의 리소스를 해결하려면 리소스 새로 고침을 선택합니다.
5. 기존 애플리케이션 리소스를 수정하려면 다음 단계를 완료합니다.
 - a. 리소스를 선택한 다음 작업에서 스택 업데이트를 선택합니다.
 - b. 스택 업데이트 페이지에서 리소스를 업데이트하려면 [리소스 컬렉션 추가](#)의 적절한 절차를 완료한 다음 이 절차로 돌아갑니다.
 - c. 저장을 선택합니다.
6. 애플리케이션에 리소스를 추가하려면 작업에서 리소스 추가를 선택하고 다음 단계를 완료합니다.
 - a. 리소스 유형 드롭다운 목록에서 리소스 유형을 선택합니다.
 - b. AppComponent 드롭다운 목록에서 AppComponent를 선택합니다.
 - c. 리소스 이름 상자에 리소스 논리 ID를 입력합니다.
 - d. 리소스 식별자 상자에 물리적 리소스 ID, 리소스 이름 또는 리소스 ARN을 입력합니다.
 - e. 추가를 선택합니다.
7. 리소스 이름을 편집하려면 리소스를 선택하고 작업에서 리소스 이름 편집을 선택한 후 다음 단계를 완료합니다.
 - a. 리소스 이름 상자에 리소스 논리 ID를 입력합니다.
 - b. 저장(Save)을 선택합니다.
8. 리소스 식별자를 편집하려면 리소스를 선택하고 작업에서 리소스 식별자 편집을 선택한 후 다음 단계를 완료합니다.
 - a. 리소스 식별자 상자에 물리적 리소스 ID, 리소스 이름 또는 리소스 ARN을 입력합니다.
 - b. 저장(Save)을 선택합니다.
9. AppComponent를 변경하려면 리소스를 선택하고 작업에서 AppComponent 변경을 선택한 후 다음 단계를 완료합니다.
 - a. AppComponent 드롭다운 목록에서 AppComponent를 선택합니다.
 - b. 추가를 선택합니다.
10. 리소스를 삭제하려면 리소스를 선택한 다음 작업에서 리소스 삭제를 선택합니다.
11. 리소스를 포함하려면 리소스를 선택한 다음 작업에서 리소스 포함을 선택합니다.

애플리케이션의 AppComponent를 편집하려면

1. 애플리케이션의 AppComponent를 편집하려면 AppComponent 탭을 선택합니다.

Note

AppComponent 리소스 그룹화에 대한 자세한 내용은 [애플리케이션 구성 요소에서 리소스 그룹화](#) 단원을 참조하세요.

AppComponent들 섹션에는 리소스가 그룹화된 모든 논리적 구성 요소가 나열됩니다. 다음과 같은 방법으로 AppComponent를 식별할 수 있습니다.

- AppComponent 이름 – 애플리케이션 구조가 검색되었을 때 이 리소스에 할당된 AWS Resilience Hub 구성 요소의 이름입니다.
 - AppComponent 유형 – AWS Resilience Hub 구성 요소의 유형입니다.
 - 소스 이름 – 입력 소스의 이름입니다. 소스 이름을 선택하여 각 애플리케이션에서 세부 정보를 봅니다. 예를 들어 AWS CloudFormation 스택에서 가져온 소스 이름을 선택하면 AWS CloudFormation의 스택 세부 정보 페이지로 리디렉션됩니다.
 - 리소스 수 – 입력 소스와 연결된 리소스의 수입니다. 숫자를 선택하면 리소스 탭에서 입력 소스의 모든 관련 리소스를 볼 수 있습니다.
2. AppComponent를 생성하려면 작업 메뉴에서 새 AppComponent 생성을 선택하고 다음 단계를 완료합니다.
 - a. AppComponent 이름 상자에 AppComponent의 이름을 입력합니다. 참고로 이 필드에 샘플 이름을 미리 입력했습니다.
 - b. AppComponent 유형 드롭다운 목록에서 AppComponent의 유형을 선택합니다.
 - c. 저장(Save)을 선택합니다.
 3. AppComponent를 편집하려면 AppComponent를 선택한 다음 작업에서 AppComponent 편집을 선택합니다.
 4. AppComponent를 삭제하려면 AppComponent를 선택한 다음 작업에서 AppComponent 삭제를 선택합니다.

리소스 목록을 변경한 후에는 애플리케이션의 초안 버전이 변경되었다는 알림을 받게 됩니다. 정확한 복원력 평가를 실행하려면 새 버전의 애플리케이션을 게시해야 합니다. 새 버전을 게시하는 방법에 대한 자세한 내용은 [새 AWS Resilience Hub 애플리케이션 버전 게시](#) 단원을 참조하세요.

애플리케이션 구성 요소 관리

Application Component(AppComponent)는 단일 단위로 작동하고 실패하는 관련 AWS 리소스 그룹입니다. 예를 들어 기본 및 복제본 데이터베이스가 있는 경우 두 데이터베이스 모두 동일한 AppComponent. AWS Resilience Hub has 규칙에 속합니다.이 규칙은 어떤 AWS 리소스가 어떤 AppComponent 유형에 속할 수 있는지를 제어합니다. 예를 들어는 속할 DBInstance 수 AWS::ResilienceHub::DatabaseAppComponent 있고 예는 속하지 않을 수 있습니다 AWS::ResilienceHub::ComputeAppComponent.

AWS Resilience Hub AppComponents는 다음 리소스를 지원합니다.

- AWS::ResilienceHub::ComputeAppComponent
 - AWS::ApiGateway::RestApi
 - AWS::ApiGatewayV2::Api
 - AWS::AutoScaling::AutoScalingGroup
 - AWS::EC2::Instance
 - AWS::ECS::Service
 - AWS::EKS::Deployment
 - AWS::EKS::ReplicaSet
 - AWS::EKS::Pod
 - AWS::Lambda::Function
 - AWS::StepFunctions::StateMachine
- AWS::ResilienceHub::DatabaseAppComponent
 - AWS::DocDB::DBCluster
 - AWS::DynamoDB::Table
 - AWS::ElastiCache::CacheCluster
 - AWS::ElastiCache::GlobalReplicationGroup
 - AWS::ElastiCache::ReplicationGroup
 - AWS::ElastiCache::ServerlessCache
 - AWS::RDS::DBCluster
 - AWS::RDS::DBInstance
- AWS::ResilienceHub::NetworkingAppComponent
 - AWS::EC2::NatGateway

- `AWS::ElasticLoadBalancing::LoadBalancer`
- `AWS::ElasticLoadBalancingV2::LoadBalancer`
- `AWS::Route53::RecordSet`
- `AWS::ResilienceHub::NotificationAppComponent`
 - `AWS::SNS::Topic`
- `AWS::ResilienceHub::QueueAppComponent`
 - `AWS::SQS::Queue`
- `AWS::ResilienceHub::StorageAppComponent`
 - `AWS::Backup::BackupPlan`
 - `AWS::EC2::Volume`
 - `AWS::EFS::FileSystem`
 - `AWS::FSx::FileSystem`

Note

현재는 Amazon FSx for Windows File Server만 AWS Resilience Hub 지원합니다.

- `AWS::S3::Bucket`

주제

- [애플리케이션 구성 요소에서 리소스 그룹화](#)

애플리케이션 구성 요소에서 리소스 그룹화

애플리케이션을 리소스와 AWS Resilience Hub 함께 로 가져올 때 AWS Resilience Hub 는 애플리케이션을 가져올 때 관련 리소스를 동일한 AppComponent로 그룹화하기 위해 최선의 노력을 기울이지만 그룹화가 항상 100% 정확하지는 않을 수 있습니다. 일부 리소스는 수동 그룹화를 위해 차단되며, 이러한 서비스에는 특정 그룹화 구성이 필요한 엄격한 종속성이 있기 때문에 해당하는 경우 자동으로 그룹화됩니다. 수동 그룹화를 위해 차단된 서비스의 전체 목록은 섹션을 참조하세요 [the section called “수동 그룹화를 위해 차단된 서비스”](#).

AWS Resilience Hub 는 애플리케이션과 리소스를 성공적으로 가져온 후 다음 작업을 수행합니다.

- 리소스를 스캔하여 새 AppComponent로 다시 그룹화하여 평가 정확도를 개선할 수 있는지 확인합니다.

- 가 새 AppComponents로 다시 그룹화할 수 있는 리소스를 AWS Resilience Hub 식별하면 권장 사항과 동일하게 표시되며 이를 수락하거나 거부할 수 있습니다. 에서 그룹화 권장 사항에 할당된 AWS Resilience Hub 신뢰 수준은 속성 및 메타데이터를 기반으로 리소스를 그룹화해야 하는 확실성 정도를 나타냅니다. 신뢰도 높음은 AWS Resilience Hub 가 해당 그룹의 리소스가 관련이 있으므로 함께 그룹화해야 한다는 신뢰 수준이 90% 이상임을 나타냅니다. 중간 신뢰 수준은 AWS Resilience Hub 가 해당 그룹의 리소스가 관련이 있으므로 함께 그룹화해야 한다는 신뢰 수준이 70%~90%임을 나타냅니다.

Note

AWS Resilience Hub 는 예상 워크로드 RTO 및 예상 워크로드 RPO를 계산하여 권장 사항을 생성할 수 있도록 올바른 그룹화를 요구합니다.

올바른 그룹화의 예는 다음과 같습니다.

- 기본 데이터베이스와 복제본을 단일 AppComponent로 그룹화합니다.
- 동일한 애플리케이션을 실행하는 Amazon EC2 인스턴스를 단일 AppComponent로 그룹화합니다.
- 한 지역의 Amazon ECS 서비스와 다른 지역의 장애 조치 Amazon ECS 서비스를 단일 AppComponent로 그룹화합니다.

리소스 그룹화 권장 사항을 검토하고 포함하는 방법에 대한 자세한 내용은 다음 주제를 AWS Resilience Hub 참조하세요.

- [AWS Resilience Hub 리소스 그룹화 권장 사항](#)
- [수동으로 리소스를 AppComponent로 그룹화](#)

수동 그룹화를 위해 차단된 서비스

AWS Resilience Hub 는 애플리케이션의 복원력 평가 및 권장 사항에 영향을 미칠 수 있는 구성 오류를 방지하기 위해 특정 AWS 서비스의 리소스를 수동으로 그룹화하지 못하도록 차단합니다. 이러한 서비스는 종속성 및 구성에 따라 자동으로 그룹화됩니다. 이러한 리소스를 포함하는 애플리케이션을 정의할 때 관계 AWS Resilience Hub, 종속성 및 복원력 요구 사항을 분석하여 정확한 평가 결과를 보장하는 최적의 그룹화를 생성합니다.

수동 그룹화를 위해 차단된 AWS 서비스 목록:

- Amazon API Gateway
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon Elastic Block Store
- Amazon Elastic File System
- Amazon Relational Database Service
- Amazon S3
- Amazon Simple Queue Service
- FSx for Windows File Server
- NAT 게이트웨이

AWS Resilience Hub 리소스 그룹화 권장 사항

이 섹션에서는에서 리소스 그룹화 권장 사항을 생성하고 검토하는 방법을 설명합니다 AWS Resilience Hub.

Note

AWSResilienceHubAssessmentExecutionPolicy AWS 관리형 정책을 AWS Resilience Hub 사용하여 작업에 필요한 IAM 권한을 부여할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 섹션을 참조하세요 [AWSResilienceHubAssessmentExecutionPolicy](#).

리소스 그룹화 권장 사항을 보려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 추가 페이지를 선택하고 리소스 그룹화 권장 사항을 검토할 애플리케이션 이름을 선택합니다.
3. 애플리케이션 구조 탭을 선택합니다.
4. 가 정보 알림을 AWS Resilience Hub 표시하는 경우 권장 사항 검토를 선택하여 모든 리소스 그룹화 권장 사항을 확인합니다. 그렇지 않으면 다음 단계를 완료하여 리소스 그룹화 권장 사항을 수동으로 생성합니다.
 - a. 리소스를 선택합니다.
 - b. 작업 메뉴에서 그룹화 권장 사항 가져오기를 선택합니다.

AWS Resilience Hub 는 리소스를 스캔하여 평가의 정확도를 높이기 위해 관련 AppComponents로 가능한 최상의 방식으로 그룹화할 수 있는 방법을 확인합니다. 에서 리소스를 그룹화할 수 있음을 AWS Resilience Hub 알게 되면 해당 리소스에 대한 정보 알림이 표시됩니다.

- c. 정보 알림이 표시되면 권장 사항 검토를 선택하여 모든 리소스 그룹화 권장 사항을 확인합니다.

다음을 사용하여 리소스 그룹화 권장 사항 검토 섹션에서 AppComponents를 식별할 수 있습니다.

- AppComponent 이름 - 리소스를 그룹화할 AppComponent의 이름입니다.
- 신뢰 수준 - 그룹화 권장 사항에서 AWS Resilience Hub의 신뢰 수준을 나타냅니다.
- 리소스 수 - AppComponent에서 그룹화할 리소스 수를 나타냅니다.
- AppComponent 유형 - AppComponent의 유형을 나타냅니다.

AppComponents에서 그룹화할 리소스를 보려면

1. [리소스 그룹화 권장 사항을 보려면](#) 절차의 단계를 완료한 다음이 절차로 돌아갑니다.
2. 리소스 그룹화 권장 사항 검토 섹션에서 확인란(AppComponent 이름에 인접)을 선택하여 선택한 AppComponent 내에서 함께 그룹화할 모든 리소스를 확인합니다. 여러 확인란을 선택하면가 선택한 AppComponents 해당 AppComponent 유형으로 그룹화하는 동적으로 생성된 권장 사항 선택 섹션을 AWS Resilience Hub 표시합니다. 선택한 AppComponent 내에서 함께 그룹화할 모든 리소스를 보려면 각 AppComponent 유형 아래의 숫자를 선택합니다.

다음을 사용하여 리소스 섹션의 선택한 AppComponent에서 그룹화할 리소스를 식별할 수 있습니다.

- 논리적 ID - 리소스의 논리적 ID를 나타냅니다. 논리적 ID는 AWS CloudFormation 스택, Terraform 상태 파일, myApplications 애플리케이션 또는의 리소스를 식별하는 데 사용되는 이름입니다 AWS Resource Groups.
- 물리적 ID - Amazon EC2 인스턴스 ID 또는 Amazon S3 버킷 이름과 같이 리소스에 대해 실제로 할당된 식별자입니다.
- 유형 - 리소스 유형을 나타냅니다.
- 리전 - 리소스가 위치한 AWS 리전입니다.

리소스 그룹화 권장 사항을 수락하려면

1. [리소스 그룹화 권장 사항을 보려면](#) 절차의 단계를 완료한 다음이 절차로 돌아갑니다.
2. 리소스 그룹화 권장 사항 검토 섹션에서 AppComponent 이름 옆에 있는 모든 확인란을 선택합니다. 특정 AppComponent를 찾으려면 AppComponent 찾기 상자에 AppComponents 이름을 입력합니다.

Note

기본적으로는 모든 리소스 그룹화 권장 사항을 AWS Resilience Hub 표시합니다. 이전에 거부된 리소스 그룹화 권장 사항으로 테이블을 필터링하려면 AppComponents 찾기 상자 옆의 드롭다운 메뉴에서 이전에 거부됨을 선택합니다.

3. 수락을 선택합니다.
4. 리소스 그룹화 권장 사항 수락 대화 상자에서 수락을 선택합니다.

AWS Resilience Hub 는 리소스 그룹화가 성공하면 정보 알림을 표시합니다. 리소스 그룹화 권장 사항의 하위 집합만 수락한 경우 리소스 그룹화 권장 사항 검토 섹션에는 수락하지 않은 모든 리소스 그룹화 권장 사항이 표시됩니다.

리소스 그룹화 권장 사항을 거부하려면

1. [리소스 그룹화 권장 사항을 보려면](#) 절차의 단계를 완료한 다음이 절차로 돌아갑니다.
2. 리소스 그룹화 권장 사항 검토 섹션에서 AppComponent 이름 옆에 있는 모든 확인란을 선택합니다. 특정 AppComponent를 찾으려면 AppComponent 찾기 상자에 AppComponents 이름을 입력합니다.

Note

기본적으로는 모든 리소스 그룹화 권장 사항을 AWS Resilience Hub 표시합니다. 이전에 거부된 리소스 그룹화 권장 사항으로 테이블을 필터링하려면 AppComponents 찾기 상자 옆에 있는 드롭다운 메뉴에서 이전에 거부됨을 선택합니다.

3. 거부를 선택합니다.
4. 리소스 그룹화 권장 사항을 거부하는 이유 중 하나를 선택한 다음 리소스 그룹화 권장 사항 거부 대화 상자에서 거부를 선택합니다.

AWS Resilience Hub 에 동일한 정보를 확인하는 정보 알림이 표시됩니다. 리소스 그룹화 권장 사항의 하위 집합만 거부한 경우 리소스 그룹화 권장 사항 검토 섹션에는 수락하지 않은 모든 리소스 그룹화 권장 사항이 표시됩니다.

수동으로 리소스를 AppComponent로 그룹화

이 섹션에서는 리소스를 AppComponent로 수동으로 그룹화하고의 리소스에 다른 AppComponent를 할당하는 방법을 설명합니다 AWS Resilience Hub.

리소스를 그룹화하려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 그룹화하려는 리소스가 포함된 애플리케이션 이름을 선택합니다.
3. 애플리케이션 구조 탭을 선택합니다.
4. 버전 탭에서 초안 상태의 애플리케이션 버전을 선택합니다.
5. 리소스 탭을 선택합니다.
6. 논리적 ID에 인접한 확인란을 선택하여 그룹화하려는 모든 리소스를 선택합니다.

Note

수동으로 추가한 리소스는 선택할 수 없습니다.

7. 작업을 선택한 다음 리소스 그룹화를 선택합니다.
8. AppComponent 선택 드롭다운 목록에서 리소스를 그룹화할 AppComponent를 선택합니다.
9. 저장(Save)을 선택합니다.
10. [새 버전 발행]을 선택합니다.
11. 애플리케이션 구조 탭을 선택합니다.
12. 게시된 버전의 애플리케이션을 보려면 다음 단계를 완료하세요.
 - a. 버전 탭에서 현재 릴리스 상태의 애플리케이션 버전을 선택합니다.
 - b. 리소스 탭을 선택합니다.

AppComponent에 리소스를 할당하려면

1. 탐색 창에서 애플리케이션을 선택합니다.

2. 애플리케이션 페이지에서 재그룹화할 리소스가 포함된 애플리케이션 이름을 선택합니다.
3. 애플리케이션 구조 탭을 선택합니다.
4. 버전에서 초안 상태의 애플리케이션 버전을 선택합니다.
5. 리소스 탭을 선택합니다.
6. 논리적 ID 옆에 있는 확인란을 선택하여 리소스를 선택합니다.
7. 작업 메뉴에서 AppComponent 변경을 선택합니다.
8. AppComponent 섹션에서 현재의 AppComponent를 삭제하려면 현재의 AppComponent 이름을 표시하는 레이블의 오른쪽 상단에서 X를 선택합니다.
9. 다른 AppComponent의 리소스를 그룹화하려면 AppComponent 선택 드롭다운 목록에서 다른 AppComponent를 선택합니다.
10. 추가를 선택합니다.
11. AppComponent 탭에서 빈 AppComponent를 모두 삭제합니다.
12. [새 버전 발행]을 선택합니다.
13. 애플리케이션 구조 탭을 선택합니다.
14. 게시된 버전의 애플리케이션을 보려면 다음 단계를 완료하세요.
 - a. 버전 탭에서 현재 릴리스 상태의 애플리케이션 버전을 선택합니다.
 - b. 리소스 탭을 선택합니다.

새 AWS Resilience Hub 애플리케이션 버전 게시

에 설명된 대로 AWS Resilience Hub 애플리케이션 리소스를 변경한 후에는 애플리케이션의 새 버전을 게시하여 정확한 복원력 평가를 실행 [AWS Resilience Hub 애플리케이션 리소스 편집](#)해야 합니다. 또한 새 권장 경보, SOP 및 테스트를 애플리케이션에 추가한 경우 새 버전의 애플리케이션을 게시해야 할 수도 있습니다.

애플리케이션의 새 버전을 게시하려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 이름을 선택해서 애플리케이션 페이지를 엽니다.
3. 애플리케이션 구조 탭을 선택합니다.
4. 새 버전 게시를 선택합니다.
5. 버전 게시 대화 상자의 이름 상자에 애플리케이션 버전의 이름을 입력하거나에서 제안한 기본 이름을 사용할 수 있습니다 AWS Resilience Hub.

6. 게시를 선택합니다.

애플리케이션의 새 버전을 게시하면 이 버전이 복원력 평가를 실행할 때 평가되는 버전이 됩니다. 또한 변경하지 않는 한 초안 버전은 출시된 버전과 동일합니다.

새 버전의 애플리케이션을 게시한 후에는 새 복원력 평가 보고서를 실행하여 애플리케이션이 여전히 복원력 정책을 준수하는지 확인하는 것이 좋습니다. 평가 실행에 대한 자세한 내용은 [에서 복원력 평가 실행 및 관리 AWS Resilience Hub](#) 단원을 참조하세요.

모든 AWS Resilience Hub 애플리케이션 버전 보기

애플리케이션 변경 사항을 추적하는 데 도움이 되도록 애플리케이션이 생성된 시점부터 애플리케이션의 이전 버전을 AWS Resilience Hub 표시합니다 AWS Resilience Hub.

애플리케이션의 모든 버전을 보려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 이름을 선택해서 애플리케이션 페이지를 엽니다.
3. 애플리케이션 구조 탭을 선택합니다.
4. 애플리케이션의 모든 이전 버전을 보려면 모든 버전 보기 전에 더하기 기호(+)를 선택합니다.는 각각 초안 및 현재 릴리스 상태를 사용하여 애플리케이션의 초안 버전과 최근 릴리스 버전을 AWS Resilience Hub 나타냅니다. 애플리케이션의 모든 버전을 선택하여 리소스, AppComponent, 입력 소스 및 기타 관련 정보를 볼 수 있습니다.

또한 다음 옵션 중 하나를 사용하여 목록을 필터링할 수도 있습니다.

- 버전 이름별 필터링 - 이름을 입력하여 애플리케이션 버전의 이름을 기준으로 결과를 필터링합니다.
- 날짜 및 시간 범위별 필터링 - 이 필터를 적용하려면 달력 아이콘을 선택하고 다음 옵션 중 하나를 선택하여 시간 범위와 일치하는 결과를 기준으로 필터링합니다.
 - 상대 범위 - 사용 가능한 옵션 중 하나를 선택하고 적용을 선택합니다.

사용자 지정 범위 옵션을 선택하는 경우 기간 입력 상자에 기간을 입력하고 시간 단위 드롭다운 목록에서 적절한 시간 단위를 선택한 다음 적용을 선택합니다.

- 상대 범위 - 날짜 및 시간 범위를 지정하려면 시작 시간과 종료 시간을 제공한 다음 적용을 선택합니다.

AWS Resilience Hub 애플리케이션의 리소스 보기

애플리케이션의 리소스를 보려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 보안 권한을 업데이트하려는 애플리케이션을 선택합니다.
3. 작업에서 리소스 보기를 선택합니다.

리소스 탭에서는 다음과 같이 리소스 테이블의 리소스를 식별할 수 있습니다.

- 논리적 ID - 논리적 ID는 AWS CloudFormation 스택, Terraform 상태 파일, myApplications 애플리케이션 또는의 리소스를 식별하는 데 사용되는 이름입니다 AWS Resource Groups.

Note

- Terraform을 사용하면 다양한 리소스 유형에 동일한 이름을 사용할 수 있습니다. 따라서 동일한 이름을 공유하는 리소스의 경우 논리적 ID 끝에 “- 리소스 유형”이 표시됩니다.
- 모든 애플리케이션 리소스의 인스턴스를 보려면 논리적 ID 앞에 있는 더하기(+) 기호를 선택합니다. 애플리케이션 리소스의 모든 인스턴스를 보려면 각 리소스의 논리적 ID 앞에 있는 더하기(+) 기호를 선택합니다.

지원되는 리소스에 대한 자세한 내용은 [the section called “지원되는 AWS Resilience Hub 리소스”](#) 단원을 참조하세요.

- 상태 - 리소스의 복원력을 AWS Resilience Hub 가 평가할지 여부를 나타냅니다.
- 리소스 유형 - 리소스 유형은 애플리케이션의 구성 요소 리소스를 식별합니다. 예를 들면 AWS::EC2::Instance는 Amazon EC2 인스턴스를 선언합니다. AppComponent 리소스 그룹화에 대한 자세한 내용은 [애플리케이션 구성 요소에서 리소스 그룹화](#) 단원을 참조하세요.
- 소스 이름 - 입력 소스의 이름입니다. 소스 이름을 선택하여 각 애플리케이션에서 세부 정보를 봅니다. 수동으로 추가한 입력 소스의 경우 링크를 사용할 수 없습니다. 예를 들어 AWS CloudFormation 스택에서 가져온 소스 이름을 선택하면의 스택 세부 정보 페이지로 리디렉션됩니다 AWS CloudFormation.
- 소스 유형 - 입력 소스의 유형입니다.
- AppComponent 유형 - 입력 소스의 유형입니다. 입력 소스에는 AWS CloudFormation 스택, myApplications 애플리케이션 AWS Resource Groups, Terraform 상태 파일 및 수동으로 추가된 리소스가 포함됩니다.

 Note

Amazon EKS 클러스터를 편집하려면 AWS Resilience Hub 애플리케이션 절차의 입력 소스 편집의 단계를 완료합니다.

- 물리적 ID – Amazon EC2 인스턴스 ID 또는 S3 버킷 이름 같은 해당 리소스에 대해 실제 할당된 식별자입니다.
 - 포함 – AWS Resilience Hub 이 해당 리소스를 애플리케이션에 포함하는지 여부를 나타냅니다.
 - AppComponents - 애플리케이션 구조가 검색될 때 이 리소스에 할당된 AWS Resilience Hub 구성 요소입니다.
 - 이름 – 애플리케이션 리소스의 이름입니다
 - 계정 - 물리적 리소스를 소유한 AWS 계정입니다.
4. 저장 및 업데이트를 선택합니다.

AWS Resilience Hub 애플리케이션 삭제

애플리케이션 최대 한도인 50개에 도달한 후에는 하나 이상의 애플리케이션을 삭제해야 더 추가할 수 있습니다.

애플리케이션을 삭제하려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 삭제할 애플리케이션을 선택합니다.
3. 작업을 선택한 후 애플리케이션 삭제를 선택합니다.
4. 삭제 상자에 삭제를 입력한 다음 삭제를 선택합니다.

애플리케이션 구성 파라미터

AWS Resilience Hub 는 애플리케이션과 연결된 리소스에 대한 추가 정보를 수집하는 입력 메커니즘을 제공합니다. 이 정보를 통해 AWS Resilience Hub 는 리소스를 더 깊이 이해하고 더 나은 복원력 권장 사항을 제공할 수 있습니다.

애플리케이션 구성 파라미터 섹션에는 AWS Elastic Disaster Recovery에 대한 지역 간 장애 조치 지원의 모든 구성 파라미터가 나열되어 있습니다. 다음을 통해 구성 파라미터를 식별할 수 있습니다.

- 주제 — 구성된 애플리케이션 영역을 나타냅니다. 장애 조치 구성을 예로 들 수 있습니다.
- 목적 -가 정보를 AWS Resilience Hub 요청한 이유를 나타냅니다.
- 파라미터 - 애플리케이션에 대한 권장 사항을 제공하는 데 AWS Resilience Hub 사용할 애플리케이션 영역과 관련된 세부 정보를 나타냅니다. 현재이 파라미터는 장애 조치 리전 하나와 연결된 계정 하나의 키 값만 사용합니다.

애플리케이션 구성 파라미터 업데이트

이 섹션에서는의 구성 파라미터를 업데이트 AWS Elastic Disaster Recovery 하고 복원력 평가를 위해 업데이트된 파라미터를 포함하도록 애플리케이션을 게시할 수 있습니다.

애플리케이션 구성 파라미터를 업데이트하려면

1. 탐색 창에서 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 편집하려는 애플리케이션 이름을 선택합니다.
3. 애플리케이션 구성 파라미터 탭을 선택합니다.
4. 업데이트를 선택합니다.
5. 계정 ID 상자에 장애 조치 계정 ID를 입력합니다.
6. 지역 드롭다운 목록에서 장애 조치 지역을 선택합니다.

Note

이 기능을 비활성화하려면 드롭다운 목록에서 “—”를 선택합니다.

7. 업데이트 및 게시를 선택합니다.

복원력 정책 관리

이 섹션에서는 애플리케이션에 대한 복원력 정책을 생성하는 방법을 설명합니다. 복원력 정책을 올바르게 설정하면 애플리케이션의 복원력 상태를 이해할 수 있습니다. 복원력 정책에는 애플리케이션이 소프트웨어, 하드웨어, 가용 영역 또는 AWS 리전과 같은 중단 유형에서 복구될 것으로 예상되는지 여부를 평가하는 데 사용하는 정보와 목표가 포함되어 있습니다. 이러한 정책은 실제 애플리케이션을 변경하거나 영향을 주지 않습니다. 여러 애플리케이션이 동일한 복원력 정책을 가질 수 있습니다.

복원력 정책을 생성할 때 Recovery Time Objective(RTO) 및 Recovery Point Objective(RPO)를 정의합니다. 목표에 따라 애플리케이션이 복원력 정책을 충족하는지 여부가 결정됩니다. 정책을 애플리케이션

선에 연결하고 복원력 평가를 실행하세요. 포트폴리오의 다양한 애플리케이션 유형에 대해 서로 다른 정책을 생성할 수 있습니다. 예를 들어 실시간 거래 애플리케이션은 월별 보고 애플리케이션과는 다른 복원력 정책을 적용할 수 있습니다.

Note

AWS Resilience Hub 를 사용하면 복원력 정책의 RTO 및 RPO 필드에 값 0을 입력할 수 있습니다. 하지만 애플리케이션을 평가하는 동안 가능한 가장 낮은 평가 결과는 거의 0에 가깝습니다. 따라서 RTO 및 RPO 필드에 값을 0으로 입력하면 예상 워크로드 RTO와 예상 워크로드 RPO 결과가 0에 가까워지고 애플리케이션의 규정 준수 상태가 정책 위반으로 설정됩니다.

이 평가는 첨부된 복원력 정책을 기준으로 애플리케이션 구성을 평가합니다. 프로세스가 끝나면는 복원력 정책의 복구 대상을 기준으로 애플리케이션이 어떻게 측정되는지에 대한 평가를 AWS Resilience Hub 제공합니다.

애플리케이션(Applications)과 복원력 정책(Resiliency policies)에서 복원력 정책을 생성할 수 있습니다. 정책에 대한 관련 세부 정보에 액세스할 수 있으며 정책을 수정 및 삭제할 수도 있습니다.

AWS Resilience Hub 는 RTO 및 RPO 대상을 사용하여 다음과 같은 잠재적 유형의 중단에 대한 복원력을 측정합니다.

- 애플리케이션(Application) — 필수 소프트웨어 서비스 또는 프로세스의 손실.
- 클라우드 인프라(Cloud infrastructure) — EC2 인스턴스와 같은 하드웨어 손실.
- 클라우드 인프라 가용 영역(AZ)(Cloud infrastructure Availability Zone (AZ)) — 하나 이상의 가용 영역을 사용할 수 없습니다.
- 클라우드 인프라 지역(Cloud infrastructure Region) — 하나 이상의 지역을 사용할 수 없습니다.

AWS Resilience Hub 를 사용하면 사용자 지정 복원력 정책을 생성하거나 권장되는 개방형 표준 복원력 정책을 사용할 수 있습니다. 사용자 지정 정책을 생성할 때는 정책의 이름을 지정하고 설명하고 정책을 정의하는 적절한 수준 또는 계층을 선택하세요. 이러한 계층에는 기본 IT 코어 서비스(Foundational IT core services), 미션 크리티컬(Mission critical), 심각(Critical), 중요(Important), 중요하지 않음(Non-critical)이 포함됩니다.

애플리케이션 등급에 적합한 계층을 선택합니다. 예를 들어 실시간 거래 시스템을 심각한 것으로 분류하고 월간 보고 애플리케이션을 중요하지 않은 것으로 분류할 수 있습니다. 표준 정책을 사용할 경우 중단 유형별로 RTO 및 RPO 목표에 대해 사전 구성된 계층과 값이 포함된 복원력 정책을 선택할 수 있습니다. 필요할 경우 계층과 RTO 및 RPO 목표를 변경할 수 있습니다.

복원력 정책(Resiliency policies)에서 또는 새 애플리케이션을 설명할 때 복원력 정책을 생성할 수 있습니다.

복원력 정책 생성

에서 복원력 정책을 생성할 AWS Resilience Hub 수 있습니다. 복원력 정책에는 애플리케이션이 소프트웨어, 하드웨어, 가용 영역 또는 AWS 리전과 같은 중단 유형에서 복구할 수 있는지 여부를 평가하는데 사용하는 정보와 목표가 포함되어 있습니다. 이러한 정책은 실제 애플리케이션을 변경하거나 영향을 주지 않습니다. 여러 애플리케이션이 동일한 복원력 정책을 가질 수 있습니다.

복원력 정책을 생성할 때 Recovery Time Objective(RTO) 및 Recovery Point Objective(RPO) 목표를 정의합니다. 평가를 실행할 때는 애플리케이션이 복원력 정책에 정의된 목표를 충족하는 것으로 추정되는지 여부를 AWS Resilience Hub 결정합니다.

이 평가는 첨부된 복원력 정책을 기준으로 애플리케이션 구성을 평가합니다. 프로세스가 끝나면는 복원력 정책의 목표에 따라 애플리케이션이 어떻게 측정되는지에 대한 평가를 AWS Resilience Hub 제공합니다.

Note

AWS Resilience Hub 를 사용하면 복원력 정책의 RTO 및 RPO 필드에 값 0을 입력할 수 있습니다. 하지만 애플리케이션을 평가하는 동안 가능한 가장 낮은 평가 결과는 거의 0에 가깝습니다. 따라서 RTO 및 RPO 필드에 값을 0으로 입력하면 예상 워크로드 RTO와 예상 워크로드 RPO 결과가 0에 가까워지고 애플리케이션의 규정 준수 상태가 정책 위반으로 설정됩니다.

애플리케이션(Applications)과 복원력 정책(Resiliency policies)에서 복원력 정책을 생성할 수 있습니다. 정책에 대한 관련 세부 정보에 액세스할 수 있으며 정책을 수정 및 삭제할 수도 있습니다.

애플리케이션(Applications)에서 복원력 정책을 만들려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. [the section called “애플리케이션을 추가하여 시작하기”](#)부터 [the section called “애플리케이션에 태그 추가”](#)까지 절차를 완료하세요.
3. 복원력 정책 섹션에서 복원력 정책 생성을 선택합니다.

복원력 정책 생성 페이지가 표시됩니다.

4. 생성 방법 선택 섹션에서 정책 생성을 선택합니다.

5. 정책의 이름을 입력합니다.
6. (선택 사항) 정책 설명을 입력합니다.
7. 계층 드롭다운 목록에서 다음 중 하나를 선택합니다.
 - 기본 IT 코어 서비스
 - 미션 크리티컬
 - 심각
 - 중요
 - 중요하지 않음
8. RTO 및 RPO 목표 모두에 대해 고객 애플리케이션 RTO 및 RPO에서 상자에 숫자 값을 입력한 다음 값이 나타내는 시간 단위를 선택합니다.

인프라 및 가용 영역에 대한 인프라 RTO 및 RPO에서 이러한 항목을 반복합니다.
9. (선택 사항) 다중 지역 애플리케이션을 사용하는 경우 지역의 RTO 및 RPO 목표를 정의하는 것이 좋습니다.

지역을 커세요. 지역 RTO 및 RPO 목표 모두에 대해 고객 애플리케이션 RTO 및 RPO에서 상자에 숫자 값을 입력한 다음 값이 나타내는 시간 단위를 선택합니다.
10. (선택 사항) 태그를 추가하려는 경우 나중에 정책을 생성하면서 추가할 수 있습니다. 태그에 대한 자세한 내용은 AWS 일반 참조 안내서의 [리소스 태깅\(Tagging resources\)](#)을 참조하세요.
11. 생성을 선택하여 정책을 생성합니다.

복원력 정책(Resiliency policies)에 복원력 정책을 만들려면

1. 왼쪽 탐색 메뉴에서 정책(Policies)을 선택합니다.
2. 복원력 정책(Resiliency policies) 섹션에서 복원력 정책 생성(Create resiliency policy)을 선택합니다.

복원력 정책 생성 페이지가 표시됩니다.

3. 정책의 이름을 입력합니다.
4. (선택 사항) 정책 설명을 입력합니다.
5. 계층에서 다음 옵션 중 하나를 선택합니다.
 - 기본 IT 코어 서비스
 - 미션 크리티컬

- 심각
 - 중요
 - 중요하지 않음
6. RTO 및 RPO 목표 모두에 대해 고객 애플리케이션 RTO 및 RPO에서 상자에 숫자 값을 입력한 다음 값이 나타내는 시간 단위를 선택합니다.

인프라 및 가용 영역에 대한 인프라 RTO 및 RPO에서 이러한 항목을 반복합니다.

7. (선택 사항) 다중 지역 애플리케이션을 사용하는 경우 지역의 RTO 및 RPO 목표를 정의하는 것이 좋습니다.

지역을 커세요. RTO 및 RPO 목표 모두에 대해 고객 애플리케이션 RTO 및 RPO에서 상자에 숫자 값을 입력한 다음 값이 나타내는 시간 단위를 선택합니다.

8. (선택 사항) 태그를 추가하려는 경우 나중에 정책을 생성하면서 추가할 수 있습니다. 태그에 대한 자세한 내용은 AWS 일반 참조 안내서의 [리소스 태깅\(Tagging resources\)](#)을 참조하세요.
9. 생성을 선택하여 정책을 생성합니다.

제안된 정책을 기반으로 복원력 정책을 만들려면

1. 왼쪽 탐색 메뉴에서 정책(Policies)을 선택합니다.
2. 생성 방법 선택 섹션에서 제안된 정책을 기반으로 정책 선택을 선택합니다.
3. 복원력 정책(Resiliency policies) 섹션에서 복원력 정책 생성(Create resiliency policy)을 선택합니다.

복원력 정책 생성 페이지가 표시됩니다.

4. 복원력 정책의 이름을 입력합니다.
5. (선택 사항) 정책 설명을 입력합니다.
6. 권장 복원력 정책 섹션에서 다음과 같은 사전 결정된 복원력 정책 계층 중 하나를 보고 선택합니다.

- 중요하지 않은 애플리케이션
- 중요 애플리케이션
- 크리티컬 애플리케이션
- 글로벌 크리티컬 애플리케이션
- 미션 크리티컬 애플리케이션

- 글로벌 미션 크리티컬 애플리케이션(Global Mission Critical Application)
- 기본 코어 서비스(Foundational Core Service)

7. 복원력 정책을 생성하려면 정책 생성을 선택합니다.

복원력 정책의 세부 정보에 액세스

복원력 정책을 열면 정책에 대한 중요한 세부 정보가 표시됩니다. 또한 복원력을 편집하거나 삭제할 수도 있습니다.

복원력 정책 세부 정보(Resiliency policy details)는 요약과 태그라는 두 가지 주요 보기로 구성됩니다.

요약

기본 정보

복원력 정책에 대한 이름, 설명, 계층, 비용 계층, 생성 날짜 등의 정보를 제공합니다.

예상 워크로드 RTO 및 예상 워크로드 RPO

이 복원력 정책과 관련된 예상 워크로드 RTO와 예상 워크로드 RPO 중단 유형을 보여 줍니다.

태그

이 보기를 사용하여 이 응용 프로그램 내부의 태그를 관리, 추가하고 삭제할 수 있습니다.

복원력 정책 세부 정보(Resiliency policy details)에서 복원력 정책을 편집하려면

1. 왼쪽 탐색 메뉴에서 정책(Policies)을 선택합니다.
2. 복원력 정책(Resiliency policy)에서 복원력 정책을 엽니다.
3. 편집을 선택합니다. 기본 정보(Basic Info), RTO 및 RPO 필드에 적절한 변경 내용을 입력합니다. 변경 사항 저장(Save changes)을 선택합니다.

복원력 정책(Resiliency policy)에서 복원력 정책을 편집하려면

1. 왼쪽 탐색 메뉴에서 정책(Policies)을 선택합니다.
2. 복원력 정책에서 복원력 정책을 선택합니다.
3. 작업(Actions)을 선택한 후 편집(Edit)을 선택합니다.
4. 기본 정보(Basic Info), RTO 및 RPO 필드에 적절한 변경 내용을 입력합니다. 변경 사항 저장(Save changes)을 선택합니다.

복원력 정책 세부 정보(Resiliency policy details)에서 복원력 정책을 삭제하려면

1. 왼쪽 탐색 메뉴에서 정책(Policies)을 선택합니다.
2. 복원력 정책(Resiliency policy)에서 복원력 정책을 엽니다.
3. Delete(삭제)를 선택합니다. 삭제를 확인한 다음 삭제>Delete)를 선택합니다.

복원력 정책(Resiliency policy)에서 복원력 정책을 삭제하려면

1. 왼쪽 탐색 메뉴에서 정책(Policies)을 선택합니다.
2. 복원력 정책에서 복원력 정책을 선택합니다.
3. 작업(Actions)을 선택한 후 삭제>Delete)를 선택합니다.
4. 삭제를 확인한 다음 삭제>Delete)를 선택합니다.

에서 복원력 평가 실행 및 관리 AWS Resilience Hub

애플리케이션이 변경되면 복원력 평가를 실행해야 합니다. 평가에서는 각 애플리케이션 구성 요소 구성을 정책과 비교하고 경보, SOP 및 테스트 권장 사항을 제시합니다. 이러한 구성 권장 사항은 복구 절차의 속도를 향상시킬 수 있습니다.

