AMS Accelerate 개념 및 절차

AMS Accelerate 사용 설명서

버전 March 31, 2026

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AMS Accelerate 사용 설명서: AMS Accelerate 개념 및 절차

Copyright © 2026 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

AMS Accelerate란 무엇입니까? 1
운영 계획 1
운영 계획 가속화 1
고급 운영 계획 2
작동 방법 2
주요 용어 3
서비스 설명 8
AWS Managed Services(AMS) AMS Accelerate 운영 계획 기능 8
지원되는 구성 11
지원되는 서비스 13
역할 및 책임 16
AMS Accelerate에서 수행한 변경 범위 29
지원되지 않는 운영 체제 30
연락처 및 에스컬레이션 31
연락 시간 31
업무 시간 32
에스컬레이션 경로 32
리소스 인벤토리 33
인프라 제어 33
시작하기 40
온보딩 40
온보딩 사전 조건 40
1단계. 계정 검색 43
2단계. 온보딩 관리 리소스 44
3단계. 기본 정책을 사용한 온보딩 기능 54
4단계. 기능 사용자 지정 63
AMS 콘솔 사용 65
AMS 패턴 66
AMS 패턴 작동 방식 67
AMS 패턴 67
자동 인스턴스 구성 70
작동 방법 70
SSM 에이전트 자동 설치 72
자동 인스턴스 구성 변경 74

AMS Accelerate에서 오프보드 ... 78
오프보딩 효과 ... 78
종속성을 사용한 오프보딩 ... 80
오프보딩 지원 받기 ... 80
알림 설정 ... 81
태그 지정 ... 82
태그 ... 83
태그란 무엇입니까? ... 83
태그 지정 작동 방식 ... 84
고객 관리형 태그 ... 84
Accelerate 관리형 태그 ... 88
고객 제공 태그 ... 88
태그 관리 도구 ... 89
리소스 태거 ... 89
CloudFormation ... 107
Terraform ... 111
인시던트 보고서, 서비스 요청 및 결제 질문 ... 113
인시던트 관리 ... 113
인시던트 관리가 무엇인가요? ... 114
인시던트 대응 및 해결 방법 ... 115
인시던트 작업 ... 115
서비스 요청 관리 ... 118
서비스 요청을 사용해야 하는 경우 ... 119
서비스 요청 관리 작동 방식 ... 120
서비스 요청 생성 ... 120
서비스 요청 모니터링 및 업데이트 ... 122
지원 API를 사용하여 서비스 요청 관리 ... 123
AMS Accelerate에서 생성한 서비스 요청에 응답 ... 123
인시던트 보고서 및 서비스 요청 테스트 ... 124
결제 질문 ... 124
계획된 이벤트 관리 ... 125
AMS PEM 기준 ... 125
PEM 유형 ... 125
AMS PEM 프로세스 ... 125
PEM FAQs ... 126
온디맨드 작업 ... 128

온디맨드 AMS 작업 요청 134
Operations on Demand 오퍼링 변경 134
보고서 및 옵션 136
요청 시 보고서 136
AMS 호스트 관리 보고서 137
AMS 백업 보고서 137
AWS Config 제어 규정 준수 보고서 140
AMS Config 규칙 응답 구성 보고서 141
인시던트 방지 및 상위 화자 보고서 모니터링 143
결제 요금 세부 정보 보고서 145
신뢰할 수 있는 수정자 보고서 146
셀프 서비스 보고서 149
내부 API 작업 150
패치 보고서(일별) 153
백업 보고서(일별) 162
인시던트 보고서(주별) 165
결제 보고서(월별) 168
집계된 보고서 170
AMS 셀프 서비스 보고서 대시보드 172
데이터 보존 정책 178
SSR에서 오프보드 179
액세스 관리 180
콘솔에 액세스 180
기능을 사용할 수 있는 권한 180
계정에 액세스하는 이유와 시기 195
액세스 트리거 195
IAM 역할 액세스 195
계정에 액세스하는 방법 197
루트를 사용하는 방법 및 시기 198
보안 관리 199
Log4j SSM 문서를 사용하여 발생 항목 검색 200
인프라 보안 모니터링 201
서비스 연결 역할 사용 202
AWS 관리형 정책 214
데이터 보호 222
Amazon Macie로 모니터링 223

GuardDuty로 모니터링 223
Amazon Route 53 Resolver DNS 방화벽을 사용하여 모니터링 224
데이터 암호화 226
AWS Identity and Access Management 226
AMS Accelerate에서 자격 증명으로 인증 226
정책을 사용하여 액세스 관리 232
Security Incident Response 233
작동 방법 234
준비 234
감지 235
분석 236
격리 237
근절 239
복구 239
사후 인시던트 보고서 240
보안 인시던트 대응 런북 240
보안 이벤트 로깅 및 모니터링 245
구성 규정 준수 245
AMS Config 규칙 라이브러리 246
위반에 대한 대응 269
규칙 예외 생성 271
AWS Config 비용 절감 272
사용자 지정 조사 결과 응답 272
인시던트 대응 274
인시던트 대응 및 온보딩 274
복원성 274
end-of-support 운영 체제에 대한 보안 제어 275
보안 모범 사례 275
변경 요청 보안 검토 275
고객 보안 위험 관리 프로세스 276
AMS Accelerate 기술 표준 277
AMS Accelerate의 표준 제어 277
환경에서 보안 위험이 높거나 매우 높은 변경 사항 289
보안 FAQ 291
AMS 운영 엔지니어는 언제 내 환경에 액세스하나요? 291
AMS 운영 엔지니어는 내 계정에 액세스할 때 어떤 역할을 맡습니까? 291

AMS 작업 엔지니어는 내 계정에 어떻게 액세스하나요? 292
AMS 관리형 AWS 계정에서 AMS의 변경 사항을 추적하려면 어떻게 해야 합니까? 292
내 계정에 대한 AMS 운영 엔지니어 액세스에 대한 프로세스 제어는 무엇입니까? 293
권한 있는 액세스는 어떻게 관리되나요? 293
AMS 운영 엔지니어가 MFA를 사용하나요? 293
AMS 직원이 조직을 떠나거나 직무 역할을 변경하면 액세스는 어떻게 되나요? 294
내 계정에 대한 AMS 운영 엔지니어 액세스를 제어하는 액세스 제어는 무엇입니까? 294
AMS는 루트 사용자 액세스를 어떻게 모니터링하나요? 294
AMS는 보안 인시던트에 어떻게 대응하나요? 295
AMS는 어떤 업계 표준 인증 및 프레임워크를 준수하나요? 295
보안 인증, 프레임워크 및 규정 준수에 대한 최신 보고서에 액세스하려면 어떻게 해야 하나요 AWS? 295
AMS는 AMS 기능의 다양한 측면에 대한 참조 아키텍처 다이어그램을 공유하나요? 296
AMS는 내 계정에 액세스하는 사용자와 액세스를 위한 비즈니스 요구 사항을 어떻게 추적하나요? 296
AMS 엔지니어는 Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift와 같은 AWS 데이터 스토리지 서비스에 저장된 데이터에 액세스할 수 있나요? 297
AMS 엔지니어는 Amazon EBS, Amazon EFS 및 Amazon FSx에 저장된 고객 데이터에 액세스할 수 있나요? 297
내 환경에 대한 권한이 높은 자동화 역할에 대한 액세스는 어떻게 제한되거나 제어되나요? .. 297
AMS는 자동화 역할에 대한 AWS Well-Architected Framework에서 권장하는 최소 권한 원칙을 어떻게 구현하나요? 297
자동화 역할과 관련된 무단 액세스 시도 또는 의심스러운 활동을 탐지하는 데 사용되는 로깅 및 모니터링 시스템은 무엇입니까? 298
자동화 인프라와 관련된 보안 인시던트 또는 침해는 어떻게 처리되며 신속한 대응 및 완화에 도움이 되는 프로토콜은 무엇입니까? 298
자동화 인프라에서 정기적인 보안 평가, 취약성 스캔 및 침투 테스트를 수행합니까? 298
자동화 인프라에 대한 액세스는 권한 있는 직원으로만 어떻게 제한되나요? 298
자동화 파이프라인에서 보안 표준을 유지하고 무단 액세스 또는 데이터 침해를 방지하기 위해 구현되는 조치는 무엇입니까? 299
권한 에스컬레이션 또는 액세스 오용을 감지하여 AMS 팀에 사전에 알리기 위해 액세스 또는 감사 로깅에 대한 이상 탐지 또는 모니터링이 켜져 있습니까? 299
AMS 관리형 계정에서 추출되는 고객 데이터 유형은 무엇이며 이를 어떻게 활용하고 저장하나요? 299
모니터링 및 이벤트 관리 301
모니터링이란 무엇입니까? 301

모니터링 작동 방식 302
EC2 인스턴스 그룹화된 알림 303
태그 기반 알림 304
AMS의 기준 모니터링 알림 305
AMS의 애플리케이션 인식 인시던트 알림 325
AppRegistry에 온보딩 및 애플리케이션 생성 325
태그를 생성하여 사례 보강 활성화 327
애플리케이션에 대한 AMS 지원 사례 심각도 사용자 지정 327
필요한 권한 검토 328
경보 관리자 328
경보 관리자의 작동 방식 329
경보 관리자 시작하기 330
경보 관리자 태그 331
경보 관리자 구성 프로필 335
추가 CloudWatch 경보 생성 352
알림의 AMS 자동 문제 해결 352
EC2 상태 확인 실패: 수정 자동화 참고 사항 358
EC2 볼륨 사용량 수정 자동화 359
Amazon RDS 스토리지 부족 이벤트 수정 자동화 360
ONTAP 볼륨 용량 수정 자동화 360
AMS 이벤트 라우터 361
AMS에서 배포한 Amazon EventBridge 관리형 규칙 361
AMS에 대한 관리형 규칙 생성 363
AMS에 대한 관리형 규칙 편집 363
AMS에 대한 관리형 규칙 삭제 364
Trusted Remediator 364
주요 이점 364
신뢰할 수 있는 수정자 작동 방식 365
주요 용어 365
신뢰할 수 있는 문제 해결사 시작하기 366
지원되는 Compute Optimizer 권장 사항 369
지원되는 Trusted Advisor 검사 372
지원되는 Security Hub CSPM 권장 사항 420
검사 문제 해결 구성 422
실행 모드 결정 워크플로 426
문제 해결 자습서 구성 426