경보 권장 사항은 정전을 감지하는 경보를 설정하는 데 도움이 됩니다. SOP 권장 사항은 백업 복구와 같은 일반적인 복구 프로세스를 관리하는 스크립트를 제공합니다. 테스트 권장 사항은 구성이 제대로 작동하는지 확인하기 위한 제안을 제공합니다. 예를 들어, 네트워크 문제로 인한 자동 규모 조정 또는 로드 밸런싱과 같은 자동 복구 프로세스 중에 애플리케이션이 복구되는지 테스트할 수 있습니다. 리소스가 한도에 도달하면 애플리케이션 경보가 트리거되는지 여부를 테스트할 수 있습니다. 또한 지정한 조건에서 SOP가 얼마나 잘 작동하는지 테스트할 수 있습니다.

주제:

- [에서 복원력 평가 실행 AWS Resilience Hub](#)
- [평가 보고서 검토](#)
- [복원력 평가 삭제](#)

에서 복원력 평가 실행 AWS Resilience Hub

의 여러 위치에서 복원력 평가를 실행할 수 있습니다 AWS Resilience Hub. 애플리케이션에 대한 자세한 내용은 [the section called “애플리케이션 관리”](#) 단원을 참조하세요.

작업 메뉴에서 복원력 평가를 실행하려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션 테이블에서 애플리케이션을 선택합니다.
3. 작업 메뉴에서 복원력 평가를 선택합니다.
4. 복원력 평가 실행 대화 상자에서 고유한 이름을 입력하거나 생성된 이름을 평가에 사용할 수 있습니다.
5. Run(실행)을 선택합니다.

평가 보고서를 검토하려면 애플리케이션에서 평가를 선택합니다. 자세한 내용은 [the section called “평가 보고서 검토”](#) 단원을 참조하십시오.

평가 탭에서 복원력 평가를 실행하려면

애플리케이션 또는 복원력 정책이 변경될 때 새 복원력 평가를 실행할 수 있습니다.

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션 테이블에서 애플리케이션을 선택합니다.
3. 평가 탭을 선택합니다.
4. 복원력 평가 실행을 선택합니다.
5. 복원력 평가 실행 대화 상자에서 고유한 이름을 입력하거나 생성된 이름을 평가에 사용할 수 있습니다.
6. Run(실행)을 선택합니다.

평가 보고서를 검토하려면 애플리케이션에서 평가를 선택합니다. 자세한 내용은 [the section called “평가 보고서 검토”](#) 단원을 참조하십시오.

평가 보고서 검토

애플리케이션의 평가 보기에서 평가 보고서를 찾을 수 있습니다.

평가 보고서를 찾으려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션에서 애플리케이션을 엽니다.
3. 평가 탭의 복원력 평가 섹션에서 평가 보고서를 선택합니다.

보고서를 열면 다음 내용이 표시됩니다.

- 평가 보고서의 전체 개요
- 복원력 개선을 위한 권장 사항.
- 경보, SOP 및 테스트 설정을 위한 권장 사항
- 태그를 생성하고 관리하여 AWS 리소스를 검색하고 필터링하는 방법

평가 보고서

이 섹션에서는 평가 보고서에 대한 개요를 제공합니다.는 각 중단 유형과 관련 애플리케이션 구성 요소를 AWS Resilience Hub 나열합니다. 또한 실제 RTO 및 RPO 정책을 나열하고 애플리케이션 구성 요소가 정책 목표를 달성할 수 있는지 여부를 결정합니다.

개요

애플리케이션 이름, 복원력 정책 이름, 보고서 생성 날짜를 표시합니다.

감지된 리소스 드리프트

이 섹션에는 게시된 애플리케이션의 최신 버전에 포함된 후 추가되거나 제거된 모든 리소스가 나열됩니다. 입력 소스 탭에서 입력 소스 다시 가져오기를 선택하여 모든 입력 소스(드리프트된 리소스 포함)를 다시 가져옵니다. 게시 및 평가를 선택하여 애플리케이션에 업데이트된 리소스를 포함하고 정확한 복원력 평가를 받습니다.

다음을 사용하여 드리프트된 입력 소스를 식별할 수 있습니다.

- 논리적 ID - 리소스의 논리적 ID를 나타냅니다. 논리적 ID는 AWS CloudFormation 스택, Terraform 상태 파일, myApplications 애플리케이션 또는의 리소스를 식별하는 데 사용되는 이름입니다 AWS Resource Groups.
- 변경 - 입력 리소스가 추가 또는 제거되었는지 나타냅니다.
- 소스 이름 - 리소스 이름을 나타냅니다. 소스 이름을 선택하여 각 애플리케이션에서 세부 정보를 봅니다. 수동으로 추가한 입력 소스의 경우 링크를 사용할 수 없습니다. 예를 들어 AWS CloudFormation 스택에서 가져온 소스 이름을 선택하면의 스택 세부 정보 페이지로 리디렉션됩니다 AWS CloudFormation.
- 리소스 유형 - 리소스 유형을 나타냅니다.
- 계정 - 물리적 리소스를 소유한 AWS 계정을 나타냅니다.

- 리전 - 리소스가 위치한 리전을 나타냅니다 AWS .

RTO

애플리케이션이 복원력 정책의 목표를 충족할 것으로 추정되는지 여부를 그래프로 보여줍니다. 이는 조직에 심각한 손상을 초래하지 않고 애플리케이션을 중단할 수 있는 시간을 기준으로 책정됩니다. 이 평가에서는 예상 워크로드 RTO를 제공합니다.

RPO

애플리케이션이 복원력 정책의 목표를 충족할 것으로 추정되는지 여부를 그래프로 보여줍니다. 이는 비즈니스에 심각한 피해가 발생하기 전에 데이터가 손실될 수 있는 시간을 기준으로 책정됩니다. 이 평가에서는 예상 워크로드 RPO를 제공합니다.

세부 정보

모든 결과 및 애플리케이션 규정 준수 드리프트 탭을 사용하여 각 중단 유형에 대한 자세한 설명을 제공합니다. 모든 결과 탭에는 규정 준수 드리프트를 포함한 모든 중단이 표시되고 애플리케이션 규정 준수 드리프트 탭에는 규정 준수 드리프트만 표시됩니다. 중단 유형에는 애플리케이션, 클라우드 인프라 (인프라 및 가용 영역), 리전이 포함되며 이에 대한 다음 정보를 제공합니다.

- AppComponent

애플리케이션을 구성하는 리소스. 예를 들어, 애플리케이션에 데이터베이스 또는 컴퓨팅 구성 요소가 있을 수 있습니다.

- 예상 RTO

정책 구성이 정책 요구 사항과 일치하는지 여부를 나타냅니다. 예상 RTO와 목표 RTO라는 두 가지 값을 제공합니다. 예를 들어 목표 RTO에서 2시간, 예상 워크로드 RTO에서 40분의 값이 표시된다면, 애플리케이션의 현재 RTO는 2시간인 반면 예상 워크로드 RTO는 40분이라는 뜻입니다. 예상 워크로드 RTO는 정책이 아닌 구성을 기준으로 계산합니다. 따라서 다중 가용 영역 데이터베이스의 경우 어떤 정책을 선택하든 가용 영역 장애에 대한 예상 워크로드 RTO는 동일합니다.

- RTO 드리프트

애플리케이션이 이전에 성공한 평가의 예상 워크로드 RTO에서 벗어난 기간을 나타냅니다. 예상 RTO와 RTO 드리프트라는 두 가지 값을 제공합니다. 예를 들어 예상 RTO에서 2시간, RTO 드리프트에서 40분의 값이 표시되면 애플리케이션이 이전 성공 평가의 예상 워크로드 RTO에서 40분정도 차이가 난다는 의미입니다.

• 예상 RPO

각 애플리케이션 구성 요소에 대해 설정한 대상 RPO 정책을 기반으로 추정하는 실제 예상 워크로드 RPO 정책을 표시합니다. AWS Resilience Hub 예를 들어, 복원력 정책에서 가용 영역 장애에 대한 RPO 목표를 1시간으로 설정했을 수 있습니다. 예상 결과는 0에 가깝게 계산될 수 있습니다. 이는 모든 거래를 커밋하는 Amazon Aurora가 여러 가용 영역에 걸친 6개 노드 중 4개 노드에서 성공한다고 가정합니다. 특정 시점으로 복원을 수행하는 데 5분이 걸릴 수 있습니다.

제공하지 않도록 선택할 수 있는 유일한 RTO 및 RPO 목표는 리전입니다. 일부 애플리케이션의 경우, 전체 리전에서 사용할 수 없게 될 수 있는 AWS 서비스에 대한 중대한 의존성이 있을 때 복구를 계획하는 것이 유용합니다.

해당 리전의 RTO 또는 RPO 목표 설정과 같은 이 옵션을 선택하면 예상 복구 시간과 해당 실패에 대한 운영 권장 사항을 받게 됩니다.

• RPO 드리프트

애플리케이션이 이전에 성공한 평가의 예상 워크로드 RPO에서 벗어난 기간을 나타냅니다. 예상 RPO 및 RPO 드리프트라는 두 가지 값을 제공합니다. 예를 들어, 예상 RPO 아래에 2시간, RPO 드리프트에서 40분의 값이 표시되면 애플리케이션이 이전의 성공적인 평가의 예상 워크로드 RPO에서 40분정도 차이가 난다는 의미입니다.

복원력 권장 사항 검토

복원력 권장 사항은 애플리케이션 구성 요소를 평가하고 예상 워크로드 RTO와 예상 워크로드 RPO, 비용 및 최소 변경으로 최적화하는 방법을 권장합니다.

를 사용하면 이 옵션을 선택해야 하는 이유에서 다음 권장 옵션 중 하나를 사용하여 복원력을 최적화할 AWS Resilience Hub 수 있습니다.

Note

- AWS Resilience Hub 는 최대 3개의 AWS Resilience Hub 권장 옵션을 제공합니다.
- 리전 RTO 및 RPO 대상을 설정하면 권장 옵션에 리전 RTO/RPO에 최적화가 AWS Resilience Hub 표시됩니다. 리전 RTO 및 RPO 대상이 설정되지 않은 경우 AZ(가용 영역 최적화) RTO/RPO가 표시됩니다. 복원력 정책을 생성하는 동안 리전 RTO/RPO 대상을 설정하는 방법에 대한 자세한 내용은 [섹션을 참조하세요](#) [복원력 정책 생성](#).
- 애플리케이션과 해당 구성의 예상 워크로드 RTO와 예상 워크로드 RPO 값은 데이터 양과 개별 AppComponent를 고려하여 결정됩니다. 그러나 이러한 값은 추정치일 뿐입니다. 자체

테스트(예: AWS Fault Injection Service)를 사용하여 실제 복구 시간이 있는지 애플리케이션을 테스트해야 합니다.

가용 영역 RTO/RPO에 최적화

가용 영역(AZ) 중단 중 가능한 가장 낮은 예상 워크로드 복구 시간(RTO/RPO)입니다. RTO 및 RPO 목표를 충족할 만큼 구성을 충분히 변경할 수 없는 경우, 구성을 정책 충족 가능성에 가깝게 만들기 위해 가장 낮은 예상 워크로드 AZ 복구 시간에 대한 정보를 받게 됩니다.

리전 RTO/RPO에 최적화

리전 중단 중 가능한 가장 낮은 예상 워크로드 복구 시간(RTO/RPO)입니다. RTO 및 RPO 목표를 충족할 만큼 구성을 충분히 변경할 수 없는 경우, 구성을 정책 충족 가능성에 가깝게 만들기 위해 가장 낮은 예상 워크로드 리전 복구 시간에 대한 정보를 받게 됩니다.

비용 최적화

발생할 수 있는 최저 비용이지만 복원력 정책을 여전히 충족할 수 있습니다. 최적화 목표를 충족할 만큼 구성을 충분히 변경할 수 없는 경우, 정책을 충족할 수 있는 가능성에 가깝게 구성을 가져오기 위해 발생할 수 있는 최저 비용에 대한 정보를 받게 됩니다.

변경을 최소화하도록 최적화

정책 목표를 달성하는 데 필요한 최소 변경 사항입니다. 최적화 목표를 충족할 만큼 구성을 충분히 변경할 수 없는 경우 정책 충족 가능성에 근접하게 구성을 가져올 수 있는 권장 변경 사항에 대한 알림을 받습니다.

최적화 범주 분류에는 다음 항목이 포함됩니다.

- 설명

에서 제안하는 구성을 설명합니다 AWS Resilience Hub.

- 변경

제안된 구성으로 전환하는 데 필요한 작업을 설명하는 텍스트 변경 목록.

- 기본 비용

권장 변경 사항과 관련된 예상 비용입니다.

Note

기본 비용은 사용량에 따라 달라질 수 있으며 Enterprise Discount Program(EDP)의 할인 또는 제안은 포함되지 않습니다.

- 예상 워크로드 RTO 및 RPO

변경 후의 예상 워크로드 RTO 및 예상 워크로드 RPO.

AWS Resilience Hub는 애플리케이션 구성 요소(AppComponent)가 복원력 정책을 준수할 수 있는지 평가합니다. AppComponent가 복원력 정책을 준수하지 않고 AWS Resilience Hub가 규정 준수를 촉진하기 위한 권장 사항을 제공할 수 없는 경우 선택한 AppComponent의 복구 시간을 AppComponent의 제약 조건 내에서 충족할 수 없기 때문일 수 있습니다. AppComponent 제약 조건의 예로는 리소스 유형, 스토리지 크기 또는 리소스 구성이 있습니다.

AppComponent의 복원력 정책 준수를 촉진하려면 AppComponent의 리소스 유형을 변경하거나 리소스가 제공할 수 있는 것과 일치하도록 복원력 정책을 업데이트합니다.

운영 권장 사항 검토

운영 권장 사항에는 AWS CloudFormation 템플릿을 통해 경보, SOPs 및 AWS FIS 실험을 설정하는 권장 사항이 포함되어 있습니다.

AWS Resilience Hub는 애플리케이션의 인프라를 코드로 다운로드하고 관리할 수 있는 AWS CloudFormation 템플릿 파일을 제공합니다. 따라서 애플리케이션 코드에 추가할 수 있도록 AWS CloudFormation에서 권장 사항을 제공합니다. AWS CloudFormation 템플릿 파일 크기가 1MB를 초과하고 리소스가 500개를 초과하는 경우는 AWS CloudFormation 템플릿 파일을 2개 이상 AWS Resilience Hub 생성합니다. 여기서 각 파일의 크기는 1MB를 초과하지 않으며 최대 500개의 리소스를 포함합니다. AWS CloudFormation 템플릿 파일이 여러 파일로 분할되면 AWS CloudFormation 템플릿 파일 이름에가 추가됩니다. partXofY여기서는 시퀀스의 파일 번호를 X 나타내고는 템플릿 파일이 분할된 총 파일 수를 Y AWS CloudFormation 나타냅니다. 예를 들어, 템플릿 파일 big-app-template5-Alarm-104849185070-us-west-2.yaml을 네 개의 파일로 나누는 경우 파일 이름은 다음과 같습니다.

- big-app-template5-Alarm-104849185070-us-west-2-part1of4.yaml
- big-app-template5-Alarm-104849185070-us-west-2-part2of4.yaml
- big-app-template5-Alarm-104849185070-us-west-2-part3of4.yaml

- `big-app-template5-Alarm-104849185070-us-west-2-part4of4.yaml`

그러나 대용량 AWS CloudFormation 템플릿의 경우 로컬 파일과 함께 CLI/API를 입력으로 사용하는 대신 Amazon Simple Storage Service URI를 제공해야 합니다.

에서 다음 작업을 수행할 AWS Resilience Hub 수 있습니다.

- 선택한 경보, SOPs 및 AWS FIS 실험을 프로비저닝할 수 있습니다. 경보, SOPs 및 AWS FIS 실험을 프로비저닝하려면 적절한 권장 사항을 선택하고 고유한 이름을 입력합니다. 선택한 권장 사항을 기반으로 템플릿을 AWS Resilience Hub 생성합니다. 템플릿에서 Amazon Simple Storage Service(S3) URL을 통해 생성된 템플릿에 액세스할 수 있습니다.
- 언제든지 애플리케이션에 권장되는 선택한 경보, SOPs 및 AWS FIS 실험을 포함하거나 제외할 수 있습니다. 자세한 내용은 [the section called “운영 권장 사항 포함 또는 제외”](#) 단원을 참조하십시오.
- 또한 애플리케이션의 태그를 검색, 생성, 추가, 제거 및 관리하고 관련 태그를 모두 볼 수 있습니다.

운영 권장 사항 포함 또는 제외

AWS Resilience Hub 는 언제든지 애플리케이션의 복원력 점수를 개선하는 데 권장되는 경보, SOPs 및 AWS FIS 실험(테스트)을 포함하거나 제외할 수 있는 옵션을 제공합니다. 운영 권장 사항을 포함하거나 제외하면 새 평가를 실행한 후에만 애플리케이션의 복원력 점수에 영향을 미칩니다. 따라서 평가를 실행하여 업데이트된 복원력 점수를 얻고 애플리케이션에 미치는 영향을 이해하는 것이 좋습니다.

애플리케이션별 권장 사항을 포함하거나 제외하도록 권한을 제한하는 방법에 대한 자세한 내용은 [the section called “AWS Resilience Hub 권장 사항을 포함하거나 제외할 수 있는 권한 제한”](#) 단원을 참조하세요.

애플리케이션에 운영 권장 사항을 포함하거나 제외하려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션에서 애플리케이션을 엽니다.
3. 평가를 선택하고 복원력 평가 테이블에서 평가를 선택합니다. 평가가 없는 경우 [the section called “에서 복원력 평가 실행 AWS Resilience Hub”](#)의 절차를 완료한 다음 이 단계로 돌아갑니다.
4. 운영 권장 사항 탭을 선택합니다.
5. 운영 권장 사항을 애플리케이션에 포함하거나 제외하려면 다음 절차를 완료합니다.

애플리케이션에서 권장 경보를 포함하거나 제외하려면

1. 경보를 제외하려면 다음 단계를 완료합니다.

- a. 경보 탭의 경보 테이블에서 제외하려는 모든 경보(구현되지 않음 상태 포함)를 선택합니다. 상태 열에서 경보의 현재 구현 상태를 식별할 수 있습니다.
- b. 작업에서 선택한 항목 제외를 선택합니다.
- c. 권장 사항 제외 대화 상자에서 다음 이유 중 하나를 선택하고(선택 사항) 선택한 항목 제외를 선택하여 선택한 경보를 애플리케이션에서 제외합니다.
 - 이미 구현됨 - Amazon CloudWatch 또는 기타 타사 서비스 공급자와 같은 AWS 서비스에 이러한 경보를 이미 구현한 경우 이 옵션을 선택합니다.
 - 관련 없음 - 경보가 비즈니스 요구 사항에 맞지 않는 경우 이 옵션을 선택합니다.
 - 구현이 너무 복잡함 - 이러한 경보가 구현하기에 너무 복잡하다고 생각되면 이 옵션을 선택합니다.
 - 기타 - 권장 사항을 제외할 다른 이유를 지정하려면 이 옵션을 선택합니다.

2. 경보를 포함하려면 다음 단계를 완료합니다.

- a. 경보 탭의 경보 테이블에서 포함하려는 모든 경보(제외 상태 포함)를 선택합니다. 상태 열에서 경보의 현재 구현 상태를 식별할 수 있습니다.
- b. 작업에서 선택한 항목 포함을 선택합니다.
- c. 권장 사항 포함 대화 상자에서 선택한 항목 포함을 선택하여 선택한 모든 경보를 애플리케이션에 포함시킵니다.

애플리케이션에 권장 표준 운영 절차(SOP)를 포함하거나 제외하려면

1. 권장 SOP를 제외하려면 다음 단계를 완료합니다.

- a. 표준 운영 절차 탭의 SOP 테이블에서 제외하려는 모든 SOP(구현됨 또는 구현되지 않음 상태)를 선택합니다. 상태 열에서 SOP의 현재 구현 상태를 식별할 수 있습니다.
- b. 작업에서 선택항목 제외를 선택하여 선택한 SOP를 애플리케이션에서 제외합니다.
- c. 권장 사항 제외 대화 상자에서 다음 이유 중 하나(선택 사항)를 선택하고 선택한 SOP를 애플리케이션에서 제외하려면 선택한 항목 제외를 선택합니다.
 - 이미 구현됨 - AWS 서비스나 다른 타사 서비스 공급자에서 이러한 SOP를 이미 구현한 경우 이 옵션을 선택합니다.

- 관련 없음 – SOP가 비즈니스 요구 사항에 맞지 않는 경우 이 옵션을 선택합니다.
- 구현이 너무 복잡함 – 이러한 SOP를 구현하기에 너무 복잡하다고 생각되면 이 옵션을 선택합니다.
- 없음 – 이유를 지정하지 않으려면 이 옵션을 선택합니다.

2. SOP를 포함하려면 다음 단계를 완료합니다.

- a. 표준 운영 절차 탭의 SOP 테이블에서 포함하려는 모든 경보(제외 상태 포함)를 선택합니다. 상태 열에서 경보의 현재 구현 상태를 식별할 수 있습니다.
- b. 작업에서 선택한 항목 포함을 선택합니다.
- c. 권장 사항 포함 대화 상자에서 선택한 항목 포함을 선택하여 선택한 모든 SOP를 애플리케이션에 포함시킵니다.

애플리케이션에 권장 테스트를 포함하거나 제외하려면

1. 권장 테스트를 제외하려면 다음 단계를 완료합니다.

- a. 오류 주입 실험 템플릿 탭의 오류 주입 실험 템플릿 테이블에서 제외하려는 모든 테스트(구현 됨 또는 구현되지 않음 상태)를 선택합니다. 상태 열에서 테스트의 현재 구현 상태를 식별할 수 있습니다.
- b. 작업에서 선택한 항목 제외를 선택합니다.
- c. 권장 사항 제외 대화 상자에서 다음 이유 중 하나를 선택하고(선택 사항) 선택한 항목 제외를 선택하여 선택한 AWS FIS 실험을 애플리케이션에서 제외합니다.
 - 이미 구현됨 - AWS 서비스 또는 다른 타사 서비스 공급자에서 이러한 테스트를 이미 구현한 경우 이 옵션을 선택합니다.
 - 관련 없음 – 테스트가 비즈니스 요구 사항에 맞지 않는 경우 이 옵션을 선택합니다.
 - 구현하기 너무 복잡함 – 이러한 테스트가 구현하기에 너무 복잡하다고 생각되면 이 옵션을 선택합니다.
 - 없음 – 이유를 지정하지 않으려면 이 옵션을 선택합니다.

2. 권장 테스트를 포함하려면 다음 단계를 완료합니다.

- a. 오류 주입 실험 템플릿 탭의 오류 주입 실험 템플릿 테이블에서 포함하려는 모든 테스트(제외 상태 포함)를 선택합니다. 상태 열에서 테스트의 현재 구현 상태를 식별할 수 있습니다.
- b. 작업에서 선택한 항목 포함을 선택합니다.

- c. 권장 사항 포함 대화 상자에서 선택한 항목 포함을 선택하여 선택한 모든 테스트를 애플리케이션에 포함시킵니다.

복원력 평가 삭제

애플리케이션의 평가 보기에서 복원력 평가를 삭제할 수 있습니다.

복원력 평가를 삭제하려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션에서 애플리케이션을 엽니다.
3. 평가의 복원력 평가 테이블에서 평가 보고서를 선택합니다.
4. 삭제를 확인하려면 삭제를 선택합니다.

보고서가 더 이상 복원력 평가 테이블에 표시되지 않습니다.

복원력 위젯에서 복원력 평가 실행 및 관리

AWS Resilience Hub 를 사용하면 myApplications in Resiliency 위젯에서 생성 및 관리되는 애플리케이션에 대한 평가를 실행할 수 있습니다. 애플리케이션을 수정할 때마다 복원력 위젯 또는 AWS Resilience Hub 콘솔에서 복원력 평가를 실행하는 것이 좋습니다. 이 평가 중에 각 애플리케이션 구성 요소의 구성은 확립된 정책 및 모범 사례에 따라 평가됩니다. 이 평가를 기반으로 평가는 경고 설정, 표준 운영 절차(SOPs 생성 및 테스트 전략 구현을 위한 권장 사항을 생성합니다. 이러한 구성 권장 사항을 구현하면 복구 절차의 속도와 효율성을 높여 인시던트 대응 속도를 높이고 잠재적 가동 중지 시간을 최소화할 수 있습니다.

경보 권장 사항은 정전을 감지하는 경보를 설정하는 데 도움이 됩니다. SOP 권장 사항은 백업 복구와 같은 일반적인 복구 프로세스를 관리하는 스크립트를 제공합니다. 테스트 권장 사항은 구성이 제대로 작동하는지 확인하기 위한 제안을 제공합니다. 예를 들어, 네트워크 문제로 인한 자동 규모 조정 또는 로드 밸런싱과 같은 자동 복구 프로세스 중에 애플리케이션이 복구되는지 테스트할 수 있습니다. 리소스가 한도에 도달하면 애플리케이션 경보가 트리거되는지 여부를 테스트할 수 있습니다. 또한 지정한 조건에서 SOP가 얼마나 잘 작동하는지 테스트할 수 있습니다.

주제:

- [복원력 위젯에서 복원력 평가 실행](#)
- [복원력 위젯에서 평가 요약 검토](#)

복원력 위젯에서 복원력 평가 실행

myApplications 위젯에서 생성된 애플리케이션의 경우 이제 복원력 위젯 및 AWS Resilience Hub 콘솔에서 복원력 평가를 실행할 수 있습니다. 콘솔에서 AWS Resilience Hub 복원력 평가를 실행하는 방법에 대한 자세한 내용은 [섹션을 참조하세요](#) [에서 복원력 평가 실행 AWS Resilience Hub](#).

Resiliency 위젯에서 기존 myApplications 애플리케이션에 대한 복원력 평가를 처음으로 실행하려면

1. [AWS 관리 콘솔](#)에 로그인합니다.
2. 왼쪽 사이드바를 확장하여 myApplications를 선택합니다.
3. 평가를 실행할 애플리케이션을 선택합니다.

사전 조건으로 AWS 콘솔에 복원력 위젯을 추가했는지 확인합니다. 이 위젯을 추가하려면 다음 단계를 완료합니다.

- a. 콘솔 홈 대시보드의 오른쪽 상단 또는 하단에서 + 위젯 추가를 선택합니다.
 - b. 위젯 제목 표시줄의 왼쪽 상단에 있는 세로 점 6개로 표시되는 드래그 표시기를 선택한 다음 콘솔 홈 대시보드로 드래그합니다.
4. 애플리케이션 평가를 선택합니다.
 5. 현재 계정의 리소스에 액세스하는 데 사용할 기존 IAM 역할을 선택하려면 IAM 역할 사용을 선택한 다음 IAM 역할 선택 드롭다운 목록에서 IAM 역할을 선택합니다.

현재 IAM 사용자를 사용하여 애플리케이션 리소스를 검색하려면 현재 IAM 사용자 권한 사용을 선택하고 현재 IAM 사용자를 사용하여 애플리케이션 리소스 검색 섹션의 내에서 필요한 기능을 활성화하기 위해 권한을 수동으로 구성해야 함을 이해합니다 AWS Resilience Hub를 선택합니다.

6. 평가를 선택합니다.

또는 매일 자동 평가를 켜면 AWS Resilience Hub 가 추가 비용 없이 매일 애플리케이션을 평가할 수 있습니다.

AWS Resilience Hub 는 다음 작업을 수행합니다.

- 에서 애플리케이션을 생성하고 연결된 리소스를 AWS Resilience Hub 자동으로 검색하고 매핑합니다.
- 복구 시간 목표(RTO) 및 복구 시점 목표(RPO)에 대해 미리 정의된 값을 사용하여 새 복원력 정책을 생성하고 할당합니다. 즉, RTO의 경우 4시간, RPO의 경우 1시간입니다. 평가를 생성한 후 복원력 정책을 수정하거나 AWS Resilience Hub 콘솔에서 다른 정책을 할당할 수 있습니다. 복원력 정책 업데이트 및 다른 정책 연결에 대한 자세한 내용은 [복원력 정책 관리](#)를 참조하세요.

- RTO 및 RPO를 기준으로 애플리케이션의 복원력을 평가하고 리소스 및 구성 변경을 지속적으로 모니터링하며 결과를 게시합니다.

Note

평가를 시작하기 전에를 사용하여 평가 실행과 관련된 잠재적 비용을 평가하는 것이 좋습니다 AWS Resilience Hub. 자세한 요금 정보는 [AWS Resilience Hub 요금](#)을 참조하세요.

Resiliency 위젯에서 기존 myApplications 애플리케이션에 대한 복원력 평가를 다시 실행하려면

1. [AWS 관리 콘솔](#)에 로그인합니다.
2. 왼쪽 사이드바를 확장하여 myApplications를 선택합니다.
3. 재평가할 애플리케이션을 선택합니다.

사전 조건으로 AWS 콘솔에 복원력 위젯을 추가했는지 확인합니다. 이 위젯을 추가하려면 다음 단계를 완료합니다.

- a. 콘솔 홈 대시보드의 오른쪽 상단 또는 하단에서 + 위젯 추가를 선택합니다.
 - b. 위젯 제목 표시줄의 왼쪽 상단에 있는 세로 점 6개로 표시되는 드래그 표시기를 선택한 다음 콘솔 홈 대시보드로 드래그합니다.
4. 복원력 위젯에서 재평가를 선택합니다.

또는 매일 자동 평가를 켜면 AWS Resilience Hub 가 추가 비용 없이 매일 애플리케이션을 평가할 수 있습니다.

복원력 위젯에서 평가 요약 검토

복원력 위젯에는 myApplications 애플리케이션의 복원력, 잠재적 취약성, 주요 성능 지표(KPIs) 및 개선을 위한 권장 조치에 대한 가장 중요하고 실행 가능한 인사이트를 제공하는 평가 결과의 스냅샷이 표시됩니다. 다음을 사용하여 가장 최근 평가에서 애플리케이션의 복원력 태세에 대해 자세히 알아볼 수 있습니다.

- 복원력 점수 기록 -이 차트는 최대 1년 동안의 애플리케이션 복원력 점수 추세를 표시합니다.
- 복원력 점수 - 최신 평가에서 평가된 애플리케이션의 복원력 점수를 나타냅니다. 이 점수는 애플리케이션이 애플리케이션의 복원력 정책을 충족하고 경보, 표준 운영 절차(SOPs) 및 AWS Fault

Injection Service (AWS FIS) 실험을 구현하기 위한 권장 사항을 얼마나 잘 따르는지 반영합니다. 번호를 선택하면 AWS Resilience Hub 콘솔의 요약 탭에 있는 복원력 점수 섹션에서 추가 정보를 볼 수 있습니다. 자세한 내용은 [평가 보고서](#) 단원을 참조하십시오.

- 정책 위반 - AWS Resilience Hub 콘솔의 평가 보고서 창에서 애플리케이션에 연결된 정책을 위반하는 모든 애플리케이션 구성 요소(AppComponents)를 보려면 아래 번호를 선택합니다. 자세한 내용은 [평가 보고서](#) 단원을 참조하십시오.
- 정책 드리프트 - 이전 평가에서 정책을 준수했지만 현재 평가를 준수하지 못한 AppComponent를 나타냅니다. AWS Resilience Hub 콘솔의 평가 보고서 창에서 AppComponent를 보려면 아래 번호를 선택합니다. 자세한 내용은 [평가 보고서](#) 단원을 참조하십시오.
- 리소스 드리프트 - AWS Resilience Hub 콘솔의 평가 보고서 창에서 최신 평가에서 드리프트한 모든 리소스를 보려면 아래 번호를 선택합니다. 자세한 내용은 [평가 보고서](#) 단원을 참조하십시오.
- Resilience Hub로 이동 - AWS Resilience Hub 콘솔에서 애플리케이션을 열려면이 옵션을 선택합니다.

경보 관리

복원력 평가를 실행할 때 운영 권장 사항 AWS Resilience Hub 의 일부로는 애플리케이션 복원력을 모니터링하기 위해 Amazon CloudWatch 경보를 설정할 것을 권장합니다. 현재 애플리케이션 구성의 리소스 및 구성 요소를 기반으로 이러한 경보를 사용하는 것이 좋습니다. 애플리케이션의 리소스와 구성 요소가 변경되는 경우 복원력 평가를 실행하여 업데이트된 애플리케이션에 대해 올바른 Amazon CloudWatch 경보가 있는지 확인해야 합니다.

또한 AWS Resilience Hub 이제는 이미 구성된 Amazon CloudWatch 경보를 자동으로 감지하여 복원력 평가에 통합하여 애플리케이션의 복원력 상태를 보다 포괄적으로 파악할 수 있습니다. 이 새로운 기능은 AWS Resilience Hub 권장 사항을 현재 모니터링 설정과 결합하여 경보 관리를 간소화하고 평가 정확도를 개선합니다. Amazon CloudWatch 경보를 구현했지만 경보를 자동으로 감지하지 AWS Resilience Hub 못하는 경우 경보를 제외하고 이유를 이미 구현됨으로 선택할 수 있습니다. 권장 사항 제외에 대한 자세한 내용은 섹션을 참조하세요 [운영 권장 사항 포함 또는 제외](#).

AWS Resilience Hub 는 AWS Resilience Hub 내부(예: Amazon CloudWatchREADME.md) 또는 외부에서 권장하는 경보를 생성할 수 있는 템플릿 파일 AWS ()을 제공합니다 AWS. 경보에 제공된 기본 값은 이러한 경보를 생성하는 데 사용되는 모범 사례를 기반으로 합니다.

주제

- [운영 권장 사항에서 경보 생성](#)
- [경보 보기](#)

운영 권장 사항에서 경보 생성

AWS Resilience Hub 는 Amazon CloudWatch에서 선택한 경보를 생성하는 세부 정보가 포함된 AWS CloudFormation 템플릿을 생성합니다. 템플릿이 생성되면 Amazon S3 URL을 통해 템플릿에 액세스하고, 템플릿을 다운로드하여 코드 파이프라인에 배치하거나, AWS CloudFormation 콘솔을 통해 스택을 생성할 수 있습니다.

AWS Resilience Hub 권장 사항을 기반으로 경보를 생성하려면 권장 경보에 대한 템플릿을 생성 AWS CloudFormation 하여 코드 기반에 포함해야 합니다.

운영 권장 사항에 경보를 만들려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션(Applications)에서 내 애플리케이션을 선택합니다.
3. 평가 탭을 선택합니다.

복원력 평가 테이블에서 다음 정보를 사용하여 평가를 식별할 수 있습니다.

- 이름 — 작성 당시 제공한 평가의 이름입니다.
 - 상태 — 평가의 실행 상태를 나타냅니다.
 - 규정 준수 상태 — 평가가 복원력 정책을 준수하는지 여부를 나타냅니다.
 - 복원력 드리프트 상태 — 애플리케이션이 이전의 성공적인 평가에서 벗어났는지 여부를 나타냅니다.
 - 앱 버전 — 애플리케이션 버전.
 - 간접적 호출자 — 평가를 간접적으로 호출하는 역할을 나타냅니다.
 - 시작 시간 — 평가 시작 시간을 나타냅니다.
 - 종료 시간 — 평가 종료 시간을 나타냅니다.
 - ARN — 평가의 Amazon 리소스 이름(ARN)입니다.
4. 복원력 평가 테이블에서 평가를 선택합니다. 평가가 없는 경우 [the section called “에서 복원력 평가 실행 AWS Resilience Hub”](#)의 절차를 완료한 다음 이 단계로 돌아갑니다.
 5. 운영 권장 사항을 선택합니다.
 6. 기본으로 선택되지 않은 경우 경보 탭을 선택합니다.

경보 테이블에서 다음을 사용하여 권장 경보를 식별할 수 있습니다.

- 이름 — 애플리케이션에 설정한 경보의 이름입니다.

- 설명 — 경보의 목적을 설명합니다.
- 상태 — Amazon CloudWatch 경보의 현재 구현 상태를 나타냅니다.

이 열에는 다음 값 중 하나를 표시합니다.

- 구현됨 -에서 권장하는 경보 AWS Resilience Hub 가 애플리케이션에 구현되었음을 나타냅니다. 아래 숫자를 선택하면 경보 테이블이 필터링되어 애플리케이션에 구현된 모든 권장 경보가 표시됩니다.
 - 구현되지 않음 -에서 권장하는 경보 AWS Resilience Hub 가 애플리케이션에 포함되어 있지만 구현되지 않았음을 나타냅니다. 아래 숫자를 선택하면 경보 테이블이 필터링되어 애플리케이션에 구현되지 않은 모든 권장 경보가 표시됩니다.
 - 제외됨 -에서 권장하는 경보 AWS Resilience Hub 가 애플리케이션에서 제외됨을 나타냅니다. 아래 숫자를 선택하면 경보 테이블이 필터링되어 애플리케이션에서 제외된 모든 권장 경보가 표시됩니다. 권장 경보를 포함하거나 제외하는 방법에 대한 자세한 내용은 [운영 권장 사항 포함 또는 제외\(Including or excluding operational recommendations\)](#)를 참조하세요.
 - 비활성 — 경보가 Amazon CloudWatch에 배포되었지만 Amazon CloudWatch에서는 상태가 INSUFFICIENT_DATA로 설정되어 있음을 나타냅니다. 아래 숫자를 선택하면 경보 테이블을 필터링하여 구현된 경보와 비활성 경보를 모두 표시합니다.
 - 구성 — 해결해야 할 보류 중인 구성 종속성이 있는지 여부를 나타냅니다.
 - 유형 — 경보 유형을 나타냅니다.
 - AppComponent — 이 경보와 관련된 애플리케이션 구성 요소(AppComponents)를 나타냅니다.
 - 참조 ID - 스택 AWS CloudFormation 이벤트의 논리적 식별자를 나타냅니다 AWS CloudFormation.
 - 권장 사항 ID - AWS CloudFormation 스택 리소스의 논리적 식별자를 나타냅니다 AWS CloudFormation.
7. 경보(Alarms) 탭에서 경보 테이블의 경보 권장 사항을 특정 상태를 기준으로 필터링하려면 아래에 있는 숫자를 선택합니다.
 8. 애플리케이션에 설정하려는 권장 경보를 선택하고 CloudFormation 템플릿 생성을 선택합니다.
 9. CloudFormation 템플릿 생성 대화 상자에서 자동 생성된 이름을 사용하거나 CloudFormation AWS CloudFormation 템플릿 이름 상자에 템플릿 이름을 입력할 수 있습니다. CloudFormation
 10. 생성(Create)을 선택합니다. AWS CloudFormation 템플릿을 생성하는 데 최대 몇 분 정도 걸릴 수 있습니다.

코드베이스에 권장 사항을 포함시키려면 다음 절차를 완료하세요.

코드 기반 AWS Resilience Hub 권장 사항을 포함하려면

1. 템플릿 탭을 선택하면 방금 만든 템플릿을 볼 수 있습니다. 다음을 사용하여 템플릿을 식별할 수 있습니다.
 - 이름 — 작성 당시 제공한 평가의 이름입니다.
 - 상태 — 평가의 실행 상태를 나타냅니다.
 - 유형 — 운영 권장 사항의 유형을 나타냅니다.
 - 형식 — 템플릿이 생성되는 형식(JSON/ 텍스트)을 나타냅니다.
 - 시작 시간 — 평가 시작 시간을 나타냅니다.
 - 종료 시간 — 평가 종료 시간을 나타냅니다.
 - ARN — 템플릿의 ARN.
2. 템플릿 세부 정보에서 템플릿 S3 경로 아래의 링크를 선택하여 Amazon S3 콘솔에서 템플릿 객체를 엽니다.
3. Amazon S3 콘솔의 객체 테이블에서 경보 폴더 링크를 선택합니다.
4. Amazon S3 경로를 복사하려면 JSON 파일 앞의 상자를 선택하고 URL 복사를 선택합니다.
5. AWS CloudFormation 콘솔에서 AWS CloudFormation 스택을 생성합니다. AWS CloudFormation 스택 생성에 대한 자세한 내용은 섹션을 참조하세요 <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html>.

AWS CloudFormation 스택을 생성하는 동안 이전 단계에서 복사한 Amazon S3 경로를 제공해야 합니다.

경보 보기

애플리케이션의 복원력을 모니터링하기 위해 설정한 모든 활성 경보를 볼 수 있습니다. 템플릿을 AWS Resilience Hub 사용하여 Amazon CloudWatch에서 경보를 생성하는 AWS CloudFormation 데 사용되는 경보 세부 정보를 저장합니다. Amazon S3 URL을 사용하여 AWS CloudFormation 템플릿에 액세스하고, 이를 다운로드하여 코드 파이프라인에 배치하거나 AWS CloudFormation 콘솔을 통해 스택을 생성할 수 있습니다.

대시보드에서 경보를 보려면 왼쪽 탐색 메뉴에서 대시보드를 선택합니다. 구현된 경보 테이블에서 다음 정보를 사용하여 구현된 경보를 식별할 수 있습니다.

- 영향을 받는 애플리케이션 — 이 경보를 구현한 애플리케이션의 이름입니다.
- 활성 경보 — 애플리케이션에서 트리거된 활성 경보의 수를 나타냅니다.

- FIS 진행 중 - 현재 애플리케이션에 대해 실행 중인 AWS FIS 실험을 나타냅니다.

애플리케이션에 구현된 경보를 보려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션 테이블에서 애플리케이션을 선택합니다.
3. 응용 프로그램 요약 페이지의 구현된 경고 테이블에는 응용 프로그램에 구현된 모든 권장 경고가 표시됩니다.

구현된 경고 테이블의 특정 경보를 찾으려면 텍스트, 속성 또는 값별 경고 찾기 상자에서 다음 필드 중 하나를 선택하고 작업을 선택한 다음 값을 입력합니다.

- 경고 이름 — 애플리케이션에 설정한 경고의 이름입니다.
- 설명 — 경고의 목적을 설명합니다.
- 상태 — Amazon CloudWatch 경고의 현재 구현 상태를 나타냅니다.

이 열에는 다음 값 중 하나를 표시합니다.

- 구현됨 -에서 권장하는 경고 AWS Resilience Hub 가 애플리케이션에 구현되었음을 나타냅니다. 운영 권장 사항 탭에서 권장 및 구현된 모든 경보를 보려면 아래 번호를 선택하세요.
- 구현되지 않음 -에서 권장하는 경고 AWS Resilience Hub 가 애플리케이션에 포함되어 있지만 구현되지 않았음을 나타냅니다. 운영 권장 사항 탭에서 권장 및 구현되지 않은 모든 경보를 보려면 아래 번호를 선택하세요.
- 제외됨 -에서 권장하는 경고 AWS Resilience Hub 가 애플리케이션에서 제외됨을 나타냅니다. 운영 권장 사항 탭에서 권장 및 제외 경보를 모두 보려면 아래 번호를 선택하세요. 권장 경보를 포함하거나 제외하는 방법에 대한 자세한 내용은 [운영 권장 사항 포함 또는 제외 \(Including or excluding operational recommendations\)](#)를 참조하세요.
- 비활성 — 경고가 Amazon CloudWatch에 배포되었지만 Amazon CloudWatch에서는 상태가 INSUFFICIENT_DATA로 설정되어 있음을 나타냅니다. 운영 권장 사항 탭에서 구현된 모든 경고와 비활성 경보를 모두 보려면 아래 번호를 선택하세요.
- 소스 템플릿 - 경고 세부 정보가 포함된 AWS CloudFormation 스택의 Amazon 리소스 이름 (ARN)을 제공합니다.
- 리소스 — 이 경고가 연결되고 구현된 리소스를 표시합니다.
- 지표 — 경고에 할당된 Amazon CloudWatch 지표를 표시합니다. CloudWatch 지표에 대한 자세한 정보는 [Amazon CloudWatch 지표](#)를 참조하세요.
- 마지막 변경 — 경고가 마지막으로 수정된 날짜 및 시간을 표시합니다.

평가에서 권장되는 경보를 보려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션 테이블에서 애플리케이션을 선택합니다.

애플리케이션을 찾으려면 애플리케이션 찾기 상자에 애플리케이션 이름을 입력합니다.

3. 평가 탭을 선택합니다.

복원력 평가 테이블에서 다음 정보를 사용하여 평가를 식별할 수 있습니다.

- 이름 — 작성 당시 제공한 평가의 이름입니다.
- 상태 — 평가의 실행 상태를 나타냅니다.
- 규정 준수 상태 — 평가가 복원력 정책을 준수하는지 여부를 나타냅니다.
- 복원력 드리프트 상태 — 애플리케이션이 이전의 성공적인 평가에서 벗어났는지 여부를 나타냅니다.
- 앱 버전 — 애플리케이션 버전.
- 간접적 호출자 — 평가를 간접적으로 호출하는 역할을 나타냅니다.
- 시작 시간 — 평가 시작 시간을 나타냅니다.
- 종료 시간 — 평가 종료 시간을 나타냅니다.
- ARN — 평가의 Amazon 리소스 이름(ARN)입니다.

4. 복원력 평가 테이블에서 평가를 선택합니다.
5. 운영 권장 사항 탭을 선택합니다.
6. 기본으로 선택되지 않은 경우 경보 탭을 선택합니다.

경보 테이블에서 다음을 사용하여 권장 경보를 식별할 수 있습니다.

- 이름 — 애플리케이션에 설정한 경보의 이름입니다.
- 설명 — 경보의 목적을 설명합니다.
- 상태 — Amazon CloudWatch 경보의 현재 구현 상태를 나타냅니다.

이 열에는 다음 값 중 하나를 표시합니다.

- 구현됨 — 경보가 애플리케이션에 구현되었음을 나타냅니다. 아래 숫자를 선택하면 경보 테이블이 필터링되어 애플리케이션에 구현된 모든 권장 경보가 표시됩니다.

- 구현되지 않음 — 경보가 애플리케이션에 구현되거나 포함되어 있지 않음을 나타냅니다. 아래 숫자를 선택하면 경보 테이블이 필터링되어 애플리케이션에 구현되지 않은 모든 권장 경보가 표시됩니다.
- 제외 — 경보가 애플리케이션에서 제외되었음을 나타냅니다. 아래 숫자를 선택하면 경보 테이블이 필터링되어 애플리케이션에서 제외된 모든 권장 경보가 표시됩니다. 권장 경보를 포함하거나 제외하는 방법에 대한 자세한 내용은 [the section called “운영 권장 사항 포함 또는 제외”](#) 단원을 참조하세요.
- 비활성 — 경보가 Amazon CloudWatch에 배포되었지만 Amazon CloudWatch에서는 상태가 INSUFFICIENT_DATA로 설정되어 있음을 나타냅니다. 아래 숫자를 선택하면 경보 테이블을 필터링하여 구현된 경보와 비활성 경보를 모두 표시합니다.
- 구성 — 해결해야 할 오류 중인 구성 종속성이 있는지 여부를 나타냅니다.
- 유형 — 경보 유형을 나타냅니다.
- AppComponent — 이 경보와 관련된 애플리케이션 구성 요소(AppComponents)를 나타냅니다.
- 참조 ID - 스택 AWS CloudFormation 이벤트의 논리적 식별자를 나타냅니다 AWS CloudFormation.
- 권장 사항 ID - AWS CloudFormation 스택 리소스의 논리적 식별자를 나타냅니다 AWS CloudFormation.

표준 운영 절차 관리

표준 운영 절차(SOP)는 정전 또는 경보 발생 시 애플리케이션을 효율적으로 복구하도록 설계된 일련의 규범적 단계입니다. 운영 중단 발생 시 적시에 복구할 수 있도록 SOP를 미리 준비, 테스트 및 측정하세요.

애플리케이션 구성 요소에 따라 준비해야 하는 SOPs를 AWS Resilience Hub 권장합니다. AWS Resilience Hub 는 Systems Manager와 협력하여 해당 SOPs의 기반으로 사용할 수 있는 여러 SSM 문서를 제공하여 SOPs.

예를 들어 기존 SSM 자동화 문서를 기반으로 디스크 공간을 추가하는 SOP를 추천할 AWS Resilience Hub 수 있습니다. 이 SSM 문서를 실행하려면 올바른 권한이 있는 특정 IAM 역할이 필요합니다.는 디스크 부족 시 실행할 SSM 자동화 문서와 해당 SSM 문서를 실행하는 데 필요한 IAM 역할을 나타내는 메타데이터를 애플리케이션에 AWS Resilience Hub 생성합니다. 그러면 이 메타데이터가 SSM 파라미터에 저장됩니다.

SSM 자동화를 구성하는 것 외에도 AWS FIS 실험을 통해 테스트하는 것도 모범 사례입니다. 따라서는 SSM 자동화 문서를 호출하는 AWS FIS 실험 AWS Resilience Hub 도 제공합니다. 이렇게 하면 애플리케이션을 사전에 테스트하여 생성한 SOP가 의도한 작업을 수행하는지 확인할 수 있습니다.

AWS Resilience Hub 는 애플리케이션 코드 기반에 추가할 수 있는 AWS CloudFormation 템플릿 형태로 권장 사항을 제공합니다. 이 템플릿은 다음을 제공합니다.

- SOP를 실행하는 데 필요한 권한이 있는 IAM 역할.
- SOP를 테스트하는 데 사용할 수 있는 AWS FIS 실험입니다.
- 어떤 SSM 문서와 어떤 IAM 역할을 SOP로 실행할지, 그리고 어떤 리소스에서 실행할지를 나타내는 애플리케이션 메타데이터가 포함된 SSM 파라미터입니다. 예: `$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`.

SOP를 만들려면 시행착오를 겪어야할 수 있습니다. 애플리케이션에 대한 복원력 평가를 실행하고 AWS Resilience Hub 권장 사항에서 AWS CloudFormation 템플릿을 생성하는 것이 좋습니다. AWS CloudFormation 템플릿을 사용하여 AWS CloudFormation 스택을 생성한 다음 SOP에서 SSM 파라미터와 기본값을 사용합니다. SOP를 실행하여 어떤 개선이 필요한지 확인해 보세요.

애플리케이션마다 요구 사항이 다르기 때문에 AWS Resilience Hub 에서 제공되는 SSM 문서의 기본 목록으로는 모든 요구 사항을 충족할 수 없습니다. 하지만 기본 SSM 문서를 복사하여 이를 기반으로 애플리케이션에 맞는 사용자 지정 문서를 만들 수 있습니다. 고유의 완전히 새로운 SSM 문서를 만들 수도 있습니다. 기본값을 수정하는 대신 SSM 문서를 직접 생성하는 경우 SOP가 실행될 때 올바른 SSM 문서가 호출되도록 SSM 파라미터와 연결해야 합니다.

필요한 SSM 문서를 생성하고 필요에 따라 파라미터와 문서 연결을 업데이트하여 SOP를 완성했으면 SSM 문서를 코드베이스에 직접 추가하고 이후에 변경하거나 사용자 지정하세요. 이렇게 하면 애플리케이션을 배포할 때마다 최신 SOP도 배포할 수 있습니다.

주제

- [AWS Resilience Hub 권장 사항을 기반으로 SOP 구축](#)
- [사용자 지정 SSM 문서 생성](#)
- [기본값 대신 사용자 정의 SSM 문서 사용](#)
- [SOP 테스트](#)
- [표준 운영 절차 보기](#)

AWS Resilience Hub 권장 사항을 기반으로 SOP 구축

AWS Resilience Hub 권장 사항을 기반으로 SOP를 빌드하려면 복원력 정책이 연결된 AWS Resilience Hub 애플리케이션이 필요하며 해당 애플리케이션에 대해 복원력 평가를 실행해야 합니다. 복원력 평가를 통해 SOP에 대한 권장 사항이 생성됩니다.

AWS Resilience Hub 권장 사항을 기반으로 SOP를 빌드하려면 권장 SOPs에 대한 AWS CloudFormation 템플릿을 생성하여 코드 기반에 포함해야 합니다.

SOP 권장 사항을 위한 AWS CloudFormation 템플릿 생성

1. AWS Resilience Hub 콘솔을 엽니다.
2. 탐색 창에서 애플리케이션을 선택합니다.
3. 애플리케이션 목록에서 SOP를 생성할 애플리케이션을 선택합니다.
4. 평가 탭을 선택합니다.
5. 복원력 평가 테이블에서 평가를 선택합니다. 평가가 없는 경우 [the section called “에서 복원력 평가 실행 AWS Resilience Hub”](#)의 절차를 완료한 다음 이 단계로 돌아갑니다.
6. 운영 권장 사항에서 표준 운영 절차를 선택합니다.
7. 포함하려는 SOP 권장 사항을 모두 선택합니다.
8. CloudFormation 템플릿 생성을 선택합니다. AWS CloudFormation 템플릿을 생성하는 데 최대 몇 분 정도 걸릴 수 있습니다.

코드베이스에 SOP 권장 사항을 포함하려면 다음 절차를 완료하세요.

코드 기반에 AWS Resilience Hub 권장 사항을 포함하려면

1. 운영 권장 사항에서 템플릿을 선택합니다.
2. 템플릿 목록에서 방금 만든 SOP 템플릿의 이름을 선택합니다.

다음 정보를 사용하여 애플리케이션에 구현된 SOP를 식별할 수 있습니다.

- SOP 이름 — 애플리케이션에 대해 정의한 SOP의 이름입니다.
- 설명 — SOP의 목적을 설명합니다.
- SSM 문서 — SOP 정의가 포함된 SSM 문서의 Amazon S3 URL입니다.
- 테스트 실행 — 최신 테스트 결과가 포함된 문서의 Amazon S3 URL입니다.

- 소스 템플릿 - SOP 세부 정보가 포함된 AWS CloudFormation 스택의 Amazon 리소스 이름 (ARN)을 제공합니다.
3. 템플릿 세부 정보에서 템플릿 S3 경로의 링크를 선택하여 Amazon S3 콘솔에서 템플릿 객체를 엽니다.
 4. Amazon S3 콘솔의 객체 테이블에서 SOP 폴더 링크를 선택합니다.
 5. Amazon S3 경로를 복사하려면 JSON 파일 앞의 상자를 선택하고 URL 복사를 선택합니다.
 6. AWS CloudFormation 콘솔에서 AWS CloudFormation 스택을 생성합니다. AWS CloudFormation 스택 생성에 대한 자세한 내용은 <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html> 섹션을 참조하세요.

AWS CloudFormation 스택을 생성하는 동안 이전 단계에서 복사한 Amazon S3 경로를 제공해야 합니다.

사용자 지정 SSM 문서 생성

애플리케이션 복구를 완전히 자동화하려면 Systems Manager(시스템 관리자) 콘솔에서 SOP에 대한 사용자 지정 SSM 문서를 생성해야 할 수 있습니다. 기존 SSM 문서를 기본으로 수정하거나 새 SSM 문서를 생성할 수 있습니다.

Systems Manager(시스템 관리자)를 사용하여 SSM 문서를 만드는 방법에 대한 자세한 내용은 [안내: 문서 작성기를 사용하여 사용자 정의 런북 만들기](#)를 참조하세요.

SSM 문서 구문에 대한 자세한 내용은 [SSM 문서 구문](#)을 참조하세요.

SSM 문서 작업 자동화에 대한 자세한 내용은 [시스템 관리자\(Systems Manager\) 자동화 작업 참조](#)를 참조하세요.

기본값 대신 사용자 정의 SSM 문서 사용

SOP에 AWS Resilience Hub 제안된 SSM 문서를 생성한 사용자 지정 문서로 바꾸려면 코드 기반에서 직접 작업합니다. 새 사용자 지정 SSM 자동화 문서를 추가하는 것 외에도 다음과 같은 작업을 수행할 수 있습니다.

1. 자동화를 실행하는 데 필요한 IAM 권한을 추가합니다.
2. AWS FIS 실험을 추가하여 SSM 문서를 테스트합니다.
3. SOP로 사용하려는 자동화 문서를 가리키는 SSM 파라미터를 추가합니다.

일반적으로에서 제안된 기본값으로 작업 AWS Resilience Hub 하고 필요에 따라 사용자 지정하는 것이 가장 효율적입니다. 예를 들어 IAM 역할에 필요한 권한을 추가하거나 제거하거나, AWS FIS 실험 설정을 변경하여 새 SSM 문서를 가리키거나, SSM 파라미터를 변경하여 새 SSM 문서를 가리킵니다.

SOP 테스트

앞서 언급한 것처럼 모범 사례는 CI/CD 파이프라인에 AWS FIS 실험을 추가하여 SOPs를 정기적으로 테스트하는 것입니다. 이렇게 하면 중단이 발생할 경우 즉시 사용할 수 있습니다.

AWS Resilience Hub제공 SOP와 사용자 지정 SOPs.

표준 운영 절차 보기

애플리케이션에서 구현된 SOP를 보려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션에서 애플리케이션을 엽니다.
3. 표준 운영 절차 탭을 선택합니다.

표준 운영 절차 요약 섹션의 구현된 표준 운영 절차 테이블에는 SOP 권장 사항에서 생성된 SOP 목록이 표시됩니다.

다음을 사용하여 SOP를 식별할 수 있습니다.

- SOP 이름 — 애플리케이션에 대해 정의한 SOP의 이름입니다.
- SSM 문서 — SOP 정의가 포함된 Amazon EC2 Systems Manager(시스템 관리자) 문서의 S3 URL입니다.
- 설명 — SOP의 목적을 설명합니다.
- 테스트 실행 — 최신 테스트 결과가 포함된 문서의 S3 URL입니다.
- 참조 ID — 참조된 SOP 권장 사항의 식별자입니다.
- 리소스 ID — SOP 권장 사항이 구현된 리소스의 식별자입니다.

평가에서 권장되는 SOP를 보려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션 테이블에서 애플리케이션을 선택합니다.

애플리케이션을 찾으려면 애플리케이션 찾기 상자에 애플리케이션 이름을 입력합니다.

3. 평가 탭을 선택합니다.

복원력 평가 테이블에서 다음 정보를 사용하여 평가를 식별할 수 있습니다.

- 이름 — 작성 당시 제공한 평가의 이름입니다.
- 상태 — 평가의 실행 상태를 나타냅니다.
- 규정 준수 상태 — 평가가 복원력 정책을 준수하는지 여부를 나타냅니다.
- 복원력 드리프트 상태 — 애플리케이션이 이전의 성공적인 평가에서 벗어났는지 여부를 나타냅니다.
- 앱 버전 — 애플리케이션 버전.
- 간접적 호출자 — 평가를 간접적으로 호출하는 역할을 나타냅니다.
- 시작 시간 — 평가 시작 시간을 나타냅니다.
- 종료 시간 — 평가 종료 시간을 나타냅니다.
- ARN — 평가의 Amazon 리소스 이름(ARN)입니다.

4. 복원력 평가 테이블에서 평가를 선택합니다.

5. 운영 권장 사항 탭을 선택합니다.

6. 표준 운영 절차 탭을 선택합니다.

표준 운영 절차 테이블에서는 다음 정보를 사용하여 권장 SOP에 대해 자세히 알아볼 수 있습니다.

- 이름 — 권장 SOP의 이름.
- 설명 — SOP의 목적을 설명합니다.
- 상태 — SOP의 현재 구현 상태를 나타냅니다. 즉, 구현됨, 구현되지 않음, 제외됨입니다.
- 구성 — 해결해야 할 보류 중인 구성 종속성이 있는지 여부를 나타냅니다.
- 유형 — SOP 유형을 나타냅니다.
- AppComponent — 이 SOP와 관련된 애플리케이션 구성 요소(AppComponents)를 나타냅니다. 지원되는 AppComponent에 대한 자세한 내용은 AppComponent의 [리소스 그룹화\(Grouping resources\)](#)를 참조하세요.
- 참조 ID - 스택 AWS CloudFormation 이벤트의 논리적 식별자를 나타냅니다 AWS CloudFormation.
- 권장 사항 ID — AWS CloudFormation에 있는 AWS CloudFormation 스택 리소스의 논리적 식별자를 나타냅니다.

AWS Fault Injection Service 실험 관리

이 섹션에서는 AWS Fault Injection Service (AWS FIS) 실험을 관리하는 방법을 설명합니다 AWS Resilience Hub. AWS FIS 실험을 실행하여 AWS 리소스의 복원력과 애플리케이션, 인프라, 가용 영역 및 AWS 리전 인시던트에서 복구하는 데 걸리는 시간을 측정합니다.

복원력을 측정하기 위해 이러한 AWS FIS 실험은 리소스 중단을 시뮬레이션합니다 AWS . 중단의 예로는 네트워크 사용 불가 오류, 장애 조치, Amazon EC2 또는 AWS ASG에서 중지된 프로세스, Amazon RDS에서 부팅 복구, 가용 영역 문제 등이 있습니다. AWS FIS 실험이 끝나면 애플리케이션이 복원력 정책의 RTO 대상에 정의된 중단 유형에서 복구할 수 있는지 여부를 추정할 수 있습니다.

의 모든 실험 AWS Resilience Hub 은를 사용하여 빌드 AWS FIS 되며 AWS FIS 작업을 실행합니다. AWS FIS 실험은 특정 AWS 서비스(예: Amazon EKS 작업)에 사용자 지정된 AWS FIS 자동화 작업만 사용합니다. AWS FIS 작업에 대한 자세한 내용은 [AWS FIS 작업 참조](#)를 참조하세요.

기본 상태에서 AWS FIS 실험을 사용하거나 요구 사항에 따라 실험을 사용자 지정할 수 있습니다. AWS Resilience Hub 콘솔 및 AWS FIS 콘솔에서 AWS FIS 실험을 관리하는 방법에 대한 자세한 내용은 다음 주제를 참조하세요.

- AWS Resilience Hub 콘솔
 - [AWS FIS 실험 보기](#)
 - [애플리케이션에서 구현 AWS FIS 된 실험 목록을 보려면](#)
 - [평가에서 권장 AWS FIS 실험을 보려면](#)
 - [the section called “ AWS FIS 실험 실행”](#)
 - [the section called “AWS Fault Injection Service 실험 실패/상태 확인”](#)
- AWS FIS 콘솔
 - [AWS FIS 실험 관리](#)
 - [AWS FIS 시나리오 라이브러리 작업](#)
 - [AWS FIS 실험 템플릿 관리](#)

실험 시작, 생성 및 실행 AWS FIS

AWS Resilience Hub 는 AWS FIS 실험과 통합하여 AWS FIS 실험을 간소화합니다. 맞춤형 권장 사항을 제공하고 애플리케이션 구성 요소(AppComponents)에 매핑된 미리 채워진 템플릿을 사용하여 AWS FIS 실험을 시작할 수 있으므로 효율적인 복원력 테스트가 가능합니다.

운영 권장 사항에서 AWS FIS 실험을 시작하려면

1. AWS Resilience Hub 콘솔을 엽니다.
2. 탐색 창에서 애플리케이션을 선택합니다.
3. 애플리케이션 목록에서 테스트 생성 대상 애플리케이션을 선택합니다.
4. 평가 탭을 선택합니다.
5. 복원력 평가 테이블에서 평가를 선택합니다. 평가가 없는 경우 [the section called “에서 복원력 평가 실행 AWS Resilience Hub”](#)의 절차를 완료한 다음 이 단계로 돌아갑니다.
6. 운영 권장 사항 탭을 선택합니다.
7. 결합 주입 실험 전에 오른쪽 화살표를 선택합니다.

이 섹션에는 애플리케이션의 스트레스 테스트 및 복원력 개선을 AWS Resilience Hub 위에서 권장하는 모든 AWS FIS 실험이 나열되어 있습니다. 구현에 따라 AWS FIS 실험은 다음 상태로 분류됩니다.

- 구현됨 -에서 권장하는 실험 AWS Resilience Hub 이 애플리케이션에 구현되었음을 나타냅니다. 실험 테이블에서 구현된 모든 실험을 보려면 아래 번호를 선택합니다.
- 부분적으로 구현됨 -에서 권장하는 실험 AWS Resilience Hub 이 애플리케이션에 부분적으로 구현되었음을 나타냅니다. 실험 테이블에서 부분적으로 구현된 모든 실험을 보려면 아래 번호를 선택합니다.
- 구현되지 않음 -에서 권장하는 실험 AWS Resilience Hub 이 애플리케이션에서 구현되지 않았음을 나타냅니다. 실험 테이블에서 구현되지 않은 모든 실험을 보려면 아래 숫자를 선택합니다.
- 제외됨 -에서 권장하는 실험 AWS Resilience Hub 이 애플리케이션에서 제외됨을 나타냅니다. 실험 테이블에서 제외된 모든 실험을 보려면 아래 숫자를 선택합니다. 권장 실험 포함 및 제외에 대한 자세한 내용은 [운영 권장 사항 포함 또는 제외](#)를 참조하세요.

실험 표에는 애플리케이션의 복원력 점수에 영향을 미치는 구현 AWS FIS 된 모든 실험이 나열되어 있습니다. 다음 정보를 사용하여 AWS FIS 실험을 식별할 수 있습니다.

- 작업 이름 - 애플리케이션에 권장되는 AWS FIS 작업을 나타냅니다. AWS FIS 실험 세부 정보 페이지에서 권장 AppComponents를 모두 보려면 작업 이름을 선택합니다. 상태가 추적 불가로 설정되면 실험이 시나리오임을 AWS FIS 나타냅니다. 시나리오 이름을 선택하여 콘솔의 시나리오 라이브러리 페이지에서 AWS FIS 세부 정보를 봅니다.
- 상태 - AWS FIS 실험의 현재 구현 상태를 나타냅니다. 즉, 구현됨, 부분 구현됨, 구현되지 않음 및 제외됨입니다.

Note

AWS FIS 시나리오는 여러 사전 정의된 작업이 있는 콘솔 전용 기능입니다. 따라서 이를 추적할 AWS Resilience Hub 수 없으며 상태를 추적 불가로 설정합니다.

- 설명 - AWS FIS 작업의 목표를 설명합니다.

8. 실험을 시작하려는 AWS FIS 작업을 선택합니다.

AWS FIS 실험 권장 사항 섹션에서 다음 정보를 사용하여 AppComponents

- 이름 - 리소스가 그룹화된 AppComponent의 이름입니다.
- 상태 - AWS FIS 작업의 현재 구현 상태를 나타냅니다. 즉, 구현됨, 부분 구현됨, 구현되지 않음 및 제외됨입니다.

Note

AWS FIS 시나리오는 여러 사전 정의된 작업이 있는 콘솔 전용 기능입니다. 따라서 이를 추적할 AWS Resilience Hub 수 없으며 상태를 추적 불가로 설정합니다.

- 대상 선택 - 실험 시작을 선택할 때 리소스가 실험에 포함되는 방법을 나타냅니다. AWS Resilience Hub 가 대상 리소스를 자동으로 결정하지 않는 경우 해당 대상 선택 필드 위에 마우스를 올려 놓으면 해당 리소스 추가에 대한 지침이 표시됩니다.
- 리소스 - AppComponent에서 그룹화된 리소스 수를 나타냅니다. 리소스 대화 상자에서 번호를 선택하여 이러한 리소스를 확인합니다. 다음을 사용하여 리소스를 식별할 수 있습니다.
 - 논리적 ID - 리소스의 논리적 ID를 나타냅니다. 논리적 ID는 AWS CloudFormation, Terraform 상태 파일, myApplications 애플리케이션, AWS Resource Groups 리소스 또는 Amazon Elastic Kubernetes Service 클러스터의 리소스를 식별하는 데 사용되는 이름입니다.
 - 물리적 ID - Amazon EC2 인스턴스 ID 또는 Amazon S3 버킷 이름과 같이 리소스에 대해 실제로 할당된 식별자를 나타냅니다.
 - 유형 - 리소스 유형을 나타냅니다.
 - 리전 - 리소스가 위치한 리전을 나타냅니다 AWS .

9. AppComponent를 선택하고 포함 또는 제외를 선택하여 각각 AWS FIS 실험에 AppComponent를 포함하거나 제외합니다.

10. 실험 시작을 선택합니다.

AWS Resilience Hub 는 AWS FIS 콘솔의 템플릿 세부 정보 지정 페이지로 리디렉션하여 새 탭에서 엽니다.

11. 실험 템플릿을 생성하려면 [콘솔을 사용하여 실험 템플릿을 생성하려면](#)의 단계를 완료합니다.

또한 템플릿 세부 정보를 입력하고 AWS FIS 콘솔을 [사용하여 실험 템플릿을 생성하려면](#)의 단계에 따라 콘솔의 템플릿 세부 정보 지정 페이지에서 다음을 선택하면 AWS Resilience Hub 는 작업 및 대상 페이지에서 리소스 유형에 대한 작업 및 대상을 자동으로 매핑하려고 시도합니다. 그러나 적용 범위를 개선하기 위해 작업 추가 및 대상 추가를 각각 선택하여 작업과 대상을 수동으로 추가하고 나머지 절차를 완료하여 실험을 생성할 수 있습니다.

AWS FIS 실험 실행

AWS FIS 콘솔에서 실험을 생성한 후 [템플릿에서 실험 시작](#)의 단계에 따라 콘솔에서 AWS FIS 실험을 실행합니다. 에서 실행한 최신 실험을 감지 AWS Resilience Hub 하려면 새 평가를 실행 AWS FIS해야 합니다. 평가 실행 방법에 대한 자세한 내용은 [에서 복원력 평가 실행 AWS Resilience Hub](#) 단원을 참조하세요.

AWS FIS 실험 보기

에서 AWS 리소스의 복원력과 애플리케이션 AWS Resilience Hub, 인프라, 가용 영역 및 AWS 리전 인스턴트에서 복구하는 데 걸리는 시간을 측정하기 위해 설정한 AWS FIS 실험을 봅니다.

대시보드에서 활성 AWS FIS 실험 목록을 보려면 왼쪽 탐색 메뉴에서 대시보드를 선택합니다.

구현된 실험 테이블에서 다음 정보를 사용하여 실험을 식별할 AWS FIS 수 있습니다.

- 실험 ID — AWS FIS 실험의 식별자.
- 작업 - AWS FIS 실험과 연결된 AWS FIS 작업을 나타냅니다. 또한 작업이 두 개 이상 있는 경우 AWS FIS 실험과 관련된 AWS FIS 작업 수를 강조 표시합니다. 세부 정보 위로 마우스를 가져가거나 세부 정보로 이동하여 세부 정보를 식별할 수 있습니다.
- 실험 템플릿 ID - 실험을 AWS FIS 생성하는 데 사용된 AWS FIS 실험 템플릿의 식별자입니다.

애플리케이션에서 구현 AWS FIS 된 실험 목록을 보려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션 테이블에서 애플리케이션을 선택합니다.

애플리케이션을 찾으려면 애플리케이션 찾기 상자에 애플리케이션 이름을 입력합니다.

3. 결합 주입 실험(Fault injection experiments)을 선택합니다.

구현된 실험 테이블에서 다음 정보를 사용하여 애플리케이션에 구현된 AWS FIS 실험을 식별할 수 있습니다.

- 실험 ID — AWS FIS 실험의 식별자.
- 작업 - AWS FIS 실험과 연결된 AWS FIS 작업을 나타냅니다. 또한 작업이 두 개 이상 있는 경우 AWS FIS 실험과 관련된 AWS FIS 작업 수를 강조 표시합니다. 세부 정보 위로 마우스를 가져가거나 세부 정보로 이동하여 세부 정보를 식별할 수 있습니다.
- 실험 템플릿 ID — AWS FIS 실험을 만드는 데 사용된 AWS FIS 실험 템플릿의 식별자입니다.

평가에서 권장 AWS FIS 실험을 보려면

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션 테이블에서 애플리케이션을 선택합니다.

애플리케이션을 찾으려면 애플리케이션 찾기 상자에 애플리케이션 이름을 입력합니다.

3. 평가 탭을 선택합니다.

평가 테이블에서 다음 정보를 사용하여 평가를 식별할 수 있습니다.

- 이름 — 작성 당시 제공한 평가의 이름입니다.
- 상태 — 평가의 실행 상태를 나타냅니다.
- 규정 준수 상태 — 평가가 복원력 정책을 준수하는지 여부를 나타냅니다.
- 복원력 - 애플리케이션이 연결된 복원력 정책에 정의된 RTO 및 RPO 대상에서 드리프트되었는지 여부를 나타냅니다.
- 앱 버전 - 평가된 애플리케이션의 버전입니다.
- 간접적 호출자 — 평가를 간접적으로 호출하는 역할을 나타냅니다.
- 시작 시간 — 평가 시작 시간을 나타냅니다.
- 종료 시간 — 평가 종료 시간을 나타냅니다.
- ARN — 평가의 Amazon 리소스 이름(ARN)입니다.

4. 평가 테이블에서 평가를 선택합니다.

5. 운영 권장 사항을 선택합니다.

6. 결합 주입 실험 전에 오른쪽 화살표를 선택합니다.

이 섹션에는 애플리케이션의 스트레스 테스트 및 복원력 개선을 AWS Resilience Hub 위해에서 권장하는 모든 AWS FIS 실험이 나열되어 있습니다. 구현에 따라 AWS FIS 실험은 다음 상태로 분류됩니다.

- 구현됨 -에서 권장하는 실험 AWS Resilience Hub 이 애플리케이션에 구현되었음을 나타냅니다. 실험 테이블에서 구현된 모든 실험을 보려면 아래 번호를 선택합니다.
- 부분적으로 구현됨 -에서 권장하는 실험 AWS Resilience Hub 이 애플리케이션에 부분적으로 구현되었음을 나타냅니다. 실험 테이블에서 부분적으로 구현된 모든 실험을 보려면 아래 번호를 선택합니다.
- 구현되지 않음 -에서 권장하는 실험 AWS Resilience Hub 이 애플리케이션에서 구현되지 않았음을 나타냅니다. 실험 테이블에서 구현되지 않은 모든 실험을 보려면 아래 숫자를 선택합니다.
- 제외됨 -에서 권장하는 실험 AWS Resilience Hub 이 애플리케이션에서 제외됨을 나타냅니다. 실험 테이블에서 제외된 모든 실험을 보려면 아래 숫자를 선택합니다. 권장 실험 포함 및 제외에 대한 자세한 내용은 [운영 권장 사항 포함 또는 제외](#)를 참조하세요.

실험 표에는 애플리케이션의 복원력 점수에 영향을 미치는 구현 AWS FIS 된 모든 실험이 나열되어 있습니다. 다음 정보를 사용하여 AWS FIS 실험을 식별할 수 있습니다.

- 작업 이름 - 애플리케이션에 권장되는 AWS FIS 작업을 나타냅니다. 상태가 추적 불가로 설정되면 실험이 시나리오임을 AWS FIS 나타냅니다. 시나리오 이름을 선택하여 콘솔의 시나리오 라이브러리 페이지에서 AWS FIS 세부 정보를 봅니다.
- 상태 - AWS FIS 실험의 현재 구현 상태를 나타냅니다. 즉, 구현됨, 부분 구현됨, 구현되지 않음 및 제외됨입니다.

Note

AWS FIS 시나리오는 여러 사전 정의된 작업이 있는 콘솔 전용 기능입니다. 따라서 이를 추적할 AWS Resilience Hub 수 없으며 상태를 추적 불가로 설정합니다.

- 설명 - AWS FIS 작업의 목표를 설명합니다.

AWS Fault Injection Service 실험 실패/상태 확인

AWS Resilience Hub 를 사용하면 시작한 실험의 상태를 추적할 수 있습니다. 자세한 내용은 [평가에서 권장 AWS FIS 실험을 보려면](#) 절차를 참조하세요.

주제

- [Systems Manager를 사용하여 AWS FISAWS 실험 실행 분석](#)
- [AWS FIS Amazon Elastic Kubernetes Service 클러스터에서 실행되는 Kubernetes 포드를 테스트하는 동안 실험 실패](#)

Systems Manager를 사용하여 AWS FISAWS 실험 실행 분석

AWS FIS 실험을 실행한 후 Systems Manager에서 실행 세부 정보를 볼 수 있습니다 AWS .

1. CloudTrail > 이벤트 기록(Event History)으로 이동합니다.
2. 실험 ID를 사용하여 사용자 이름을 기준으로 이벤트를 필터링합니다.
3. 자동화 실행 시작(StartAutomationExecution) 항목을 확인합니다. 요청 ID는 SSM 자동화 ID입니다.
4. AWS Systems Manager > 자동화로 이동합니다.
5. SSM 자동화 ID를 사용하여 실행 ID(Execution ID)별로 필터링하고 자동화 세부 정보를 확인합니다.

모든 Systems Manager 자동화를 사용하여 실행을 분석할 수 있습니다. 자세한 내용은 [AWS Systems Manager Automation](#) 사용 설명서를 참조하세요. 실행 입력 파라미터는 실행 세부 정보의 입력 파라미터 섹션에 나타나며 AWS FIS 실험에 나타나지 않는 선택적 파라미터를 포함합니다.

실행 단계 내의 특정 단계로 드릴다운하여 단계 상태 및 기타 단계 세부 정보에 대한 정보를 찾을 수 있습니다.

일반적인 오류

평가 보고를 실행하는 동안 발생하는 일반적인 오류는 다음과 같습니다.

- 테스트/SOP 실험이 실행되기 전에 경고 템플릿이 배포되지 않았습니다. 이로 인해 자동화 단계에서 오류 메시지가 발생합니다.
- 오류 메시지: The following parameters were not found: [/ResilienceHub/Alarm/3dee49a1-9877-452a-bb0c-a958479a8ef2/nat-gw-alarm-bytes-out-to-source-2020-09-21_nat-02ad9bc4fbd4e6135]. Make sure all the SSM parameters in automation document are created in SSM Parameter Store..

- 해결 방법: 결함 주입 실험을 다시 실행하기 전에 관련 경보를 렌더링하고 결과 템플릿을 배포해야 합니다.
- 실행 역할의 권한이 누락되었습니다. 이 오류 메시지는 제공된 실행 역할에 권한이 없는 경우 발생하며 단계 세부 정보에 나타납니다.
- 오류 메시지: An error occurred (Unauthorized Operation) when calling the DescribeInstanceStatus operation: You are not authorized to perform this operation. Please Refer to Automation Service Troubleshooting Guide for more diagnosis details.
- 해결 방법: 올바른 실행 역할을 제공했는지 확인하세요. 이 작업을 완료했다면 필요한 권한을 추가하고 평가를 다시 실행하세요.
- 실행에 성공했지만 예상한 결과를 얻지 못했습니다. 이는 잘못된 파라미터 또는 내부 자동화 문제로 인한 것입니다.
- 오류 메시지: 실행이 성공했으므로 오류 메시지가 표시되지 않습니다.
- 해결 방법: 개별 단계에서 예상 입력 및 출력을 검사하기 전에 입력 파라미터를 확인하고 AWS FIS 실험 실행 분석에 설명된 대로 실행된 단계를 살펴봅니다.

AWS FIS Amazon Elastic Kubernetes Service 클러스터에서 실행되는 Kubernetes 포드를 테스트하는 동안 실험 실패

Amazon EKS 클러스터에서 실행되는 Kubernetes 포드를 테스트하는 동안 발생하는 일반적인 Amazon Elastic Kubernetes Service (Amazon EKS) 오류는 다음과 같습니다.

- AWS FIS 실험 또는 Kubernetes 서비스 계정에 대한 IAM 역할의 잘못된 구성입니다.
- 오류 메시지:
 - Error resolving targets. Kubernetes API returned ApiException with error code 401.
 - Error resolving targets. Kubernetes API returned ApiException with error code 403.
 - Unable to inject AWS FIS Pod: Kubernetes API returned status code 403. Check Amazon EKS logs for more details.
- 해결 방법: 다음을 확인하세요.
 - [AWS FISaws:eks:pod 작업 사용](#)의 지침을 따랐는지 확인하세요.
 - 필요한 RBAC 권한과 올바른 네임스페이스를 사용하여 Kubernetes 서비스 계정을 생성하고 구성했는지 확인하세요.

- 제공된 IAM 역할(테스트 AWS CloudFormation 스택의 출력 참조)을 Kubernetes 사용자에게 매핑했는지 확인합니다.
- AWS FIS 포드를 시작할 수 없음: 최대 실패한 사이드카 컨테이너에 도달했습니다. 이는 일반적으로 메모리가 AWS FIS 사이드카 컨테이너를 실행하기에 충분하지 않을 때 발생합니다.
- 오류 메시지: Unable to heartbeat FIS Pod: Max failed sidecar containers reached.
- 해결 방법: 이 오류를 방지하는 한 가지 방법은 사용 가능한 메모리 또는 CPU에 맞춰 목표 부하 비율을 줄이는 것입니다.
- 실험 시작 시 알람 어설션이 실패했습니다. 이 오류는 관련 경보에 데이터 포인트가 없기 때문에 발생합니다.
- 오류 메시지: Assertion failed for the following alarms. 어설션이 실패한 모든 경보를 나열합니다.
- 해결 방법: Container Insights가 경보에 맞게 올바르게 설치되어 있고 경보가 켜져 있지 않은지 (ALARM 상태) 확인하세요.

복원력 점수 이해

이 섹션에서는 AWS Resilience Hub 가 다양한 중단 시나리오에서 애플리케이션 준비 상태를 정량화하는 방법을 설명합니다.

AWS Resilience Hub 는 애플리케이션의 복원력을 나타내는 복원력 점수를 제공합니다. 이 점수는 애플리케이션이 애플리케이션의 복원력 정책, 경보, 표준 운영 절차(SOP) 및 테스트를 충족하기 위한 권장 사항을 얼마나 잘 따르고 있는지를 반영합니다. 애플리케이션이 사용하는 리소스 유형에 따라서는 경보, SOPs 및 각 중단 유형에 대한 테스트 세트를 AWS Resilience Hub 권장합니다.

최고 복원력 점수는 100점입니다. 가능한 최고 점수 또는 최고 점수를 얻으려면 애플리케이션에 모든 권장 경보, SOP 및 테스트를 구현해야 합니다. 예를 들어,는 하나의 경보와 하나의 SOP가 포함된 하나의 테스트를 AWS Resilience Hub 권장합니다. 테스트가 실행되어 경보가 발생하고 관련 SOP가 시작됩니다. 테스트가 성공적으로 수행되고 애플리케이션이 복원력 정책을 충족하는 경우 100점에 가깝거나 100점의 복원력 점수를 받습니다.

첫 번째 평가를 실행한 후는 애플리케이션에서 운영 권장 사항을 제외하는 옵션을 AWS Resilience Hub 제공합니다. 제외된 권장 사항이 복원력 점수에 미치는 영향을 이해하려면 평가를 새로 실행해야 합니다. 하지만 언제든지 애플리케이션에 제외된 권장 사항을 포함하고 새 평가를 실행할 수 있습니다. 경보, SOP 및 테스트 권장 사항의 포함 및 제외에 대한 자세한 내용은 [the section called “운영 권장 사항 포함 또는 제외”](#) 단원을 참조하세요.

애플리케이션의 복원력 점수에 액세스

탐색 메뉴에서 대시보드 또는 애플리케이션을 선택하여 애플리케이션의 복원력 점수를 볼 수 있습니다.

대시보드에서 복원력 점수에 액세스

1. 왼쪽 탐색 메뉴에서 대시보드를 선택합니다.
2. 시간별 애플리케이션 복원력 점수의 최대 4개 애플리케이션 선택 드롭다운 목록에서 애플리케이션을 하나 이상 선택합니다.
3. 복원력 점수 차트에 선택한 모든 애플리케이션의 복원력 점수가 표시됩니다.

애플리케이션에서 복원력 점수에 액세스

1. 왼쪽 탐색 메뉴에서 애플리케이션을 선택합니다.
2. 애플리케이션에서 애플리케이션을 엽니다.
3. 요약을 선택합니다.