문제 해결 작업 ... 429
문제 해결 로그 ... 432
와 빠른 통합 ... 438
모범 사례 ... 440
FAQ ... 440
EKS 모니터링 및 인시던트 관리 ... 444
Amazon EKS의 모니터링 및 인시던트 관리란 무엇입니까? ... 444
Amazon EKS에 대한 모니터링 및 인시던트 관리 작동 방식 ... 445
AMS 책임 매트릭스(RACI) ... 446
기준 알림 ... 448
알림 및 작업 ... 448
요구 사항 ... 454
온보딩 ... 456
오프보드 ... 457
연속성 관리 ... 458
연속성 관리 작동 방식 ... 458
AMS 백업 계획 선택 ... 459
기본 AMS 백업 계획 ... 459
향상된 백업 계획 ... 460
데이터에 민감한 백업 계획 ... 460
AMS Accelerate 온보딩 백업 계획 ... 461
백업을 위해 리소스에 태그 지정 ... 462
AMS 볼트에서 백업 보기 ... 463
백업 모니터링 및 보고 ... 464
패치 관리 ... 466
패치 적용 권장 사항 ... 467
패치 책임 권장 사항 ... 467
애플리케이션 팀을 위한 지침 ... 468
보안 운영 팀을 위한 지침 ... 469
거버넌스 및 규정 준수 팀을 위한 지침 ... 469
고가용성 Windows 애플리케이션을 위한 예제 설계 ... 469
패치 권장 사항 FAQs ... 470
패치 창 생성 ... 470
패치 유지 관리 기간 제한 ... 471
패치 생성 화요일 패치 창: AMS 콘솔 ... 472
패치 창 생성: CloudFormation ... 473

패치 창 생성: Systems Manager 콘솔 474
패치 창 생성: Systems Manager CLI 475
후크가 있는 패치 477
AMS 패치 후크 RACI 477
패치 후크용 SSM 문서 생성 478
SSM Command 문서를 AMS 패치 후크로 사용하도록 AMS 패치 유지 관리 기간 구성 478
AMS Accelerate 패치 기준 480
기본 패치 기준 480
사용자 지정 패치 기준 481
온디맨드 패치 권한 481
패치 알림 및 패치 실패 이해 482
패치 서비스 요청 및 이메일 알림 482
CloudWatch Events를 통한 패치 알림 483
패치 실패 조사 487
AMS Resource Scheduler를 사용한 비용 최적화 488
Resource Scheduler에서 리소스 사용 488
온보딩 리소스 스케줄러 490
Resource Scheduler 사용자 지정 490
Resource Scheduler 사용 491
기간 및 일정 작업 494
리소스 태깅 500
비용 예측기 500
경보 억제기 501
로그 관리 502
로그 관리 - AWS CloudTrail 502
CloudTrail 로그 액세스 및 감사 504
CloudTrail 로그 보호 및 유지 504
Amazon EC2 로그 액세스 504
Amazon EC2 로그 유지 504
로그 관리 - Amazon EC2 504
로그 관리 - Amazon VPC 흐름 로그 506
변경 사항 추적 507
변경 레코드 보기 508
기본 쿼리 509
쿼리에서 날짜/시간 필터 수정 516
기본 쿼리 예제 517

레코드 권한 변경 528
AWS Systems Manager Accelerate의 530
사용 가능한 AMS Accelerate SSM 문서 530
AMS Accelerate SSM 문서 버전 530
Systems Manager 요금 531
문서 이력 532
이전 업데이트 553
..... dlxxvii

AMS Accelerate란 무엇입니까?

Amazon Web Services용 AMS Accelerate(AWS)에 오신 것을 환영합니다. AMS Accelerate는 운영 우수성을 달성하는 데 도움이 되는 다양한 운영 서비스를 제공합니다 AWS. 클라우드에서 막 시작하든, 현재 팀을 강화하려고 하든, 장기 운영 솔루션이 필요하든 관계없이 Accelerate는 클라우드에서 운영 목표를 달성하는 데 도움이 될 수 있습니다. AWS 서비스 자동화, 구성 및 실행서 라이브러리와를 활용하여 신규 및 기존 AWS 환경 모두에 대한 end-to-end 운영 솔루션을 제공합니다.

Accelerate 서비스는 네이티브 AWS 서비스 및 기능 제품군을 활용하여 포괄적인 인프라 관리 기능 세트를 제공합니다. 이 내에서 AWS 서비스 Accelerate는 큐레이션된 모니터링 제어, 탐지 가드레일, 자동화 및 런북 세트를 생성하고 유지 관리하여 규정을 준수하고 안전한 방식으로 인프라를 운영합니다.

주제

- AMS 운영 계획
- AMS Accelerate 운영 계획 사용
- AMS 키 용어
- 서비스 설명
- Accelerate에서 지원되지 않는 운영 체제의 기능
- 연락처 및 에스컬레이션
- Accelerate의 리소스 인벤토리

AMS 운영 계획

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

두 운영 계획에 대한 자세한 기능 비교는 AWS Managed Services 기능을 참조하세요.

AMS Accelerate 운영 계획

AMS Accelerate는 신규 또는 기존 AWS 환경의 day-to-day 인프라 관리를 운영하는 데 도움이 되는 AMS 운영 계획입니다. AMS Accelerate는 모니터링, 인시던트 관리 및 보안과 같은 운영 서비스를 제

공합니다. 또한 AMS Accelerate는 정기적인 패치가 필요한 Amazon EC2 기반 워크로드에 대한 선택적 패치 추가 기능을 제공합니다.

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

AMS Advanced 운영 계획

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

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

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

AMS Accelerate 운영 계획 사용

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

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

AMS Accelerate는 운영을 간소화할 수 있지만 애플리케이션 개발, 배포, 테스트 및 튜닝, 관리에 대한 책임은 여전히 사용자에게 있습니다. AMS Accelerate는 인시던트, 경보, 문제 해결 및 일부 서비스 요청의 결과로만 계정을 변경합니다. AMS Accelerate는 사용자를 대신하여 계정의 리소스를 프로비

저닝하지 않습니다. AMS Accelerate는 애플리케이션에 영향을 미치는 인프라 문제에 대한 문제 해결 지원을 제공하지만, AMS Accelerate는 사용자의 지식 및 승인 없이 애플리케이션 구성에 액세스하거나 검증하지 않습니다. AMS Accelerate 서비스 및 변경 사항은 AWS 콘솔 및 APIs에서 직접 제공되므로 AWS 및 사용 가능한 AWS Marketplace 솔루션과 함께 기존 계정을 계속 활용할 수 있습니다. AMS Accelerate는 코드infrastructure-as-code 템플릿(예: CloudFormation 템플릿)에서 코드를 수정하지 않지만 운영 및 보안 모범 사례를 따르기 위해 필요한 변경 사항에 대해 팀을 안내할 수 있습니다.

AMS 키 용어

- AMS Advanced: AMS Advanced 설명서의 "서비스 설명" 섹션에 설명된 서비스입니다. 서비스 설명을 참조하세요.
- AMS 고급 계정: AWS AMS 고급 온보딩 요구 사항의 모든 요구 사항을 항상 충족하는 계정입니다. AMS Advanced 혜택, 사례 연구 및 영업 담당자에게 문의하는 방법에 대한 자세한 내용은 AWS Managed Services를 참조하세요.
- AMS Accelerate Accounts: AWS AMS Accelerate 온보딩 요구 사항의 모든 요구 사항을 항상 충족하는 계정입니다. AMS Accelerate 시작하기를 참조하세요.
- AWS Managed Services: AMS 및 또는 AMS Accelerate.
- AWS Managed Services 계정: AMS 계정 및 또는 AMS Accelerate 계정.
- 중요 권장 사항: 리소스 또는에 대한 잠재적 위험 또는 중단을 방지하기 위해 조치가 필요함을 알리는 서비스 요청을 AWS 통해에서 발급한 권장 사항입니다 AWS 서비스. 지정된 날짜까지 중요 권장 사항을 따르지 않기로 결정한 경우 결정으로 인한 모든 손해에 대한 책임은 전적으로 사용자에게 있습니다.
- 고객 요청 구성: 다음에서 식별되지 않은 모든 소프트웨어, 서비스 또는 기타 구성:
  - Accelerate: 지원되는 구성 또는 AMS Accelerate, 서비스 설명.
  - AMS Advanced: 지원되는 구성 또는 AMS Advanced, 서비스 설명.
- 인시던트 통신: AMS는 AMS Accelerate용 지원 센터와 AMS용 AMS 콘솔에서 생성된 인시던트를 통해 인시던트를 전달하거나 사용자가 AMS로 인시던트를 요청합니다. AMS Accelerate 콘솔은 대시보드의 인시던트 및 서비스 요청 요약과 자세한 내용은 지원 센터 링크를 제공합니다.
- 관리형 환경: AMS Advanced 계정 및 또는 AMS에서 운영하는 AMS Accelerate 계정.

  AMS Advanced의 경우 여기에는 다중 계정 랜딩 존(MALZ) 및 단일 계정 랜딩 존(SALZ) 계정이 포함됩니다.
- 결제 시작 날짜:가 AWS Managed Services 온보딩 이메일에서 요청한 정보를 AWS 수신한 다음 영업일입니다. AWS Managed Services 온보딩 이메일은 계정에서 AWS Managed Services를 활성화하는 데 필요한 정보를 수집 AWS 하기 위해에서 사용자에게 보내는 이메일을 말합니다.

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

1. 호환되는 AWS 계정에 대한 액세스 권한을 부여하고 AWS Managed Services에 전달합니다.
2. AWS Managed Services는 AWS Managed Services 계정을 설계하고 빌드합니다.

- 서비스 종료: 서비스 요청을 통해 AWS 최소 30일 전에 알림을 제공하여 어떤 이유로든 AWS Managed Services 모든 AWS Managed Services 계정 또는 지정된 AWS Managed Services 계정에 대해 AWS Managed Services를 종료할 수 있습니다. 서비스 종료 날짜에 다음 중 하나를 수행합니다.
  1. AWS 모든 AWS Managed Services 계정 또는 해당하는 경우 지정된 AWS Managed Services 계정의 제어를 사용자에게 인계하거나
  2. 양 당사자는 해당하는 경우 모든 AWS Managed Services 계정 또는 지정된 AWS Managed Services 계정에서 AWS 액세스 권한을 부여하는 AWS Identity and Access Management 역할을 제거합니다.
- 서비스 종료 날짜: 서비스 종료 날짜는 30일의 필수 종료 알림 기간이 끝나는 달의 마지막 날입니다. 필수 종료 알림 기간이 해당 월의 20일 이후인 경우 서비스 종료 날짜는 다음 달의 마지막 날입니다. 다음은 종료 날짜에 대한 예제 시나리오입니다.
  - 종료 알림이 4월 12일에 제공된 경우 30일 알림은 5월 12일에 종료됩니다. 서비스 종료 날짜는 5월 31일입니다.
  - 종료 알림이 4월 29일에 제공된 경우 30일 알림은 5월 29일에 종료됩니다. 서비스 종료 날짜는 6월 30일입니다.
- AWS Managed Services:makes를 제공하면 서비스 시작 날짜부터 각 AWS Managed Services 계정에 대한 AWS Managed Services에 액세스하고 사용할 수 있습니다. AWS
- 지정된 AWS Managed Services 계정에 대한 종료: 서비스 요청(“AMS 계정 종료 요청”)을 통해 AWS 알림을 제공하여 어떤 이유로든 지정된 AWS Managed Services 계정에 AWS Managed Services 대한 AWS Managed Services를 종료할 수 있습니다.

인시던트 관리 용어:

- 이벤트: AMS 환경의 변경 사항입니다.
- 알림: 지원되는의 이벤트가 임계값을 AWS 서비스 초과하고 경보를 트리거할 때마다 알림이 생성되고 연락처 목록으로 알림이 전송됩니다. 또한 인시던트 목록에 인시던트가 생성됩니다.

- 인시던트: AWS Managed Services 또는 사용자가 보고한 대로 영향을 미치는 AMS 환경 또는 AWS Managed Services의 예상치 못한 중단 또는 성능 저하입니다.
- 문제: 하나 이상의 인시던트에 대한 공유된 근본 원인입니다.
- 인시던트 해결 또는 인시던트 해결:
  - AMS가 해당 인시던트와 관련하여 사용할 수 없는 모든 AMS 서비스 또는 리소스를 사용 가능한 상태로 복원한 경우
  - AMS에서 사용할 수 없는 스택 또는 리소스를 사용 가능한 상태로 복원할 수 없다고 판단한 경우
  - AMS가 사용자가 승인한 인프라 복원을 시작했습니다.
- 인시던트 대응 시간: 인시던트를 생성하는 시점과 AMS가 콘솔, 이메일, 서비스 센터 또는 전화를 통해 초기 응답을 제공하는 시점 간의 시간 차이입니다.
- 인시던트 해결 시간: AMS 또는 사용자가 인시던트를 생성하는 시점과 인시던트가 해결되는 시점 간의 시간 차이입니다.
- 인시던트 우선 순위: AMS 또는 사용자가 인시던트의 우선 순위를 낮음, 중간 또는 높음으로 지정하는 방법입니다.
  - 낮음: AMS 서비스의 중요하지 않은 문제입니다.
  - 중간: 관리형 환경 내의 AWS 서비스를 사용할 수 있지만 의도한 대로 작동하지 않습니다(해당 서비스 설명에 따라).
  - 높음: (1) AMS 콘솔 또는 관리형 환경 내의 하나 이상의 AMS APIs를 사용할 수 없거나, (2) 관리형 환경 내의 하나 이상의 AMS 스택 또는 리소스를 사용할 수 없고 사용 불가능으로 인해 애플리케이션이 기능을 수행할 수 없습니다.

  AMS는 위 지침에 따라 인시던트를 다시 분류할 수 있습니다.
- 인프라 복원: 인시던트 해결이 불가능할 때 달리 지정하지 않는 한 영향을 받는 스택의 템플릿을 기반으로 기존 스택을 재배포하고 마지막으로 알려진 복원 지점을 기반으로 데이터 복원을 시작합니다.

인프라 용어:

- 관리형 프로덕션 환경: 고객의 프로덕션 애플리케이션이 있는 고객 계정입니다.
- 관리형 비프로덕션 환경: 개발 및 테스트용 애플리케이션과 같은 비프로덕션 애플리케이션만 포함하는 고객 계정입니다.
- AMS 스택: AMS에서 단일 단위로 관리하는 하나 이상의 AWS 리소스 그룹입니다.
- 변경 불가능한 인프라: Amazon EC2 Auto Scaling 그룹(ASGs)에 일반적으로 사용되는 인프라 유지 관리 모델로, 업데이트된 인프라 구성 요소(AMI)는 현재 위치에서 업데이트되지 않고 모든 배포

AWS에 대해 대체됩니다. 변경 불가능한 인프라의 장점은 모든 구성 요소가 항상 동일한 기반에서 생성되므로 동기 상태를 유지하는 것입니다. 변형성은 AMI 구축을 위한 도구 또는 워크플로와 무관합니다.

- 변경 가능한 인프라: Amazon EC2 Auto Scaling 그룹이 아니며 단일 인스턴스 또는 단 몇 개의 인스턴스를 포함하는 스택에 일반적으로 사용되는 인프라 유지 관리 모델입니다. 이 모델은 수명 주기가 시작될 때 시스템을 배포한 다음 시간이 지남에 따라 해당 시스템에 업데이트를 계층화하는 기존의 하드웨어 기반 시스템 배포를 가장 잘 나타냅니다. 시스템에 대한 모든 업데이트는 인스턴스에 개별적으로 적용되며 애플리케이션 또는 시스템 재시작으로 인해 시스템 가동 중지(스택 구성에 따라 다름)가 발생할 수 있습니다.
- 보안 그룹: 인바운드 및 아웃바운드 트래픽을 제어하는 인스턴스의 가상 방화벽입니다. 보안 그룹은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 따라서 VPC의 서브넷에 있는 각 인스턴스에는 서로 다른 보안 그룹 세트가 할당될 수 있습니다.
- 서비스 수준 계약(SLAs): 예상 서비스 수준을 정의하는 AMS 계약의 일부입니다.
- SLA 사용 불가 및 사용 불가:
  - 오류가 발생하는 API 요청입니다.
  - 사용자가 제출한 콘솔 요청으로 5xx HTTP 응답이 발생합니다(서버가 요청을 수행할 수 없음).
  - AMS 관리형 인프라에서 스택 또는 리소스를 구성하는 모든 AWS 서비스 오퍼링은 서비스 상태 대시보드에 표시된 대로 “서비스 중단” 상태입니다.
  - AMS 제외로 인해 직접 또는 간접적으로 발생하는 사용 불가는 서비스 크레딧 자격을 결정하는 데 고려되지 않습니다. 사용 불가 기준을 충족하지 않는 한 서비스는 사용 가능한 것으로 간주됩니다.
- 서비스 수준 목표(SLOs): AMS 서비스에 대한 특정 서비스 목표를 정의하는 AMS 계약의 일부입니다.

패치 용어:

- 필수 패치: 환경 또는 계정의 보안 상태를 손상시킬 수 있는 문제를 해결하기 위한 중요한 보안 업데이트입니다. ‘중요 보안 업데이트’는 AMS 지원 운영 체제의 공급업체가 ‘중요’로 평가한 보안 업데이트입니다.
- 발표된 패치와 릴리스된 패치: 패치는 일반적으로 일정에 따라 발표되고 릴리스됩니다. 발생한 패치는 패치의 필요성이 발견되면 발표되며, 일반적으로 패치가 릴리스된 직후 발표됩니다.
- 패치 추가 기능: AWS Systems Manager (SSM) 기능을 활용하는 AMS 인스턴스에 대한 태그 기반 패치를 제공하므로 인스턴스에 태그를 지정하고 구성한 기준 및 창을 사용하여 해당 인스턴스에 패치를 적용할 수 있습니다.
- 패치 방법:

  - 현재 위치 패치: 기존 인스턴스를 변경하여 수행되는 패치입니다.
  - AMI 대체 패치: 기존 EC2 Auto Scaling 그룹 시작 구성의 AMI 참조 파라미터를 변경하여 수행되는 패치입니다.
- 패치 공급자(OS 공급업체, 타사): 패치는 애플리케이션의 공급업체 또는 관리 기관에서 제공합니다.
- 패치 유형:
  - CSU(Critical Security Update): 지원되는 운영 체제의 공급업체가 "Critical"로 평가한 보안 업데이트입니다.
  - 중요 업데이트(IU): 지원되는 운영 체제의 공급업체가 “중요”로 평가한 보안 업데이트 또는 “중요”로 평가한 비보안 업데이트입니다.
  - 기타 업데이트(OU): CSU 또는 IU가 아닌 지원되는 운영 체제의 공급업체에 의한 업데이트입니다.
- 지원되는 패치: AMS는 운영 체제 수준 패치를 지원합니다. 보안 취약성 또는 기타 버그를 수정하거나 성능을 개선하기 위해 공급업체에서 업그레이드를 릴리스합니다. 현재 지원되는 OSs 목록은 지원 구성을 참조하세요.

보안 용어:

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

서비스 요청 조건:

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

기타 용어:

- AWS Managed Services 인터페이스: AMS: AWS Managed Services 고급 콘솔, AMS CM API 및 지원 API. AMS Accelerate의 경우: 지원 콘솔 및 지원 API.