복원력 점수 차트에는 최대 1년 동안 애플리케이션의 복원력 점수 추세가 표시됩니다. 다음을 사용하여 가능한 최대 복원력 점수를 개선하고 달성하기 위해 해결해야 하는 작업 항목, 복원력 정책 위반 및 운영 권장 사항을 AWS Resilience Hub 표시합니다.

- 복원력 점수를 높이고 가능한 최대 복원력 점수를 달성하기 위해 완료해야 하는 조치 항목을 보려면 조치 항목 탭을 선택합니다. 이 옵션을 선택하면 다음이 AWS Resilience Hub 표시됩니다.
 - RTO/RPO - 애플리케이션 복원력 정책의 위반을 해결하기 위해 수정해야 하는 복구 시간 (RTO/RPO) 수를 나타냅니다. 애플리케이션 평가 보고서에서 RTO/RPO 세부 정보를 보려면 값을 선택합니다.
 - 경고 - 애플리케이션에 구현해야 하는 권장 Amazon CloudWatch 경보의 수를 나타냅니다. 값을 선택하면 애플리케이션의 평가 보고서에서 수정해야 하는 Amazon CloudWatch 경보를 볼 수 있습니다.
 - SOP - 애플리케이션에 구현해야 하는 권장 SOP의 수를 나타냅니다. 값을 선택하면 애플리케이션의 평가 보고서에서 수정해야 할 SOP를 확인할 수 있습니다.
 - FIS - 애플리케이션에 구현해야 하는 권장 테스트 수를 나타냅니다. 값을 선택하면 애플리케이션의 평가 보고서에서 수정해야 할 테스트를 확인할 수 있습니다.
- 복원력 점수에 영향을 미치는 각 구성 요소의 점수를 보려면 점수 분석을 선택합니다. 선택하면 AWS Resilience Hub 에 다음이 표시됩니다.

- RTO/RPO 규정 준수 - 애플리케이션 구성 요소(AppComponents)가 애플리케이션의 복원력 정책에 정의된 예상 워크로드 복구 시간 및 목표 복구 시간을 얼마나 준수하는지를 나타냅니다. 값을 선택하면 애플리케이션 평가 보고서에서 RTO/RPO 추정치를 확인할 수 있습니다.
- 경보 구현 - 구현된 Amazon CloudWatch 경보의 실제 기여도를 애플리케이션의 복원력 점수에 대해 가능한 최대 기여도와 비교하여 나타냅니다. 값을 선택하면 애플리케이션의 평가 보고서에서 구현된 Amazon CloudWatch 경보를 볼 수 있습니다.
- 구현된 SOP - 구현된 SOP의 실제 기여도를 애플리케이션의 복원력 점수에 대해 가능한 최대 기여도와 비교하여 나타냅니다. 값을 선택하면 애플리케이션 평가 보고서에서 구현된 SOP를 확인할 수 있습니다.
- FIS 실험 구현 - 구현된 테스트의 실제 기여도를 애플리케이션의 복원력 점수에 대해 가능한 최대 기여도와 비교하여 나타냅니다. 값을 선택하면 애플리케이션의 평가 보고서에서 구현된 테스트를 확인할 수 있습니다.
- 복원력 정책 위반과 운영 권장 사항을 보려면 오른쪽 화살표를 선택하여 정책 위반 및 운영 권장 사항 분류 섹션을 확장하세요. 확장하면에 다음이 AWS Resilience Hub 표시됩니다.
- 복원력 정책 위반 - 애플리케이션의 복원력 정책을 위반하는 애플리케이션 구성 요소의 수를 나타냅니다. 애플리케이션 평가 보고서의 복원력 권장 사항 탭에서 세부 정보를 보려면 RTO/RPO 옆의 값을 선택합니다.
- 운영 권장 사항- 미해결 및 제외 탭을 사용하여 애플리케이션의 복원력을 향상시키기 위해 구현되거나 실행되지 않은 운영 권장 사항을 표시합니다. 운영 권장 사항에는 비활성 상태인 권장 사항과 구현되지 않은 권장 사항이 모두 포함됩니다.

구현해야 하는 운영 권장 사항을 보려면 미해결 탭을 선택합니다. 이 옵션을 선택하면 다음이 AWS Resilience Hub 표시됩니다.

- 경보 - 구현해야 하는 권장 Amazon CloudWatch 경보의 수를 나타냅니다.
- SOP - 구현해야 하는 권장 SOP의 수를 나타냅니다.
- FIS - 구현해야 하는 권장 테스트 수를 나타냅니다.

애플리케이션에서 제외된 운영 권장 사항을 보려면 제외 탭을 선택합니다. 선택하면 다음이 AWS Resilience Hub 표시됩니다.

- 경보 - 애플리케이션에서 제외된 권장 Amazon CloudWatch 경보의 수를 나타냅니다.
- SOP - 애플리케이션에서 제외된 권장 SOP의 수를 나타냅니다.
- FIS - 애플리케이션에서 제외된 권장 테스트의 수를 나타냅니다.

복원력 점수 계산

이 섹션의 표는 각 권장 사항 유형의 점수 구성 요소와 애플리케이션의 복원력 점수를 결정하는 AWS Resilience Hub 데에서 사용하는 공식을 설명합니다. 각 권장 사항 유형의 구성 요소를 채점하기 AWS Resilience Hub 위하에서 결정한 모든 결과 값과 애플리케이션의 복원력 점수는 가장 가까운 지점으로 반올림됩니다. 예를 들어 세 개의 경보 중 두 개가 구현된 경우 점수는 $13.33((2/3) * 20)$ 점이 됩니다. 이 값은 13점으로 반올림됩니다. 테이블 내 공식에 사용되는 가중치에 대한 자세한 내용은 [the section called “앱 구성 요소의 가중치 및 중단 유형”](#) 단원을 참조하세요.

일부 채점 구성 요소는 ScoringComponentResiliencyScore API를 통해서만 얻을 수 있습니다. 이 API에 대한 자세한 내용은 구성 요소 복원력 [ScoringComponentResiliencyScore](#)을 참조하세요.

테이블

- [각 추천 유형의 채점 구성 요소를 계산하는 공식](#)
- [복원력 점수를 계산하는 공식](#)
- [AppComponents 및 중단 유형에 대한 복원력 점수를 계산하는 공식](#)

다음 표에서는에서 각 권장 사항 유형의 점수 요소를 계산 AWS Resilience Hub 하는 데 사용하는 공식을 설명합니다.

각 추천 유형의 채점 구성 요소를 계산하는 공식

채점 구성 요소	설명	공식	예제
테스트 적용 범위(T)	총 AWS Resilience Hub 의 권장 테스트 수 중에서 성공적으로 구현되고 제외된 테스트 수를 기준으로 한 정규화된 점수(0~100점)입니다.  Note 복원력 점수를 계산하려면가 구현된 것으로 간주 AWS Resilience Hub 하려면 권장 테스트가	$T = ((\text{Total number of tests implemented}) + (\text{Total number of tests excluded})) / (\text{Total number of tests recommended})$ 공식의 일부는 다음과 같습니다. 구성된 총 테스트 수 - AWS CloudFormation 템플릿을 생성하고 AWS	20개의 AWS Resilience Hub 권장 테스트 중 10개를 구현하고 5개의 테스트를 제외한 경우 테스트 범위는 다음과 같이 계산됩니다. $T = (10 + 5) / 20$ 즉, $T = .75$ or 75 points

채점 구성 요소	설명	공식	예제
	지난 30일 동안 성공적으로 실행되어야 합니다.	CloudFormation 콘솔에 업로드할 때 구성된 총 테스트 수를 나타냅니다. - 권장 총 테스트 수 - 애플리케이션 리소스를 AWS Resilience Hub 기반으로 권장하는 테스트를 나타냅니다. - 제외된 총 테스트 수 - 애플리케이션에서 제외한 권장 테스트 수를 나타냅니다.	

채점 구성 요소	설명	공식	예제
경보 적용 범위 (A)	총 AWS Resilience Hub 권장 Amazon CloudWatch 경보 수 중에서 성공적으로 구현되고 제외된 Amazon CloudWatch 경보 수를 기준으로 정규화된 점수 (0~100점).  Note 복원력 점수를 계산하려면 권장 경보는 AWS Resilience Hub 가 구현된 것으로 간주할 수 있는 준비 상태여야 합니다.	$A = ((\text{Total number of alarms implemented}) + (\text{Total number of alarms excluded})) / (\text{Total number of alarms recommended})$ 공식의 일부는 다음과 같습니다. - 구성된 총 경보 수 - AWS CloudFormation 템플릿을 생성하고 AWS CloudFormation 콘솔에 업로드할 때 구성된 총 Amazon CloudWatch 경보 수를 나타냅니다. - 권장 총 경보 수 - 애플리케이션 리소스를 AWS Resilience Hub 기반으로 권장하는 Amazon CloudWatch 경보를 나타냅니다. - 제외된 총 경보 수 - 애플리케이션에서 제외한 권장 Amazon CloudWatch 경보의 수를 나타냅니다.	AWS Resilience Hub 권장 Amazon CloudWatch 경보 20개 중 10개를 구현하고 5개의 Amazon CloudWatch 경보를 제외한 경우, Amazon CloudWatch 경보의 적용 범위는 다음과 같이 계산됩니다. $A = (10 + 5) / 20$ 즉, A = .75 or 75 points

채점 구성 요소	설명	공식	예제
SOP 적용 범위 (S)	총 AWS Resilience Hub 권장 SOP 수 중 성공적으로 구현되고 제외된 SOP의 수를 기준으로 한 정규화된 점수(0~100점)입니다.	$S = ((\text{Total number of SOPs implemented}) + (\text{Total number of SOPs excluded})) / (\text{Total number of SOPs recommended})$ 공식의 일부는 다음과 같습니다. - 구성된 총 SOPs 수 - AWS CloudFormation 템플릿을 생성하고 AWS CloudFormation 콘솔에 업로드할 때 구성된 총 SOPs 수를 나타냅니다. - 권장 SOPs의 총 수 - 애플리케이션 리소스를 AWS Resilience Hub 기반으로에서 권장SOPs를 나타냅니다. - 제외된 총 SOP 수 - 애플리케이션에서 제외된 권장 SOP 수를 나타냅니다.	20개의 AWS Resilience Hub 권장 SOP 중 10개를 구현하고 5개의 SOP를 제외한 경우 SOP 적용 범위는 다음과 같이 계산됩니다. $S = (10 + 5) / 20$ 즉, $S = .75$ or 75 points

채점 구성 요소	설명	공식	예제
RTO/RPO 규정 준수 (P)	해당 복원력 정책을 충족하는 애플리케이션을 기준으로 한 정규화된 점수(0~100 점)입니다.	$P = \frac{\text{Total weights of disruption types meeting the application's resiliency policy}}{\text{Total weights of all disruption types}}$	애플리케이션 복구 정책이 가용 영역(AZ) 및 인프라 중단 유형에 대해서만 충족하는 경우 복원력 정책 점수(P)는 다음과 같이 계산됩니다. - 리전별 RTO 및 RPO 목표를 설정한 경우 P는 다음과 같이 계산됩니다. $P = (20 + 30) / 100$ 즉, $P = .5$ or 50 points - 리전별 RTO 및 RPO 대상을 설정하지 않은 경우 P는 다음과 같이 계산됩니다. $P = (22.22 + 33.33) / 99.9$ 즉, $P = .55$ or 55 points

다음 표에서는에서 전체 애플리케이션의 복원력 점수를 계산 AWS Resilience Hub 하는 데 사용하는 공식을 설명합니다.

복원력 점수를 계산하는 공식

채점 구성 요소	설명	공식	예제
애플리케이션 복원력 점수 (RS)	애플리케이션이 해당 복원력 정책을 충족하는 것을 기준으로 정규화된 복원력 점수(0~100점)입니다. 애플리케이션별 복원력 점수는 모든 권장 사항 유형의 가중 평균입니다. 즉: RS = Weighted Average (T, A, S, P)	애플리케이션별 복원력 점수는 다음 공식을 사용하여 계산됩니다: $RS = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))$	각 권장 사항 유형 테이블의 적용 범위를 계산하는 공식은 다음과 같습니다. • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 애플리케이션별 복원력 점수는 다음과 같이 계산됩니다. $RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)$ 즉, RS = .65 or 65 points

다음 표에서는가 애플리케이션 구성 요소(AppComponents) 및 중단 유형에 대한 복원력 점수를 계산 AWS Resilience Hub 하는 데 사용하는 공식을 설명합니다. 하지만 다음 AWS Resilience Hub API를 통해서만 AppComponent 및 중단 유형의 복원력 점수를 얻을 수 있습니다.

- RSo를 획득하기 위한 [DescribeAppAssessment](#)
- RSao와 RSA를 획득하기 위한 [ListAppComponentCompliances](#)

AppComponent 및 중단 유형에 대한 복원력 점수를 계산하는 공식

채점 구성 요소	설명	공식	예제
AppComponent 및 중단 유형별 복원력 점수 (RSao)	AppComponent가 중단 유형별 복원력 정책을 충족하는 것을 기준으로 한 정규화된 점수(0~100 점)입니다. AppComponent 및 중단 유형별 복원력 점수는 모든 권장 사항 유형의 가중 평균입니다. 즉: RSao = Weighted Average (T, A, S, P) T, A, S, P의 값은 모든 권장 테스트, 경보, SOP에 대해 계산되고 AppComponent의 복원력	AppComponent별 및 중단 유형별 복원력 점수는 다음 공식을 사용하여 계산됩니다. $RSao = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))$	모든 권장 사항 유형에 대한 RSao 가정은 다음과 같습니다. • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 AppComponent 및 중단 유형별 복원력 점수는 다음과 같이 계산됩니다. $RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)$

채점 구성 요소	설명	공식	예제
	정책 및 중단 유형을 충족합니다.		즉, RSao = .65 or 65 points
AppComponent별 복원력 점수 (RSa)	복원력 정책 충족을 기준으로 한 정규화된 점수(0~100 점)입니다. AppComponent당 복원력 점수는 모든 권장 사항 유형의 가중 평균입니다. 즉: RSa = Weighted Average (T, A, S, P) T, A, S, P의 값은 모든 권장 테스트, 경보, SOP에 대해 계산되고 AppComponent의 복원력 정책 충족합니다.	AppComponent당 복원력 점수는 다음 공식을 사용하여 계산됩니다. $RSa = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))$	모든 권장 사항 유형에 대한 RSa 가정은 다음과 같습니다. • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 AppComponent당 복원력 점수는 다음과 같이 계산됩니다. $RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)$ 즉, RSa = .65 or 65 points

채점 구성 요소	설명	공식	예제
중단 유형별 복원력 점수 (RSo)	복원력 정책 충족을 기준으로 한 정규화된 점수(0~100점)입니다. 중단 유형별 복원력 점수는 모든 권장 사항 유형의 가중 평균입니다. 즉: RSo = Weighted Average (T, A, S, P) T, A, S, P의 값은 모든 권장 테스트, 경보, SOP에 대해 계산되고 복원력 정책 및 중단 유형을 충족합니다.	장애 유형별 복원력 점수는 다음 공식을 사용하여 계산됩니다. $RSo = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))$	모든 권장 사항 유형에 대한 RSo 가정은 다음과 같습니다. • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 장애 유형별 복원력 점수는 다음과 같이 계산됩니다. $RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)$ 즉, RSo = .65 or 65 points

가중치

AWS Resilience Hub 는 총 복원력 점수에 대해 각 권장 유형에 가중치를 할당합니다.

다음 표에는 경보, SOPs, 회의 복원력 정책 및 중단 유형의 가중치가 나와 있습니다. 중단 유형에는 애플리케이션, 인프라, AZ 및 리전이 포함됩니다.

Note

정책에 리전 RTO 또는 RPO 대상을 정의하지 않도록 선택하면 리전이 정의되지 않은 경우 가중치 옆에 표시된 대로 다른 중단 유형의 가중치가 그에 따라 증가합니다.

경보, SOP, 테스트, 정책 목표에 대한 가중치

추천 유형	가중치
경보	20 포인트
SOP	20 포인트
테스트	20 포인트
복원력 정책충족	40 포인트

중단 유형에 대한 가중치

중단 유형	리전 정의 시 가중치	리전이 정의되지 않은 경우의 가중치
Application	40 포인트	44.44 포인트
인프라	30 포인트	33.33 포인트
가용 영역	20 포인트	22.22 포인트
리전	10 포인트	N/A

를 사용하여 애플리케이션에 운영 권장 사항 통합 AWS CloudFormation

운영 권장 사항 페이지에서 CloudFormation 템플릿 생성을 선택하면 애플리케이션의 특정 경보, 표준 운영 절차(SOP) 또는 AWS FIS 실험을 설명하는 AWS CloudFormation 템플릿을 AWS Resilience Hub 생성합니다. AWS CloudFormation 템플릿은 Amazon S3 버킷에 저장되며 운영 권장 사항 페이지의 템플릿 세부 정보 탭에서 템플릿에 대한 S3 경로를 확인할 수 있습니다.

예를 들어 아래 목록은에서 렌더링한 경보 권장 사항을 설명하는 JSON 형식 AWS CloudFormation 템플릿을 보여줍니다 AWS Resilience Hub. Employees라는 DynamoDB 테이블에 대한 읽기 제한 경보입니다.

템플릿 Resources 섹션은 DynamoDB 테이블의 읽기 제한 이벤트 수가 1을 초과할 때 활성화되는 AWS::CloudWatch::Alarm 경보를 설명합니다. 그리고 두 AWS::SSM::Parameter 리소스는 AWS Resilience Hub 가 실제 애플리케이션을 스캔할 필요 없이 설치된 리소스를 식별할 수 있도록 메타데이터를 정의합니다.

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "SNSTopicARN" : {
      "Type" : "String",
      "Description" : "The ARN of the Amazon SNS topic to which alarm status changes are to be sent. This must be in the same Region being deployed.",
      "AllowedPattern" : "^arn:(aws|aws-cn|aws-iso|aws-iso-[a-z]{1}|aws-us-gov):sns:([a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-[0-9]):[0-9]{12}:[A-Za-z0-9/][A-Za-z0-9-:/+=, @.-]{1,256}$"
    }
  },
  "Resources" : {

    "ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm" :
    {
      "Type" : "AWS::CloudWatch::Alarm",
      "Properties" : {
        "AlarmDescription" : "An Alarm by AWS Resilience Hub that alerts when the number of read-throttle events are greater than 1.",
        "AlarmName" : "ResilienceHub-ReadThrottleEventsAlarm-2020-04-01_Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9",
        "AlarmActions" : [ {
          "Ref" : "SNSTopicARN"
        } ],
        "MetricName" : "ReadThrottleEvents",
        "Namespace" : "AWS/DynamoDB",
        "Statistic" : "Sum",
        "Dimensions" : [ {
          "Name" : "TableName",
          "Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
        } ],
        "Period" : 60,
        "EvaluationPeriods" : 1,
```

```

        "DatapointsToAlarm" : 1,
        "Threshold" : 1,
        "ComparisonOperator" : "GreaterThanOrEqualToThreshold",
        "TreatMissingData" : "notBreaching",
        "Unit" : "Count"
    },
    "Metadata" : {
        "AWS::ResilienceHub::Monitoring" : {
            "recommendationId" : "dynamodb:alarm:health-read_throttle_events:2020-04-01"
        }
    }
},

"dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm"
{
    "Type" : "AWS::SSM::Parameter",
    "Properties" : {
        "Name" : "/ResilienceHub/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/dynamodb-
alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-DynamoDBTable-
PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
            "Fn::Sub" :
"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
    }
},

"dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm"
{
    "Type" : "AWS::SSM::Parameter",
    "Properties" : {
        "Name" : "/ResilienceHub/Info/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/
dynamodb-alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-
DynamoDBTable-PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
            "Fn::Sub" : "{\"alarmName\":
\\\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\\\",
\\\"referenceId\\\":\\\"dynamodb:alarm:health_read_throttle_events:2020-04-01\\\",
\\\"resourceId\\\":\\\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\\\",\\\"relatedSOPs\\\":
[\\\"dynamodb:sop:update_provisioned_capacity:2020-04-01\\\"]}"
        }
    }
},

```

```

        "Description" : "SSM Parameter for identifying installed resources."
    }
}
}
}

```

AWS CloudFormation 템플릿 수정

경보, SOP 또는 AWS FIS 리소스를 기본 애플리케이션에 통합하는 가장 쉬운 방법은 애플리케이션 템플릿을 설명하는 템플릿에 다른 리소스로 추가하는 것입니다. 아래에 제공된 JSON 형식 파일은 AWS CloudFormation 템플릿에서 DynamoDB 테이블이 설명되는 방식에 대한 기본 개요를 제공합니다. 실제 애플리케이션에는 추가 테이블과 같은 몇 가지 리소스가 더 포함될 가능성이 높습니다.

```

{
  "AWSTemplateFormatVersion": "2010-09-09T00:00:00.000Z",
  "Description": "Application Stack with Employees Table",
  "Outputs": {
    "DynamoDBTable": {
      "Description": "The DynamoDB Table Name",
      "Value": {"Ref": "Employees"}
    }
  },
  "Resources": {
    "Employees": {
      "Type": "AWS::DynamoDB::Table",
      "Properties": {
        "BillingMode": "PAY_PER_REQUEST",
        "AttributeDefinitions": [
          {
            "AttributeName": "USER_ID",
            "AttributeType": "S"
          },
          {
            "AttributeName": "RANGE_ATTRIBUTE",
            "AttributeType": "S"
          }
        ],
        "KeySchema": [
          {
            "AttributeName": "USER_ID",
            "KeyType": "HASH"
          },
          {

```

```
        "AttributeName": "RANGE_ATTRIBUTE",
        "KeyType": "RANGE"
    }
],
"PointInTimeRecoverySpecification": {
    "PointInTimeRecoveryEnabled": true
},
"Tags": [
    {
        "Key": "Key",
        "Value": "Value"
    }
],
"LocalSecondaryIndexes": [
    {
        "IndexName": "resiliencehub-index-local-1",
        "KeySchema": [
            {
                "AttributeName": "USER_ID",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "RANGE_ATTRIBUTE",
                "KeyType": "RANGE"
            }
        ],
        "Projection": {
            "ProjectionType": "ALL"
        }
    }
],
"GlobalSecondaryIndexes": [
    {
        "IndexName": "resiliencehub-index-1",
        "KeySchema": [
            {
                "AttributeName": "USER_ID",
                "KeyType": "HASH"
            }
        ],
        "Projection": {
            "ProjectionType": "ALL"
        }
    }
]
```

```

    ]
  }
}
}
}

```

경보 리소스를 애플리케이션과 함께 배포하려면 이제 하드코딩된 리소스를 애플리케이션 스택의 동적 참조로 바꿔야 합니다.

따라서 `AWS::CloudWatch::Alarm` 리소스 정의에서 다음을 변경합니다.

```
"Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
```

다음과 같이 하세요.

```
"Value" : {"Ref": "Employees"}
```

그리고 `AWS::SSM::Parameter` 리소스 정의에서 다음을 변경합니다.

```

"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededDynamoDBEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\": \"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\": \"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\", \"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"

```

다음과 같이 하세요.

```

"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\": \"dynamodb:alarm:health_read_throttle_events:2020-04-01\", \"resourceId
\": \"${Employees}\", \"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"

```

SOPs 및 AWS FIS 실험용 AWS CloudFormation 템플릿을 수정할 때 하드코딩된 참조 IDs를 하드웨어 변경 후에도 계속 작동하는 동적 참조로 대체하는 동일한 접근 방식을 취합니다.

DynamoDB 테이블에 대한 참조를 사용하여 AWS CloudFormation 가 다음을 수행하도록 허용합니다.

- 먼저 데이터베이스 테이블을 생성합니다.
- 항상 경보에서 생성된 리소스의 실제 ID를 사용하고에서 리소스를 교체해야 AWS CloudFormation 하는 경우 경보를 동적으로 업데이트합니다.

 Note

스택 [중첩 또는 별도의 스택](#)에서 리소스 출력 참조와 같이 사용하여 AWS CloudFormation 애플리케이션 리소스를 관리하기 위한 고급 방법을 선택할 수 있습니다. [AWS CloudFormation](#) (하지만 추천 스택을 기본 스택과 분리하여 유지하려면 두 스택 간에 정보를 전달하는 방법을 구성해야 합니다.)

또한 HashiCorp의 Terraform과 같은 타사 도구를 사용하여 코드형 인프라(IaC)를 프로비저닝할 수도 있습니다.

AWS Resilience Hub APIs 사용하여 애플리케이션 설명 및 관리

AWS Resilience Hub 콘솔을 사용하여 애플리케이션을 설명하고 관리하기 위한 대안으로 AWS Resilience Hub 를 사용하면 AWS Resilience Hub APIs. 이 장에서는 AWS Resilience Hub APIs를 사용하여 애플리케이션을 생성하는 방법을 설명합니다. 또한 API를 실행해야 하는 순서와 적절한 예제와 함께 제공해야 하는 파라미터 값을 정의합니다. 자세한 정보는 다음의 주제를 참조하세요.

- [the section called “애플리케이션 준비”](#)
- [the section called “애플리케이션 실행 및 분석”](#)
- [the section called “애플리케이션 수정”](#)

애플리케이션 준비

애플리케이션을 준비하려면 먼저 애플리케이션을 생성하고 복원력 정책을 할당한 다음 입력 소스에서 애플리케이션 리소스를 가져와야 합니다. 애플리케이션을 준비하는 데 사용되는 AWS Resilience Hub APIs에 대한 자세한 내용은 다음 주제를 참조하세요.

- [the section called “애플리케이션 만들기”](#)
- [the section called “복원력 정책 생성”](#)
- [the section called “애플리케이션 리소스 가져오기 및 가져오기 상태 모니터링”](#)
- [the section called “애플리케이션을 게시하고 복원력 정책을 할당합니다.”](#)

애플리케이션 생성

에서 새 애플리케이션을 생성하려면 CreateApp API를 호출하고 고유한 애플리케이션 이름을 제공해야 AWS Resilience Hub합니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html 단원을 참조하세요.

다음 예제는 CreateApp API를 사용하여 AWS Resilience Hub 에서 새 애플리케이션 newApp을 만드는 방법을 보여줍니다.

요청

```
aws resiliencehub create-app --name newApp
```

응답

```
{
  "app": {
    "appArn": "<App_ARN>",
    "name": "newApp",
    "creationTime": "2022-10-26T19:48:00.434000+03:00",
    "status": "Active",
    "complianceStatus": "NotAssessed",
    "resiliencyScore": 0.0,
    "tags": {},
    "assessmentSchedule": "Disabled"
  }
}
```

복원력 정책 생성

애플리케이션을 만든 후에는 CreateResiliencyPolicy API를 사용하여 애플리케이션의 복원력 상태를 파악할 수 있는 복원력 정책을 생성해야 합니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html 단원을 참조하세요.

다음 예제에서는 CreateResiliencyPolicy API를 AWS Resilience Hub 사용하여 애플리케이션에 newPolicy 대한를 생성하는 방법을 보여줍니다.

요청

```
aws resiliencehub create-resiliency-policy \
--policy-name newPolicy --tier NonCritical \
--policy '{"AZ": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Hardware": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Software": {"rtoInSecs": 172800,"rpoInSecs": 86400}}'
```

응답

```
{
  "policy": {
    "policyArn": "<Policy_ARN>",
    "policyName": "newPolicy",
    "policyDescription": "",

```

```

    "dataLocationConstraint": "AnyLocation",
    "tier": "NonCritical",
    "estimatedCostTier": "L1",
    "policy": {
      "AZ": {
        "rtoInSecs": 172800,
        "rpoInSecs": 86400
      },
      "Hardware": {
        "rtoInSecs": 172800,
        "rpoInSecs": 86400
      },
      "Software": {
        "rtoInSecs": 172800,
        "rpoInSecs": 86400
      }
    },
    "creationTime": "2022-10-26T20:48:05.946000+03:00",
    "tags": {}
  }
}

```

입력 소스에서 리소스 가져오기 및 가져오기 상태 모니터링

AWS Resilience Hub 는 애플리케이션에 리소스를 가져오기 위해 다음 APIs를 제공합니다.

- **ImportResourcesToDraftAppVersion** – 이 API를 사용하면 다양한 입력 소스에서 애플리케이션의 초안 버전으로 리소스를 가져올 수 있습니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html 단원을 참조하세요.
- **PublishAppVersion** – 이 API는 업데이트된 AppComponent와 함께 새 버전의 애플리케이션을 게시합니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html 단원을 참조하세요.
- **DescribeDraftAppVersionResourcesImportStatus** – 이 API를 사용하면 애플리케이션 버전으로의 리소스 가져오기 상태를 모니터링할 수 있습니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html 단원을 참조하세요.

다음 예제는 AWS Resilience Hub 에서 ImportResourcesToDraftAppVersion API를 사용하여 애플리케이션으로 리소스를 가져오는 방법을 보여줍니다.

요청

```
aws resiliencehub import-resources-to-draft-app-version \
--app-arn <App_ARN> \
--terraform-sources '["s3StateFileUrl": <S3_URI>"]'
```

응답

```
{
  "appArn": "<App_ARN>",
  "appVersion": "draft",
  "sourceArns": [],
  "status": "Pending",
  "terraformSources": [
    {
      "s3StateFileUrl": <S3_URI>
    }
  ]
}
```

다음 예제는 AWS Resilience Hub 에서 CreateAppVersionResource API를 사용하여 애플리케이션에 리소스를 수동으로 추가하는 방법을 보여줍니다.

요청

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

응답

```
{
  "appArn": "<App_ARN>",
  "appVersion": "draft",
  "physicalResource": {
    "resourceName": "backup-efs",
```

```

    "logicalResourceId": {
      "identifier": "backup-efs"
    },
    "physicalResourceId": {
      "identifier": "<Physical_resource_id_ARN>",
      "type": "Arn"
    },
    "resourceType": "AWS::EFS::FileSystem",
    "appComponents": [
      {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
      }
    ]
  }
}

```

다음 예제는 AWS Resilience Hub 에서 DescribeDraftAppVersionResourcesImportStatus API를 사용하여 리소스의 가져오기 상태를 모니터링하는 방법을 보여줍니다.

요청

```

aws resiliencehub describe-draft-app-version-resources-import-status \
--app-arn <App_ARN>

```

응답

```

{
  "appArn": "<App_ARN>",
  "appVersion": "draft",
  "status": "Success",
  "statusChangeTime": "2022-10-26T19:55:18.471000+03:00"
}

```

애플리케이션 초안 버전 게시 및 복원력 정책 할당

평가를 실행하기 전에 먼저 애플리케이션의 초안 버전을 게시하고 애플리케이션의 출시된 버전에 복원력 정책을 할당해야 합니다.

애플리케이션의 초안 버전을 게시하고 복원력 정책을 할당하려면

1. 애플리케이션의 초안 버전을 게시하려면 PublishAppVersion API를 사용합니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html 단원을 참조하세요.

다음 예제에서는 PublishAppVersion API를 AWS Resilience Hub 사용하여 애플리케이션의 초안 버전을 게시하는 방법을 보여줍니다.

요청

```
aws resiliencehub publish-app-version \  
--app-arn <App_ARN>
```

응답

```
{  
  "appArn": "<App_ARN>",  
  "appVersion": "release"  
}
```

2. UpdateApp API를 사용하여 애플리케이션의 출시된 버전에 복원력 정책을 적용합니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html 단원을 참조하세요.

다음 예제에서는 UpdateApp API를 AWS Resilience Hub 사용하여 릴리스된 애플리케이션 버전에 복원력 정책을 적용하는 방법을 보여줍니다.

요청

```
aws resiliencehub update-app \  
--app-arn <App_ARN> \  
--policy-arn <Policy_ARN>
```

응답

```
{
  "app": {
    "appArn": "<App_ARN>",
    "name": "newApp",
    "policyArn": "<Policy_ARN>",
    "creationTime": "2022-10-26T19:48:00.434000+03:00",
    "status": "Active",
    "complianceStatus": "NotAssessed",
    "resiliencyScore": 0.0,
    "tags": {
      "resourceArn": "<App_ARN>"
    },
    "assessmentSchedule": "Disabled"
  }
}
```

AWS Resilience Hub 복원력 평가 실행 및 관리

새 버전의 애플리케이션을 게시한 후에는 새 복원력 평가를 실행하고 결과를 분석하여 애플리케이션이 복원력 정책에 정의된 예상 워크로드 RTO와 예상 RPO를 충족하는지 확인해야 합니다. 평가에서는 각 애플리케이션 구성 요소 구성을 정책과 비교하고 경보, SOP 및 테스트 권장 사항을 제시합니다.

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “복원력 평가 실행 및 모니터링”](#)
- [the section called “복원력 정책 생성”](#)

AWS Resilience Hub 복원력 평가 실행 및 모니터링

에서 복원력 평가를 실행 AWS Resilience Hub 하고 상태를 모니터링하려면 다음 APIs를 사용해야 합니다.

- **StartAppAssessment** – 이 API는 애플리케이션에 대한 새 평가를 생성합니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html 단원을 참조하세요.
- **DescribeAppAssessment** – 이 API는 애플리케이션에 대한 평가를 설명하고 평가 완료 상태를 제공합니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html 단원을 참조하세요.

다음 예제는 AWS Resilience Hub 에서 StartAppAssessment API 사용 시 새 평가 실행을 시작하는 방법을 보여줍니다.

요청

```
aws resiliencehub start-app-assessment \  
--app-arn <App_ARN> \  
--app-version release \  
--assessment-name first-assessment
```

응답

```
{  
  "assessment": {  
    "appArn": "<App_ARN>",  
    "appVersion": "release",  
    "invoker": "User",  
    "assessmentStatus": "Pending",  
    "startTime": "2022-10-27T08:15:10.452000+03:00",  
    "assessmentName": "first-assessment",  
    "assessmentArn": "<Assessment_ARN>",  
    "policy": {  
      "policyArn": "<Policy_ARN>",  
      "policyName": "newPolicy",  
      "dataLocationConstraint": "AnyLocation",  
      "policy": {  
        "AZ": {  
          "rtoInSecs": 172800,  
          "rpoInSecs": 86400  
        },  
        "Hardware": {  
          "rtoInSecs": 172800,  
          "rpoInSecs": 86400  
        },  
        "Software": {  
          "rtoInSecs": 172800,  
          "rpoInSecs": 86400  
        }  
      }  
    },  
    "tags": {}  
  }  
}
```

```
}
```

다음 예제는 AWS Resilience Hub 에서 DescribeAppAssessment API 사용 시 평가 상태를 모니터링하는 방법을 보여줍니다. assessmentStatus 변수에서 평가 상태를 추출할 수 있습니다.

요청

```
aws resiliencehub describe-app-assessment \  
--assessment-arn <Assessment_ARN>
```

응답

```
{  
  "assessment": {  
    "appArn": "<App_ARN>",  
    "appVersion": "release",  
    "cost": {  
      "amount": 0.0,  
      "currency": "USD",  
      "frequency": "Monthly"  
    },  
    "resiliencyScore": {  
      "score": 0.27,  
      "disruptionScore": {  
        "AZ": 0.42,  
        "Hardware": 0.0,  
        "Region": 0.0,  
        "Software": 0.38  
      }  
    },  
    "compliance": {  
      "AZ": {  
        "achievableRtoInSecs": 0,  
        "currentRtoInSecs": 4500,  
        "currentRpoInSecs": 86400,  
        "complianceStatus": "PolicyMet",  
        "achievableRpoInSecs": 0  
      },  
      "Hardware": {  
        "achievableRtoInSecs": 0,  
        "currentRtoInSecs": 2595601,  
        "currentRpoInSecs": 2592001,  
      }  
    }  
  }  
}
```

```

        "complianceStatus": "PolicyBreached",
        "achievableRpoInSecs": 0
    },
    "Software": {
        "achievableRtoInSecs": 0,
        "currentRtoInSecs": 4500,
        "currentRpoInSecs": 86400,
        "complianceStatus": "PolicyMet",
        "achievableRpoInSecs": 0
    }
},
"complianceStatus": "PolicyBreached",
"assessmentStatus": "Success",
"startTime": "2022-10-27T08:15:10.452000+03:00",
"endTime": "2022-10-27T08:15:31.883000+03:00",
"assessmentName": "first-assessment",
"assessmentArn": "<Assessment_ARN>",
"policy": {
    "policyArn": "<Policy_ARN>",
    "policyName": "newPolicy",
    "dataLocationConstraint": "AnyLocation",
    "policy": {
        "AZ": {
            "rtoInSecs": 172800,
            "rpoInSecs": 86400
        },
        "Hardware": {
            "rtoInSecs": 172800,
            "rpoInSecs": 86400
        },
        "Software": {
            "rtoInSecs": 172800,
            "rpoInSecs": 86400
        }
    }
},
"tags": {}
}
}

```

평가 결과 검사

평가가 성공적으로 완료되면 다음 API를 사용하여 평가 결과를 검토할 수 있습니다.

- **DescribeAppAssessment** – 이 API를 사용하면 복원력 정책을 기준으로 애플리케이션의 현재 상태를 추적할 수 있습니다. 또한 `complianceStatus` 변수에서 규정 준수 상태를 추출하고 `resiliencyScore` 구조에서 각 중단 유형에 대한 복원력 점수를 추출할 수도 있습니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html 단원을 참조하세요.
- **ListAlarmRecommendations** – 이 API를 사용하면 평가의 Amazon 리소스 이름(ARN)을 사용해 경보 권장 사항을 얻을 수 있습니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html 단원을 참조하세요.

Note

SOP 및 FIS 테스트 권장 사항을 얻으려면 `ListSopRecommendations` 및 `ListTestRecommendations` API를 사용합니다.

다음 예제는 `ListAlarmRecommendations` API를 사용하는 평가의 Amazon 리소스 이름(ARN)을 사용하여 경보 권장 사항을 얻는 방법을 보여줍니다.

Note

SOP 및 FIS 테스트 권장 사항을 얻으려면 `ListSopRecommendations` 또는 `ListTestRecommendations` 중 하나로 바꿉니다.

요청

```
aws resiliencehub list-alarm-recommendations \  
--assessment-arn <Assessment_ARN>
```

응답

```
{  
  "alarmRecommendations": [  
    {  
      "recommendationId": "78ece7f8-c776-499e-baa8-b35f5e8b8ba2",  
      "referenceId": "app_common:alarm:synthetic_canary:2021-04-01",  
      "name": "AWSResilienceHub-SyntheticCanaryInRegionAlarm_2021-04-01",  
      "description": "A monitor for the entire application, configured to  
constantly verify that the application API/endpoints are available",  
    }  
  ]  
}
```

```

    "type": "Metric",
    "appComponentName": "appcommon",
    "items": [
      {
        "resourceId": "us-west-2",
        "targetAccountId": "12345678901",
        "targetRegion": "us-west-2",
        "alreadyImplemented": false
      }
    ],
    "prerequisite": "Make sure Amazon CloudWatch Synthetics is setup to monitor
the application (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/
latest/monitoring/CloudWatch_Synthetics_Canaries.html\" target=\"_blank\">docs</a>).
\nMake sure that the Synthetics Name passed in the alarm dimension matches the name of
the Synthetic Canary. It Defaults to the name of the application.\n"
  },
  {
    "recommendationId": "d9c72c58-8c00-43f0-ad5d-0c6e5332b84b",
    "referenceId": "efs:alarm:percent_io_limit:2020-04-01",
    "name": "AWSResilienceHub-EFSHighIoAlarm_2020-04-01",
    "description": "An alarm by AWS Resilience Hub that reports when Amazon EFS
I/O load is more than 90% for too much time",
    "type": "Metric",
    "appComponentName": "storageappcomponent-rlb",
    "items": [
      {
        "resourceId": "fs-0487f945c02f17b3e",
        "targetAccountId": "12345678901",
        "targetRegion": "us-west-2",
        "alreadyImplemented": false
      }
    ]
  },
  {
    "recommendationId": "09f340cd-3427-4f66-8923-7f289d4a3216",
    "referenceId": "efs:alarm:mount_failure:2020-04-01",
    "name": "AWSResilienceHub-EFSMountFailureAlarm_2020-04-01",
    "description": "An alarm by AWS Resilience Hub that reports when volume
failed to mount to EC2 instance",
    "type": "Metric",
    "appComponentName": "storageappcomponent-rlb",
    "items": [
      {
        "resourceId": "fs-0487f945c02f17b3e",

```

```

        "targetAccountId": "12345678901",
        "targetRegion": "us-west-2",
        "alreadyImplemented": false
    }
],
    "prerequisite": "* Make sure Amazon EFS utils are installed(see the <a href=\"https://github.com/aws/efs-utils#installation\" target=\"_blank\">docs</a>).\n* Make sure cloudwatch logs are enabled in efs-utils (see the <a href=\"https://github.com/aws/efs-utils#step-2-enable-cloudwatch-log-feature-in-efs-utils-config-file-etcamazonefsefs-utilsconf\" target=\"_blank\">docs</a>).\n* Make sure that you've configured `log_group_name` in `/etc/amazon/efs/efs-utils.conf`, for example: `log_group_name = /aws/efs/utils`. \n* Use the created `log_group_name` in the generated alarm. Find `LogGroupName: REPLACE_ME` in the alarm and make sure the `log_group_name` is used instead of REPLACE_ME.\n"
},
{
    "recommendationId": "b0f57d2a-1220-4f40-a585-6dab1e79cee2",
    "referenceId": "efs:alarm:client_connections:2020-04-01",
    "name": "AWSResilienceHub-EFSHighClientConnectionsAlarm_2020-04-01",
    "description": "An alarm by AWS Resilience Hub that reports when client connection number deviation is over the specified threshold",
    "type": "Metric",
    "appComponentName": "storageappcomponent-rlb",
    "items": [
        {
            "resourceId": "fs-0487f945c02f17b3e",
            "targetAccountId": "12345678901",
            "targetRegion": "us-west-2",
            "alreadyImplemented": false
        }
    ]
},
{
    "recommendationId": "15f49b10-9bac-4494-b376-705f8da252d7",
    "referenceId": "rds:alarm:health-storage:2020-04-01",
    "name": "AWSResilienceHub-RDSInstanceLowStorageAlarm_2020-04-01",
    "description": "Reports when database free storage is low",
    "type": "Metric",
    "appComponentName": "databaseappcomponent-hji",
    "items": [
        {
            "resourceId": "terraform-202206231414261158000000001",
            "targetAccountId": "12345678901",
            "targetRegion": "us-west-2",

```