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

서비스 설명

AMS Accelerate는 AWS 인프라 운영을 관리하기 위한 AWS Managed Services 서비스의 운영 계획입니다.

AWS Managed Services(AMS) AMS Accelerate 운영 계획 기능

AMS Accelerate는 다음과 같은 기능을 제공합니다.

- 인시던트 관리:

  인시던트 관리는 AMS 서비스가 보고된 인시던트에 대응하는 데 사용하는 프로세스입니다.

  AMS Accelerate는 인시던트를 사전에 탐지 및 대응하고 팀이 문제를 해결할 수 있도록 지원합니다. 계정에 대해 선택한 응답 수준에 따라 응답 시간 SLAs를 사용하여 AWS 지원 센터를 사용하여 연중무휴 AMS Accelerate 운영 엔지니어에게 문의할 수 있습니다.
- 모니터링:

  모니터링은 AMS 서비스가 리소스를 추적하는 데 사용하는 프로세스입니다.

AMS Accelerate에 등록된 계정은 노이즈를 줄이고 발생할 수 있는 인시던트를 식별하도록 최적화된 Amazon CloudWatch 이벤트 및 경보의 기본 배포로 구성됩니다. 알림을 받은 후 AMS 팀은 자동화된 문제 해결, 사람 및 프로세스를 사용하여 리소스를 정상 상태로 되돌리고 적절한 경우 팀과 협력하여 행동에 대한 학습과 이를 방지하는 방법에 대한 인사이트를 제공합니다. 문제 해결에 실패하면 AMS가 인시던트 관리 프로세스를 시작합니다. 기본 구성 파일을 업데이트하여 기준을 변경할 수 있습니다.

- 보안:

  보안 관리는 AMS 서비스가 리소스를 보호하는 데 사용하는 프로세스입니다. AWS Managed Services는 AWS Config 규칙 및 Amazon GuardDuty를 비롯한 여러 제어를 사용하여 정보 자산을 보호하고 AWS 인프라를 안전하게 유지하는 데 도움이 됩니다.

  AMS Accelerate는 모든 계정이 보안 AWS Config 규칙 및 운영 무결성에 대한 업계 표준을 준수하도록 및 수정 작업 라이브러리를 유지 관리합니다.는 기록된 리소스 간의 구성 변경을 AWS Config 규칙 지속적으로 추적합니다. 변경 사항이 규칙 조건을 위반하는 경우 AMS는 조사 결과를 보고하고 위반의 심각도에 따라 위반을 자동으로 또는 요청으로 해결할 수 있도록 허용합니다. 인터넷 보안 센터(CIS), 미국 국립 표준 기술 연구소(NIST) 클라우드 보안 프레임워크(CSF), 건강 보험 양도 및 책임에 관한 법률(HIPAA), 결제 카드 산업(PCI) 데이터 보안 표준(DSS)에서 설정한 표준을 AWS Config 규칙 쉽게 준수할 수 있습니다.

  또한 AMS Accelerate는 Amazon GuardDuty를 활용하여 AWS 환경에서 잠재적으로 승인되지 않았거나 악의적인 활동을 식별합니다. GuardDuty 결과는 AMS에서 연중무휴 모니터링합니다. AMS는 고객과 협력하여 모범 사례 권장 사항을 기반으로 조사 결과 및 수정 사항이 미치는 영향을 이해합니다. 또한 AMS는 Amazon Macie를 지원하여 개인 건강 정보(PHI), 개인 식별 정보(PII) 및 금융 데이터와 같은 민감한 데이터를 보호합니다. 마지막으로 AMS는 관리형 계정에서 생성된 모든 Amazon Route 53 Resolver ALERT 및 BLOCK 이벤트를 모니터링하고 분류하여 네트워크 트래픽을 추가로 검사하고 탐지 기능을 강화합니다.

- 패치 관리:

  패치 관리는 AMS 서비스가 리소스를 업데이트하는 데 사용하는 프로세스입니다.

  패치 추가 기능이 있는 AWS 계정의 경우 AWS Managed Services는 선택한 유지 관리 기간 동안 지원되는 운영 체제의 Amazon EC2 인스턴스에 공급업체 업데이트를 적용하고 설치합니다. AMS는 패치 적용 전에 인스턴스의 스냅샷을 생성하고 패치 설치를 모니터링하며 결과를 알려줍니다. 패치가 실패하면 AMS는 실패를 조사하고 문제 해결을 위한 조치를 권장합니다. 또는 AMS는 요청 시 인스턴스를 롤백으로 복원합니다. AMS는 패치 규정 준수 적용 범위에 대한 보고서를 제공하고 비즈니스에 권장되는 조치를 조언합니다.

- 백업 관리:

  AMS는 백업 관리를 사용하여 리소스의 스냅샷을 생성합니다.

  AWS Managed Services는에서 지원하는 AWS 서비스에 대한 스냅샷을 생성, 모니터링 및 저장합니다 AWS Backup. 계정 및 애플리케이션을 온보딩하는 동안 AWS Backup 계획을 생성하여 백업 일정, 빈도 및 보존 기간을 정의합니다. 계획을 리소스에 연결합니다. AMS는 모든 백업 작업을 추적하고 백업 작업이 실패하면 문제 해결을 실행하도록 팀에 알립니다. AMS는 필요한 경우 스냅샷을 활용하여 인시던트 발생 시 복원 작업을 수행합니다. AMS는 백업 적용 범위 보고서와 백업 상태 보고서를 제공합니다.

- 문제 관리:

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

- 지정된 전문가:

  또한 AMS Accelerate는 조직과 협력하고 운영 및 보안 우수성을 촉진할 클라우드 서비스 제공 관리자(CSDM) 및 클라우드 아키텍트(CA)를 지정합니다. CSDM 및 CA는 구성 및 온보딩 AMS Accelerate 도중 및 이후에 지침을 제공하고, 운영 지표에 대한 월별 보고서를 제공하고, AWS Cost Explorer, Cost and Usage Reports, 등의 도구를 사용하여 잠재적 비용 절감을 식별합니다 Trusted Advisor.

- 작업 도구:

  AMS Accelerate는 AWS에서 워크로드의 인프라에 대한 지속적인 작업을 제공할 수 있습니다. 패치, 백업, 모니터링 및 인시던트 관리 서비스는 리소스에 태그를 지정하고 AWS Systems Manager , (SSM) 및 CloudWatch 에이전트가 SSM 및 Amazon CloudWatch 서비스와 상호 작용할 수 있도록 권한을 부여하는 IAM 인스턴스 프로파일을 사용하여 Amazon EC2 인스턴스에 설치 및 구성해야 합니다. AMS Accelerate는 규칙에 따라 리소스에 태그를 지정하는 데 도움이 되는 Resource Tagger와 Amazon EC2 인스턴스에 필요한 에이전트를 설치하는 자동화된 인스턴스 구성을 제공합니다. 변경할 수 없는 인프라 관행을 따르는 경우 콘솔 또는 infrastructure-as-code 템플릿에서 직접 사전 조건을 완료할 수 있습니다.

- 비용 최적화:

  AMS Resource Scheduler는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, Amazon Relational Database Service(RDS) 인스턴스 및 Amazon EC2 Auto Scaling 그룹의 시작 및 중지를

자동화합니다. AMS Resource Scheduler를 사용하면 사용하지 않는 리소스를 중지하고 용량이 필요할 때 다시 시작하여 운영 비용을 절감할 수 있습니다.

- 로깅 및 보고:

  AWS Managed Services는 CloudWatch, CloudTrail 및 Amazon VPC 흐름 로그에서 작업의 결과로 생성된 로그를 집계하고 저장합니다. AMS에서 로깅하면 인시던트 해결 및 시스템 감사를 더 빠르게 수행할 수 있습니다. 또한 AMS Accelerate는 실행 요약 및 인사이트, 운영 지표, 관리형 리소스, AMS 서비스 수준 계약(SLA) 준수, 지출, 절감 및 비용 최적화에 대한 재무 지표를 포함하여 AMS의 주요 성능 지표를 요약하는 월별 서비스 보고서를 제공합니다. 보고서는 지정된 AMS 클라우드 서비스 제공 관리자(CSDM)가 제공합니다.
- 서비스 요청 관리:

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

모든 AMS Accelerate 고객은 인시던트 관리, 모니터링, 보안 모니터링, 로그 기록, 사전 필수 도구, 백업 관리 및 보고 기능으로 시작합니다. AMS 패치 관리 추가 기능을 추가 가격으로 추가할 수 있습니다.

> **Note**
>
> 에서 지원되지 않는 기능 목록은 AMS Accelerate의 차이점을 AWS GovCloud (US)참조하세요. AWS GovCloud (US)

지원되는 구성

AMS Accelerate는 다음 구성을 지원합니다.

- 언어: 영어.
- 리전: AWS 리전 서비스 웹 페이지에서 AWS Managed Services에서 지원하는 AWS 리전을 참조하세요.

> **Note**
>
> 2019년 3월 20일 이전에 도입된 AWS 리전은 "기존" 리전으로 간주되며 기본적으로 활성화됩니다. 이 날짜 이후에 도입된 리전은 "옵트인" 리전이며 기본적으로 비활성화되어 있습니다. 계정이 여러 리전을 사용하고 "옵트인" 리전이 활성화된 계정에 AMS Accelerate를 기본

리전으로 온보딩하는 경우 AMS 보고 기능은 해당 리전에서만 사용할 수 있습니다. 기본 리전을 설정하지 않은 경우 마지막으로 방문한 리전이 기본 리전입니다.
리전을 활성화하려면 리전 활성화를 참조하세요. 기본 리전을 설정하려면 리전 선택을 참조하세요. 각 리전의 옵트인 상태 목록은 Amazon Elastic Compute Cloud 사용 설명서의 사용 가능한 리전을 참조하세요.

- 운영 체제 아키텍처(x86-64 또는 ARM64): Systems Manager와 CloudWatch에서 모두 지원하는 .
- 지원되는 운영 체제:
  - AlmaLinux 8.3-8.9, 9.x(AlmaLinux는 x86 아키텍처에서만 지원됨)
  - Amazon Linux 2023
  - Amazon Linux 2(예상 AMS 지원 종료일 2026년 6월 30일)
  - Oracle Linux 9.x, 8.x
  - Red Hat Enterprise Linux(RHEL) 9.x, 8.x
  - SUSE Linux Enterprise Server 15 SP6
  - SUSE Linux Enterprise Server for SAP 15 SP3 이상
  - Microsoft Windows Server 2025, 2022, 2019, 2016
  - Ubuntu 20.04, 22.04, 24.04
- 지원되는 지원 종료(EOS) 운영 체제:

> **Note**
>
> 지원 종료(EOS) 운영 체제는 운영 체제 제조업체의 일반 지원 기간을 벗어나며 보안 위험이 증가합니다. EOS 운영 체제는 AMS 필수 에이전트가 운영 체제를 지원하고 다음과 같은 경우에만 지원되는 구성으로 간주됩니다.
>
> 1. 업데이트를 받을 수 있도록 운영 체제 공급업체의 지원을 확대한 경우
> 2. EOS OS를 사용하는 모든 인스턴스는 Accelerate 사용 설명서의 AMS에서 지정한 보안 제어를 따르거나
> 3. 사용자는 AMS에 필요한 다른 보상 보안 제어를 준수합니다.
>
> AMS가 더 이상 EOS OS를 지원할 수 없는 경우 AMS는 운영 체제를 업그레이드하기 위한 중요 권장 사항을 발행합니다.
> AMS 필수 에이전트에는 Amazon CloudWatch AWS Systems Manager, 엔드포인트 보안(EPS) 에이전트 및 Active Directory(AD) 브리지(Linux만 해당)가 포함될 수 있지만 이에 국한되지 않습니다.

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

- AWS Control Tower 를 사용하여 다중 계정 환경을 관리하는 경우 Accelerate와의 호환성 AWS Control Tower 을 위해 최신 버전의를 실행하고 있는지 확인합니다. 2.7 이전 AWS Control Tower 버전(2021년 4월 릴리스)을 사용하는 환경은 지원되지 않습니다. 업데이트 방법에 대한 자세한 내용은 랜딩 존 업데이트를 AWS Control Tower참조하세요. https://docs.aws.amazon.com/controltower/latest/userguide/update-controltower.html

지원되는 서비스

AWS Managed Services는 다음 서비스에 대한 운영 관리 지원 AWS 서비스를 제공합니다. 각 AWS 서비스는 고유하므로 AMS의 운영 관리 지원 수준은 기본 AWS 서비스의 특성과 특성에 따라 달라집니다. AWS Managed Services가 다음 목록에서 지원되는 것으로 명시적으로 식별되지 않은 소프트웨어 또는 서비스에 대한 서비스를 제공하도록 요청하는 경우 이러한 고객 요청 구성에 대해 제공되는 모든 AWS Managed Services는 서비스 약관에 따라 "베타 서비스"로 취급됩니다.

- 인시던트: 모든 AWS 서비스
- 서비스 요청: 모든 AWS 서비스
- 패치: Amazon EC2
- 백업 및 복원: 모두에서 AWS 서비스 지원됩니다 AWS Backup. 에서 지원하는 서비스 목록은 AWS Backup 지원되는 리소스를 AWS Backup참조하세요.
- Resource Scheduler: Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, Amazon Relational Database Service(RDS) 및 Amazon EC2 Auto Scaling 그룹
- 운영 이벤트에 대해 모니터링되는 서비스: 지원되는 검사 및 Application Load Balancer Trusted Advisor, Aurora, Amazon EC2, Elastic Load Balancing, Amazon FSx for NetApp ONTAP, Amazon FSx for Windows File Server, NAT 게이트웨이(Network Address Translation(NAT) 서비스), OpenSearch Health Dashboard, Amazon Redshift, Amazon Relational Database Service(Amazon

RDS), Site-to-Site VPN. AMS Accelerate가 서비스의 일부로 모니터링하는 항목에 대해 자세히 알아보려면 AMS의 기준 모니터링에서 알림을 참조하세요.

- 보안 구성 규칙: AWS 계정, GuardDuty, Macie, Amazon API Gateway, AWS Certificate Manager, AWS Config, CloudTrail, CloudWatch, AWS CodeBuild, AWS Database Migration Service, Amazon DynamoDB, Amazon EC2, Amazon ElastiCache, Amazon Elastic Block Store(Amazon EBS), Amazon Elastic File System(Amazon EFS), Amazon Elastic Kubernetes Service(Amazon EKS), Elastic Load Balancing, Amazon OpenSearch Service, Amazon EMR, AWS Identity and Access Management (IAM), AWS Key Management Service AWS Lambda, Amazon Redshift, Amazon Relational Database Service, Amazon S3, Amazon SageMaker AI AWS Secrets Manager , Amazon Simple Notification Service AWS Systems Manager, Amazon VPC(보안 그룹, 볼륨, 탄력적 IP 주소, VPN 연결, 인터넷 게이트웨이), Amazon VPC 흐름 로그로 모니터링되는 서비스. 자세한 내용은 Accelerate의 구성 규정 준수 및 Accelerate의 데이터 보호 섹션을 참조하세요. AWS Managed Services의 보고서 탭에서를 통해 액세스할 수 있는 프라이빗 보안 가이드 AWS Artifact에서 추가 AMS 보안 정보를 찾을 수 있습니다.

> **Note**
>
> 아시아 태평양(말레이시아) 리전용 AMS Accelerate는 Amazon Macie를 사용한 모니터링, Amazon EKS에 대한 모니터링 및 인시던트 관리, Amazon EFS FileSystem, Amazon EC2 NatGateway 및 Amazon EKS 클러스터 리소스 모니터링을 지원하지 않습니다. 또한 SSM 에이전트 자동 설치를 지원하지 않습니다.

> **Note**
>
> 중동(UAE) 리전용 AMS Accelerate는 다음 표에 설명된 범위 내 기능 세트를 지원합니다. AMS 계정 콘솔 및이 리전의 인스턴스에 대한 액세스는 인바운드 서비스 요청 트리거에 의해서만 구동됩니다. 중동(UAE) 리전에서 Accelerate의 가용성에 대한 자세한 내용은 계정 관리자 또는 AWS Cloud Service Delivery Manager(CSDM)에 문의하십시오.

중동(UAE) 리전의 AMS Accelerate 범위 내 기능	기능 설명
인시던트 관리	AMS는 팀이 문제를 해결하는 데 도움이 되는 인시던트 대응 및 지원을 제공합니다. AMS가 인시

중동(UAE) 리전의 AMS Accelerate 범위 내 기능	기능 설명
	던트 관리를 지원하려면 서비스 요청을 제출해야 합니다. AMS는이 리전의 인시던트를 사전에 감지하거나 대응하지 않습니다.
모니터링	서비스 요청을 수신한 후 AMS는 리소스 수정을 지원할 수 있습니다. AMS는 자동화된 문제 해결, 사람 및 프로세스를 사용하여 리소스를 정상 상태로 되돌립니다. AMS는이 리전에서 기존 CloudWatch 이벤트 및 경보를 구성하지 않습니다. 기존 모니터링 도구가 있는 경우 클라우드 아키텍트(CA) 및 CSDM 평가에 따라 리소스를 선제적으로 추적할 수 있습니다.
보안	사용자로부터 서비스 요청을 받은 후 AMS는 보안 문제 해결을 지원할 수 있습니다. AMS는 AWS Config 규칙 및 GuardDuty와 같은 보안 제어를 배포하거나이 리전의 보안 조사 결과를 모니터링하지 않습니다. 기존 보안 도구가 있는 경우 CA 및 CSDM 평가에 따라 선제적 보안 모니터링을 사용할 수 있습니다.
패치 관리	AMS는 선택한 유지 관리 기간 동안 지원되는 운영 체제의 Amazon EC2 인스턴스에 공급업체 업데이트를 적용하고 사전 패치 스냅샷을 생성할 수 있습니다. AMS가 패치 관리를 지원하려면 서비스 요청을 제출해야 합니다. 이 리전에서는 AMS 패치 알림 및 보고서를 사용할 수 없습니다.
백업 관리	AMS는에서 AWS 서비스 지원하는에 대한 스냅샷을 생성 및 저장 AWS Backup하고 백업 문제 해결을 지원할 수 있습니다. AMS가 백업 관리를 지원하려면 서비스 요청을 제출해야 합니다. AMS는이 리전의 백업 작업을 추적하지 않습니다.

중동(UAE) 리전의 AMS Accelerate 범위 내 기능	기능 설명
지정된 전문가	AMS는 고객 조직과 협력하고 운영 및 보안 우수성을 촉진할 클라우드 아키텍트(CA) 및 클라우드 서비스 제공 관리자(CSDM)를 지정합니다.
서비스 요청 관리	관리형 환경, AMS 또는 AWS 서비스 제품에 대한 정보를 요청하려면 AMS Accelerate 콘솔을 통해 서비스 요청을 제출합니다. 이 표에 설명된 대로 및 기능에 대한 “방법” 질문에 대한 AWS 서비스 서비스 요청을 제출하거나이 리전에서 사용할 수 있는 AMS 서비스를 요청할 수 있습니다.

역할 및 책임

AMS Accelerate 책임, 책임, 상담 및 정보에 입각한 RACI 매트릭스는 다양한 활동에 대해 고객 또는 AMS에 기본 책임을 할당합니다. 이 표에서는 ("고객") 책임과 ("AMS Accelerate") 책임에 대해 설명합니다.

이 AMS Accelerate에서 수행한 변경 범위 섹션에는 AMS가 계정을 변경할 권한이 있는 특정 상황과 AMS가 절대 수행하지 않는 일부 유형의 변경 사항이 나열되어 있습니다.