```

        "alreadyImplemented": false
      }
    ]
  },
  {
    "recommendationId": "c1906101-cea8-4f77-be7b-60abb07621f5",
    "referenceId": "rds:alarm:health-connections:2020-04-01",
    "name": "AWSResilienceHub-RDSInstanceConnectionSpikeAlarm_2020-04-01",
    "description": "Reports when database connection count is anomalous",
    "type": "Metric",
    "appComponentName": "databaseappcomponent-hji",
    "items": [
      {
        "resourceId": "terraform-20220623141426115800000001",
        "targetAccountId": "12345678901",
        "targetRegion": "us-west-2",
        "alreadyImplemented": false
      }
    ]
  },
  {
    "recommendationId": "f169b8d4-45c1-4238-95d1-ecdd8d5153fe",
    "referenceId": "rds:alarm:health-cpu:2020-04-01",
    "name": "AWSResilienceHub-RDSInstanceOverUtilizedCpuAlarm_2020-04-01",
    "description": "Reports when database used CPU is high",
    "type": "Metric",
    "appComponentName": "databaseappcomponent-hji",
    "items": [
      {
        "resourceId": "terraform-20220623141426115800000001",
        "targetAccountId": "12345678901",
        "targetRegion": "us-west-2",
        "alreadyImplemented": false
      }
    ]
  },
  {
    "recommendationId": "69da8459-cbe4-4ba1-a476-80c7ebf096f0",
    "referenceId": "rds:alarm:health-memory:2020-04-01",
    "name": "AWSResilienceHub-RDSInstanceLowMemoryAlarm_2020-04-01",
    "description": "Reports when database free memory is low",
    "type": "Metric",
    "appComponentName": "databaseappcomponent-hji",
    "items": [

```

```

        {
            "resourceId": "terraform-20220623141426115800000001",
            "targetAccountId": "12345678901",
            "targetRegion": "us-west-2",
            "alreadyImplemented": false
        }
    ],
},
{
    "recommendationId": "67e7902a-f658-439e-916b-251a57b97c8a",
    "referenceId": "ecs:alarm:health-service_cpu_utilization:2020-04-01",
    "name": "AWSResilienceHub-ECSServiceHighCpuUtilizationAlarm_2020-04-01",
    "description": "An alarm by AWS Resilience Hub that triggers when CPU
utilization of ECS tasks of Service exceeds the threshold",
    "type": "Metric",
    "appComponentName": "computeappcomponent-nrz",
    "items": [
        {
            "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
            "targetAccountId": "12345678901",
            "targetRegion": "us-west-2",
            "alreadyImplemented": false
        }
    ]
},
{
    "recommendationId": "fb30cb91-1f09-4abd-bd2e-9e8ee8550eb0",
    "referenceId": "ecs:alarm:health-service_memory_utilization:2020-04-01",
    "name": "AWSResilienceHub-ECSServiceHighMemoryUtilizationAlarm_2020-04-01",
    "description": "An alarm by AWS Resilience Hub for Amazon ECS that
indicates if the percentage of memory that is used in the service, is exceeding
specified threshold limit",
    "type": "Metric",
    "appComponentName": "computeappcomponent-nrz",
    "items": [
        {
            "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
            "targetAccountId": "12345678901",
            "targetRegion": "us-west-2",
            "alreadyImplemented": false
        }
    ]
},
{

```

```

    "recommendationId": "1bd45a8e-dd58-4a8e-a628-bdbee234efed",
    "referenceId": "ecs:alarm:health-service_sample_count:2020-04-01",
    "name": "AWSResilienceHub-ECSServiceSampleCountAlarm_2020-04-01",
    "description": "An alarm by AWS Resilience Hub for Amazon ECS that triggers
if the count of tasks isn't equal Service Desired Count",
    "type": "Metric",
    "appComponentName": "computeappcomponent-nrz",
    "items": [
      {
        "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
        "targetAccountId": "12345678901",
        "targetRegion": "us-west-2",
        "alreadyImplemented": false
      }
    ],
    "prerequisite": "Make sure the Container Insights on Amazon ECS is enabled:
(see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/
deploy-container-insights-ECS-cluster.html\" target=\"_blank\">docs</a>).\"
  }
]
}

```

다음 예제는 ListAppComponentRecommendations API를 사용하여 구성 권장 사항 현재 복원력을 개선하는 방법에 대한 권장 사항)을 얻는 방법을 보여줍니다.

요청

```

aws resiliencehub list-app-component-recommendations \
--assessment-arn <Assessment_ARN>

```

응답

```

{
  "componentRecommendations": [
    {
      "appComponentName": "computeappcomponent-nrz",
      "recommendationStatus": "MetCanImprove",
      "configRecommendations": [
        {
          "cost": {
            "amount": 0.0,
            "currency": "USD",

```

```

        "frequency": "Monthly"
    },
    "appComponentName": "computeappcomponent-nrz",
    "recommendationCompliance": {
        "AZ": {
            "expectedComplianceStatus": "PolicyMet",
            "expectedRtoInSecs": 1800,
            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
            "expectedRpoInSecs": 86400,
            "expectedRpoDescription": "Based on the frequency of the
backups"
        },
        "Hardware": {
            "expectedComplianceStatus": "PolicyMet",
            "expectedRtoInSecs": 1800,
            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
            "expectedRpoInSecs": 86400,
            "expectedRpoDescription": "Based on the frequency of the
backups"
        },
        "Software": {
            "expectedComplianceStatus": "PolicyMet",
            "expectedRtoInSecs": 1800,
            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
            "expectedRpoInSecs": 86400,
            "expectedRpoDescription": "Based on the frequency of the
backups"
        }
    },
    "optimizationType": "LeastCost",
    "description": "Current Configuration",
    "suggestedChanges": [],
    "haArchitecture": "BackupAndRestore",
    "referenceId": "original"
},
{
    "cost": {
        "amount": 0.0,
        "currency": "USD",
        "frequency": "Monthly"
    },

```

```

    "appComponentName": "computeappcomponent-nrz",
    "recommendationCompliance": {
      "AZ": {
        "expectedComplianceStatus": "PolicyMet",
        "expectedRtoInSecs": 1800,
        "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
        "expectedRpoInSecs": 86400,
        "expectedRpoDescription": "Based on the frequency of the
backups"
      },
      "Hardware": {
        "expectedComplianceStatus": "PolicyMet",
        "expectedRtoInSecs": 1800,
        "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
        "expectedRpoInSecs": 86400,
        "expectedRpoDescription": "Based on the frequency of the
backups"
      },
      "Software": {
        "expectedComplianceStatus": "PolicyMet",
        "expectedRtoInSecs": 1800,
        "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
        "expectedRpoInSecs": 86400,
        "expectedRpoDescription": "Based on the frequency of the
backups"
      }
    },
    "optimizationType": "LeastChange",
    "description": "Current Configuration",
    "suggestedChanges": [],
    "haArchitecture": "BackupAndRestore",
    "referenceId": "original"
  },
  {
    "cost": {
      "amount": 14.74,
      "currency": "USD",
      "frequency": "Monthly"
    },
    "appComponentName": "computeappcomponent-nrz",
    "recommendationCompliance": {

```

```

    "AZ": {
      "expectedComplianceStatus": "PolicyMet",
      "expectedRtoInSecs": 0,
      "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 in multiple AZs and CapacityProviders with
MinSize > 1",
      "expectedRpoInSecs": 0,
      "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
    },
    "Hardware": {
      "expectedComplianceStatus": "PolicyMet",
      "expectedRtoInSecs": 0,
      "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 and CapacityProviders with MinSize > 1",
      "expectedRpoInSecs": 0,
      "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
    },
    "Software": {
      "expectedComplianceStatus": "PolicyMet",
      "expectedRtoInSecs": 1800,
      "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
      "expectedRpoInSecs": 86400,
      "expectedRpoDescription": "Based on the frequency of the
backups"
    }
  },
  "optimizationType": "BestAZRecovery",
  "description": "Stateful Amazon ECS service with launch type Amazon
EC2 and Amazon EFS storage, deployed in multiple AZs. AWS Backup is used to backup
Amazon EFS and copy snapshots in-Region.",
  "suggestedChanges": [
    "Add AWS Auto Scaling Groups and Capacity Providers in multiple
AZs",
    "Change desired count of the setup",
    "Remove Amazon EBS volume"
  ],
  "haArchitecture": "BackupAndRestore",
  "referenceId": "ecs:config:ec2-multi_az-efs-backups:2022-02-16"
}

```

```

    ]
  },
  {
    "appComponentName": "databaseappcomponent-hji",
    "recommendationStatus": "MetCanImprove",
    "configRecommendations": [
      {
        "cost": {
          "amount": 0.0,
          "currency": "USD",
          "frequency": "Monthly"
        },
        "appComponentName": "databaseappcomponent-hji",
        "recommendationCompliance": {
          "AZ": {
            "expectedComplianceStatus": "PolicyMet",
            "expectedRtoInSecs": 1800,
            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
            "expectedRpoInSecs": 86400,
            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary).",
            "Hardware": {
              "expectedComplianceStatus": "PolicyMet",
              "expectedRtoInSecs": 1800,
              "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
              "expectedRpoInSecs": 86400,
              "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary).",
              "Software": {
                "expectedComplianceStatus": "PolicyMet",
                "expectedRtoInSecs": 1800,
                "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                "expectedRpoInSecs": 86400,

```

```

        "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
```

},

```

    },
    "optimizationType": "LeastCost",
    "description": "Current Configuration",
    "suggestedChanges": [],
    "haArchitecture": "BackupAndRestore",
    "referenceId": "original"
  },
  {
    "cost": {
      "amount": 0.0,
      "currency": "USD",
      "frequency": "Monthly"
    },
    "appComponentName": "databaseappcomponent-hji",
    "recommendationCompliance": {
      "AZ": {
        "expectedComplianceStatus": "PolicyMet",
        "expectedRtoInSecs": 1800,
        "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
        "expectedRpoInSecs": 86400,
        "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
```

},

```

      "Hardware": {
        "expectedComplianceStatus": "PolicyMet",
        "expectedRtoInSecs": 1800,
        "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
        "expectedRpoInSecs": 86400,
        "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
```

},

```

      "Software": {
        "expectedComplianceStatus": "PolicyMet",
        "expectedRtoInSecs": 1800,
```

```

        "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
        "expectedRpoInSecs": 86400,
        "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary).",
    },
    },
    "optimizationType": "LeastChange",
    "description": "Current Configuration",
    "suggestedChanges": [],
    "haArchitecture": "BackupAndRestore",
    "referenceId": "original"
},
{
    "cost": {
        "amount": 76.73,
        "currency": "USD",
        "frequency": "Monthly"
    },
    "appComponentName": "databaseappcomponent-hji",
    "recommendationCompliance": {
        "AZ": {
            "expectedComplianceStatus": "PolicyMet",
            "expectedRtoInSecs": 120,
            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
            "expectedRpoInSecs": 0,
            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
        },
        "Hardware": {
            "expectedComplianceStatus": "PolicyMet",
            "expectedRtoInSecs": 120,
            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
            "expectedRpoInSecs": 0,
            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
        },
        "Software": {
            "expectedComplianceStatus": "PolicyMet",
            "expectedRtoInSecs": 900,

```

```

        "expectedRtoDescription": "Estimate time to backtrack to a
stable state.",
        "expectedRpoInSecs": 300,
        "expectedRpoDescription": "Estimate for latest restorable
time for point in time recovery."
    }
},
"optimizationType": "BestAZRecovery",
"description": "Aurora database cluster with one read replica, with
backtracking window of 24 hours.",
"suggestedChanges": [
    "Add read replica in the same Region",
    "Change DB instance to a supported class (db.t3.small)",
    "Change to Aurora",
    "Enable cluster backtracking",
    "Enable instance backup with retention period 7"
],
"haArchitecture": "WarmStandby",
"referenceId": "rds:config:aurora-backtracking"
}
]
},
{
    "appComponentName": "storageappcomponent-rlb",
    "recommendationStatus": "BreachedUnattainable",
    "configRecommendations": [
        {
            "cost": {
                "amount": 0.0,
                "currency": "USD",
                "frequency": "Monthly"
            },
            "appComponentName": "storageappcomponent-rlb",
            "recommendationCompliance": {
                "AZ": {
                    "expectedComplianceStatus": "PolicyMet",
                    "expectedRtoInSecs": 0,
                    "expectedRtoDescription": "No data loss in your system",
                    "expectedRpoInSecs": 0,
                    "expectedRpoDescription": "No data loss in your system"
                },
                "Hardware": {
                    "expectedComplianceStatus": "PolicyBreached",
                    "expectedRtoInSecs": 2592001,

```

```

        "expectedRtoDescription": "No recovery option configured",
        "expectedRpoInSecs": 2592001,
        "expectedRpoDescription": "No recovery option configured"
    },
    "Software": {
        "expectedComplianceStatus": "PolicyMet",
        "expectedRtoInSecs": 900,
        "expectedRtoDescription": "Time to recover Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
        "expectedRpoInSecs": 86400,
        "expectedRpoDescription": "Recovery Point Objective for
Amazon EFS from backups, derived from backup frequency"
    }
},
"optimizationType": "BestAZRecovery",
"description": "Amazon EFS with backups configured",
"suggestedChanges": [
    "Add additional availability zone"
],
"haArchitecture": "MultiSite",
"referenceId": "efs:config:with_backups:2020-04-01"
},
{
    "cost": {
        "amount": 0.0,
        "currency": "USD",
        "frequency": "Monthly"
    },
    "appComponentName": "storageappcomponent-rlb",
    "recommendationCompliance": {
        "AZ": {
            "expectedComplianceStatus": "PolicyMet",
            "expectedRtoInSecs": 0,
            "expectedRtoDescription": "No data loss in your system",
            "expectedRpoInSecs": 0,
            "expectedRpoDescription": "No data loss in your system"
        },
        "Hardware": {
            "expectedComplianceStatus": "PolicyBreached",
            "expectedRtoInSecs": 2592001,
            "expectedRtoDescription": "No recovery option configured",
            "expectedRpoInSecs": 2592001,
            "expectedRpoDescription": "No recovery option configured"
        }
    }
},

```

```

        "Software": {
            "expectedComplianceStatus": "PolicyMet",
            "expectedRtoInSecs": 900,
            "expectedRtoDescription": "Time to recover Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
            "expectedRpoInSecs": 86400,
            "expectedRpoDescription": "Recovery Point Objective for
Amazon EFS from backups, derived from backup frequency"
        },
        "optimizationType": "BestAttainable",
        "description": "Amazon EFS with backups configured",
        "suggestedChanges": [
            "Add additional availability zone"
        ],
        "haArchitecture": "MultiSite",
        "referenceId": "efs:config:with_backups:2020-04-01"
    }
}
]
}
}

```

애플리케이션 수정

AWS Resilience Hub 를 사용하면 애플리케이션의 초안 버전을 편집하고 변경 사항을 새(게시된) 버전에 게시하여 애플리케이션 리소스를 수정할 수 있습니다. AWS Resilience Hub 는 복원력 평가를 실행하기 위해 업데이트된 리소스가 포함된 애플리케이션의 게시된 버전을 사용합니다.

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “리소스를 수동으로 추가합니다.”](#)
- [the section called “리소스를 단일 애플리케이션 구성 요소로 그룹화”](#)
- [the section called “AppComponent에서 리소스 제외하기”](#)

애플리케이션에 리소스 수동 추가

리소스가 입력 소스의 일부로 배포되지 않은 경우 CreateAppVersionResource API AWS Resilience Hub 를 사용하여 애플리케이션에 리소스를 수동으로 추가할 수 있습니다. 이 API

에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html 단원을 참조하세요.

다음 파라미터를 이 API에 입력해야 합니다.

- 애플리케이션의 Amazon 리소스 이름(ARN)입니다.
- 리소스의 논리적 ID
- 리소스의 물리적 ID
- AWS CloudFormation 유형

다음 예제는 AWS Resilience Hub 에서 CreateAppVersionResource API를 사용하여 애플리케이션에 리소스를 수동으로 추가하는 방법을 보여줍니다.

요청

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

응답

```
{
  "appArn": "<App_ARN>",
  "appVersion": "draft",
  "physicalResource": {
    "resourceName": "backup-efs",
    "logicalResourceId": {
      "identifier": "backup-efs"
    },
    "physicalResourceId": {
      "identifier": "<Physical_resource_id_ARN>",
      "type": "Arn"
    },
    "resourceType": "AWS::EFS::FileSystem",
    "appComponents": [
      {
```

```

        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
]
}
}

```

리소스를 단일 애플리케이션 구성 요소로 그룹화

Application Component(AppComponent)는 단일 단위로 작동하고 실패하는 관련 AWS 리소스 그룹입니다. 예를 들어, 대기 배포로 사용되는 리전 간 워크로드가 있는 경우, AWS Resilience Hub에는 어떤 AWS 리소스가 어떤 유형의 AppComponent에 속할 수 있는지에 대한 규칙이 있습니다.는 다음 리소스 관리 APIs를 사용하여 리소스를 단일 AppComponent로 그룹화할 수 있도록 AWS Resilience Hub 허용합니다.

- **UpdateAppVersionResource** – 이 API는 애플리케이션의 리소스 세부 정보를 업데이트합니다. 이 API에 대한 자세한 내용은 [UpdateAppVersionResource](#) 단원을 참조하세요.
- **DeleteAppVersionAppComponent** – 이 API는 애플리케이션에서 AppComponent를 삭제합니다. 이 API에 대한 자세한 내용은 [DeleteAppVersionAppComponent](#) 단원을 참조하세요.

다음 예제에서는 DeleteAppVersionAppComponent API를 AWS Resilience Hub 사용하여 애플리케이션의 리소스 세부 정보를 업데이트하는 방법을 보여줍니다.

요청

```

aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component

```

응답

```

{
  "appArn": "<App_ARN>",
  "appVersion": "draft",
  "AppComponent": {
    "name": "new-app-component",
    "type": "AWS::ResilienceHub::StorageAppComponent",
    "id": "new-app-component"
  }
}

```

```
}
}
```

다음 예제에서는 UpdateAppVersionResource API를 AWS Resilience Hub 사용하여 이전 예제에서 생성된 빈 AppComponent를 삭제하는 방법을 보여줍니다.

요청

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component
```

응답

```
{
  "appArn": "<App_ARN>",
  "appVersion": "draft",
  "appComponent": {
    "name": "new-app-component",
    "type": "AWS::ResilienceHub::StorageAppComponent",
    "id": "new-app-component"
  }
}
```

AppComponent에서 리소스 제외하기

AWS Resilience Hub 를 사용하면 UpdateAppVersionResource API를 사용하여 평가에서 리소스를 제외할 수 있습니다. 애플리케이션의 복원력을 계산할 때는 이러한 리소스가 고려되지 않습니다. 이 API에 대한 자세한 내용은 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html 단원을 참조하세요.

Note

입력 소스에서 가져온 리소스만 제외할 수 있습니다.

다음 예제는 AWS Resilience Hub 에서 UpdateAppVersionResource API를 사용할 때 애플리케이션의 리소스를 제외하는 방법을 보여줍니다.

요청

```
aws resiliencehub update-app-version-resource \  
--app-arn <App_ARN> \  
--resource-name "ec2instance-nvz" \  
--excluded
```

응답

```
{  
  "appArn": "<App_ARN>",  
  "appVersion": "draft",  
  "physicalResource": {  
    "resourceName": "ec2instance-nvz",  
    "logicalResourceId": {  
      "identifier": "ec2",  
      "terraformSourceName": "test.state.file"  
    },  
    "physicalResourceId": {  
      "identifier": "i-0b58265a694e5ffc1",  
      "type": "Native",  
      "awsRegion": "us-west-2",  
      "awsAccountId": "123456789101"  
    },  
    "resourceType": "AWS::EC2::Instance",  
    "appComponents": [  
      {  
        "name": "computeappcomponent-nrz",  
        "type": "AWS::ResilienceHub::ComputeAppComponent"  
      }  
    ]  
  }  
}
```

의 보안 AWS Resilience Hub

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. [공동 책임 모델](#)은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 규정 [AWS 준수 프로그램](#) 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 [AWS 제공 범위 내 서비스 규정 준수 프로그램](#) 제공 범위 내 서비스를 AWS Resilience Hub 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다 AWS Resilience Hub. 다음 주제에서는 보안 및 규정 준수 목표를 충족 AWS Resilience Hub 하도록 구성하는 방법을 보여줍니다. 또한 AWS Resilience Hub 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

내용

- [의 데이터 보호 AWS Resilience Hub](#)
- [AWS Resilience Hub의 자격 증명 및 액세스 관리](#)
- [의 인프라 보안 AWS Resilience Hub](#)

의 데이터 보호 AWS Resilience Hub

AWS [공동 책임 모델](#)의 데이터 보호에 적용됩니다 AWS Resilience Hub. 이 모델에 설명된 대로 AWS 는 모든 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시 FAQ](#)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 [AWS 공동 책임 모델 및 GDPR](#) 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [CloudTrail 추적 작업을](#) 참조하세요.
- AWS 암호화 솔루션과 내부의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [Federal Information Processing Standard\(FIPS\) 140-3](#)을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Resilience Hub 또는 기타 AWS 서비스 에서 콘솔, API, AWS CLI 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

저장된 데이터 암호화

AWS Resilience Hub 는 저장 데이터를 암호화합니다. 의 데이터는 투명한 서버 측 암호화를 사용하여 저장 시 암호화 AWS Resilience Hub 됩니다. 이를 사용하면 중요한 데이터 보호와 관련된 운영 부담 및 복잡성을 줄일 수 있습니다. 유틸리티 암호화를 사용하면 암호화 규정 준수 및 규제 요구 사항이 필요한, 보안에 민감한 애플리케이션을 구축할 수 있습니다.

전송 중 암호화

AWS Resilience Hub 는 서비스와 기타 통합 AWS 서비스 간에 전송 중인 데이터를 암호화합니다. AWS Resilience Hub 와 통합 서비스 간에 전달되는 모든 데이터는 TLS(전송 계층 보안)를 사용하여 암호화됩니다.는 AWS 서비스 전반의 특정 유형의 대상에 대해 사전 구성된 작업을 AWS Resilience Hub 제공하고 대상 리소스에 대한 작업을 지원합니다.

AWS Resilience Hub의 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와주는입니다. IAM 관리자는 AWS Resilience Hub 리소스를 사용할 수 있는 인증(로그인) 및 권한 부여(권한 있음)를 받을 수 있는 사용자를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는입니다.

주제

- [대상](#)
- [ID를 통한 인증](#)
- [정책을 사용하여 액세스 관리](#)
- [AWS Resilience Hub와 IAM의 작동 방식](#)
- [IAM 역할 및 권한 설정](#)
- [AWS Resilience Hub 자격 증명 및 액세스 문제 해결](#)
- [AWS Resilience Hub 액세스 권한 참조](#)
- [AWS 에 대한 관리형 정책 AWS Resilience Hub](#)
- [AWS Resilience Hub 페르소나 및 IAM 권한 참조](#)
- [로 Terraform 상태 파일 가져오기 AWS Resilience Hub](#)
- [Amazon Elastic Kubernetes Service 클러스터에 대한 AWS Resilience Hub 액세스 활성화](#)
- [Amazon Simple Notification Service 주제에 AWS Resilience Hub 게시하도록 활성화](#)
- [AWS Resilience Hub 권장 사항을 포함하거나 제외할 수 있는 권한 제한](#)

대상

사용 방법 AWS Identity and Access Management (IAM)은 AWS Resilience Hub에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - AWS Resilience Hub 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 AWS Resilience Hub 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. AWS Resilience Hub의 기능에 액세스할 수 없는 경우 섹션을 참조하세요 [AWS Resilience Hub 자격 증명 및 액세스 문제 해결](#).

서비스 관리자 - 회사에서 AWS Resilience Hub 리소스를 책임지고 있는 경우 AWS Resilience Hub에 대한 전체 액세스 권한이 있을 수 있습니다. 서비스 사용자가 액세스해야 하는 AWS Resilience Hub 기능과 리소스를 결정하는 것은 사용자의 작업입니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 AWS Resilience Hub에서 IAM을 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [AWS Resilience Hub와 IAM의 작동 방식](#).

IAM 관리자 - IAM 관리자인 경우 AWS Resilience Hub에 대한 액세스를 관리하는 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다. IAM에서 사용할 수 있는 AWS Resilience Hub 자격 증명 기반 정책 예제를 보려면 섹션을 참조하세요 [AWS Resilience Hub의 자격 증명 기반 정책 예제](#).

ID를 통한 인증

인증은 자격 증명 AWS 으로 로그인하는 방법입니다. IAM 사용자 또는 AWS 계정 루트 사용자 IAM 역할을 수임하여 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. [AWS 계정](#)

AWS 프로그래밍 방식으로 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 [API 요청용AWS Signature Version 4](#)를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 다중 인증(MFA)을 사용하여 계정의 보안을 강화할 것을 AWS 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 [다중 인증](#) 및 IAM 사용 설명서에서 [IAM의AWS 다중 인증](#)을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 테루트 사용자라고 하며 계정을 생성하

는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 [루트 사용자 보안 인증이 필요한 작업](#)을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스할 때 역할을 AWS 계정수입하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 자격 증명 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 [IAM Identity Center란 무엇인가요?](#)를 참조하세요.

IAM 사용자 및 그룹

[IAM 사용자](#)는 한 사람 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 가능하다면 암호 및 액세스 키와 같은 장기 자격 증명에 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명에 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체](#)를 참조하세요.

[IAM 그룹](#)은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수입할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 [IAM 사용자 사용 사례](#)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수입하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console 수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 사용하여 역할을 수입할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 [역할 수입 방법](#)을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- **페더레이션 사용자 액세스** - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 [Create a role for a third-party identity provider \(federation\)](#)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [권한 집합](#)을 참조하세요.
- **임시 IAM 사용자 권한** - IAM 사용자 또는 역할은 IAM 역할을 수입하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- **교차 계정 액세스** - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부에서는 (역할을 프록시로 사용하는 대신) 정책을 리소스에 직접 연결할 AWS 서비스 수 있습니다. 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 [IAM의 교차 계정 리소스 액세스](#)를 참조하세요.
- **교차 서비스 액세스** - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
- **전달 액세스 세션(FAS)** - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와 의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [전달 액세스 세션](#)을 참조하세요.

- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 [IAM 역할](#)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [Create a role to delegate permissions to an AWS 서비스](#)를 참조하세요.
- 서비스 연결 역할 - 서비스 연결 역할은 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여](#)를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 [JSON 정책 개요](#)를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, iam:GetRole 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지

를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 [고객 관리형 정책으로 사용자 지정 IAM 권한 정의](#)를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다. AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 [관리형 정책 및 인라인 정책 중에서 선택](#)을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [위탁자를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF 및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 [액세스 제어 목록\(ACL\) 개요](#)를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. Principal 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포

함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 [IAM 엔티티에 대한 권한 경계](#)를 참조하세요.

- 서비스 제어 정책(SCPs) - SCPs는 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여려를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔티티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 [Service control policies](#)을 참조하세요.
- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [리소스 제어 정책\(RCPs\)](#)을 참조하세요.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 [세션 정책](#)을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 가 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 [정책 평가 로직](#)을 참조하세요.

AWS Resilience Hub와 IAM의 작동 방식

IAM을 사용하여 AWS Resilience Hub에 대한 액세스를 관리하기 전에 AWS Resilience Hub에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

AWS Resilience Hub와 함께 사용할 수 있는 IAM 기능

IAM 기능	AWS Resilience Hub 지원
ID 기반 정책	예

IAM 기능	AWS Resilience Hub 지원
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC(정책 내 태그)	부분
임시 자격 증명	예
전달 액세스 세션(FAS)	예
서비스 역할	예

AWS Resilience Hub 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방식을 전체적으로 알아보려면 IAM 사용 설명서의 [AWS IAM으로 작업하는 서비스를](#) 참조하세요.

AWS Resilience Hub에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 [고객 관리형 정책으로 사용자 지정 IAM 권한 정의](#)를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 [IAM JSON 정책 요소 참조](#)를 참조하세요.

AWS Resilience Hub의 자격 증명 기반 정책 예제

AWS Resilience Hub 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS Resilience Hub의 자격 증명 기반 정책 예제](#).

AWS Resilience Hub 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [위탁자를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 있는 계정에 있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 [교차 계정 리소스 액세스](#)를 참조하세요.

AWS Resilience Hub에 대한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

AWS Resilience Hub 작업 목록을 보려면 서비스 승인 참조의 [AWS Resilience Hub에서 정의한 작업을](#) 참조하세요.

AWS Resilience Hub의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
resiliencehub
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
  "resiliencehub:action1",
  "resiliencehub:action2"
]
```

AWS Resilience Hub 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS Resilience Hub의 자격 증명 기반 정책 예제](#).

AWS Resilience Hub에 대한 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 [Amazon 리소스 이름\(ARN\)](#)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"

```

AWS Resilience Hub 리소스 유형 및 해당 ARNs의 목록을 보려면 서비스 승인 참조의 [AWS Resilience Hub에서 정의한 리소스](#)를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 [AWS Resilience Hub에서 정의한 작업](#)을 참조하세요.

AWS Resilience Hub 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS Resilience Hub의 자격 증명 기반 정책 예제](#).

AWS Resilience Hub의 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Condition 요소(또는 Condition 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. Condition 요소는 옵션입니다. 같거나 작음과 같은 [조건 연산자](#)를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition 요소를 지정하거나 단일 Condition 요소에서 여러 키를 지정하는 경우, AWS는 논리적 AND 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 OR 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [IAM 정책 요소: 변수 및 태그](#)를 참조하세요.

AWS는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 [AWS 전역 조건 컨텍스트 키](#)를 참조하세요.

AWS Resilience Hub 조건 키 목록을 보려면 서비스 권한 부여 참조의 [AWS Resilience Hub에 사용되는 조건 키](#)를 참조하세요. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 [AWS Resilience Hub에서 정의한 작업을](#) 참조하세요.

AWS Resilience Hub 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS Resilience Hub의 자격 증명 기반 정책 예제](#).

AWS Resilience Hub ACLs

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

AWS Resilience Hub를 사용한 ABAC

ABAC 지원(정책의 태그): 부분적

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다.에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할)와 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 [조건 요소](#)에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 [ABAC 권한 부여를 통한 권한 정의](#)를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 [속성 기반 액세스 제어\(ABAC\) 사용](#)을 참조하세요.

AWS Resilience Hub에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인할 때 일부 AWS 서비스 가 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 비롯한 자세한 내용은 [AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는](#)를 참조하세요.

사용자 이름과 암호를 제외한 방법을 AWS Management Console 사용하여 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 [사용자에서 IAM 역할로 전환\(콘솔\)](#)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신에 임시 자격 증명을 동적으로 생성하는 `access AWS`. AWS recommends에 액세스할 수 있습니다. 자세한 정보는 [IAM의 임시 보안 자격 증명](#) 섹션을 참조하세요.

AWS Resilience Hub에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS를 호

출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스 함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [전달 액세스 세션](#)을 참조하세요.

AWS Resilience Hub의 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 [IAM 역할](#)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [Create a role to delegate permissions to an AWS 서비스](#)를 참조하세요.

Warning

서비스 역할에 대한 권한을 변경하면 AWS Resilience Hub 기능이 중단될 수 있습니다. AWS Resilience Hub가 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

AWS Resilience Hub의 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 AWS Resilience Hub 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성\(콘솔\)](#)을 참조하세요.

각 리소스 유형에 대한 ARNs 형식을 포함하여 AWS Resilience Hub에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 [AWS Resilience Hub에 사용되는 작업, 리소스 및 조건 키](#)를 참조하세요.

주제

- [정책 모범 사례](#)
- [AWS Resilience Hub 콘솔 사용](#)
- [사용자가 자신의 고유한 권한을 볼 수 있도록 허용](#)

- [사용 가능한 AWS Resilience Hub 애플리케이션 나열](#)
- [애플리케이션 평가 시작](#)
- [애플리케이션 평가 삭제](#)
- [특정 애플리케이션에 대한 권장 사항 템플릿 생성](#)
- [특정 애플리케이션에 대한 권장 사항 템플릿 삭제](#)
- [특정 복원력 정책으로 애플리케이션 업데이트](#)

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 AWS Resilience Hub 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 [AWS 관리형 정책](#) 또는 [AWS 직무에 대한 관리형 정책](#)을 참조하세요.
- 최소 권한 적용 - IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 [IAM의 정책 및 권한](#)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 조건을 사용하여 AWS 서비스와 같은 특징을 통해 사용되는 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 [IAM Access Analyzer에서 정책 검증](#)을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정칩니다. API 작업을 직접 호출할 때 MFA가 필요하다면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 [MFA를 통한 보안 API 액세스](#)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 [IAM의 보안 모범 사례](#)를 참조하세요.

AWS Resilience Hub 콘솔 사용

AWS Resilience Hub 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해에서 AWS Resilience Hub 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API에만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 여전히 AWS Resilience Hub 콘솔을 사용할 수 있도록 하려면 AWS Resilience Hub *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책을 엔티티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 [사용자에게 권한 추가](#)를 참조하세요.

다음 정책은 사용자에게 AWS Resilience Hub 콘솔의 모든 리소스를 나열하고 볼 수 있는 권한을 부여하지만 생성, 업데이트 또는 삭제할 수 있는 권한은 부여하지 않습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resiliencehub:List*",
        "resiliencehub:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}

```

사용 가능한 AWS Resilience Hub 애플리케이션 나열

다음 정책은 사용자에게 사용 가능한 AWS Resilience Hub 애플리케이션을 나열할 수 있는 권한을 부여합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:ListApps"
      ]
    }
  ]
}

```

```

    ],
    "Resource": [
        "*"
    ]
  }
]
}

```

애플리케이션 평가 시작

다음 정책은 사용자에게 특정 AWS Resilience Hub 애플리케이션에 대한 평가를 시작할 수 있는 권한을 부여합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:StartAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}

```

애플리케이션 평가 삭제

다음 정책은 사용자에게 특정 AWS Resilience Hub 애플리케이션에 대한 평가를 삭제할 수 있는 권한을 부여합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
        "resiliencehub>DeleteAppAssessment"
      ],

```

```

    "Resource": [
      "arn:aws:resiliencehub:*:*:app/appId"
    ]
  }
]
}

```

특정 애플리케이션에 대한 권장 사항 템플릿 생성

다음 정책은 사용자에게 특정 AWS Resilience Hub 애플리케이션에 대한 권장 사항 템플릿을 생성할 수 있는 권한을 부여합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:CreateRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}

```

특정 애플리케이션에 대한 권장 사항 템플릿 삭제

다음 정책은 사용자에게 특정 AWS Resilience Hub 애플리케이션에 대한 권장 사항 템플릿을 삭제할 수 있는 권한을 부여합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
        "resiliencehub>DeleteRecommendationTemplate"
      ],
      "Resource": [

```

```

        "arn:aws:resiliencehub:*:*:app/appId"
    ]
}
]
}

```

특정 복원력 정책으로 애플리케이션 업데이트

다음 정책은 사용자에게 특정 복원력 정책으로 AWS Resilience Hub 애플리케이션을 업데이트할 수 있는 권한을 부여합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:UpdateApp"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ],
      "Condition": {
        "StringLike": { "resiliencehub:policyArn" : "arn:aws:resiliencehub:us-
west-2:111122223333:resiliency-policy/*" }
      }
    }
  ]
}

```

IAM 역할 및 권한 설정

AWS Resilience Hub 를 사용하면 애플리케이션에 대한 평가를 실행하는 동안 사용할 IAM 역할을 구성할 수 있습니다. 애플리케이션 리소스에 대한 읽기 전용 액세스 권한을 얻도록 AWS Resilience Hub 을 구성하는 방법은 여러 가지가 있습니다. 그러나 AWS Resilience Hub 은 다음 방법을 권장합니다.

- 역할 기반 액세스 -이 역할은 현재 계정에서 정의되고 사용됩니다. AWS Resilience Hub 는이 역할을 수입하여 애플리케이션의 리소스에 액세스합니다.

역할 기반 액세스를 제공하려면 역할에 다음이 포함되어야 합니다.

- 리소스를 읽을 수 있는 읽기 전용 권한
(AWSResilienceHubAssessmentExecutionPolicy관리형 정책을 사용하는 것이AWS Resilience Hub 좋습니다).
- 이 역할을 수입하는 신뢰 정책으로, AWS Resilience Hub 서비스 보안 주체가이 역할을 수입할 수 있습니다. 계정에 이러한 역할이 구성되어 있지 않은 경우 AWS Resilience Hub 는 해당 역할을 생성하는 지침을 표시합니다. 자세한 내용은 [the section called “권한 설정”](#) 단원을 참조하십시오.

Note

호출자 역할 이름만 제공하고 리소스가 다른 계정에 있는 경우 AWS Resilience Hub 는 다른 계정의이 역할 이름을 사용하여 교차 계정 리소스에 액세스합니다. 선택적으로 간접 호출자 역할 이름 대신 사용될 다른 계정의 역할 ARN을 구성할 수 있습니다.

- 현재 IAM 사용자 액세스 — AWS Resilience Hub 가 현재 IAM 사용자를 사용하여 애플리케이션 리소스에 액세스합니다. 리소스가 다른 계정에 있는 경우 AWS Resilience Hub 는 리소스에 액세스하기 위해 다음 IAM 역할을 수입합니다.
- 현재 계정에서 AwsResilienceHubAdminAccountRole
- 다른 계정에서 AwsResilienceHubExecutorAccountRole

또한 예약된 평가를 구성하면가 AwsResilienceHubPeriodicAssessmentRole 역할을 수 AWS Resilience Hub 임합니다. 그러나 역할 및 권한을 수동으로 구성해야 하고 일부 기능(예: 드리프트 알림)AwsResilienceHubPeriodicAssessmentRole이 예상대로 작동하지 않을 수 있으므로 사용하는 것은 권장되지 않습니다.

AWS Resilience Hub 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 AWS Resilience Hub 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- [AWS Resilience Hub에서 작업을 수행할 권한이 없음](#)
- [iam:PassRole을 수행하도록 인증되지 않음](#)
- [내 외부의 사람이 내 AWS Resilience Hub 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.](#)

AWS Resilience Hub에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 resiliencehub:*GetWidget* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
resiliencehub:GetWidget on resource: my-example-widget
```

이 경우, resiliencehub:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

iam:PassRole 작업을 수행할 권한이 없다는 오류가 수신되면 AWS Resilience Hub에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 AWS Resilience Hub에서 작업을 수행하려고 marymajor 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 AWS Resilience Hub 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제

어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- AWS Resilience Hub가 이러한 기능을 지원하는지 여부를 알아보려면 섹션을 참조하세요 [AWS Resilience Hub와 IAM의 작동 방식](#).
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 [IAM 사용 설명서의 소유 AWS 계정 한 다른의 IAM 사용자에게 액세스 권한 제공을 참조하세요](#).
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [타사 AWS 계정 소유에 대한 액세스 권한 제공](#)을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [외부에서 인증된 사용자에게 액세스 권한 제공\(ID 페더레이션\)](#)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 [IAM의 크로스 계정 리소스 액세스](#)를 참조하세요.

AWS Resilience Hub 액세스 권한 참조

AWS Identity and Access Management (IAM)을 사용하여 애플리케이션 리소스에 대한 액세스를 관리하고 사용자, 그룹 또는 역할에 적용되는 IAM 정책을 생성할 수 있습니다.

모든 AWS Resilience Hub 애플리케이션은 [the section called “간접 호출자 역할”](#) (IAM 역할)을 사용하거나 현재 IAM 사용자 권한(교차 계정 및 예약된 평가를 위한 사전 정의된 역할 세트와 함께)을 사용하도록 구성할 수 있습니다. 이 역할에서는가 다른 AWS 리소스 또는 애플리케이션 리소스에 액세스하는 AWS Resilience Hub 데 필요한 권한을 정의하는 정책을 연결할 수 있습니다. 호출자 역할에는 AWS Resilience Hub Service Principal에 추가된 신뢰 정책이 있어야 합니다.

애플리케이션에 대한 권한을 관리하려면 [the section called “AWS 관리형 정책”](#)을 사용하는 것이 좋습니다. 이러한 관리형 정책을 수정하지 않고 사용하거나 이를 시작점으로 사용하여 자체적으로 제한적 정책을 작성할 수 있습니다. 정책은 추가 선택적 조건을 사용하여 다양한 작업에 대한 리소스 수준에서 사용자 권한을 제한할 수 있습니다.

애플리케이션 리소스가 서로 다른 계정(보조/리소스 계정)에 있는 경우 애플리케이션 리소스가 포함된 각 계정에 새 역할을 설정해야 합니다.

Note

워크로드 리소스에 대한 VPC 엔드포인트를 정의하는 경우 VPC 엔드포인트 정책이 리소스에 액세스하기 AWS Resilience Hub 위해에 대한 읽기 전용 액세스를 제공하는지 확인합니다. 자세한 정보는 [엔드포인트 정책을 사용하여 VPC 엔드포인트에 대한 액세스 제어](#)를 참조하세요.

주제

- [the section called “IAM 역할 사용”](#)
- [the section called “현재 IAM 사용자 권한 사용”](#)

IAM 역할 사용

AWS Resilience Hub 는 미리 정의된 기존 IAM 역할을 사용하여 기본 계정 또는 보조/리소스 계정의 리소스에 액세스합니다. 리소스에 액세스하기 위한 권장 권한 옵션입니다.