AMS Accelerate RACI 매트릭스

AMS Accelerate는 AWS 인프라를 관리합니다. 다음 표에는 관리형 환경 내에서 실행되는 애플리케이션의 수명 주기 활동에 대한 사용자 및 AMS Accelerate의 역할과 책임에 대한 개요가 나와 있습니다.

- R은 작업을 달성하기 위해 작업을 수행하는 책임 당사자를 의미합니다.
- C는 일반적으로 주제 전문가로서 의견을 구하고 양자 통신이 이루어지는 Consulted를 의미합니다.
- 나는 종종 작업 완료 시에만 진행 상황에 대한 정보를 받는 당사자인 Informed를 의미합니다.

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

활동	Customer	AWS Managed Services(AMS)
AMS 패턴		
새 패턴 생성	I	R
패턴 배포 및 사용자 지정	R	C, I
패턴 테스트 및 제거	R	I
애플리케이션 수명 주기		
애플리케이션 개발	R	I
애플리케이션 인프라 요구 사항, 분석 및 설계	R	I
애플리케이션 배포	R	I
AWS 리소스 배포	R	I
애플리케이션 모니터링	R	I
애플리케이션 테스트/최적화	R	I
애플리케이션 문제 해결	R	I
문제 해결	R	I
AWS 인프라에 지원되는 모니터링	C	R
AWS 네트워크 문제에 대한 인시던트 대응	C	R

활동	Customer	AWS Managed Services(AMS)
AWS 리소스 문제에 대한 인시던트 대응	C	R
관리형 계정 온보딩		
AMS 팀 및 도구에 대한 AWS 관리형 계정에 대한 액세스 권한 부여	R	C
계정에 도구를 배포할 수 있도록 계정 또는 환경에서 변경 사항을 구현합니다. 예를 들어 서비스 제어 정책(SCPs)의 변경 사항	R	C
EC2 인스턴스에 SSM 에이전트 설치	R	C
AMS 서비스를 제공하는 데 필요한 도구를 설치하고 구성합니다. 예: CloudWatch 에이전트, 패치 적용 스크립트, 경보, 로그 등	I	R
AMS 엔지니어의 액세스 및 자격 증명 수명 주기 관리	I	R
AMS 서비스를 구성하는 데 필요한 모든 입력을 수집합니다. 예: 패치 유지 관리 기간, 일정 및 대상	R	I
AMS 서비스 구성 요청 및 모든 필수 입력 제공	R	I
고객의 요청에 따라 AMS 서비스를 구성합니다. 예: 패치 유지 관리 기간, 리소스 태거 및 경보 관리자	C	R
AWS 계정 및 인스턴스에 액세스하는 데 사용되는 로컬 디렉터리 서비스에 대한 사용자 및 해당 권한의 수명 주기 관리	R	I
예약 인스턴스 최적화 권장	I	R
신뢰할 수 있는 문제 해결사에 계정(들) 온보딩	C,I	R
패치 관리		
패치 유지 관리 기간, 패치 기준 및 대상을 구성하는 데 필요한 모든 입력 수집	R	I

활동	Customer	AWS Managed Services(AMS)
패치 유지 관리 기간 및 기준의 구성을 요청하고 모든 필수 입력 제공	R	I
고객의 요청에 따라 패치 유지 관리 기간, 패치 기준 및 대상 구성	C	R
지원되는 OS 및 EC2 인스턴스용 지원되는 OS가 사전 설치된 소프트웨어에 대한 해당 업데이트를 모니터링합니다.	I	R
지원되는 OS 및 유지 관리 기간 적용 범위에 대한 업데이트 누락 보고서	I	R
업데이트를 적용하기 전에 인스턴스의 스냅샷 생성	I	R
고객 구성당 EC2 인스턴스에 업데이트 적용	I	R
EC2 인스턴스에 대한 실패한 업데이트 조사	C	R
Auto-Scaling 그룹(ASGs)의 AMIs 및 스택 업데이트	R	C
Windows 운영 체제 및 Windows Update에서 관리하는 운영 체제에 설치된 Microsoft 패키지에 패치 적용	I	R
Windows Update에서 관리하지 않는 패치 설치 애플리케이션, 소프트웨어 또는 애플리케이션 종속성	R	I
Linux 운영 체제 및 운영 체제의 기본 패키지 관리자(예: Yum, Apt, Zypper)에 의해 관리가 활성화된 모든 패키지에 패치 적용	I	R
Linux 운영 체제의 기본 패키지 관리자에서 관리하지 않는 패치 설치 애플리케이션, 소프트웨어 또는 애플리케이션 종속성	R	I
백업		
백업 계획 및 대상 리소스를 구성하는 데 필요한 모든 입력 수집	R	I
백업 계획 구성 요청 및 모든 필수 입력 제공	R	I
고객의 요청에 따라 백업 계획 및 대상 구성	C	R

활동	Customer	AWS Managed Services(AMS)
백업 일정 및 대상 리소스 지정	R	I
계획당 백업 수행	I	R
실패한 백업 작업 조사	I	R
백업 작업 상태 및 백업 범위에 대한 보고서	I	R
백업 검증	R	I
인시던트 관리의 일환으로 지원되는 AWS 서비스 리소스의 리소스에 대한 백업 복원 요청	R	I
지원되는 AWS 서비스의 리소스에 대한 백업 복원 활동 수행	I	R
영향을 받는 사용자 지정 또는 타사 애플리케이션 복원	R	I
네트워킹		
관리VPCs, IGWs, Direct Connect 및 기타 AWS 네트워킹 서비스의 프로비저닝 및 구성	R	I
관리형 계정 내에서 AWS 보안 Groups/NAT/NACL 구성 및 운영	R	I
고객 네트워크 내의 네트워킹 구성 및 구현(예: DirectConnect)	R	I
AWS 네트워크 내 네트워킹 구성 및 구현	R	I
보안 그룹을 포함하여 네트워크 보안을 위해 AMS에서 정의한 모니터	I	R
네트워크 수준 로깅 구성 및 관리(VPC 흐름 로그 등)	I	R
로깅		
모든 애플리케이션 변경 로그 기록	R	I

활동	Customer	AWS Managed Services(AMS)
AWS 인프라 변경 로그 기록	I	R
AWS 감사 추적 활성화 및 집계	I	R
AWS 리소스에서 로그 집계	I	R
모니터링 및 해결		
경보 관리자, 리소스 태거 및 경보 임계값을 구성하는 데 필요한 모든 입력 수집	R	I
경보 관리자의 구성을 요청하고 모든 필수 입력 제공	R	I
고객의 요청에 따라 경보 관리자, 리소스 태거 및 경보 임계값을 구성합니다.	C	R
고객 구성당 AMS CloudWatch 기준 지표 및 경보 배포	I	R
기준 CloudWatch 지표 및 경보를 사용하여 지원되는 AWS 리소스 모니터링	I	R
AWS 리소스의 알림 조사	C	R
정의된 구성을 기반으로 알림 문제 해결 또는 인시던트 생성	I	R
고객별 모니터 정의, 모니터링 및 조사	R	I
애플리케이션 모니터링의 알림 조사	R	C
문제 해결을 위한 Trusted Advisor 검사 구성	R	C
지원되는 Trusted Advisor 검사 자동 해결	I	R
지원되는 Trusted Advisor 검사를 수동으로 수정	R	C
문제 해결 상태 보고	I	R

활동	Customer	AWS Managed Services(AMS)
문제 해결 실패 문제 해결	R	C
보안 아키텍처		
AMS 리소스 및 코드에서 보안 문제 및 잠재적 위협 검토	I	R
AMS 리소스 및 코드에 보안 제어를 구현하여 보안 위험 완화	I	R
계정 및 해당 AWS 리소스의 보안 관리를 위해 지원되는 AWS 서비스 활성화	I	R
AMS 엔지니어의 계정 및 OS 액세스에 대한 권한 있는 자격 증명 관리	I	R
보안 위험 관리		
GuardDuty 및 Macie와 같은 보안 관리를 위해 지원되는 AWS 서비스 모니터링	I	R
AMS 정의 Config 규칙을 정의하고 생성하여 AWS 리소스가 인터넷 보안 센터(CIS) 및 NIST 보안 모범 사례를 준수하는지 감지합니다.	I	R
AMS 정의 Config 규칙 모니터링	I	R
Config 규칙의 적합성 상태 보고	I	R
필요한 Config 규칙 목록 정의 및 해결	I	R
AMS 정의 Config 규칙 수정의 영향 평가	R	I
AWS 계정의 AMS 정의 Config 규칙 문제 해결 요청	R	I
AMS 정의 Config 규칙에서 제외된 리소스 추적	R	I
AWS 계정에서 지원되는 AMS 정의 Config 규칙 수정	C	R
AWS 계정에서 지원되지 않는 AMS 정의 Config 규칙 수정	R	I

활동	Customer	AWS Managed Services(AMS)
고객별 Config 규칙 정의, 모니터링 및 조사	R	I
인시던트 관리		
AWS 리소스에서 AMS가 탐지한 인시던트에 대해 알림	I	R
AWS 리소스의 인시던트 알림	R	I
모니터링을 기반으로 AWS 리소스에 대한 인시던트 알림	I	R
애플리케이션 성능 문제 및 중단 처리	R	I
인시던트 우선 순위 분류	I	R
인시던트 대응 제공	I	R
사용 가능한 백업이 있는 리소스에 대한 인시던트 해결 또는 인프라 복원 제공	C	R
보안 인시던트 대응 - 준비		
통신		
AMS가 보안 이벤트 알림 및 보안 에스컬레이션 중에 사용할 수 있도록 고객 보안 연락처 세부 정보 제공 및 업데이트	R	I
보안 이벤트 및 보안 에스컬레이션 중에 사용할 제공된 고객 보안 연락처 세부 정보를 저장하고 관리합니다.	C	R
훈련		
인시던트 대응 프로세스 중에 AMS를 지원하는 설명서를 고객에게 제공	I	R
보안 게임 데이를 통해 인시던트 대응 프로세스 중에 공동 책임 연습	R	R
리소스 관리		