주제

- [the section called “간접 호출자 역할”](#)
- [the section called “교차 AWS 계정 액세스를 위한 다른 계정의 역할”](#)

간접 호출자 역할

AWS Resilience Hub 호출자 역할은 AWS 서비스 및 리소스에 액세스하기 위해 수입하는 AWS Identity and Access Management AWS Resilience Hub (IAM) 역할입니다. 예를 들어, CFN 템플릿과 이 템플릿에서 생성하는 리소스에 액세스할 수 있는 권한이 있는 간접 호출자 역할을 생성할 수 있습니다. 이 페이지에서는 애플리케이션 간접 호출자 역할을 생성하고 보고 관리하는 방법에 대한 정보를 제공합니다.

애플리케이션을 생성할 때 간접 호출자 역할을 제공합니다. AWS Resilience Hub 은 리소스를 가져 오거나 평가를 시작할 때 리소스에 액세스할 수 있도록 이 역할을 수입합니다. 가 호출자 역할을 올바르게 수입 AWS Resilience Hub 하려면 역할의 신뢰 정책에서 AWS Resilience Hub 서비스 보안 주체 (resiliencehub.amazonaws.com)를 신뢰할 수 있는 서비스로 지정해야 합니다.

애플리케이션의 간접 호출자 역할을 보려면 탐색 창에서 애플리케이션을 선택한 다음 애플리케이션 페이지의 작업 메뉴에서 권한 업데이트를 선택합니다.

언제든지 애플리케이션 간접 호출자 역할에 권한을 추가하거나 제거할 수 있으며, 애플리케이션 리소스에 액세스하는 데 다른 역할을 사용하도록 애플리케이션을 구성할 수 있습니다.

주제

- [the section called “IAM 콘솔에서 간접 호출자 역할 생성”](#)
- [the section called “IAM API를 사용한 역할 관리”](#)
- [the section called “JSON 파일을 사용하여 신뢰 정책 정의”](#)

IAM 콘솔에서 간접 호출자 역할 생성

AWS Resilience Hub 가 AWS 서비스 및 리소스에 액세스할 수 있도록 하려면 IAM 콘솔을 사용하여 기본 계정에서 호출자 역할을 생성해야 합니다. IAM 콘솔을 사용하여 역할을 생성하는 방법에 대한 자세한 내용은 [AWS 서비스에 대한 역할 생성\(콘솔\)을 참조하세요](#).

IAM 콘솔을 사용하여 기본 계정에서 간접 호출자 역할을 만들려면

1. <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. 사용자 지정 신뢰 정책을 선택하고 사용자 지정 신뢰 정책 창에서 다음 정책을 복사한 후 다음을 선택합니다.

Note

리소스가 서로 다른 계정에 있는 경우 각 계정에서 역할을 만들고 다른 계정에는 보조 계정 신뢰 정책을 사용해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

}

4. 권한 추가 페이지의 권한 정책 섹션에서 속성 또는 정책 이름을 기준으로 정책을 필터링하고 Enter 누르기 상자에 `AWSResilienceHubAssessmentExecutionPolicy`을 입력합니다.
5. 정책을 선택하고 다음을 선택합니다.
6. 역할 세부 정보 섹션에서 역할 이름 상자에 고유한 역할 이름 (예: `AWSResilienceHubAssessmentRole`)을 입력합니다.

이 필드에는 영숫자와 "+=, .@-_"문자만 입력할 수 있습니다.
7. (선택 사항) 설명 상자에 역할에 대한 설명을 입력합니다.
8. 역할 생성을 선택합니다.

6단계에서 역할에 대한 사용 사례와 권한을 편집하려면 1단계: 신뢰할 수 있는 엔터티 선택 또는 2단계: 권한 추가 섹션의 오른쪽에 있는 편집 버튼을 선택합니다.

간접 호출자 역할 및 리소스 역할(해당하는 경우)을 만든 후 이러한 역할을 사용하도록 애플리케이션을 구성할 수 있습니다.

Note

애플리케이션을 생성하거나 업데이트할 때는 현재 IAM 사용자/역할에 간접 호출자 역할에 대한 `iam:passRole` 권한이 있어야 합니다. 하지만 평가를 실행하는 데는 이 권한이 필요하지 않습니다.

IAM API를 사용한 역할 관리

역할의 신뢰 정책은 지정된 보안 주체에게 역할을 맡을 수 있는 권한을 부여합니다. AWS Command Line Interface (AWS CLI)를 사용하여 역할을 생성하려면 `create-role` 명령을 사용합니다. 이 명령을 사용할 때는 신뢰 정책 인라인을 지정할 수 있습니다. 다음 예제에서는 AWS Resilience Hub 서비스에 보안 주체에게 역할을 수임할 수 있는 권한을 부여하는 방법을 보여줍니다.

Note

JSON 문자열의 이스케이프 따옴표(' ') 요구 사항은 셸 버전에 따라 다릅니다.

샘플 `create-role`

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{
  "Version": "2012-10-17", "Statement":
  [
    {
      "Effect": "Allow",
      "Principal": {"Service": "resiliencehub.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}'
```

JSON 파일을 사용하여 신뢰 정책 정의

별도의 JSON 파일을 사용하고 `create-role` 명령을 실행하여 역할에 대한 신뢰 정책을 정의할 수도 있습니다. 다음 예제에서 **trust-policy.json**은 현재 디렉터리의 신뢰 정책이 포함된 파일입니다. 이 정책은 **create-role** 명령을 실행하여 역할에 연결됩니다. **create-role** 명령의 출력은 샘플 출력(Sample Output)에 표시됩니다. 역할에 권한을 추가하려면 역할에 정책 추가(`attach-policy-to-role`) 명령을 사용하며 `AWSResilienceHubAssessmentExecutionPolicy` 관리형 정책을 추가하는 것부터 시작할 수 있습니다. 관리형 정책에 대한 자세한 내용은 [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#) 단원을 참조하세요.

샘플 **trust-policy.json**

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": "resiliencehub.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }]
}
```

샘플 **create-role**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-
role-policy-document file://trust-policy.json
```

샘플 출력

```
{
  "Role": {
    "Path": "/",
    "RoleName": "AWSResilienceHubAssessmentRole",
    "RoleId": "AROAQFOXMP6TZ6ITKWND",
    "Arn": "arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole",
    "CreateDate": "2020-01-17T23:19:12Z",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [{
        "Effect": "Allow",
        "Principal": {
          "Service": "resiliencehub.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }]
    }
  }
}
```

샘플 **attach-policy-to-role**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAssessmentExecutionPolicy
```

교차 AWS 계정 액세스를 위한 다른 계정의 역할 - 선택 사항

리소스가 보조/리소스 계정에 있는 경우가 애플리케이션을 AWS Resilience Hub 성공적으로 평가할 수 있도록 각 계정에 역할을 생성해야 합니다. 역할 생성 절차는 신뢰 정책 구성을 제외하면 간접 호출자 역할 생성 프로세스와 비슷합니다.

Note

리소스가 있는 보조 계정에서 역할을 만들어야 합니다.

주제

- [the section called “IAM 콘솔에서 보조/리소스 계정용 역할 생성”](#)
- [the section called “IAM API를 사용한 역할 관리”](#)

- [the section called “JSON 파일을 사용하여 신뢰 정책 정의”](#)

IAM 콘솔에서 보조/리소스 계정으로 역할 생성

AWS Resilience Hub 가 다른 AWS 계정의 AWS 서비스 및 리소스에 액세스할 수 있도록 하려면 이러한 각 계정에서 역할을 생성해야 합니다.

IAM 콘솔을 사용하여 IAM 콘솔에서 보조/리소스 계정에 대한 역할을 만들려면

1. <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. 사용자 지정 신뢰 정책을 선택하고 사용자 지정 신뢰 정책 창에서 다음 정책을 복사한 후 다음을 선택합니다.

Note

리소스가 서로 다른 계정에 있는 경우 각 계정에서 역할을 만들고 다른 계정에는 보조 계정 신뢰 정책을 사용해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. 권한 추가 페이지의 권한 정책 섹션에서 속성 또는 정책 이름을 기준으로 정책을 필터링하고 Enter 누르기 상자에 `AWSResilienceHubAssessmentExecutionPolicy`을 입력합니다.
5. 정책을 선택하고 다음을 선택합니다.

6. 역할 세부 정보 섹션에서 역할 이름 상자에 고유한 역할 이름 (예: AWSResilienceHubAssessmentRole) 을 입력합니다.
7. (선택 사항) 설명 상자에 역할에 대한 설명을 입력합니다.
8. 역할 생성을 선택합니다.

6단계에서 역할에 대한 사용 사례와 권한을 편집하려면 1단계: 신뢰할 수 있는 엔터티 선택 또는 2 단계: 권한 추가 섹션의 오른쪽에 있는 편집 버튼을 선택합니다.

또한 간접 호출자 역할에 sts:assumeRole 권한을 추가하여 간접 호출자가 보조 계정의 역할을 맡을 수 있도록 해야 합니다.

생성한 각 보조 역할의 간접 호출자 역할에 다음 정책을 추가합니다.

```
{
  "Effect": "Allow",
  "Resource": [
    "arn:aws:iam::secondary_account_id_1:role/RoleInSecondaryAccount_1",
    "arn:aws:iam::secondary_account_id_2:role/RoleInSecondaryAccount_2",
    ...
  ],
  "Action": [
    "sts:AssumeRole"
  ]
}
```

IAM API를 사용한 역할 관리

역할의 신뢰 정책은 지정된 보안 주체에게 역할을 맡을 수 있는 권한을 부여합니다. AWS Command Line Interface (AWS CLI)를 사용하여 역할을 생성하려면 `create-role` 명령을 사용합니다. 이 명령을 사용할 때는 신뢰 정책 인라인을 지정할 수 있습니다. 다음 예제에서는 AWS Resilience Hub 서비스 보안 주체에게 역할을 수임할 수 있는 권한을 부여하는 방법을 보여줍니다.

Note

JSON 문자열의 이스케이프 따옴표(' ') 요구 사항은 셸 버전에 따라 다릅니다.

샘플 `create-role`

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-document '{"Version": "2012-10-17", "Statement": [{"Effect": "Allow", "Principal": {"AWS": ["arn:aws:iam::primary_account_id:role/InvokerRoleName"]}, "Action": "sts:AssumeRole"}]}'
```

별도의 JSON 파일을 사용하여 역할에 대한 신뢰 정책을 정의할 수도 있습니다. 다음 예제에서 `trust-policy.json`은 최신 디렉터리의 파일입니다.

JSON 파일을 사용하여 신뢰 정책 정의

별도의 JSON 파일을 사용하고 `create-role` 명령을 실행하여 역할에 대한 신뢰 정책을 정의할 수도 있습니다. 다음 예제에서 **`trust-policy.json`**은 현재 디렉터리의 신뢰 정책이 포함된 파일입니다. 이 정책은 **`create-role`** 명령을 실행하여 역할에 연결됩니다. **`create-role`** 명령의 출력은 샘플 출력(Sample Output)에 표시됩니다. 역할에 권한을 추가하려면 역할에 정책 추가(`attach-policy-to-role`) 명령을 사용하며 `AWSResilienceHubAssessmentExecutionPolicy` 관리형 정책을 추가하는 것부터 시작할 수 있습니다. 관리형 정책에 대한 자세한 내용은 [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#) 단원을 참조하세요.

샘플 **`trust-policy.json`**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

샘플 **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-document file:///trust-policy.json
```

샘플 출력

```
{
  "Role": {
    "Path": "/",
    "RoleName": "AWSResilienceHubAssessmentRole2",
    "RoleId": "AROAT2GICMEDJML6EVQRG",
    "Arn": "arn:aws:iam::262412591366:role/AWSResilienceHubAssessmentRole2",
    "CreateDate": "2023-08-02T07:49:23+00:00",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "AWS": [
              "arn:aws:iam::262412591366:role/
AWSResilienceHubAssessmentRole"
            ]
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  }
}
```

샘플 **attach-policy-to-role**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAssessmentExecutionPolicy.
```

현재 IAM 사용자 권한 사용

현재 IAM 사용자 권한을 사용하여 평가를 생성하고 실행하려면 이 방법을 사용하세요.

AWSResilienceHubAssessmentExecutionPolicy 관리형 정책을 IAM 사용자 또는 사용자와 연결된 역할에 연결할 수 있습니다.

단일 계정 설정

위에서 언급한 관리형 정책을 사용하면 IAM 사용자와 동일한 계정에서 관리되는 애플리케이션에 대한 평가를 충분히 실행할 수 있습니다.

예정된 평가 설정

AWS Resilience Hub 이 예정된 평가 관련 작업을 수행할 수 있게 하려면 새 역할 `AwsResilienceHubPeriodicAssessmentRole`을 생성해야 합니다.

Note

- 역할 기반 액세스(위에서 언급한 간접 호출자 역할)를 사용하는 동안에는 이 단계가 필요하지 않습니다.
- 역할 이름은 `AwsResilienceHubPeriodicAssessmentRole`이어야 합니다.

AWS Resilience Hub 가 예약된 평가 관련 작업을 수행하도록 활성화하려면

1. `AWSResilienceHubAssessmentExecutionPolicy` 관리형 정책을 역할에 연결합니다.
2. 다음 정책을 추가합니다. 여기서는 애플리케이션이 정의된 `primary_account_id` AWS 계정이며 평가를 실행합니다. 또한 예약된 평가의 역할 (`AwsResilienceHubPeriodicAssessmentRole`)에 연결된 신뢰 정책을 추가해야 합니다. 이 정책은 AWS Resilience Hub 서비스가 예약된 평가의 역할을 수임할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::primary_account_id:role/AwsResilienceHubAdminAccountRole"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::primary_account_id:role/AwsResilienceHubAssessmentEKSAccessRole"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

예정된 평가의 역할에 대한 신뢰 정책(**AwsResilienceHubPeriodicAssessmentRole**)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

교차 계정 설정

AWS Resilience Hub를 여러 계정과 함께 사용하는 경우 다음 IAM 권한 정책이 필요합니다. 사용 사례에 따라 각 AWS 계정에 다른 권한이 필요할 수 있습니다. 크로스 계정 액세스를 위해 AWS Resilience Hub를 설정할 때는 다음과 같은 계정 및 역할을 고려합니다.

- 기본 계정 — 애플리케이션을 만들고 평가를 실행하려는 AWS 계정입니다.
- 보조/리소스 계정(들) - 리소스가 위치한 AWS 계정(들).

Note

- 역할 기반 액세스(위에서 언급한 간접 호출자 역할)를 사용하는 동안에는 이 단계가 필요하지 않습니다.
- Amazon Elastic Kubernetes Service에 액세스할 수 있는 권한을 구성하는 방법에 대한 자세한 내용은 [the section called “Amazon EKS 클러스터에 대한 AWS Resilience Hub 액세스 활성화” 단원을 참조하세요.](#)

기본 계정 설정

기본 계정 `AwsResilienceHubAdminAccountRole`에서 새 역할을 생성하고 이를 수임할 수 있는 AWS Resilience Hub 액세스를 활성화해야 합니다. 이 역할은 리소스가 포함된 AWS 계정의 다른 역할에 액세스하는 데 사용됩니다. 리소스를 읽을 권한이 없어야 합니다.

Note

- 역할 이름은 `AwsResilienceHubAdminAccountRole`이어야 합니다.
- 기본 계정에서 생성해야 합니다.
- 현재 IAM 사용자/역할에는 이 역할을 수임할 `iam:assumeRole` 권한이 있어야 합니다.
- `secondary_account_id_1/2/...`을 관련 보조 계정 식별자로 바꾸세요.

다음 정책은 계정의 다른 역할에 있는 리소스에 액세스할 수 있는 실행기 권한을 역할에 제공합니다 AWS .

```
{
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Resource": [
          "arn:aws:iam::secondary_account_id_1:role/AwsResilienceHubExecutorAccountRole",
          "arn:aws:iam::secondary_account_id_2:role/AwsResilienceHubExecutorAccountRole",
          ...
        ],
        "Action": [
          "sts:AssumeRole"
        ]
      }
    ]
  }
}
```

관리자 역할(`AwsResilienceHubAdminAccountRole`)의 신뢰 정책은 다음과 같습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::primary_account_id:role/caller_IAM_role"
  },
  "Action": "sts:AssumeRole"
},
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubPeriodicAssessmentRole"
  },
  "Action": "sts:AssumeRole"
}
]
```

보조/리소스 계정 설정

각 보조 계정에서 새 `AwsResilienceHubExecutorAccountRole` 계정을 만들고 위에서 만든 관리자 역할을 활성화하여 이 역할을 수임해야 합니다. 이 역할은에서 애플리케이션 리소스를 스캔하고 평가하는 AWS Resilience Hub 데 사용되므로 적절한 권한도 필요합니다.

하지만 `AWSResilienceHubAssessmentExecutionPolicy` 관리형 정책을 역할에 연결하고 실행자 역할 정책을 연결해야 합니다.

실행자 역할 신뢰 정책은 다음과 같습니다.

```
{
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "AWS": "arn:aws:iam::primary_account_id:role/AwsResilienceHubAdminAccountRole"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
}
```

AWS 에 대한 관리형 정책 AWS Resilience Hub

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 [고객 관리형 정책](#)을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 AWS 관리형 정책에 정의된 권한을 AWS 업데이트하면 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS 는 새 AWS 서비스 가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 [AWS 관리형 정책](#)을 참조하세요.

AWSResilienceHubAssessmentExecutionPolicy

AWSResilienceHubAssessmentExecutionPolicy을 IAM 자격 증명에 연결할 수 있습니다. 평가를 실행하는 동안이 정책은 평가를 실행할 수 있는 액세스 권한을 다른 AWS 서비스에 부여합니다.

권한 세부 정보

이 정책은 경보 AWS FIS 와 SOP 템플릿을 Amazon Simple Storage Service(Amazon S3) 버킷에 게시할 수 있는 적절한 권한을 제공합니다. Amazon S3 버킷 이름은 aws-resilience-hub-artifacts-로 시작해야 합니다. 다른 Amazon S3 버킷에 게시하려는 경우 CreateRecommendationTemplate API를 직접적으로 호출하면서 게시할 수 있습니다. 자세한 내용은 [권장 사항 템플릿 생성\(CreateRecommendationTemplate\)](#)을 참조하세요.

이 정책에는 다음 권한이 포함되어 있습니다.

- Amazon CloudWatch(CloudWatch) — 애플리케이션을 모니터링하기 위해 Amazon CloudWatch에 설정한 모든 구현된 경보를 가져옵니다. 또한 ResilienceHub 네임스페이스에 있는 애플리케이션의 복원력 점수에 대한 CloudWatch 지표를 게시하는 데 cloudwatch:PutMetricData을 사용합니다.

- Amazon Data Lifecycle Manager - AWS 계정과 연결된 Amazon Data Lifecycle Manager 리소스에 대한 Describe 권한을 얻고 제공합니다.
- Amazon DevOpsGuru - AWS 계정과 연결된 Amazon DevOpsGuru 리소스를 나열하고 이에 대한 Describe 권한을 제공합니다.
- Amazon DocumentDB - 계정 AWS 과 연결된 Amazon DocumentDB 리소스를 나열하고 이에 대한 Describe 권한을 제공합니다.
- Amazon DynamoDB (DynamoDB) — AWS 계정과 연결된 Amazon DynamoDB 리소스를 나열하고 Describe 권한을 제공합니다.
- Amazon ElastiCache(ElastiCache) - AWS 계정과 연결된 ElastiCache 리소스에 대한 Describe 권한을 제공합니다.
- Amazon ElastiCache(Redis OSS) Serverless(ElastiCache(Redis OSS) Serverless) - 계정 AWS 과 연결된 ElastiCache(Redis OSS) Serverless 구성에 대한 Describe 권한을 제공합니다.
- Amazon Elastic Compute Cloud(Amazon EC2) — AWS 계정과 연결된 Amazon EC2 리소스를 나열하고 Describe 권한을 제공합니다.
- Amazon Elastic Container Registry(Amazon ECR) - AWS 계정과 연결된 Amazon ECR 리소스에 대한 Describe 권한을 제공합니다.
- Amazon Elastic Container Service(Amazon ECS) - AWS 계정과 연결된 Amazon ECS 리소스에 대한 Describe 권한을 제공합니다.
- Amazon Elastic File System(Amazon EFS) - AWS 계정과 연결된 Amazon EFS 리소스에 대한 Describe 권한을 제공합니다.
- Amazon Elastic Kubernetes Service(Amazon EKS) — AWS 계정과 연결된 Amazon EKS 리소스를 나열하고 권한을 Describe 제공합니다.
- Amazon EC2 Auto Scaling - AWS 계정과 연결된 Amazon EC2 Auto Scaling 리소스를 나열하고 이에 대한 Describe 권한을 제공합니다.
- Amazon EC2 Systems Manager(SSM) - AWS 계정과 연결된 SSM 리소스에 대한 Describe 권한을 제공합니다.
- AWS Fault Injection Service (AWS FIS) - AWS 계정과 연결된 AWS FIS 실험 및 실험 템플릿에 대한 Describe 권한을 나열하고 제공합니다.
- Amazon FSx for Windows File Server(Amazon FSx) - 계정 AWS 과 연결된 Amazon FSx 리소스에 대한 Describe 권한을 나열하고 제공합니다.
- Amazon RDS - AWS 계정과 연결된 Amazon RDS 리소스를 나열하고 이에 대한 Describe 권한을 제공합니다.

- Amazon Route 53(Route 53) — AWS 계정과 연결된 Route 53 리소스를 나열하고 Describe 권한을 제공합니다.
- Amazon Route 53 Resolver - AWS 계정과 연결된 Amazon Route 53 Resolver 리소스에 대한 Describe 권한을 나열하고 제공합니다.
- Amazon Simple Notification Service(SNS) — AWS 계정과 연결된 Amazon SNS 리소스를 나열하고 Describe 권한을 제공합니다.
- Amazon Simple Queue Service(Amazon SQS) — AWS 계정과 연결된 Amazon SQS 리소스를 나열하고 Describe 권한을 제공합니다.
- Amazon Simple Storage Service(Amazon S3) - 계정 AWS 과 연결된 Amazon S3 리소스에 대한 Describe 권한을 나열하고 제공합니다.

 Note

평가를 실행하는 동안 관리형 정책에서 업데이트해야 하는 누락된 권한이 있는 경우는 s3:GetBucketLogging 권한을 사용하여 평가를 AWS Resilience Hub 성공적으로 완료합니다. 그러나 AWS Resilience Hub 는 누락된 권한을 나열하는 경고 메시지를 표시하고 이를 추가할 유예 기간을 제공합니다. 지정된 유예 기간 내에 누락된 권한을 추가하지 않으면 평가가 실패합니다.

- AWS Backup - AWS 계정과 연결된 Amazon EC2 Auto Scaling 리소스를 나열하고 Describe 권한을 가져옵니다.
- AWS CloudFormation - 계정 AWS 과 연결된 AWS CloudFormation 스택의 리소스에 대한 Describe 권한을 나열하고 가져옵니다.
- AWS DataSync - AWS 계정과 연결된 AWS DataSync 리소스에 대한 Describe 권한을 나열하고 제공합니다.
- AWS Directory Service - AWS 계정과 연결된 AWS Directory Service 리소스에 대한 Describe 권한을 나열하고 제공합니다.
- AWS Elastic Disaster Recovery (Elastic Disaster Recovery) - AWS 계정과 연결된 Elastic Disaster Recovery 리소스에 대한 Describe 권한을 제공합니다.
- AWS Lambda (Lambda) - 계정 AWS 과 연결된 Lambda 리소스에 대한 Describe 권한을 나열하고 제공합니다.
- AWS Resource Groups (리소스 그룹) - 계정 AWS 과 연결된 Resource Groups 리소스에 대한 Describe 권한을 나열하고 제공합니다.
- AWS Service Catalog (서비스 카탈로그) - 계정 AWS 과 연결된 서비스 카탈로그 리소스를 나열하고 Describe 권한을 제공합니다.

- AWS Step Functions - AWS 계정과 연결된 AWS Step Functions 리소스에 대한 Describe 권한을 나열하고 제공합니다.
- Elastic Load Balancing - AWS 계정과 연결된 Elastic Load Balancing 리소스에 대한 Describe 권한을 나열하고 제공합니다.
- ssm:GetParametersByPath— 이 권한을 사용하여 애플리케이션에 구성된 CloudWatch 경보, 테스트 또는 SOP를 관리합니다.

AWS 계정이 평가를 실행하는 동안 팀에 AWS 서비스에 액세스하는 데 필요한 권한을 제공하는 사용자, 사용자 그룹 및 역할에 권한을 추가하려면 다음 IAM 정책이 필요합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSResilienceHubFullResourceStatement",
      "Effect": "Allow",
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "docdb-elastic:GetCluster",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListTagsForResource",
        "drs:DescribeJobs",
```

```
"drs:DescribeSourceServers",
"drs:GetReplicationConfiguration",
"ds:DescribeDirectories",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:ListGlobalTables",
"dynamodb:ListTagsOfResource",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeFastSnapshotRestores",
"ec2:DescribeFleets",
"ec2:DescribeHosts",
"ec2:DescribeInstances",
"ec2:DescribeNatGateways",
"ec2:DescribePlacementGroups",
"ec2:DescribeRegions",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ecr:DescribeRegistry",
"ecs:DescribeCapacityProviders",
"ecs:DescribeClusters",
"ecs:DescribeContainerInstances",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:ListContainerInstances",
"ecs:ListServices",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodegroup",
"eks:ListFargateProfiles",
"eks:ListNodegroups",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeServerlessCaches",
"elasticahce:DescribeServerlessCacheSnapshots",
"elasticache:DescribeSnapshots",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
```

```
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"fis:GetExperiment",
"fis:GetExperimentTemplate",
"fis:ListExperiments",
"fis:ListExperimentResolvedTargets",
"fis:ListExperimentTemplates",
"fsx:DescribeFileSystems",
"lambda:GetFunctionConcurrency",
"lambda:GetFunctionConfiguration",
"lambda:ListAliases",
"lambda:ListEventSourceMappings",
"lambda:ListFunctionEventInvokeConfigs",
"lambda:ListVersionsByFunction",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBInstanceAutomatedBackups",
"rds:DescribeDBInstances",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyTargets",
"rds:DescribeDBSnapshots",
"rds:DescribeGlobalClusters",
"rds:ListTagsForResource",
"resource-groups:GetGroup",
"resource-groups:ListGroupResources",
"route53-recovery-control-config:ListClusters",
"route53-recovery-control-config:ListControlPanels",
"route53-recovery-control-config:ListRoutingControls",
"route53-recovery-readiness:GetReadinessCheckStatus",
"route53-recovery-readiness:GetResourceSet",
"route53-recovery-readiness:ListReadinessChecks",
"route53:GetHealthCheck",
"route53:ListHealthChecks",
"route53:ListHostedZones",
"route53:ListResourceRecordSets",
"route53resolver:ListResolverEndpoints",
"route53resolver:ListResolverEndpointIpAddresses",
"s3:ListBucket",
"servicecatalog:GetApplication",
"servicecatalog:ListAssociatedResources",
"sns:GetSubscriptionAttributes",
```

```

        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
    ],
    "Resource": "*"
},
{
    "Sid": "AWSResilienceHubApiGatewayStatement",
    "Effect": "Allow",
    "Action": [
        "apigateway:GET"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
    ]
},
{
    "Sid": "AWSResilienceHubS3ArtifactStatement",
    "Effect": "Allow",
    "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
    ],
    "Resource": "arn:aws:s3::aws-resilience-hub-artifacts-*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid": "AWSResilienceHubS3AccessStatement",
    "Effect": "Allow",
    "Action": [
        "s3:GetBucketLocation",

```

```

        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid": "AWSResilienceHubCloudWatchStatement",
    "Effect": "Allow",
    "Action": [
        "cloudwatch:PutMetricData"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "cloudwatch:namespace": "ResilienceHub"
        }
    }
},
{
    "Sid": "AWSResilienceHubSSMStatement",
    "Effect": "Allow",
    "Action": [
        "ssm:GetParametersByPath"
    ],
    "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
}
]
}

```

AWS Resilience HubAWS 관리형 정책에 대한 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Resilience Hub 이후의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS Resilience Hub 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWSResilienceHubAssessmentExecutionPolicy - 변경 사항	AWS Resilience Hub 는 평가를 실행하는 AWS FIS 동안에서 실험AWSResilienceHubAssessmentExecutionPolicy 에 액세스할 수 있도록 List 및 Get 권한을 부여하도록 업데이트했습니다.	2024년 12월 17일
AWSResilienceHubAssessmentExecutionPolicy - 변경 사항	AWS Resilience Hub 는 평가를 실행하는 동안 Amazon ElastiCache(Redis OSS) Serverless의 리소스 및 구성에 액세스할 수 있는 Describe 권한을 부여AWSResilienceHubAssessmentExecutionPolicy 하도록 업데이트했습니다.	2024년 9월 25일
AWSResilienceHubAssessmentExecutionPolicy - 변경 사항	AWS Resilience Hub 는 Amazon DocumentDB, Elastic Load Balancing 및 평가를 실행하는 AWS Lambda 동안 리소스 및 구성에 액세스할 수 있는 Describe 권한을 부여AWSResilienceHubAssessmentExecutionPolicy 하도록 업데이트했습니다.	2024년 8월 1일

변경 사항	설명	날짜
AWSResilienceHubAssessmentExecutionPolicy - 변경 사항	AWS Resilience Hub 가 평가를 실행하는 동안 Amazon FSx for Windows File Server 구성을 읽을 수 있는 Describe 권한을 부여AWSResilienceHubAssessmentExecutionPolicy 하도록를 업데이트했습니다.	2024년 3월 26일
AWSResilienceHubAssessmentExecutionPolicy - 변경 사항	AWS Resilience Hub 가 평가를 실행하는 동안 구성을 읽을 수 있는 Describe 권한을 부여AWSResilienceHubAssessmentExecutionPolicy 하도록를 AWS Step Functions 업데이트했습니다.	2023년 10월 30일
AWSResilienceHubAssessmentExecutionPolicy - 변경 사항	AWS Resilience Hub 에서 평가를 실행하는 동안 Amazon RDS의 리소스에 액세스할 수 있는 Describe 권한을 부여AWSResilienceHubAssessmentExecutionPolicy 하도록를 업데이트했습니다.	2023년 10월 5일
AWSResilienceHubAssessmentExecutionPolicy - 신규	이 AWS Resilience Hub 정책은 평가를 실행하기 위한 다른 AWS 서비스에 대한 액세스를 제공합니다.	2023년 6월 26일
AWS Resilience Hub 변경 사항 추적 시작	AWS Resilience Hub 는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2023년 6월 15일

AWS Resilience Hub 페르소나 및 IAM 권한 참조

AWSResilienceHubAssessmentExecutionPolicy AWS 관리형 정책 및 다음 페르소나별 정책 중 하나를 AWS Resilience Hub 사용하여 작업해야 하는 페르소나에 IAM 권한을 부여할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 섹션을 참조하세요 [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#).

페르소나에 대한 정책은 AWS Resilience Hub 다음에서 제안합니다.

- [인프라 애플리케이션 관리자 페르소나에 대한 IAM 권한](#)
- [비즈니스 연속성 관리자 페르소나에 대한 IAM 권한](#)
- [애플리케이션 소유자 페르소나에 대한 IAM 권한](#)
- [읽기 전용 액세스 권한을 부여하기 위한 IAM 권한](#)

인프라 애플리케이션 관리자 페르소나에 대한 IAM 권한

다음 정책은 인프라 애플리케이션 관리자 페르소나에 필요한 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InfrastructureApplicationManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub>DeleteAppAssessment",
        "resiliencehub>DeleteAppInputSource",
        "resiliencehub>DeleteAppVersionAppComponent",
        "resiliencehub>DeleteAppVersionResource",
        "resiliencehub>DeleteRecommendationTemplate",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",

```

```

        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource"
    ],
    "Resource": "*"
}
]
}

```

비즈니스 연속성 관리자 페르소나에 대한 IAM 권한

다음 정책은 비즈니스 연속성 관리자 페르소나에 필요한 권한을 부여합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BusinessContinuityManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub>DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}

```

애플리케이션 소유자 페르소나에 대한 IAM 권한

다음 정책은 애플리케이션 소유자 페르소나에 필요한 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ApplicationOwner",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:BatchUpdateRecommendationStatus",
        "resiliencehub:CreateApp",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub>DeleteApp",
        "resiliencehub>DeleteAppAssessment",
        "resiliencehub>DeleteAppInputSource",
        "resiliencehub>DeleteAppVersionAppComponent",
        "resiliencehub>DeleteAppVersionResource",
        "resiliencehub>DeleteRecommendationTemplate",
        "resiliencehub>DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:ImportResourcesToDraftAppVersion",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateApp",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

읽기 전용 액세스 권한을 부여하기 위한 IAM 권한

다음 정책은 읽기 전용 액세스에 필요한 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnly",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources"
      ],
      "Resource": "*"
    }
  ]
}
```

로 Terraform 상태 파일 가져오기 AWS Resilience Hub

AWS Resilience Hub 는 Amazon Simple Storage Service 관리형 키(SSE-S3) 또는 관리형 키(SSE-KMS)를 사용하여 서버 측 암호화(SSE)를 사용하여 AWS Key Management Service 암호화된 Terraform 상태 파일 가져오기를 지원합니다. Terraform 상태 파일이 고객 제공 암호화 키 (SSE-C) 를 사용하여 암호화된 경우 AWS Resilience Hub를 사용하여 가져올 수 없습니다.

Terraform 상태 파일을 로 가져오려면 상태 파일이 있는 위치에 따라 다음과 같은 IAM 정책이 AWS Resilience Hub 필요합니다.

기본 계정에 있는 Amazon S3 버킷에서 Terraform 상태 파일 가져오기

기본 계정의 Amazon S3 버킷에 있는 Terraform 상태 파일에 대한 AWS Resilience Hub 의 읽기 액세스를 허용하려면 다음 Amazon S3 버킷 정책 및 IAM 정책이 필요합니다.

- 버킷 정책 - 기본 계정에 있는 대상 Amazon S3 버킷의 버킷 정책입니다. 자세한 내용은 다음 예제를 참조하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
  },
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
},
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
  },
  "Action": "s3:ListBucket",
  "Resource": "arn:aws:s3:::<s3-bucket-name>"
}
]
```

- 자격 증명 정책 -이 애플리케이션에 정의된 호출자 역할 또는 기본 AWS 계정의 AWS 현재 IAM 역할에 대한 연결된 자격 증명 정책 AWS Resilience Hub 입니다. 자세한 내용은 다음 예제를 참조하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

Note

AWSResilienceHubAssessmentExecutionPolicy 관리형 정책을 사용하는 경우 ListBucket 권한이 필요하지 않습니다.

Note

KMS를 사용하여 Terraform 상태 파일을 암호화하는 경우 다음 kms:Decrypt 권한을 추가해야 합니다.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
  ],
  "Resource": "<arn_of_kms_key>"
}
```

보조 계정에 있는 Amazon S3 버킷에서 Terraform 상태 파일 가져오기

- 버킷 정책 - 보조 계정 중 하나에 있는 대상 Amazon S3 버킷의 버킷 정책입니다. 자세한 내용은 다음 예제를 참조하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-to-state-file>"
    },
    {

```

```

    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
  }
]
}

```

- 자격 증명 정책 - 기본 계정 AWS Resilience Hub 에서 실행 중인 AWS 계정 역할에 연결된 AWS 자격 증명 정책입니다. 자세한 내용은 다음 예제를 참조하세요.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}

```

Note

AWSResilienceHubAssessmentExecutionPolicy 관리형 정책을 사용하는 경우 ListBucket 권한이 필요하지 않습니다.