활동	Customer	AWS Managed Services(AMS)
알림, 알림 상관 관계, 노이즈 감소 및 추가 규칙에 AWS 서비스 대해 지원되는 보안 관리 구성	I	R
비즈니스에 대한 각 자산의 가치 및 중요도에 대한 세부 정보를 포함하여 AWS 리소스(Amazon EC2, Amazon S3 등)의 포괄적인 인벤토리를 유지 관리합니다. 이 정보는 효과적인 억제 전략을 결정하는 데 중요한 역할을 합니다.	R	C
AWS 태그를 사용하여 리소스 및 워크로드 식별	R	C
로그 보존 및 아카이브 정의 및 구성	I	R
AWS 계정, 서비스 및 액세스 관리에 대한 조직의 보안 정책 및 구성을 정의하고 적용하여 안전한 기준 설정	R	I
보안 인시던트 대응 - 탐지		
로깅, 지표 및 모니터링		
인스턴스 및 계정에 대한 이벤트 관리를 활성화하도록 로깅 및 모니터링 구성	I	R
보안 알림 AWS 서비스 에 지원되는 모니터	I	R
엔드포인트 보안 도구 배포 및 관리	R	I
엔드포인트 보안을 사용하여 인스턴스에서 맬웨어 모니터링	R	I
아웃바운드 메시징을 통해 감지된 이벤트를 고객에게 알림	I	R
내부 이해관계자 커뮤니케이션 및 리더십 업데이트를 조정하여 응답 시간 개선	R	I
AMS 표준 탐지 서비스 정의, 배포 및 유지 관리(예: Amazon GuardDuty 및 AWS Config)	C	R

활동	Customer	AWS Managed Services(AMS)
AWS 인프라 변경 로그 기록	R	I
애플리케이션에 대한 이벤트 관리를 활성화하기 위한 로깅, 모니터링 활성화 및 구성	R	C
지원되는 AWS 보안 서비스(예: Amazon GuardDuty)에 대한 허용 목록, 거부 목록 및 사용자 지정 탐지 구현 및 유지 관리	R	R
보안 이벤트 보고		
AMS에 의심스러운 활동 또는 활성 보안 조사 알림	R	I
감지된 보안 이벤트 및 인시던트를 고객에게 알림	I	R
보안 인시던트 대응 프로세스를 트리거할 수 있는 계획된 이벤트에 알림	R	I
보안 인시던트 대응 - 분석		
조사 및 분석		
지원되는 탐지 소스에서 생성된 지원되는 보안 알림에 대한 초기 응답 수행	I	R
사용 가능한 데이터를 사용하여 거짓/참 긍정 평가	R	R
필요한 경우 고객과 공유할 영향을 받는 인스턴스의 스냅샷 생성	I	R
관리 연속성, 파일 시스템 분석, 메모리 포렌식 및 바이너리 분석과 같은 포렌식 작업 수행	R	C
애플리케이션 로그를 수집하여 조사 지원	R	I
데이터 및 로그를 수집하여 보안 알림에 대한 조사 지원	R	R
보안 조사에 AWS 서비스 내 SMEs 참여	C	R

활동	Customer	AWS Managed Services(AMS)
조사 중에 지원되는의 조사 로그 AWS 서비스 를 고객에게 공유	I	R
통신		
관리형 리소스에 대한 AMS 탐지 소스의 알림 및 알림 전송	I	R
애플리케이션 보안 이벤트에 대한 알림 및 알림 관리	R	I
보안 인시던트 조사 중에 고객 보안 연락 담당자 참여	R	I
보안 인시던트 대응 - 포함		
억제 전략 및 실행		
위험을 평가하고 억제 전략을 결정하여 잠재적 서비스 영향을 확인합니다.	R	C
추가 분석을 위해 영향을 받는 시스템을 백업합니다.	I	R
애플리케이션 및 워크로드 포함(애플리케이션별 구성 또는 응답 활동을 통해)	R	C
보안 인시던트 및 영향을 받는 리소스를 기반으로 억제 전략 정의	I	R
영향을 받는 시스템의 특정 시점 백업에 대한 암호화 및 보안 저장 활성화	C	R
EC2 인스턴스, 네트워크 및 IAM을 포함한 AWS 리소스에 대해 지원되는 격리 작업 실행	I	R
보안 인시던트 대응 - 제거		
근절 전략 및 실행		
고객 애플리케이션 워크로드에서 보안 인시던트 및 영향을 받는 리소스를 기반으로 근절 옵션 정의	C	R

활동	Customer	AWS Managed Services(AMS)
합의된 근절 전략, 근절 실행 시기 및 결과를 결정합니다.	R	I
AMS 관리형 워크로드에서 보안 인시던트 및 영향을 받는 리소스를 기반으로 근절 단계 정의	C	R
위협을 제거하고 EC2 인스턴스, 네트워크 및 IAM 근절을 포함한 AWS 리소스를 강화합니다.	R	C
위협 제거 및 애플리케이션 및 워크로드 강화(애플리케이션별 구성 또는 대응 활동을 통해)	R	I
보안 인시던트 대응 - 복구		
복구 준비 및 실행		
고객의 요청에 따라 백업 계획 및 대상 구성	I	R
백업 계획을 검토하여 AMS 관리형 워크로드 복원	R	I
지원되는의 리소스에 대한 백업 복원 활동 수행 AWS 서비스	I	R
고객 애플리케이션, APP 구성 및 배포 설정을 백업하고 백업 계획을 검토하여 인시던트 발생 후 고객 애플리케이션 및 워크로드를 복원합니다.	R	I
애플리케이션 및 고객 워크로드 복원(애플리케이션별 복원 단계를 통해)	R	I
보안 인시던트 대응 - 인시던트 사후 보고서		
인시던트 사후 보고		
필요에 따라 고객 사후 인시던트와 적절한 교훈 및 조치 항목 공유	I	R
문제 관리		
인시던트를 상호 연관시켜 문제 식별	I	R

활동	Customer	AWS Managed Services(AMS)
문제에 대한 근본 원인 분석(RCA) 수행	I	R
문제 해결	I	R
애플리케이션 문제 식별 및 해결	R	I
서비스 관리		
서비스 요청을 사용하여 정보 요청	R	I
서비스 요청에 회신	I	R
비용 최적화 권장 사항 제공	I	R
월별 서비스 보고서 준비 및 전달	I	R
변경 관리		
관리형 환경에서 리소스를 프로비저닝하고 업데이트하기 위한 변경 관리 프로세스 및 도구	R	I
애플리케이션 변경 일정 유지 관리	R	I
예정된 유지 관리 기간에 대한 알림	R	I
AMS 작업의 변경 사항 기록	I	R
비용 최적화		
Resource Scheduler를 구성하는 데 필요한 모든 입력 수집	R	I
Resource Scheduler의 온보딩, 구성 요청 및 모든 필수 입력 제공	R	I
고객 구성당 Resource Scheduler 배포	C, I	R
고객 계정에서 Resource Scheduler 비활성화 및 활성화	R	C

활동	Customer	AWS Managed Services(AMS)
일정 생성, 삭제, 설명 및 업데이트	C	R
기간 생성, 삭제, 설명 및 업데이트	C	R
Resource Scheduler를 사용하여 문제 조사 및 해결	I	R
Resource Scheduler 오프보딩 요청	R	I
계정에서 Resource Scheduler 오프보드	C, I	R

AMS Accelerate에서 수행한 변경 범위

AMS Accelerate는 다음에 설명된 특정 목적 및 상황에 대해서만 변경합니다. AMS는 콘솔 또는 APIs를 사용하여 인프라 수준에서만 변경합니다. AMS는 애플리케이션, 컨트롤 또는 도메인 계층을 변경하지 않습니다. 사전 빌드된 쿼리 세트를 사용하여 AMS(또는 다른 사용자)의 변경 사항을 볼 수 있습니다. 이를 수행하려면 섹션을 참조하세요AMS Accelerate 계정의 변경 사항 추적.

AWS resources

AMS Accelerate는 다음 상황에서만 AWS 리소스를 배포하거나 업데이트합니다.

- AMS에 필요한 도구 및 리소스를 배포하고 업데이트합니다.
- AMS 모니터링의 일부로 이벤트 및 경보에 대한 응답입니다.
- 의 일부로 보안 문제를 해결하려면Accelerate의 위반에 대한 대응(규정 미준수 리소스가 보안 모범 사례를 준수하도록 설정)
- 인시던트 대응의 일환으로 문제 해결 및 복원 중.
- 다음과 같은 AMS 기능을 구성하기 위한 고객 요청에 응답하는 경우:
  - 경보 관리자
  - 리소스 태거
  - 패치 기준 및 유지 관리 기간
  - 리소스 스케줄러
  - 백업 계획

AMS Accelerate는 이러한 상황 외에는 리소스를 배포하거나 업데이트하지 않습니다. 다른 상황에서 변경하기 위해 AMS의 도움이 필요한 경우 온디맨드 작업을 사용하는 것이 좋습니다.

운영 체제 소프트웨어

AMS Accelerate는 서비스 수준 계약에 정의된 인시던트 해결을 통해 사용할 수 없는 상황에서 운영 체제 소프트웨어를 변경할 수 있습니다. AMS는의 일부로 운영 체제를 변경할 수도 있습니다AMS Accelerate의 자동 인스턴스 구성.

애플리케이션 코드 및 구성

AMS Accelerate는 코드를 수정하지 않지만(예: AWS CloudFormation 템플릿, 기타 infrastructure-as-code 템플릿 또는 Lambda 함수) 운영 및 보안 모범 사례를 따르기 위해 필요한 변경 사항을 팀에 안내할 수 있습니다. AMS Accelerate는 애플리케이션에 영향을 미치는 인프라 문제에 대한 문제 해결 지원을 제공하지만 AMS Accelerate는 애플리케이션 구성에 액세스하거나 검증하지 않습니다.