Note

KMS를 사용하여 Terraform 상태 파일을 암호화하는 경우 다음 kms:Decrypt 권한을 추가해야 합니다.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
  ],
  "Resource": "<arn_of_kms_key>"
}
```

Amazon Elastic Kubernetes Service 클러스터에 대한 AWS Resilience Hub 액세스 활성화

AWS Resilience Hub 는 Amazon EKS 클러스터의 인프라를 분석하여 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터의 복원력을 평가합니다.는 Kubernetes 역할 기반 액세스 제어 (RBAC) 구성을 AWS Resilience Hub 사용하여 Amazon EKS 클러스터의 일부로 배포되는 다른 Kubernetes(K8) 워크로드를 평가합니다. 가 워크로드 분석 및 평가를 위해 Amazon EKS 클러스터를 쿼리 AWS Resilience Hub 하려면 다음을 완료해야 합니다.

- Amazon EKS 클러스터와 동일한 계정에서 기존 AWS Identity and Access Management (IAM) 역할을 생성하거나 사용합니다.
- Amazon EKS 클러스터에 대한 IAM 사용자 및 역할 액세스를 활성화하고 Amazon EKS 클러스터 내의 K8 리소스에 추가 읽기 전용 권한을 부여하세요. Amazon EKS 클러스터에 대한 IAM 사용자 및 역할 액세스를 활성화하는 방법에 대한 자세한 내용은 [클러스터에 대한 IAM 사용자 및 역할 액세스 활성화 - Amazon EKS](#)를 참조하세요.

IAM 엔터티를 사용하는 Amazon EKS 클러스터에 대한 액세스는 Amazon EKS 컨트롤 플레인에서 실행되는 [AWS IAM Authenticator for Kubernetes](#)에 의해 사용 설정됩니다. 인증자는 aws-auth ConfigMap에서 구성 정보를 가져옵니다.

Note

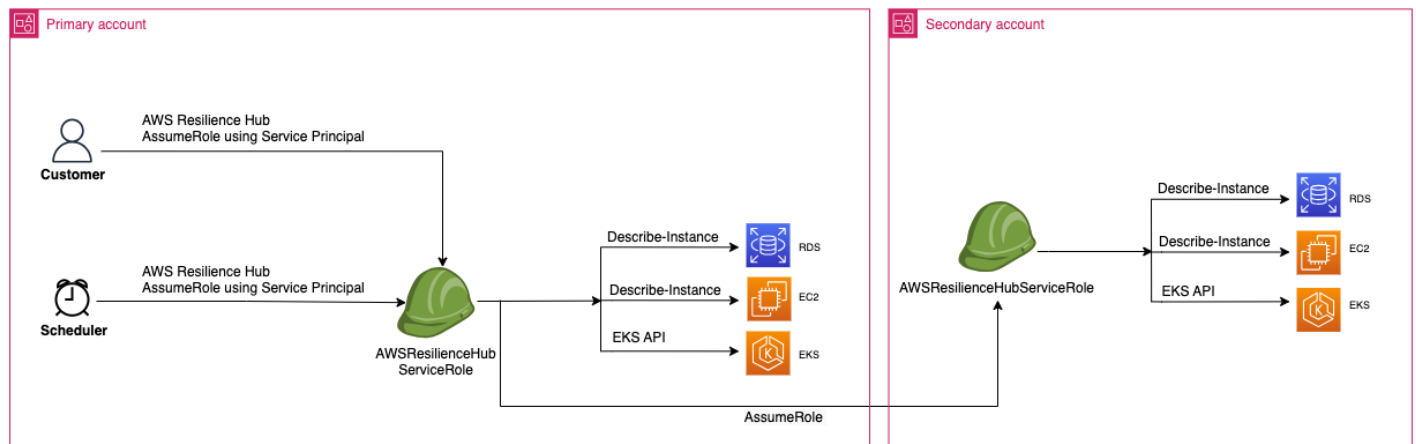
- aws-auth ConfigMap 설정에 대한 자세한 내용은 GitHub의 [Full Configuration Format](#)을 참조하세요.
- 다양한 IAM 자격 증명에 대한 자세한 내용은 IAM 사용자 설명서에서 [자격 증명\(사용자, 그룹 및 역할\)](#)을 섹션을 참조하세요.
- Kubernetes 역할 기반 액세스 제어(RBAC) 구성에 대한 자세한 내용은 [Using RBAC Authorization\(RBAC 승인 사용\)](#)을 참조하세요.

AWS Resilience Hub는 계정의 IAM 역할을 사용하여 Amazon EKS 클러스터 내의 리소스를 쿼리합니다. 가 Amazon EKS 클러스터 내의 리소스 AWS Resilience Hub에 액세스하려면 사용하는 IAM 역할을 Amazon EKS 클러스터 내의 리소스에 대한 충분한 읽기 전용 권한이 있는 Kubernetes 그룹에 매핑해야 AWS Resilience Hub합니다.

AWS Resilience Hub는 다음 IAM 역할 옵션 중 하나를 사용하여가 Amazon EKS 클러스터 리소스에 액세스할 수 있도록 허용합니다.

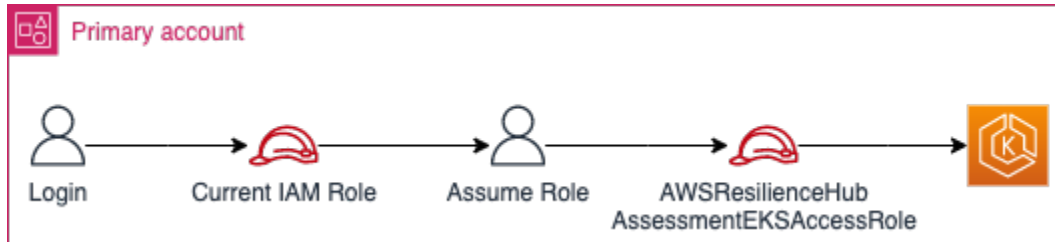
- 애플리케이션이 리소스에 액세스하는 데 역할 기반 액세스를 사용하도록 구성된 경우, 애플리케이션을 생성할 때 AWS Resilience Hub에게 전달된 간접 호출자 역할 또는 보조 계정 역할은 평가 중에 Amazon EKS 클러스터에 액세스하는 데 사용됩니다.

다음 개념 다이어그램은 애플리케이션이 역할 기반 애플리케이션으로 구성된 경우가 Amazon EKS 클러스터에 AWS Resilience Hub 액세스하는 방법을 보여줍니다.

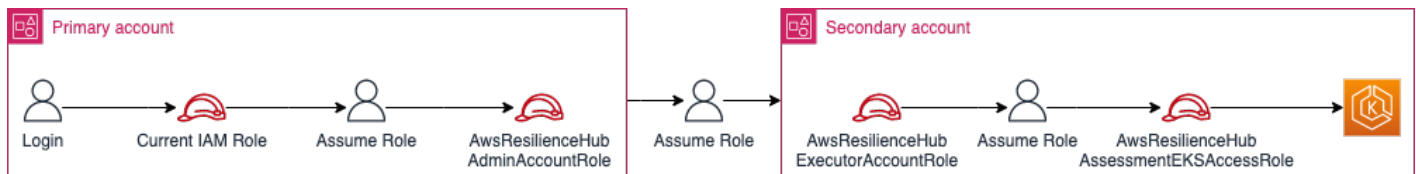


- 현재 IAM 사용자를 사용하여 리소스에 액세스하도록 애플리케이션을 구성한 경우 Amazon EKS 클러스터와 동일한 계정에서 `AwsResilienceHubAssessmentEKSAccessRole`의 이름으로 새 IAM 역할을 생성해야 합니다. 그러면 이 IAM 역할을 사용하여 Amazon EKS 클러스터에 액세스할 수 있습니다.

다음 개념 다이어그램은 애플리케이션이 현재 IAM 사용자 권한을 사용하도록 구성된 경우가 기본 계정에 배포된 Amazon EKS 클러스터에 AWS Resilience Hub 액세스하는 방법을 보여줍니다.



다음 개념 다이어그램은 애플리케이션이 현재 IAM 사용자 권한을 사용하도록 구성된 경우가 보조 계정에 배포된 Amazon EKS 클러스터에 AWS Resilience Hub 액세스하는 방법을 보여줍니다.



Amazon EKS 클러스터의 리소스에 대한 AWS Resilience Hub 액세스 권한 부여

AWS Resilience Hub 를 사용하면 필요한 권한을 구성한 경우 Amazon EKS 클러스터에 있는 리소스에 액세스할 수 있습니다.

Amazon EKS 클러스터 내에서 리소스를 검색하고 평가하는 데 필요한 권한을 AWS Resilience Hub 에 부여하려면

1. Amazon EKS 클러스터에 액세스할 수 있도록 IAM 역할을 구성합니다.

역할 기반 액세스를 사용하여 애플리케이션을 구성한 경우 이 단계를 건너뛰고 2단계로 진행하여 애플리케이션을 생성하는 데 사용한 역할을 사용할 수 있습니다. AWS Resilience Hub 이 IAM roles 역할을 사용하는 방법에 대한 자세한 내용은 [the section called “AWS Resilience Hub와 IAM의 작동 방식”](#) 단원을 참조하세요.

현재 IAM 사용자 권한을 사용하여 애플리케이션을 구성한 경우 Amazon EKS 클러스터와 동일한 계정에 `AwsResilienceHubAssessmentEKSAccessRole` IAM 역할을 생성해야 합니다. 그러면 Amazon EKS 클러스터에 액세스하는 동안 이 IAM 역할이 사용됩니다.

애플리케이션을 가져오고 평가하는 동안은 IAM 역할을 AWS Resilience Hub 사용하여 Amazon EKS 클러스터의 리소스에 액세스합니다. 이 역할은 Amazon EKS 클러스터와 동일한 계정에 생성되어야 하며 Amazon EKS 클러스터를 평가하는 AWS Resilience Hub 데에 필요한 권한이 포함된 Kubernetes 그룹과 매핑됩니다.

Amazon EKS 클러스터가 AWS Resilience Hub 호출 계정과 동일한 계정에 있는 경우 다음 IAM 신뢰 정책을 사용하여 역할을 생성해야 합니다. 이 IAM 신뢰 정책에서 `caller_IAM_role`는 현재 계정에서 APIs를 호출하는 데 사용됩니다 AWS Resilience Hub.

Note

`caller_IAM_role`는 AWS 사용자 계정과 연결된 역할입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Amazon EKS 클러스터가 교차 계정(AWS Resilience Hub 호출 계정과 다른 계정)에 있는 경우 다음 `AwsResilienceHubAssessmentEKSAccessRole` IAM 신뢰 정책을 사용하여 IAM 역할을 생성해야 합니다.

Note

사전 조건으로 AWS Resilience Hub 사용자 계정과 다른 계정에 배포된 Amazon EKS 클러스터에 액세스하려면 다중 계정 액세스를 구성해야 합니다. 자세한 내용은 단원을 참조하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/AwsResilienceHubExecutorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. AWS Resilience Hub 애플리케이션에 대한 `ClusterRole` 및 `ClusterRoleBinding` (또는 `RoleBinding`) 역할을 생성합니다.

`ClusterRole` 및 `ClusterRoleBinding`을 생성하면 Amazon EKS 클러스터의 특정 네임스페이스에 속하는 리소스를 분석하고 평가하는 AWS Resilience Hub 데 필요한 읽기 전용 권한을 부여합니다.

AWS Resilience Hub 를 사용하면 다음 중 하나를 완료하여 복원력 평가를 생성하기 위해 네임스페이스에 대한 액세스를 제한할 수 있습니다.

- a. 모든 네임스페이스에 대한 읽기 액세스 권한을 AWS Resilience Hub 애플리케이션에 부여합니다.

가 Amazon EKS 클러스터 내의 모든 네임스페이스에서 리소스의 복원력을 평가 AWS Resilience Hub 하려면 `ClusterRole`을 생성해야 합니다 `ClusterRoleBinding`.

- `resilience-hub-eks-access-cluster-role` (`ClusterRole`) -가 Amazon EKS 클러스터를 평가하는 AWS Resilience Hub 데 필요한 권한을 정의합니다.
- `resilience-hub-eks-access-cluster-role-binding` (`ClusterRoleBinding`) — Amazon EKS 클러스터에서 `resilience-hub-eks-access-group` 이름이 지정된 그룹을 정의하여 AWS Resilience Hub에서 사용자에서 복원력 평가를 실행하기 위해 필요한 권한을 부여합니다.

모든 네임스페이스에 대한 읽기 액세스 권한을 AWS Resilience Hub 애플리케이션에 부여하는 템플릿은 다음과 같습니다.

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
- apiGroups:
  - ""
  resources:
  - pods
  - replicationcontrollers
  - nodes
  verbs:
  - get
  - list
- apiGroups:
  - apps
  resources:
  - deployments
  - replicasets
  verbs:
  - get
  - list
- apiGroups:
  - policy
  resources:
  - poddisruptionbudgets
  verbs:
  - get
  - list
- apiGroups:
  - autoscaling.k8s.io
  resources:
  - verticalpodautoscalers
  verbs:
  - get
  - list
- apiGroups:
```

```

    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
  - karpenter.sh
  resources:
    - provisioners
    - nodepools
  verbs:
    - get
    - list
- apiGroups:
  - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF

```

- b. 특정 네임스페이스 AWS Resilience Hub 를 읽을 수 있는 액세스 권한을 부여합니다.

를 사용하여 특정 네임스페이스 세트 내의 리소스에 액세스 AWS Resilience Hub 하도록을 제한할 수 있습니다 RoleBinding. 이를 위해서는 다음 역할을 생성해야 합니다.

- **ClusterRole** - Amazon EKS 클러스터 내의 특정 네임스페이스에 있는 리소스에 액세스하고 복원력을 평가 AWS Resilience Hub 하려면 다음 **ClusterRole** 역할을 생성해야 합니다.
- **resilience-hub-eks-access-cluster-role**— 특정 네임스페이스 내의 리소스를 평가하는 데 필요한 권한을 지정합니다.
- **resilience-hub-eks-access-global-cluster-role** - Amazon EKS 클러스터 내에서 특정 네임스페이스와 연결되지 않은 클러스터 범위 리소스를 평가하는 데 필요한 권한을 지정합니다. 이는 애플리케이션의 복원력을 평가하기 위해 Amazon EKS 클러스터의 클러스터 범위 리소스(예: 노드)에 액세스할 수 있는 권한이 AWS Resilience Hub 필요합니다.

ClusterRole 역할을 생성하기 위한 템플릿은 다음과 같습니다.

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
  - apiGroups:
    - ""
    resources:
    - pods
    - replicationcontrollers
    verbs:
    - get
    - list
  - apiGroups:
    - apps
    resources:
    - deployments
    - replicaset
    verbs:
    - get
    - list
  - apiGroups:
    - policy
    resources:
    - poddisruptionbudgets
```

```
    verbs:
      - get
      - list
  - apiGroups:
    - autoscaling.k8s.io
    resources:
      - verticalpodautoscalers
    verbs:
      - get
      - list
  - apiGroups:
    - autoscaling
    resources:
      - horizontalpodautoscalers
    verbs:
      - get
      - list

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-global-cluster-role
rules:
  - apiGroups:
    - ""
    resources:
      - nodes
    verbs:
      - get
      - list
  - apiGroups:
    - karpenter.sh
    resources:
      - provisioners
      - nodepools
    verbs:
      - get
      - list
  - apiGroups:
    - karpenter.k8s.aws
    resources:
      - awsnodetemplates
      - ec2nodeclasses
```

```

verbs:
  - get
  - list

---
EOF

```

- RoleBinding 역할 -이 역할은가 특정 네임스페이스 내의 리소스에 액세스하는 AWS Resilience Hub 데 필요한 권한을 부여합니다. 즉, 각 네임스페이스에 RoleBinding 역할을 생성하여가 지정된 네임스페이스 내의 리소스 AWS Resilience Hub 에 액세스할 수 있도록 해야 합니다.

Note

ClusterAutoscaler을 자동 스케일링에 사용하는 경우 kube-system에서 추가로 RoleBinding를 생성해야 합니다. 이는 kube-system 네임스페이스의 일부인 ClusterAutoscaler을 평가하는 데 필요합니다.

이렇게 하면 Amazon EKS 클러스터 AWS Resilience Hub 를 평가하는 동안 kube-system 네임스페이스 내의 리소스를 평가하는 데 필요한 권한을 부여할 수 있습니다.

RoleBinding 역할을 생성하기 위한 템플릿은 다음과 같습니다.

```

cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
  namespace: <namespace>
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io

---

```

EOF

- ClusterRoleBinding 역할 -이 역할은가 클러스터 범위 리소스에 액세스하는 AWS Resilience Hub 데 필요한 권한을 부여합니다.

ClusterRoleBinding 역할을 생성하기 위한 템플릿은 다음과 같습니다.

```
cat << EOF | kubectl apply -f -
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-global-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-global-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

3. resilience-hub-eks-access-group를 Amazon EKS 클러스터에 액세스하는 데 사용되는 IAM 역할과 매핑하도록 aws-auth ConfigMap을 업데이트하세요.

이 단계는 1단계에서 사용한 IAM 역할과 2단계에서 생성된 Kubernetes 그룹 간의 매핑을 생성합니다. 이 매핑은 Amazon EKS 클러스터 내의 리소스에 액세스할 수 있는 권한을 IAM 역할에 부여합니다.

Note

- ROLE-NAME은 Amazon EKS 클러스터에 액세스하는 데 사용되는 IAM 역할을 나타냅니다.
- 애플리케이션이 역할 기반 액세스를 사용하도록 구성된 경우 역할은 애플리케이션을 생성하는 AWS Resilience Hub 동안 전달되는 호출자 역할 또는 보조 계정 역할이어야 합니다.

- 현재 IAM 사용자를 사용하여 리소스에 액세스하도록 애플리케이션을 구성한 경우 해당 사용자는 반드시 `AwsResilienceHubAssessmentEKSAccessRole`이어야 합니다.
- `ACCOUNT-ID`는 Amazon EKS 클러스터의 AWS 계정 ID여야 합니다.

다음 방법 중 하나를 사용하여 `aws-auth ConfigMap`를 설치할 수 있습니다.

- `eksctl` 사용하기

다음 명령을 실행하여 `aws-auth ConfigMap`를 업데이트합니다.

```
eksctl create iamidentitymapping \
  --cluster <cluster-name> \
  --region=<region-code> \
  --arn arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>\
  --group resilience-hub-eks-access-group \
  --username AwsResilienceHubAssessmentEKSAccessRole
```

- `ConfigMap` 언더 데이터 `mapRoles` 섹션에 IAM 역할 세부 정보를 추가하여 `aws-auth ConfigMap`를 수동으로 편집할 수 있습니다. `aws-auth ConfigMap`를 편집하려면 다음 명령을 입력합니다.

```
kubectl edit -n kube-system configmap/aws-auth
```

`mapRoles` 섹션에는 다음 파라미터가 포함될 수 있습니다.

- `rolearn` — 추가될 IAM 역할의 [Amazon 리소스 이름\(ARN\)](#)입니다.
 - ARN 구문 — `arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`.
- `username` — Kubernetes 내에서 IAM 역할에 매핑할 사용자 이름 (`AwsResilienceHubAssessmentEKSAccessRole`)
- `groups` — 그룹 이름은 2단계 (`resilience-hub-eks-access-group`) 에서 만든 그룹 이름과 일치해야 합니다.

Note

`mapRoles` 섹션이 없는 경우 이 섹션을 수동으로 추가해야 합니다.

다음 템플릿을 사용하여 ConfigMap 언더 데이터 mapRoles 섹션에 IAM 역할 세부 정보를 추가합니다.

```
- groups:
  - resilience-hub-eks-access-group
  rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
  username: AwsResilienceHubAssessmentEKSAccessRole
```

Amazon Simple Notification Service 주제에 AWS Resilience Hub 게시하도록 활성화

이 섹션에서는 AWS Resilience Hub 가 Amazon Simple Notification Service(Amazon SNS) 주제에 애플리케이션에 대한 알림을 게시하도록 활성화하는 방법을 설명합니다. Amazon SNS 주제에 푸시 알림을 설정하려면 다음이 있는지 확인하세요.

- 활성 AWS Resilience Hub 애플리케이션입니다.
- 가 알림을 전송 AWS Resilience Hub 해야 하는 기존 Amazon SNS 주제입니다. Amazon SNS 주제 생성에 대한 자세한 내용은 [Amazon SNS 주제 생성](#)을 참조하세요.

AWS Resilience Hub 가 Amazon SNS 주제에 알림을 게시하도록 하려면 Amazon SNS 주제의 액세스 정책을 다음과 같이 업데이트해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubPublish",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name"
    }
  ]
}
```

Note

AWS Resilience Hub 를 사용하여 옵트인 리전의 메시지를 기본적으로 활성화된 리전에 있는 주제에 게시하는 경우 Amazon SNS 주제에 대해 생성된 리소스 정책을 수정해야 합니다. 원금 값을 `resiliencehub.amazonaws.com`에서 `resiliencehub.<opt-in-region>.amazonaws.com`로 변경합니다.

서버 측 암호화 (SSE) Amazon SNS 주제를 사용하는 경우 AWS Resilience Hub 에게 Amazon SNS 암호화 키에 대한 Decrypt 및 GenerateDataKey * 액세스 권한이 있는지 확인해야 합니다.

및에 대한 Decrypt GenerateDataKey* 액세스를 제공하려면 정책에 AWS Key Management Service 액세스할 수 있는 다음 권한을 포함해야 AWS Resilience Hub합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubDecrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id"
    }
  ]
}
```

AWS Resilience Hub 권장 사항을 포함하거나 제외할 수 있는 권한 제한

AWS Resilience Hub 를 사용하면 애플리케이션당 추천을 포함하거나 제외하도록 권한을 제한할 수 있습니다. 다음 IAM 신뢰 정책을 사용하여 애플리케이션별 권장 사항을 포함하거나 제외하도록 권한을 제한할 수 있습니다. 이 IAM 신뢰 정책에서는 `caller_IAM_role` (AWS 사용자 계정과 연결됨)가 현재 계정에서 APIs를 호출하는 데 사용됩니다 AWS Resilience Hub.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": "resiliencyhub:BatchUpdateRecommendationStatus",
    "Resource": "arn:aws:resiliencyhub:us-west-2:12345678900:app/0e6237b7-23ba-4103-
adb2-91811326b703"
  }
]
```

의 인프라 보안 AWS Resilience Hub

관리형 서비스인 Amazon Web Services: 보안 프로세스 개요 백서에 설명된 AWS 글로벌 네트워크 보안 절차로 AWS Resilience Hub 보호됩니다. https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

AWS 게시된 API 호출을 사용하여 네트워크를 AWS Resilience Hub 통해 액세스합니다. 클라이언트가 전송 계층 보안(TLS) 1.2 이상을 지원해야 합니다. TLS 1.3 이상을 권장합니다. 클라이언트는 Ephemeral Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 PFS(전달 완전 보안, Perfect Forward Secrecy)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 보안 암호 액세스 키를 사용하여 서명해야 합니다. 또는 [AWS Security Token Service](#)(AWS STS)를 사용하여 임시 자격 증명을 생성하여 요청에 서명할 수 있습니다.

AWS 서비스에 대한 복원력 검사

이 장에서는 애플리케이션의 복원력 태세가 영향을 받지 않도록 지원되는 AWS 서비스에 AWS Resilience Hub 대해에서 수행하는 다양한 복원력 검사에 대한 세부 정보를 제공합니다. 이러한 검사는 각 Application Component(AppComponent)의 복원력 정책에 정의된 값을 기준으로 복구 시간 목표(RTO) 및 복구 시점 목표(RPO)를 추정합니다. 평가에는 애플리케이션, 인프라 장애, AZ 중단 및 리전 장애와 같은 다양한 유형의 중단이 포함됩니다. 그러나 이러한 검사를 실행하려면 리소스에 액세스할 수 있도록 AWS Resilience Hub에 관련 IAM 권한을 제공해야 합니다. 이 장에서가 리소스에 액세스하고 복원력 검사를 수행할 수 있도록 허용하는 AWS Resilience Hub에 필요한 IAM 권한에 대해 자세히 알아보려면 섹션을 참조하세요 [AWS에 대한 관리형 정책](#) [AWS Resilience Hub](#).

AWS 서비스

- [Amazon Elastic File System](#)
- [Amazon Relational Database Service](#) 및 [Amazon Aurora](#)
- [Amazon Simple Storage Service\(S3\)](#)
- [Amazon DynamoDB](#)
- [Amazon Elastic Compute Cloud](#)
- [Amazon EBS](#)
- [AWS Lambda](#)
- [Amazon Elastic Kubernetes 서비스](#)
- [Amazon Simple Notification Service](#)
- [Amazon Simple Queue Service](#)
- [Amazon Elastic Container Service](#)
- [Elastic Load Balancing](#)
- [Amazon API Gateway](#)
- [Amazon DocumentDB](#)
- [NAT 게이트웨이](#)
- [Amazon Route 53](#)
- [Amazon Application Recovery Controller\(ARC\)](#)
- [Amazon FSx for Windows File Server](#)
- [AWS Step Functions](#)
- [Amazon ElastiCache \(Redis OSS\)](#)

Amazon Elastic File System

이 섹션에서는 Amazon Elastic File System과 관련된 모든 복원력 검사 및 권장 사항을 나열합니다. Amazon Elastic File System에 대한 자세한 내용은 [Amazon Elastic File System 설명서를](#) 참조하세요.

파일 시스템 유형

AWS Resilience Hub 는 파일 시스템 유형: 리전 또는 One Zone을 확인합니다. 파일 시스템 유형은 인프라 또는 AZ 중단 시 복원력에 영향을 미칩니다. 파일 시스템 유형에 대한 자세한 내용은 [Amazon EFS 파일 시스템의 가용성 및 내구성을](#) 참조하세요.

파일 시스템 백업

AWS Resilience Hub 는 배포된 파일 시스템에 대한 AWS Backup 계획이 정의되어 있는지 확인합니다. 또한 Cross-Region 백업 옵션이 활성화되어 있는지 확인하여 정책에서 요구하는 경우 리전 수준 중단에 대한 적용 범위를 보장합니다.

데이터 복제

AWS Resilience Hub 는 배포된 파일 시스템에 대해 리전 내 또는 리전 간 Amazon EFS 데이터 복제가 정의되어 있는지 확인합니다. Amazon EFS 데이터 복제는 애플리케이션, 인프라, AZ 및 리전 수준에서 예상 RTO 및 예상 RPO를 개선하는 데 도움이 됩니다. 또한 애플리케이션 중단 시 파일 시스템 복원력을 활성화 AWS Backup 하기 위해 리전 내와 결합되었는지 AWS Resilience Hub 확인합니다.

Amazon Relational Database Service 및 Amazon Aurora

이 섹션에서는 Amazon Relational Database Service 및 Amazon Aurora에 특정한 모든 복원력 검사 및 권장 사항을 나열합니다. Amazon Relational Database Service 및 Amazon Aurora에 대한 자세한 내용은 [Amazon Relational Database Service 설명서를](#) 참조하세요.

단일 AZ 배포

AWS Resilience Hub 는 데이터베이스가 단일 인스턴스로 배포되었는지 확인하고, 결정된 경우 보조 인스턴스 및 읽기 전용 복제본을 지원하지 않음을 나타냅니다.

다중 AZ 배포

AWS Resilience Hub 는 데이터베이스가 보조 인스턴스 또는 읽기 전용 복제본과 함께 배포되었는지 확인합니다. 데이터베이스가 읽기 전용 복제본과 함께 배포된 경우,는 AZ 중단 시 장애 조치를 허용하도록 다른 AZ에 배포되었는지 AWS Resilience Hub 확인합니다.

백업

AWS Resilience Hub 는 배포된 데이터베이스 인스턴스에 다음 백업 기능이 적용되는지 확인합니다.

- AWS Backup 자동 백업 옵션을 사용한 계획
- AWS Backup 정책에 필요한 경우 리전 간 백업 복사본으로 계획
- 타사 백업 시스템의 수동 스냅샷

리전 간 장애 조치

AWS Resilience Hub 는 복원력 정책에 정의된 RTO 및 RPO 대상을 확인하여 리전 중단으로부터 복구합니다. 또한 AWS Resilience Hub 는 다음과 같은 리전 간 아키텍처를 식별하여 리전 중단을 처리할 수 있습니다.

- 리전 간 스냅샷 사본이 포함된 리전 내 백업
- 다른 리전의 읽기 전용 복제본
- 다른 리전에 보조 클러스터가 있는 Amazon Aurora 글로벌 데이터베이스
- 다른 리전에 헤드리스 보조 클러스터가 있는 Amazon Aurora 글로벌 데이터베이스

더 빠른 리전 내 장애 조치

AWS Resilience Hub 는 인프라 또는 AZ 중단 중에 복원력 정책에 정의된 RTO 및 RPO 대상을 확인합니다. 또한 AWS Resilience Hub 는 다음과 같은 리전 내 아키텍처를 식별하여 애플리케이션, 인프라 및 AZ 중단을 처리할 수 있습니다.

- 리전 내 백업
- 다른 AZ의 읽기 전용 복제본
- 다른 AZ에 읽기 전용 복제본이 있는 Aurora 클러스터
- Amazon Relational Database Service의 다중 AZ 인스턴스(Amazon RDS)
- Amazon RDS 다중 AZ 클러스터
- 다른 AZ에 읽기 전용 복제본이 있는 Amazon RDS의 단일 인스턴스

Amazon Simple Storage Service(S3)

이 섹션에서는 Amazon Simple Storage Service(Amazon S3. Amazon S3에 대한 자세한 내용은 [Amazon S3 설명서를](#) 참조하세요.

버전 관리

AWS Resilience Hub 는 Amazon S3 버킷이 버전 관리가 활성화된 상태로 구성되어 있는지 확인합니다.

예약된 백업

AWS Resilience Hub 는 배포된 Amazon Simple Storage Service(Amazon S3) 버킷에 대한 AWS Backup 계획이 정의되어 있는지 확인합니다. 또한 정책에 리전 수준 중단에 대한 적용 범위가 필요한 경우 리전 간 백업 옵션이 활성화되어 있는지 확인합니다.

시점 복구

AWS Resilience Hub 는 복원력 정책의 RPO 대상에 point-in-time으로 복구(PITR)가 필요한지 확인합니다. 그러나 PITR에는 교차 리전 백업이 지원되지 않습니다. 따라서 리전 간 백업 옵션이 활성화된 기존 예약 AWS Backup 계획을 사용하거나 새 계획을 생성합니다.

데이터 복제

AWS Resilience Hub 는 배포된 Amazon S3 버킷에 대해 동일한 리전 복제(SRR) 및 교차 리전 복제(CRR)가 정의되어 있는지 확인합니다. Amazon S3 데이터 복제는 애플리케이션, 인프라, AZ 및 리전 수준에서 예상 워크로드 RTO 및 예상 워크로드 RPO를 개선합니다. 또한 객체 버전의 삭제는 대상 Amazon S3 버킷에 복제되지 않으므로 객체의 물리적 삭제로부터 보호합니다. 또한 복원력 정책에 정의된 RTO 대상을 기반으로 Amazon S3 복제 시간 제어(S3 RTC)를 활성화해야 하는지 여부를 AWS Resilience Hub 확인합니다. 이 청구 가능한 기능은 15분 이내에 소스 버킷 객체의 99.99%를 복제합니다.

- AWS Backup 자동 백업 옵션을 사용한 계획
- AWS Backup 정책에 필요한 경우 리전 간 백업 복사본으로 계획
- 타사 백업 시스템의 수동 스냅샷

Amazon DynamoDB

이 섹션에서는 Amazon DynamoDB에 특정한 모든 복원력 검사 및 권장 사항을 나열합니다. Amazon DynamoDB에 대한 자세한 내용은 [Amazon DynamoDB 설명서를](#) 참조하세요.

예약된 백업

AWS Resilience Hub 는 배포된 테이블에 백업이 이미 정의되어 있는지 확인합니다. 또한 리전 수준 중단에 대한 적용 범위가 필요한 경우 정책에 대해 리전 간 백업을 구성해야 하는지도 확인합니다.

시점 복구

AWS Resilience Hub 는 복원력 정책의 RPO 목표에 따라 point-in-time으로 복구(PITR)가 필요한지 확인합니다. 그러나 PITR에는 교차 리전 백업이 지원되지 않습니다. 따라서 리전 간 백업 옵션이 활성화된 기존 예약 AWS Backup 계획을 사용하거나 새 계획을 생성합니다.

글로벌 테이블

AWS Resilience Hub 는 배포된 Amazon DynamoDB 테이블이 다른 리전에 하나 이상의 복제본이 있는 글로벌 테이블로 정의되어 있는지 확인합니다. 글로벌 테이블을 설정하면 리전 수준에서 예상 워크로드 RTO와 예상 워크로드 RPO가 개선되고 액티브-액티브 또는 액티브-패시브 다중 리전 모드에서 작업할 수 있는 기능도 제공됩니다. AWS Backup 또는 Amazon DynamoDB PITR을 리전 중 하나에서 사용하여 애플리케이션 중단을 처리할 수 있습니다.

Amazon Elastic Compute Cloud

이 섹션에서는 Amazon Elastic Compute Cloud에 특정한 모든 복원력 검사 및 권장 사항을 나열합니다. Amazon Elastic Compute Cloud에 대한 자세한 내용은 [Amazon Elastic Compute Cloud 설명서를](#) 참조하세요.

상태 저장 인스턴스

AWS Resilience Hub 는 다음 기준 중 하나가 충족되는 경우 Amazon EC2 인스턴스를 상태 저장 인스턴스로 식별합니다.

- DeleteOnTermination 속성이이 인스턴스에 연결된 하나 이상의 Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 false로 설정된 경우.

- Amazon Data Lifecycle Manager 또는 AWS Backup 계획이 Amazon EC2 인스턴스 또는 하나 이상의 Amazon EBS 볼륨에 연결된 경우.
- AWS Elastic Disaster Recovery 가 Amazon EC2 인스턴스 스토리지 볼륨을 복제하는 데 사용되는 경우.

Note

Amazon EC2 인스턴스가 위의 기준 중 하나라도 충족하지 않는 경우는 이를 상태 비저장 Amazon EC2 인스턴스로 AWS Resilience Hub 취급합니다.

Auto Scaling 그룹

AWS Resilience Hub 는 상태 비저장 Amazon EC2 인스턴스 그룹을 확인합니다. 검색된 경우 다중 AZ 구성의 Auto Scaling 그룹(ASG)을 사용하여 동일한를 오케스트레이션하는 것이 좋습니다. 기존 ASG 가 식별되면 ARH는 여러 가용 영역에 걸쳐 구성되었는지 확인합니다. 스팟 Amazon EC2 인스턴스만 사용하여 ASG를 정의하는 경우 스팟 Amazon EC2 인스턴스를 사용할 수 없는 경우 복원력을 개선하기 위해 온디맨드 Amazon EC2 인스턴스로 용량을 늘리는 것이 좋습니다.

Amazon EC2 플릿

AWS Resilience Hub 는 Amazon EC2 플릿을 식별하고 다중 AZ 배포로 정의되었는지, 스팟 Amazon EC2 인스턴스만 사용하는지 확인합니다. Amazon EC2 플릿을 다중 AZ 배포로 정의하면 AZ 중단 시 복원력이 향상됩니다. 온디맨드 인스턴스로 Amazon EC2 플릿을 보강하면 스팟 인스턴스를 사용할 수 없을 때 복원력이 향상됩니다.

Amazon EBS

이 섹션에서는 Amazon EBS와 관련된 모든 복원력 검사 및 권장 사항을 나열합니다. Amazon EBS에 대한 자세한 내용은 [Amazon EBS 설명서를](#) 참조하세요.

예약된 백업

AWS Resilience Hub 는 Amazon EBS 볼륨에 다음 중 하나 또는 둘 다 정의되어 있는지 확인합니다.

- Amazon EC2 인스턴스에 연결된 특정 Amazon EBS 볼륨에 대한 백업 규칙입니다.
- Amazon EC2 인스턴스에 Amazon EBS 지원 AMI를 생성하는 백업 규칙입니다.

- 타사 백업 시스템의 수동 스냅샷입니다.

또한 정책에 리전 수준 중단에 대한 적용 범위가 필요한 경우는 백업 규칙에 리전 간 백업 옵션이 활성화되어 있는지 AWS Resilience Hub 확인합니다.

데이터 백업 및 복제

AWS Resilience Hub 는 다음 기준 중 하나가 충족되는 경우 Amazon EBS 볼륨이 상태 저장 볼륨으로 간주됨을 식별합니다.

- DeleteOnTermination 속성이이 Amazon EBS 볼륨에 대해 false로 설정된 경우.
- Amazon Data Lifecycle Manager 또는 AWS Backup 계획이이 Amazon EBS 볼륨 또는 연결된 Amazon EC2 인스턴스와 연결된 경우.
- AWS Elastic Disaster Recovery 가 Amazon EC2 인스턴스 스토리지 볼륨을 복제하는 데 사용되는 경우.

AWS Lambda

이 섹션에는 관련된 모든 복원력 검사 및 권장 사항이 나열되어 있습니다 AWS Lambda. 에 대한 자세한 내용은 [AWS Lambda 설명서를](#) AWS Lambda참조하세요.

고객 Amazon VPC 액세스

AWS Resilience Hub 는 VPC에 연결된 AWS Lambda 함수를 식별합니다. Amazon VPC의 서로 다른 AZs에 AWS Lambda 있는 서브넷에 연결하면 AZ 중단 시 함수 복원력이 지원됩니다.

Dead Letter Queue(DLQ)

AWS Resilience Hub 는 실패한 요청을 저장하기 위해 AWS Lambda 함수에 DLQ(Dead Letter Queue)가 연결되어 있는지 확인합니다. DLQ를 AWS Lambda 함수에 연결하면요청의 데이터 손실을 방지하고 나중에 실패한 요청을 다시 처리할 수 있습니다.

Amazon Elastic Kubernetes 서비스

이 섹션에서는 Amazon Elastic Kubernetes Service(Amazon EKS)와 관련된 모든 복원력 검사 및 권장 사항을 나열합니다. Amazon EKS에 대한 자세한 내용은 [Amazon EKS 설명서를](#) 참조하세요.

다중 AZ 배포

AWS Resilience Hub 는 포드 배포가 여러 AZs. 복원력 정책에 리전 중단 시 적용 범위가 필요한 경우 다른 리전의 추가 Amazon EKS 클러스터가 필요합니다. 이 추가 Amazon EKS 클러스터는 여러 AZs.

배포와 ReplicaSet 비교

AWS Resilience Hub 는 배포 대신 ReplicaSets 또는 포드 객체를 사용하는지 확인합니다. ReplicaSets 또는 포드 객체를 배포로 바꾸면 포드 업데이트가 새 버전의 소프트웨어로 간소화되고 다른 유용한 기능이 포함됩니다.

배포 유지 관리

AWS Resilience Hub 는 배포에 다음 모범 사례가 사용되는지 확인합니다.

- PDB(Pod Disruption Budget) 사용 - PDB를 사용하면 언제든지 중단될 수 있는 워크로드의 포드 수에 제한을 설정하여 가용성을 개선할 수 있습니다.
- 자체 관리형 노드 그룹을 Amazon EKS 관리형 노드 그룹으로 대체 -이 대체는 유지 관리 중에 작업자 노드 이미지 업데이트를 간소화합니다.
- 배포당 동적 CPU 및 메모리 요청 지원 - 이러한 요청은 Kubernetes가 포드의 요구 사항에 맞는 노드를 선택하는 데 도움이 됩니다.
- 모든 컨테이너에 대한 라이브니스 및 준비 프로브 구성 - 라이브니스 프로브를 구성하면 비기능적 포드를 다시 시작하여 복원력을 개선하는 데 도움이 됩니다. 준비 프로브를 구성하면 트래픽을 사용량이 많은 포드에서 우회하여 가용성을 개선할 수 있습니다.
- Karpenter, Cluster Autoscaler 또는 구성 AWS Fargate - 이러한 구성을 통해 Amazon EKS 클러스터의 인프라를 확장하고 워크로드 수요를 충족할 수 있습니다.
- Horizontal Pod Autoscaler 구성 -이 구성을 통해 Amazon EKS 클러스터는 요청 처리 수요에 맞게 워크로드를 자동으로 확장할 수 있습니다.

Amazon Simple Notification Service

이 섹션에서는 Amazon Simple Notification Service(Amazon SNS)와 관련된 모든 복원력 검사 및 권장 사항을 나열합니다. Amazon SNS에 대한 자세한 내용은 [Amazon SNS 설명서](#)를 참조하세요.

주제 구독

AWS Resilience Hub 는 수신 메시지가 손실되지 않도록 Amazon SNS 주제에 하나 이상의 구독이 연결되어 있는지 확인합니다.

Amazon Simple Queue Service

이 섹션에서는 Amazon Simple Queue Service(Amazon SQS)와 관련된 모든 복원력 검사 및 권장 사항을 나열합니다. Amazon SQS에 대한 자세한 내용은 [Amazon SQS 설명서를](#) 참조하세요.

Dead Letter Queue(DLQ)

AWS Resilience Hub 는 구독자에게 성공적으로 전달할 수 없는 메시지를 처리하기 위해 Amazon SQS 대기열에 연결된 DLQ가 있는지 확인합니다.

Amazon Elastic Container Service

이 섹션에서는 Amazon Elastic Container Service(Amazon ECS)와 관련된 모든 복원력 검사 및 권장 사항을 나열합니다. Amazon ECS에 대한 자세한 내용은 [Amazon ECS 설명서를](#) 참조하세요.

다중 AZ 배포

AWS Resilience Hub 는 Amazon EC2 또는 AWS Fargate 시작 유형을 기반으로 Amazon EC2 태스크 또는 서비스가 여러 AZs에서 실행 중인지 확인합니다. 정책에 리전 중단에 대한 적용 범위가 필요한 경우 다른 리전의 추가 Amazon ECS 클러스터가 필요합니다. 또한 추가 클러스터는 여러 AZs.

Elastic Load Balancing

이 섹션에는 Elastic Load Balancing과 관련된 모든 복원력 검사 및 권장 사항이 나열되어 있습니다. Elastic Load Balancing에 대한 자세한 내용은 [Elastic Load Balancing 설명서를](#) 참조하세요.

다중 AZ 배포

AWS Resilience Hub 는 Elastic Load Balancing이 여러 AZs에서 실행 중인지 확인합니다.

정책에 리전 중단에 대한 적용 범위가 필요한 경우 다른 리전의 추가 Elastic Load Balancing이 필요합니다. 다른 리전에 위치한 추가 Elastic Load Balancing도 여러 AZs.

Amazon API Gateway

이 섹션에서는 Amazon API Gateway와 관련된 모든 복원력 검사 및 권장 사항을 나열합니다. Amazon API Gateway에 대한 자세한 내용은 [Amazon API Gateway 설명서를](#) 참조하세요.

리전 간 배포

정책에서 리전 종단을 고려해야 하는 경우는 다른 리전에 Amazon API Gateway API 리소스가 추가로 배포되었는지 AWS Resilience Hub 확인합니다.

프라이빗 API 다중 AZ 배포

AWS Resilience Hub 는 API가 Amazon API Gateway 내에서 프라이빗으로 정의되어 있는지 확인합니다. 프라이빗 APIs는 여러 AZs.

Amazon DocumentDB

이 섹션에는 Amazon DocumentDB와 관련된 모든 점검 및 권장 사항이 나열되어 있습니다. Amazon DocumentDB에 대한 자세한 내용은 [Amazon DocumentDB 설명서를](#) 참조하세요.

다중 AZ 배포

AWS Resilience Hub 는 Amazon DocumentDB 클러스터가 여러 AZs에 배포되었는지 확인합니다. 정책에 리전 종단에 대한 적용 범위가 필요한 경우 다른 리전에 추가 보조 Amazon DocumentDB 클러스터가 필요합니다. 다른 리전에 위치한 추가 Amazon DocumentDB 클러스터도 여러 AZs에서 실행이 확인됩니다.

탄력적 클러스터 및 다중 AZ 배포

AWS Resilience Hub 는 Amazon DocumentDB Elastic 클러스터 샤드가 다른 AZs에 배포된 읽기 전용 복제본을 사용하고 있는지 확인합니다.

탄력적 클러스터 및 수동 스냅샷

AWS Resilience Hub 는 Amazon DocumentDB Elastic 클러스터에 대해 수동 스냅샷이 정기적으로 생성되는지 확인합니다. 수동 스냅샷은 지속성을 높이고 비즈니스 요구 사항에 맞게 스냅샷 빈도를 유연하게 설정할 수 있습니다.

NAT 게이트웨이

이 섹션에는 NAT Gateway와 관련된 모든 점검 및 권장 사항이 나열되어 있습니다. NAT 게이트웨이에 대한 자세한 내용은 [NAT 게이트웨이를 참조하세요](#).

다중 AZ 배포

AWS Resilience Hub 는 NAT Gateway가 여러 AZs에 배포되었는지 확인합니다. 정책에 리전 중단에 대한 적용 범위가 필요한 경우 다른 리전에서 추가 NAT Gateway 배포가 필요합니다. 다른 리전에 위치한 추가 NAT 게이트웨이라도 여러 AZs.

Amazon Route 53

이 섹션에는 Amazon Route 53과 관련된 모든 점검 및 권장 사항이 나열되어 있습니다. Amazon Route 53에 대한 자세한 내용은 [Amazon Route 53 설명서를 참조하세요](#).

다중 AZ 배포

AWS Resilience Hub 는 Amazon Route 53 호스팅 영역 레코드가 동일한 리전의 여러 대상으로 정의되어 있는지, 그리고 이러한 대상이 여러 AZs에 배포되어 있는지 확인합니다. 정책에 리전 중단에 대한 적용 범위가 필요한 경우 AWS Resilience Hub 는 Amazon Route 53 호스팅 영역 레코드가 리전당 여러 대상이 있는 여러 리전에 정의되어 있는지, 그리고 이러한 대상이 여러 AZs에 배포되었는지 확인합니다.

Amazon Application Recovery Controller(ARC)

이 섹션에는 Amazon Application Recovery Controller(ARC)(ARC)와 관련된 모든 점검 및 권장 사항이 나열되어 있습니다. ARC에 대한 자세한 내용은 [ARC 설명서를 참조하세요](#).

다중 AZ 배포

AWS Resilience Hub 는 여러 리전에 유사한 리소스가 배포되었는지 확인하고는 ARC 준비 확인을 정의하여 리전 중단 시 가용성과 준비 상태를 높이는 모범 사례를 권장합니다. 시간당 추가 요금이 발생한다는 알림을 받게 됩니다.

Amazon FSx for Windows File Server

이 섹션에는 Amazon FSx for Windows File Server와 관련된 모든 확인 및 권장 사항이 나열되어 있습니다. Amazon FSx for Windows File Server에 대한 자세한 내용은 [Amazon FSx for Windows File Server 설명서를](#) 참조하세요.

파일 시스템 유형

AWS Resilience Hub 는 파일 시스템 유형: Regional 또는 One Zone. 파일 시스템 유형은 인프라 또는 AZ 중단 시 복원력에 영향을 미칩니다. 파일 시스템 유형에 대한 자세한 내용은 [Amazon EFS](#)를 참조하세요.

파일 시스템 백업

AWS Resilience Hub AWS Backup 는 배포된 파일 시스템에 정의되어 있는지 확인합니다. 또한 정책에 리전 수준 중단에 대한 적용 범위가 필요한 경우 cross-Region backup 옵션이 활성화되어 있는지 확인합니다.

데이터 복제

AWS Resilience Hub 는 배포된 파일 시스템에 대해 리전 내 또는 리전 간 예약된 AWS DataSync 데이터 복제 작업이 정의되어 있는지 확인합니다.

AWS DataSync 예약된 데이터 복제 작업은 인프라, AZ 및 리전 수준에서 예상 워크로드 RTO 및 예상 워크로드 RPO를 개선할 수 있습니다. 또한 애플리케이션 중단 시 복구를 AWS Backup 위해 리전 내와 결합할 수 있습니다.

AWS Step Functions

이 섹션에는 관련된 모든 점검 및 권장 사항이 나열되어 있습니다 AWS Step Functions. 에 대한 자세한 내용은 [AWS Step Functions 설명서를](#) 참조하세요.

버전 관리 및 별칭

AWS Resilience Hub 는 AWS Step Functions 워크플로가 버전 관리 및 별칭을 사용하여 재배포 시간을 개선하는지 확인합니다.

리전 간 배포

AWS Resilience Hub 는 리전 중단 시 복구할 수 있도록 동일한 AWS Step Functions 워크플로 유형의 워크플로가 다른 리전에 배포되었는지 확인합니다.

Amazon ElastiCache (Redis OSS)

이 섹션에는 Amazon ElastiCache(Redis OSS)와 관련된 모든 점검 및 권장 사항이 나열되어 있습니다.

Amazon ElastiCache(Redis OSS)에 대한 자세한 내용은 [Amazon ElastiCache 설명서를](#) 참조하세요.

단일 AZ 배포

AWS Resilience Hub 는 Amazon ElastiCache(Redis OSS) 클러스터가 단일 노드로 배포되었는지 아니면 단일 가용 영역에 있는 모든 노드와 함께 배포되었는지 확인합니다.

단일 AZ 배포

AWS Resilience Hub 는 Amazon ElastiCache(Redis OSS) 클러스터가 여러 가용 영역에 걸쳐 복제 그룹(클러스터 모드 활성화 클러스터와 클러스터 모드 비활성화 클러스터 모두)으로 배포되어 가용 영역 중단 시 장애 조치를 허용하는지 확인합니다.

리전 간 장애 조치

AWS Resilience Hub 는 복원력 정책에 정의된 RTO 및 RPO 대상을 확인하여 리전 중단으로부터 복구합니다. 또한 AWS Resilience Hub 는 여러 리전에 배포된 Amazon ElastiCache(Redis OSS) 글로벌 데이터 스토어 클러스터를 식별할 수 있습니다.

백업

AWS Resilience Hub 는 배포된 Amazon ElastiCache(Redis OSS) 또는 자체 설계된 클러스터에 다음 백업 기능이 적용되는지 확인합니다.

- 자동 백업
- 타사 백업 시스템의 수동 백업

AWS Resilience Hub 는 백업을 사용하지 않는 경우 백업을 복구 방법으로 권장하지 않습니다. 그러나 데이터 불일치가 발생할 경우 캐시 계층을 재설정하고 기본 스토리지에서 데이터를 다시 생성할 수 있습니다.

더 빠른 리전 내 장애 조치

AWS Resilience Hub 는 인프라 또는 AZ 중단 중에 복원력 정책에 정의된 RTO 및 RPO 대상을 확인합니다. 또한 AWS Resilience Hub 는 다음과 같은 리전 내 아키텍처를 식별하여 인프라 및 AZ 중단으로부터 복구할 수 있습니다.

- 클러스터 모드 비활성화된 유형의 Amazon ElastiCache(Redis OSS) 클러스터에 대한 다른 가용 영역의 보조 대기 노드 인스턴스입니다.
- 클러스터 모드 지원 유형의 Amazon ElastiCache(Redis OSS) 클러스터에 대한 모든 샤드당 다른 가용 영역의 보조 대기 노드 인스턴스입니다.

다른 서비스와 함께 사용

이 섹션에서는와 상호 작용하는 AWS 서비스에 대해 설명합니다 AWS Resilience Hub.

주제

- [AWS CloudFormation](#)
- [AWS CloudTrail](#)
- [AWS Systems Manager](#)
- [AWS Trusted Advisor](#)

AWS CloudFormation

AWS Resilience Hub 는 AWS 리소스 및 인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있도록 리소스를 모델링하고 설정하는 데 도움이 되는 AWS CloudFormation 서비스와 통합됩니다. 원하는 모든 AWS 리소스(예: AWS::ResilienceHub::ResiliencyPolicy 및 AWS::ResilienceHub::App)를 설명하고 해당 리소스를 AWS CloudFormation 프로비저닝하고 구성하는 템플릿을 생성합니다.

를 사용하면 템플릿을 재사용하여 AWS Resilience Hub 리소스를 일관되고 반복적으로 설정할 AWS CloudFormation 수 있습니다. 리소스를 한 번 설명한 다음 여러 AWS 계정 및 리전에서 동일한 리소스를 반복적으로 프로비저닝합니다.

AWS Resilience Hub 및 AWS CloudFormation 템플릿

AWS Resilience Hub 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 [AWS CloudFormation 템플릿](#)을 이해해야 합니다. 템플릿은 JSON 또는 YAML로 서식 지정된 텍스트 파일입니다. 이러한 템플릿은 AWS CloudFormation 스택에서 프로비저닝하려는 리소스를 설명합니다. JSON 또는 YAML에 익숙하지 않은 경우 AWS CloudFormation Designer를 사용하여 AWS CloudFormation 템플릿을 시작할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서에서 [AWS CloudFormation Designer이란 무엇입니까?](#)를 참조하세요.

AWS Resilience Hub 는에서 AWS::ResilienceHub::ResiliencyPolicy 및 AWS::ResilienceHub::App 생성을 지원합니다 AWS CloudFormation. AWS::ResilienceHub::ResiliencyPolicy 및 AWS::ResilienceHub::App에 대한 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 [AWS Resilience Hub 리소스 유형 참조](#)를 참조하세요.

AWS CloudFormation 스택을 사용하여 AWS Resilience Hub 애플리케이션을 정의할 수 있습니다. 스택을 사용하면 관련 리소스를 단일 단위로 관리할 수 있습니다. 스택에는 웹 서버 또는 네트워킹 규칙과 같은 웹 애플리케이션을 실행하는 데 필요한 모든 리소스가 포함될 수 있습니다.

에 대해 자세히 알아보기 AWS CloudFormation

에 대한 자세한 내용은 다음 리소스를 AWS CloudFormation 참조하세요.

- [AWS CloudFormation](#)
- [AWS CloudFormation 사용 설명서](#)
- [AWS CloudFormation API Reference](#)
- [AWS CloudFormation 명령줄 인터페이스 사용 설명서](#)

AWS CloudTrail

AWS Resilience Hub 는 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다 AWS Resilience Hub. CloudTrail은에 대한 모든 API 호출을 이벤트 AWS Resilience Hub 로 캡처합니다. 캡처되는 호출에는 AWS Resilience Hub 콘솔의 호출과 AWS Resilience Hub API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하는 경우 이벤트를 포함하여 CloudTrail 이벤트를 Amazon S3 버킷으로 지속적으로 전송할 수 있습니다 AWS Resilience Hub. 트레일을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 수행된 요청, 요청이 수행된 AWS Resilience Hub IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하세요.

AWS Systems Manager

AWS Resilience Hub 는 Systems Manager와 협력하여 해당 SOPs의 기반으로 사용할 수 있는 여러 SSM 문서를 제공하여 SOPs.

AWS Resilience Hub 는 다른 Systems Manager 문서를 실행하는 데 필요한 IAM 역할이 포함된 AWS CloudFormation 템플릿을 제공하며, 특정 문서에 필요한 권한이 있는 문서당 하나의 역할입니다. AWS CloudFormation 템플릿으로 스택을 생성한 후 IAM 역할을 설정하고 Systems Manager 자동화 문서가 다양한 복구 절차를 위해 실행되도록 Systems Manager 파라미터에 메타데이터를 저장합니다.

SOP를 사용하는 방법에 대한 자세한 내용은 [표준 운영 절차 관리](#) 단원을 참조하세요.

AWS Trusted Advisor

AWS Trusted Advisor 는 배포를 식별, 우선 순위 지정 및 최적화하는 데 도움이 되는 AWS 모범 사례 권장 사항이 있는 중앙 집중식 홈입니다. AWS는 AWS 환경을 AWS Trusted Advisor 검사한 다음 비용을 절감하거나 시스템 가용성 및 성능을 개선하거나 보안 격차를 좁힐 기회가 있을 때 확인을 통해 권장 사항을 제공합니다. 이러한 검사는 목적에 따라 여러 범주로 나뉩니다. 다양한 체크인 범주에 대한 자세한 내용은 [AWS Support](#) 사용 설명서를 AWS Trusted Advisor참조하세요.

AWS Trusted Advisor 는 내결함성 범주 AWS Resilience Hub 에서의 각 애플리케이션에 대한 복원력 검사를 통해 여러 가지 높은 수준의 복원력 권장 사항을 제공합니다. 내결함성 범주에는 애플리케이션을 테스트하여 복원력과 신뢰성을 확인하는 모든 검사가 나열됩니다. 이러한 검사는 복원력 위험을 야기하고 비즈니스 연속성을 위한 애플리케이션 가용성에 영향을 미칠 수 있는 AppComponent 장애 및 정책 위반이 있는 경우 알리를 제공합니다. 또한 권장 작업 섹션에서 이러한 위험을 줄일 수 있는 기회를 개선하는 복원력 권장 사항을 제공하며, 이를 해결해야 합니다 AWS Resilience Hub. 의 각 애플리케이션에 대한 권장 사항에 대한 자세한 내용은에 제공된 자세한 권장 사항을 참조하는 AWS Trusted Advisor것이 좋습니다 AWS Resilience Hub.

AWS Trusted Advisor 는의 각 애플리케이션에 대해 AWS Resilience Hub다음과 같은 검사를 제공합니다.

- AWS Resilience Hub 애플리케이션 복원력 점수 -의 최신 평가에서 애플리케이션의 복원력 점수를 AWS Resilience Hub 확인하고 복원력 점수가 특정 값 미만인 경우 알려줍니다.

알림 기준

- 녹색 - 애플리케이션의 복원력 점수가 70 이상임을 나타냅니다.
- 노란색 - 애플리케이션의 복원력 점수가 40~69임을 나타냅니다.
- 빨간색 - 애플리케이션의 복원력 점수가 40 미만임을 나타냅니다.

권장 작업

복원력을 개선하고 애플리케이션에 가장 적합한 복원력 점수를 얻으려면 애플리케이션 리소스의 가장 최근에 업데이트된 버전으로 평가를 실행하고 해당하는 경우 제안된 운영 권장 사항을 구현합니다. 평가 실행, 검토 및 구현, 운영 권장 사항 검토 및 포함/제외, 동일한 평가 구현에 대한 자세한 내용은 다음 주제를 참조하세요.

- [the section called “에서 복원력 평가 실행 AWS Resilience Hub”](#)
- [the section called “평가 보고서 검토”](#)
- [the section called “복원력 권장 사항 검토”](#)

- [the section called “운영 권장 사항 포함 또는 제외”](#)
- AWS Resilience Hub 애플리케이션 정책 위반 - AWS Resilience Hub 애플리케이션이 애플리케이션에 대해 설정한 RTO 및 RPO 대상을 충족하는지 확인하고 애플리케이션이 RTO 및 RPO 대상을 충족하지 않는 경우 알려줍니다.

알림 기준

- 녹색 - 애플리케이션에 정책이 있고 예상 워크로드 RTO 및 예상 워크로드 RPO가 RTO 및 RPO 목표를 충족함을 나타냅니다.
- 노란색 - 애플리케이션에 정책이 있고 평가되지 않았음을 나타냅니다.
- 빨간색 - 애플리케이션에 정책이 있고 예상 워크로드 RTO 및 예상 워크로드 RPO가 RTO 및 RPO 목표를 충족하지 않음을 나타냅니다.

권장 작업

애플리케이션의 예상 워크로드 RTO 및 예상 워크로드 RPO가 정의된 RTO 및 RPO 목표를 여전히 충족하는지 확인하려면 애플리케이션 리소스의 가장 최근에 업데이트된 버전으로 정기적으로 평가를 실행합니다. 또한 애플리케이션의 복원력 정책이 위반되지 않도록 하려면 평가 보고서를 검토하고 제안된 복원력 권장 사항을 구현하는 것이 좋습니다. 가 사용자를 대신하여 매일 평가를 실행할 수 있도록 AWS Resilience Hub 하고, 평가를 실행하고, 복원력 권장 사항을 검토하고, 이를 구현하는 방법에 대한 자세한 내용은 다음 주제를 참조하세요.

- [the section called “애플리케이션 리소스 편집”](#) (가 사용자를 대신하여 매일 평가를 실행 AWS Resilience Hub 하도록 하려면 애플리케이션 절차의 드리프트 알림 설정을 편집하여 일일 자동 평가 확인란을 선택하는 단계를 완료하세요.)
- [the section called “에서 복원력 평가 실행 AWS Resilience Hub”](#)
- [the section called “평가 보고서 검토”](#)
- [the section called “복원력 권장 사항 검토”](#)
- [the section called “운영 권장 사항 포함 또는 제외”](#)
- AWS Resilience Hub 애플리케이션 평가 기간 -의 각 애플리케이션에 대한 평가를 실행한 후 마지막으로 확인한 시간을 확인합니다 AWS Resilience Hub. 지정된 일수 동안 평가를 실행하지 않은 경우 알림이 표시됩니다.

알림 기준

- 녹색 - 지난 30일 동안 애플리케이션에 대한 평가를 실행했음을 나타냅니다.
- 노란색 - 지난 30일 동안 애플리케이션에 대한 평가를 실행하지 않았음을 나타냅니다.

권장 작업

평가를 정기적으로 실행하여 애플리케이션의 복원력 상태를 관리하고 개선합니다 AWS. 사용자를 대신하여 매일 애플리케이션을 평가 AWS Resilience Hub 하려면 AWS Resilience Hub 드리프트 알림에서 이 애플리케이션 일일 자동 평가 확인란을 선택하여 애플리케이션을 활성화할 수 있습니다. 이 애플리케이션 일일 자동 평가를 선택하려면에서 애플리케이션 절차의 드리프트 알림을 편집하려면 확인란을 완료합니다???

 Note

이 확인은 한 번 이상 평가된 애플리케이션의 평가 기간만 결정합니다 AWS Resilience Hub.

- AWS Resilience Hub 애플리케이션 구성 요소 확인 - 애플리케이션의 애플리케이션 구성 요소 (AppComponent)를 복구할 수 없는지 확인합니다. 즉, 중단 이벤트 발생 시이 AppComponent가 복구되지 않으면 알 수 없는 데이터 손실 및 시스템 가동 중지가 발생할 수 있습니다. 알림 기준이 빨간색으로 설정된 경우 AppComponent를 복구할 수 없음을 나타냅니다.

권장 작업

AppComponent가 복구 가능한지 확인하려면 복원력 권장 사항을 검토 및 구현한 다음 새 평가를 실행합니다. 복원력 권장 사항 검토에 대한 자세한 내용은 섹션을 참조하세요 [the section called “복원력 권장 사항 검토”](#).

사용에 대한 자세한 내용은 [AWS Support 사용 설명서를](#) AWS Trusted Advisor참조하세요.

AWS Resilience Hub 사용 설명서의 문서 기록

다음 표에서는 이 릴리스에 대한 설명서를 설명합니다 AWS Resilience Hub.

- API 버전: 최신
- 최종 설명서 업데이트: 2024년 12월 17일

변경 사항	설명	날짜
AWS Resilience Hub 는 이미 구현된 Amazon CloudWatch 경보를 통합합니다.	AWS Resilience Hub 이 제는 이미 구성된 Amazon CloudWatch 경보를 자동으로 감지하고 복원력 평가에 통합하여 애플리케이션의 복원력 상태를 보다 포괄적으로 파악할 수 있습니다. 이 새로운 기능은 AWS Resilience Hub 권장 사항과 현재 모니터링 설정을 결합하여 경보 관리를 간소화하고 평가 정확도를 개선합니다. 자세한 내용은 경보 관리 단원을 참조하십시오.	2024년 12월 17일
AWS Resilience Hub 는 맞춤형 AWS Fault Injection Service 실험을 통해 간소화된 복원력 테스트를 제공하는 추가 기능을 지원했습니다.	AWS Resilience Hub 는 이제 AWS Fault Injection Service (AWS FIS)와의 향상된 통합을 지원하여 특정 애플리케이션 컨텍스트를 기반으로 AWS FIS 작업 및 시나리오를 사용하여 복원력을 개선하는 맞춤형 권장 사항을 제공합니다. 권장 실험 또는 자체 테스트를 실행하면 복원력 점수가 향상되어 시	2024년 12월 17일

간 경과에 따른 변화를 추적할 수 있습니다.

자세한 정보는 다음의 주제를 참조하세요.

- [AWSResilienceHubAssessmentExecutionPolicy](#)
- [AWS Fault Injection Service 실험 관리](#)
- [AWS Resilience Hub – 복원력 테스트](#)

[AWS Resilience Hub 요약 보기 소개](#)

AWS Resilience Hub의 새로운 요약 보기는 명확한 차트와 그래프를 통해 애플리케이션의 복원력을 개괄적으로 시각적으로 표현하여 애플리케이션 포트폴리오의 상태를 시각화하고 중단을 견디고 복구할 수 있는 애플리케이션의 능력을 효율적으로 관리하고 개선할 수 있습니다. 새 요약 보기 외에도 요약 보기를 지원하는 데이터를 내보내 이해관계자 커뮤니케이션을 위한 사용자 지정 보고서를 생성할 수 있습니다.

2024년 11월 21일

자세한 내용은 [the section called “AWS Resilience Hub 요약”](#) 단원을 참조하십시오.

[AWS Resilience Hub 는 myApplications 대시보드에 복원력 위젯을 도입합니다.](#)

myApplications 대시보드의 새로운 복원력 위젯은 애플리케이션의 복원력 태세 평가 및 모니터링을 간소화합니다. 이를 통해에서 수동으로 복제할 필요 없이 myApplications에 정의된 애플리케이션의 복원력을 빠르게 평가할 수 있습니다 AWS Resilience Hub.

2024년 10월 22일

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “AWS Resilience Hub 및 myApplications”](#)
- [the section called “복원력 위젯에서 복원력 평가 관리”](#)

[AWS Resilience Hub Amazon ElastiCache\(Redis OSS\) Serverless에 대한 지원 확장](#)

AWS Resilience Hub 는 이제 Amazon ElastiCache(Redis OSS) 서버리스 및 글로벌 데이터 스토어를 포함하여 Amazon ElastiCache(Redis OSS)를 사용하는 애플리케이션을 평가하고 향상된 복원력 권장 사항을 제공합니다. 여기에는 리전 및 다중 리전 설정에 대한 지침과 다중 AZ 배포, 리소스 그룹화 및 백업에 대한 전략이 포함됩니다. 또한 애플리케이션의 복원력 태세에 대한 향상된 제어를 제공하기 위해 Amazon ElastiCache(Redis OSS)에 맞게 조정된 Amazon CloudWatch 경보를 AWS Resilience Hub 제공합니다. Amazon ElastiCache

2024년 9월 25일

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “애플리케이션 구성 요소 관리”](#)
- [the section called “지원되는 AWS Resilience Hub 리소스”](#)
- [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#)

[AWS Resilience Hub 그룹화 권장 사항 소개](#)

2024년 8월 1일

AWS Resilience Hub 는 애플리케이션을 온보딩하는 동안 리소스를 애플리케이션 구성 요소(AppComponents로 그룹화하는 새로운 스마트 그룹화 옵션을 도입했습니다. 에서 복원력 평가를 실행할 때는 리소스를 적절한 AppComponent로 정확하게 그룹화하여 최적화되고 실행 가능한 권장 사항을 받는 AWS Resilience Hub 것이 중요합니다. 이 옵션은 복잡한 애플리케이션 또는 리전 간 애플리케이션에 적합하여 애플리케이션을 온보딩하는 데 걸리는 시간을 줄이고 현재 사용할 수 있는 기존 애플리케이션 온보딩 워크플로를 보완합니다.

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “애플리케이션 구성 요소 관리”](#)
- [the section called “AWS Resilience Hub 리소스 그룹화 권장 사항”](#)

[AWS Resilience Hub 에서 새 평가 요약 위젯 소개](#)

AWS Resilience Hub 는 Amazon Bedrock 생성형 AI 기능을 사용하여 복잡한 복원력 데이터를 매우 실행 가능한 인사이트로 변환하는 새로운 평가 요약 위젯을 도입했습니다. 이러한 평가 요약은 중요한 조사 결과를 추출하고, 위험의 우선순위를 지정하고, 복원력을 개선하기 위한 단계를 권장합니다. 가장 영향력 있는 요소에 집중하면 평가를 훨씬 더 쉽게 이해할 수 있으므로 복원력 태세의 가장 중요한 요소에 초점을 맞춘 영향력이 큰 정보를 얻을 수 있습니다.

2024년 8월 1일

자세한 내용은 [the section called “평가 요약”](#) 단원을 참조하십시오.

[AWS Resilience Hub Amazon DocumentDB에 대한 지원 확장](#)

이 AWS Resilience Hub 정책을 통해 Amazon DocumentDB, Elastic Load Balancing 및 평가를 실행하는 AWS Lambda 동안 리소스 및 구성에 액세스할 수 있는 Describe 권한을 부여할 수 있습니다.

2024년 8월 1일

AWS 관리형 정책에 대한 자세한 내용은 섹션을 참조하십시오 [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#).

AWS Resilience Hub 는 애플리케이션 복원력 드리프트 감지 기능을 확장합니다.

AWS Resilience Hub 는 새로운 유형의 드리프트 감지 - 애플리케이션 리소스 드리프트를 도입하여 드리프트 감지 기능을 확장했습니다. 이 개선 사항은 애플리케이션의 입력 소스 내에서 리소스 추가 또는 삭제와 같은 변경 사항을 감지합니다. 예약된 평가 및 드리프트 알림 서비스를 활성화 AWS Resilience Hub 하고 드리프트가 발생할 때마다 알림을 받을 수 있습니다. 최신 복원력 평가는 드리프트를 식별하고 애플리케이션을 복원력 정책 준수로 되돌리는 문제 해결 작업을 제공합니다.

2024년 5월 8일

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “드리프트 감지”](#)
- [the section called “예약된 평가 및 드리프트 알림 설정”](#)

AWS Trusted Advisor 개선 사항

AWS Resilience Hub 는 복구할 수 없는 애플리케이션 구성요소(AppComponents)를 식별하는 검사를 AWS Trusted Advisor 추가하여에 대한 지원을 확장했습니다.

2024년 3월 28일

자세한 내용은 [the section called “AWS Trusted Advisor”](#) 단원을 참조하십시오.

[AWS Resilience Hub 권장 경보에 대한 지원 확장](#)

AWS Resilience Hub 는 README.md 템플릿 파일을 AWS Resilience Hub 내부 AWS (예: Amazon CloudWatch) 또는 외부에서에서 권장하는 경보를 생성할 수 있는 값으로 업데이트했습니다 AWS.

자세한 내용은 [the section called “경보 관리”](#) 단원을 참조하십시오.

2024년 3월 26일

[AWS Resilience Hub Amazon FSx for Windows File Server에 대한 지원 확장](#)

2024년 3월 26일

AWS Resilience Hub 는 애플리케이션의 복원력을 평가하면서 Amazon FSx for Windows File Server 리소스에 대한 평가 지원을 확장합니다. Amazon FSx for Windows File Server를 사용하는 애플리케이션의 경우는 가용 영역(AZ) 및 다중 AZ 배포, 백업 계획, 데이터 복제를 포함하는 새로운 복원력 권장 사항을 AWS Resilience Hub 제공합니다.는 리전 내 및 리전 간 배포 모두에 대해 Microsoft Active Directory에 대한 파일 시스템 종속성을 포함하여 Amazon FSx for Windows File Server를 AWS Resilience Hub 지원합니다.

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “지원되는 AWS Resilience Hub 리소스”](#)
- [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#)
- [the section called “애플리케이션 구성 요소에서 리소스 그룹화”](#)

[AWS Resilience Hub 는 복원력 점수에 대한 추가 정보를 제공합니다.](#)

AWS Resilience Hub 는 애플리케이션의 복원력 상태를 개선하는 데 필요한 작업을 쉽게 탐색하고 이해하는 데 도움이 되도록 복원력 점수 사용자 환경을 업데이트했습니다.

2023년 11월 9일

자세한 내용은 [the section called “복원력 점수 이해”](#) 단원을 참조하십시오.

[AWS Resilience Hub Amazon Elastic Kubernetes Service\(Amazon EKS\) 리소스를 포함하는 애플리케이션에 대한 지원을 확장합니다.](#)

AWS Resilience Hub 는 Amazon EKS 리소스가 포함된 애플리케이션에 대한 지원을 확장하여 새로운 운영 권장 사항을 포함합니다. Amazon EKS 클러스터의 리소스를 포함하는 평가를 실행하는 동안 이제 애플리케이션의 복원력 상태를 개선하는 데 도움이 되는 테스트 및 경보를 실행할 것을 권장합니다.

2023년 11월 9일

자세한 내용은 [the section called “AWS Fault Injection Service 실험 관리”](#) 단원을 참조하십시오.

[AWS Resilience Hub 는 애플리케이션 수준에서 추가 정보를 제공합니다.](#)

AWS Resilience Hub 는 애플리케이션 수준에서 예상 워크로드 RTO 및 예상 워크로드 RPO에 대한 추가 정보를 제공합니다. 이 추가 정보는 최근에 성공한 평가에서 얻은 애플리케이션의 가능한 최대 예상 워크로드 RTO와 예상 워크로드 RPO를 나타냅니다. 이 값은 모든 중단 유형의 최대 예상 워크로드 RTO와 예상 워크로드 RPO입니다.

자세한 내용은 [the section called “애플리케이션 관리”](#) 단원을 참조하십시오.

2023년 10월 30일

[AWS Resilience Hub](#)[AWS Step Functions 리소스에 대한 평가 지원 확장](#)

2023년 10월 30일

AWS Resilience Hub 는 애플리케이션의 복원력을 평가하면서 AWS Step Functions 리소스에 대한 평가 지원을 확장합니다.는 상태 시스템 유형(표준 또는 Express 워크플로)을 포함한 AWS Step Functions 구성을 AWS Resilience Hub 분석합니다. 또한 AWS Resilience Hub 는 예상 워크로드 복구 시간 목표(RTO) 및 예상 워크로드 복구 시점 목표(RPO)를 충족하는 데 도움이 되는 권장 사항을 제공합니다. AWS Step Functions 리소스를 포함한 애플리케이션을 평가하려면 AWS 관리형 정책을 사용하거나 구성을 AWS Resilience Hub 읽을 AWS Step Functions 수 있도록 특정 권한을 수동으로 추가하여 필요한 권한을 설정해야 합니다.

이러한 관련 권한에 대한 자세한 내용은 [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#) 단원을 참조하세요.

AWS Resilience Hub 운영 권장 사항 제외 허용

AWS Resilience Hub에는 경고, 표준 운영 절차(SOPs) 및 AWS Fault Injection Service (AWS FIS) 테스트를 포함한 운영 권장 사항을 제외할 수 있는 기능이 추가되었습니다. 예서 평가를 실행하는 동안 평가된 애플리케이션의 복원력을 높이는 방법에 대한 예상 복구 시간과 권장 사항이 AWS Resilience Hub에 제공됩니다. 이제 권장 사항 제외 워크플로를 사용하여 관련 없는 권장 경고, SOPs 및 AWS FIS 테스트를 제외할 수 있습니다. 제외 워크플로는 제안된 플랫폼 이외의 플랫폼을 사용하거나 다른 방법으로 권장 사항을 이미 구현한 경우 유용합니다.

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “운영 권장 사항 포함 또는 제외”](#)
- [the section called “AWS Resilience Hub 권장 사항을 포함하거나 제외할 수 있는 권한 제한”](#)

2023년 8월 9일

에 대한 권한 설계 개선 AWS Resilience Hub

2023년 8월 2일

AWS Resilience Hub 는 AWS Identity and Access Management (IAM) 역할을 구성하는 동안 유연성을 제공하는 새로운 권한 설계를 도입했습니다 AWS Resilience Hub. 또한 권한을 단일 역할로 통합하여 사용자와 팀에 의미 있는 사용자 지정 역할 이름을 만들 수 있습니다. 의 새 관리형 정책을 AWS Resilience Hub 사용하면 지원되는 서비스에 대한 적절한 권한을 가질 수 있습니다. 현재 사용 권한 설정 방법이 마음에 드시면 계속해서 수동 구성을 지원할 예정입니다.

AWS 관리형 정책에 대한 자세한 내용은 섹션을 참조하세요 [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#).

[를 사용한 애플리케이션 복원력 드리프트 감지 AWS Resilience Hub](#)

2023년 8월 2일

AWS Resilience Hub 를 사용하면 애플리케이션 복원력을 해결하는 데 필요한 작업을 사전에 감지하고 이해할 수 있습니다. Amazon Simple Notification Service(SNS)가 예상 워크로드 Recovery Time Objective (RTO) 또는 예상 Recovery Point Objective(RPO)가 목표 달성에서 더 이상 조직의 비즈니스 목표를 충족하지 못하는 상태로 이동했을 때 알림을 수신할 수 있도록 합니다. 평가를 수동으로 실행하면서 복원력 문제를 사후에 찾아내는 것에서 Amazon SNS 주제를 통해 사전 예방적으로 알림을 받는 것으로 전환하면 잠재적인 장애를 조기에 예측하고 복구 목표를 달성할 것이라는 확신을 더할 수 있습니다.

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “예약된 평가 및 드리프트 알림 설정”](#)
- [the section called “애플리케이션 리소스 편집”](#)

[AWS Resilience Hub Amazon Relational Database Service 및 Amazon Aurora에 대한 지원 개선](#)

2023년 8월 2일

AWS Resilience Hub 는 Amazon Relational Database Service 프록시와 헤드리스 및 Amazon Aurora DB 데이터베이스 구성에 대한 평가 지원을 확장합니다. 또한 Amazon RDS가 포함된 애플리케이션을 평가하는 동안 이제 서로 다른 데이터베이스 엔진을 구분하여 보다 정확한 예상 워크로드 복구 시간 목표(RTOs) 제공할 것입니다. AWS Resilience Hub 는 AWS 환경 내에서 복원력 모범 사례를 구현하기 위한 추가 작업도 제공합니다. 모범 사례에는 Amazon RDS용 DevOps Guru를 통한 성능 인사이트, 향상된 모니터링, 지원되는 데이터베이스 엔진에서의 블루/그린 배포 자동화가 포함될 수 있습니다.

가 평가에 지원되는 모든 서비스의 리소스를 포함하는 AWS Resilience Hub 데 필요한 권한에 대한 자세한 내용은 [섹션을 참조하세요the section called “AWSResilienceHubAssessmentExecutionPolicy”](#).

[AWS Resilience Hub Amazon Elastic Block Store 스냅샷에 대한 지원 확장](#)

AWS Resilience Hub 는 Amazon Elastic Block Store(Amazon EBS)에 대한 평가 지원을 확장하여 직접 APIs. 확장 지원은 Amazon Data Lifecycle Manager(Amazon Data Lifecycle Manager) 또는 AWS 백업을 사용하는 고객에 대한 현재 지원에 추가됩니다.

자세한 내용은 [Amazon Elastic Block Store\(Amazon EBS\)](#)를 참조하세요.

2023년 8월 2일

[Amazon Elastic Compute Cloud 개선](#)

2023년 6월 27일

AWS Resilience Hub 는 Amazon Elastic Compute Cloud(Amazon EC2)에 대한 지원을 확장했습니다. 크기가 다른 애플리케이션의 경우 AWS를 사용하면 Amazon EC2를 사용하는 고객이 사용 사례에 적합한 구성을 선택할 수 있습니다.는 다음 Amazon EC2 구성에 대한 평가를 AWS Resilience Hub 지원합니다.

- 온디맨드 인스턴스.
- AWS Backup 및에 의한 인스턴스 백업 AWS Elastic Disaster Recovery.
- Amazon Application Recovery Controller(ARC) (ARC)를 사용한 오토 스케일링 지원

앞으로는 스팟 인스턴스, 전용 호스트, 전용 인스턴스, 배치 그룹 및 플릿을 포함하도록 평가 지원이 확대될 예정입니다.

자세한 내용은 [the section called “AWS Resilience Hub 액세스 권한 참조”](#) 단원을 참조하십시오.

[AWS 관리형 정책 업데이트](#)

평가를 실행하기 위해 다른 AWS 서비스에 대한 액세스를 제공하는 새 정책이 추가되었습니다.

2023년 6월 26일

자세한 내용은 [the section called “AWSResilienceHubAssessmentExecutionPolicy”](#) 단원을 참조하십시오.

[새로운 Amazon DynamoDB 운영 권장 경보](#)

Amazon DynamoDB를 사용하는 애플리케이션의 경우 AWS Resilience Hub 이제는 온디맨드 및 프로비저닝된 용량 모드와 글로벌 테이블에 대한 복원력 위험을 경고하는 새로운 경보 세트를 제공합니다. 새 경보에 액세스하려면 사용 중인 역할의 [AWS Identity and Access Management \(IAM\) 정책을 업데이트](#)해야 할 수 있습니다.

2023년 5월 2일

자세한 내용은 [the section called “AWS Resilience Hub 액세스 권한 참조”](#) 단원을 참조하십시오.

[AWS Trusted Advisor 개선 사항](#)

2023년 5월 2일

AWS Resilience Hub 는 Amazon DynamoDB를 사용하는 AWS Trusted Advisor 및 애플리케이션에 대한 지원을 확장했습니다. 와 AWS Trusted Advisor 함께를 사용하면 이제 이전 30일 동안 애플리케이션이 평가되지 않은 경우 알림을 받을 AWS Resilience Hub수 있습니다. 이 알림은 복원력에 영향을 줄 수 있는 변경 사항이 있는지 파악하기 위해 애플리케이션을 재평가하라는 메시지를 표시합니다.

AWS Resilience Hub 평가 명령 확인에 대한 자세한 내용은 [the section called “AWS Trusted Advisor”](#) 단원을 참조하세요.

[Amazon Simple Storage Service에 대한 추가 지원](#)

2023년 3월 21일

Amazon Simple Storage Service(Amazon S3) 교차 리전 복제(Amazon S3 CRR)/Amazon S3 동일 리전 복제(SRR), 버전 관리 및 AWS 백업에 대한 현재 지원 외에도 AWS Resilience Hub 이제 다중 리전 액세스 포인트, Amazon S3 복제 시간 제어(Amazon S3 RTC) 및 AWS 백업 point-in-time 복구(PITR) 구성에 대해 Amazon S3를 평가합니다.Amazon S3

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “AWS Resilience Hub 액세스 권한 참조”](#)
- [Amazon S3 스토리지 관리](#)

[Amazon Elastic Kubernetes Service에 대한 추가 지원](#)

2023년 3월 21일

AWS Resilience Hub 는 Amazon EKS 클러스터를 애플리케이션 복원력을 정의, 검증 및 추적하는 데 지원되는 리소스로 추가했습니다. 고객은 Amazon EKS 클러스터를 신규 또는 기존 애플리케이션에 추가하고 복원력 개선을 위한 평가 및 권장 사항을 받을 수 있습니다. 고객은 AWS CloudFormation, Terraform AWS Resource Groups 및 myApplications를 사용하여 애플리케이션 리소스를 추가할 수 있습니다. 또한 고객은 각 클러스터에 하나 이상의 네임스페이스가 있는 하나 이상의 리전에 하나 이상의 Amazon EKS 클러스터를 직접 추가할 수 있습니다. 이를 통해 AWS Resilience Hub 는 단일 및 교차 리전 평가 및 권장 사항을 제공할 수 있습니다. 배포, 복제본, ReplicationControllers 및 포드를 검사하는 것 외에도 AWS Resilience Hub 는 전체 클러스터 복원력을 분석합니다.는 상태 비저장 Amazon EKS 클러스터 워크로드를 AWS Resilience Hub 지원합니다. 새로운 기능은 AWS Resilience Hub 가 지원되는 모든 AWS 리전에서 사용할 수 있습니다.

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “애플리케이션 리소스 관리”](#)
- [the section called “EKS 클러스터를 추가합니다.”](#)
- [the section called “AWS Resilience Hub 액세스 권한 참조”](#)
- [AWS 리전 서비스](#)

[Amazon Elastic File System에 대한 추가 지원](#)

Amazon Elastic File System(Amazon EFS) 백업에 대한 현재 지원 외에도 AWS Resilience Hub 는 이제 Amazon EFS 복제 및 AZ 구성을 위해 Amazon EFS를 평가합니다.

2023년 3월 21일

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “지원되는 AWS Resilience Hub 리소스”](#)
- [Amazon Elastic File System이란 무엇입니까?](#)

애플리케이션 입력 소스 지원

AWS Resilience Hub 는 이제 애플리케이션 소스에 대한 투명성을 제공합니다. 이를 통해 애플리케이션의 입력 소스를 추가, 삭제 및 다시 가져오고 새 애플리케이션 버전을 게시할 수 있습니다.

2023년 2월 21일

자세한 내용은 [the section called “애플리케이션 리소스 편집”](#) 단원을 참조하십시오.

애플리케이션 구성 파라미터 지원

AWS Resilience Hub 는 이제 애플리케이션과 연결된 리소스에 대한 추가 정보를 수집하는 입력 메커니즘을 제공합니다. 이 정보를 통해 AWS Resilience Hub 는 리소스를 더 깊이 이해하고 더 나은 복원력 권장 사항을 제공할 수 있습니다.

2023년 2월 21일

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “애플리케이션 구성 파라미터”](#)
- [the section called “애플리케이션 구성 파라미터 구성”](#)
- [the section called “애플리케이션 구성 파라미터 업데이트”](#)

[Amazon Elastic Block Store에 대한 추가 지원](#)

2023년 2월 21일

Amazon Elastic Block Store(Amazon EBS) 볼륨에 대한 현재 지원 외에도 AWS Resilience Hub 는 이제 Amazon Data Lifecycle Manager 및 Amazon EBS 빠른 스냅샷 복원(FSR)을 통해 Amazon EBS 스냅샷을 평가합니다.

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “AWS Resilience Hub 액세스 권한 참조”](#)
- [Amazon Elastic Block Store\(Amazon EBS\)](#)

와 통합 AWS Trusted Advisor

AWS Trusted Advisor 사용자는에서 평가한 계정과 연결된 애플리케이션을 볼 수 있습니다 AWS Resilience Hub. 는 최신 복원력 점수를 AWS Trusted Advisor 표시하고 대상 복원력 정책(RTO 및 RPO)이 충족되었는지 여부를 나타내는 상태를 제공합니다. 평가가 실행될 때마다 AWS Trusted Advisor 는 최신 결과로 AWS Resilience Hub 업데이트합니다. AWS Trusted Advisor 는 AWS 계정을 지속적으로 분석하고 AWS 모범 사례 및 AWS Well-Architected 지침을 따르는 데 도움이 되는 권장 사항을 제공하는 서비스입니다.

2022년 11월 18일

자세한 내용은 [the section called “AWS Trusted Advisor”](#) 단원을 참조하십시오.

[Amazon Simple Notification Service\(SNS\)에 대한 지원](#)

AWS Resilience Hub 이제는 구독자를 포함한 Amazon SNS 구성을 분석하여 Amazon SNS를 사용하여 애플리케이션을 평가하고 애플리케이션에 대한 조직의 예상 워크로드 복구 목표(예상 워크로드 RTO 및 예상 워크로드 RPO)를 충족하기 위한 권장 사항을 제공합니다. Amazon SNS는 게시자(생산자)의 메시지를 구독자(소비자)에게 전달하는 관리형 서비스입니다.

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “지원되는 AWS Resilience Hub 리소스”](#)
- [the section called “ID 및 액세스 관리”](#)
- [the section called “애플리케이션 구성 요소에서 리소스 그룹화”](#)

2022년 11월 16일

[Amazon Application Recovery Controller\(ARC\)\(Amazon ARC\)에 대한 추가 지원](#)

2022년 11월 16일

AWS Resilience Hub 이제는 Amazon ARC for Elastic Load Balancing 및 Amazon Relational Database Service(Amazon RDS)를 평가합니다. 여기에는 Amazon ARC가 언제 도움이 될지에 대한 조언이 포함됩니다. AWS Resilience Hub Amazon ARC 평가는 확장을 통해 AWS ASG(AWS Auto Scaling Group) 및 Amazon DynamoDB를 지원합니다. Amazon ARC는 애플리케이션에 고가용성을 제공하므로 전체 애플리케이션을 장애 조치 리전으로 신속하게 장애 조치할 수 있습니다.

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “지원되는 AWS Resilience Hub 리소스”](#)
- [the section called “ID 및 액세스 관리”](#)

AWS 백업에 대한 추가 지원

AWS Resilience Hub 이제는 Amazon ARC for Elastic Load Balancing 및 Amazon Relational Database Service(Amazon RDS)를 평가합니다. 여기에는 Amazon ARC가 언제 도움이 될지에 대한 조언이 포함됩니다. AWS Resilience Hub Amazon ARC 평가는 확장을 통해 AWS ASG(AWS Auto Scaling Group) 및 Amazon DynamoDB를 지원합니다. Amazon ARC는 애플리케이션에 고가용성을 제공하므로 전체 애플리케이션을 장애 조치 리전으로 신속하게 장애 조치할 수 있습니다.

2022년 11월 16일

자세한 정보는 다음의 주제를 참조하세요.

- [the section called “지원되는 AWS Resilience Hub 리소스”](#)
- [the section called “ID 및 액세스 관리”](#)

콘텐츠 업데이트: 새 애플리케이션 구성 요소 리소스 추가

AppComponent 그룹화 섹션의 지원되는 Application Component 리소스 목록에 Route53 및 AWS Backup을 추가했습니다.

2022년 7월 1일

새 콘텐츠: 애플리케이션 규정 준수 상태 개념

변경 감지 상태 유형이 추가되었습니다.

2022년 6월 2일

소개 AWS Resilience Hub

AWS Resilience Hub 이제를 사용할 수 있습니다. 이 가이드에서는 이를 사용하여 인프라를 분석 AWS Resilience Hub 하고, AWS 앱의 복원력을 개선하기 위한 권장 사항을 얻고, 복원력 점수를 검토하는 방법을 설명합니다.

2021년 11월 10일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조의 [AWS 용어집](#)을 참조하세요.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.