Accelerate에서 지원되지 않는 운영 체제의 기능

지원되지 않는 운영 체제는에 나열되지 않은 운영 체제입니다지원되는 구성. AMS는 지원되지 않는 운영 체제가 있는 인스턴스를 AWS 베타 및 미리 보기 서비스 약관이 적용되는 "고객 요청 구성"으로 간주합니다.

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

기능	참고
인시던트 관리	AMS는 인시던트 대응을 제공합니다.
서비스 요청 관리	AMS는 서비스 요청에 응답합니다.
모니터링	AMS는 Amazon EC2 시스템 상태 확인 및 인스턴스 상태 확인을 모니터링하고 이에 응답합니다. 시스템 상태 확인에는 네트워크 연결 손실, 시스템 전원 손실, 물리적 호스트의 소프트웨어 문제, 네트워크 연결성에 영향을 미치는 물리적 호스트의 하드웨어 문제가 포함됩니다. 인스턴스 상태 확인에는 잘못된 네트워킹 또는 시작 구성, 메모리 소진, 손상된 파일 시스템 및 호환되지 않는 커널이 포함됩니다.

기능	참고
보안 관리	AMS는 Amazon EC2 GuardDuty 조사 결과 및 AWS Config 규칙을 모니터링하고 이에 응답합니다.
백업 관리	AMS는 AMS 사용자 지정 AWS Backup 계획 및 볼트를 사용하여 EC2용 Accelerate에서 연속성 관리를 제공합니다.

연락처 및 에스컬레이션

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

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

연락 시간

여러 가지 이유로 AMS Accelerate에 문의할 수 있습니다.

Feature	AMS Accelerate
	프리미엄 티어
서비스 요청	24/7
인시던트 관리(P2-P3)	24/7
백업 및 복구	24/7

Feature	AMS Accelerate
	프리미엄 티어
패치 관리	24/7
모니터링 및 알림	24/7
클라우드 서비스 제공 관리자(CSDM)	월요일~금요일: 08:00~17:00, 현지 업무 시간

업무 시간

Feature	AMS Accelerate
	프리미엄 티어
서비스 요청	24/7
인시던트 관리(P1)	24/7
인시던트 관리(P2-P3)	24/7
백업 및 복구	24/7
패치 관리	24/7
모니터링 및 알림	24/7
클라우드 서비스 제공 관리자(CSDM)	월요일~금요일: 09:00~17:00, 현지 업무 시간

에스컬레이션 경로

AMS는 계정에 적용된 AMS 서비스 수준 계약에 따라 인시던트 관리 및 서비스 요청 관리를 통해 연중무휴로 고객을 지원합니다.

관리형 환경에 영향을 미치는 AWS 또는 AMS 서비스 성능 문제를 보고하려면 AMS 콘솔을 사용하여 인시던트 사례를 제출합니다. 자세한 내용은 Accelerate를 위한 인시던트 제출을 참조하세요. AMS 인시던트 관리에 대한 일반적인 정보는 섹션을 참조하세요AMS Accelerate의 인시던트 관리.

정보나 조언을 요청하거나 AMS에서 추가 서비스를 요청하려면 AMS 콘솔을 사용하여 서비스 요청을 제출합니다. 자세한 내용은 Accelerate에서 서비스 요청 생성을 참조하세요. AMS 서비스 요청에 대한 일반 정보는 섹션을 참조하세요Accelerate의 서비스 요청 관리.

Accelerate의 리소스 인벤토리

AMS Accelerate가 AWS 계정 또는 계정에 배포하는 모든 리소스는 `resource_inventory.zip` 파일(Excel 스프레드시트)에 나열됩니다.

> **Note**
>
> 리소스 이름 열에서 접두사 CFN:은 리소스 이름 대신 CloudFormation 논리적 ID를 나타냅니다. S3 버킷 정책과 같이 이름이 지정되지 않은 리소스에 대해 표시됩니다.

AMS는에 설명된 대로 서비스 세트를 배포합니다서비스 설명. 빈 계정에 배포하면 배포 비용이 저렴하지만 사용률이 증가함에 따라 비용이 증가합니다. 예를 들어 로그가 생성되고 리소스가 변경되면 구성 규칙이 호출됩니다.

구성 규칙을 여러 번 변경하면 여러 구성 규정 준수 호출이 트리거되어 비용이 증가할 수 있습니다. 인스턴스 모니터링에 사용되는 Amazon CloudWatch에도 동일한 가능성이 적용됩니다. 모니터링이 세분화될수록 서비스 비용이 높아집니다. AWS Backup 는 또 다른 예입니다. 여러 개의 백업이 저장되어 있거나 보존 기간이 더 긴 경우 더 많은 스토리지를 사용하고 비용이 더 높습니다.

이러한 수치는 예측하기 어렵습니다. 클라우드 서비스 제공 관리자(CSDM)와의 월별 비즈니스 검토 중에 변경 사항을 추적하고 비용 절감 기회 영역을 식별하기 위해 노력합니다.

인프라 제어

AMS Accelerate는 특정 제어에서 잘못된 구성으로 플래그가 지정될 수 있는 리소스를 배포합니다. 그러나 이러한 구성은 의도적인 비용 최적화 절충이거나 보상 제어의 적용을 받습니다. AMS는이 설명서의 정보를 사용하여 제어를 활성화하거나 예외를 표시할 것을 권장합니다 AWS Security Hub.

주제

- Accelerate의 자체 문제 해결 Security Hub 제어
- Accelerate의 기타 Security Hub 제어

Accelerate의 자체 문제 해결 Security Hub 제어

Accelerate에서 다음과 같은 자체 문제 해결 제어를 사용할 수 있습니다.

주제

- S3.7 - S3 범용 버킷은 리전 간 복제를 사용해야 합니다.
- S3.11 - S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.
- S3.13 - S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.
- S3.15 - S3 범용 버킷에는 객체 잠금이 활성화되어 있어야 합니다.
- Config.1 - 리소스 기록을 위해 서비스 연결 역할을 활성화하고 사용해야 AWS Config 합니다.

S3.7 - S3 범용 버킷은 리전 간 복제를 사용해야 합니다.

리소스:

- arn:aws:s3::ams-a<account_id>-alarmmanager-<region>
- arn:aws:s3::ams-a<account_id>-patch-data-reporting-<region>
- arn:aws:s3::ams-a<account_id>-patch-data-reporting-<region>-audit
- arn:aws:s3:::ams-config-recorder-bucket-<account_id>
- arn:aws:s3:::ams-config-recorder-bucket-<account_id>-audit

AMS 인프라 구성 요소에서 사용하는 S3 버킷에는 비용을 최적화하기 위해 리전 간 복제가 활성화되어 있지 않습니다. 리전 간 복제를 활성화하면 리전 간 데이터 복제에 대한 데이터 전송 요금과 대상 리전의 추가 스토리지 비용이 발생합니다. 내부 AMS 작업을 지원하고 기본적으로 지리적 중복이 필요하지 않은 버킷의 경우 교차 리전 복제는 필요한 이점을 제공하지 않고 상당한 지속적인 비용을 추가합니다.

이러한 버킷은 경보 관리, 패치 보고 및 구성 기록과 같은 운영 데이터를 단일 리전 내에 저장하므로 일반적인 AMS 작업에는 리전 간 복제가 필요하지 않습니다. 그러나 AMS는 특정 재해 복구 또는 규정 준수 요구 사항에 따라 이러한 버킷에서 리전 간 복제를 활성화할 수 있는 기능을 제공합니다. 사용 사례에 맞게 리전 간 복제를 구성하는 데 도움이 필요한 경우 AMS에 문의하세요.

S3.11 - S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다.

리소스:

- arn:aws:s3::ams-a<account_id>-alarmmanager-<region>
- arn:aws:s3::ams-a<account_id>-patch-data-reporting-<region>

- arn:aws:s3::ams-a<account_id>-patch-data-reporting-<region>-audit
- arn:aws:s3:::ams-config-recorder-bucket-<account_id>
- arn:aws:s3:::ams-config-recorder-bucket-<account_id>-audit

AMS 인프라 구성 요소에서 사용하는 S3 버킷에는 비용을 최적화하기 위한 이벤트 알림이 활성화되어 있지 않습니다. S3 이벤트 알림을 활성화하면 알림 전송 메커니즘(예: Amazon Simple Notification Service, SQS 또는 AWS Lambda 호출)에 대한 요금이 발생하며, 이는 S3 작업 볼륨에 따라 추가될 수 있습니다. 자세한 내용은 Amazon SNS 요금을 참조하세요.

이러한 버킷은 내부 AMS 작업을 지원하며 기본적으로 이벤트 기반 워크플로가 필요하지 않으므로 불필요한 비용을 방지하기 위해 이벤트 알림을 활성화하지 않았습니다. 그러나 AMS는 특정 모니터링 또는 자동화 요구 사항에 따라 이러한 버킷에서 이벤트 알림을 활성화하는 기능을 제공합니다. 사용 사례에 맞게 이벤트 알림을 구성하는 데 도움이 필요한 경우 AMS에 문의하세요.

S3.13 - S3 범용 버킷에는 수명 주기 구성이 있어야 합니다.

리소스:

- arn:aws:s3:::ams-config-recorder-bucket-<account_id>
- arn:aws:s3:::ams-config-recorder-bucket-<account_id>-audit

과거에는 이러한 S3 리소스가 속한 구성 요소에 비용 효율성 이유로 이러한 구성이 포함되지 않았습니다. 그러나 AMS는 구성을 사용하여이 제어를 수정할 수 있는 기능을 제공합니다. 도움이 필요한 경우 AMS에 문의하세요.

S3.15 - S3 범용 버킷에는 객체 잠금이 활성화되어 있어야 합니다.

리소스:

- arn:aws:s3::ams-a<account_id>-alarmmanager-<region>

AMS Alarm Manager 시스템에서 사용하는 S3 버킷에는 비용 효율성 고려 사항으로 인해 객체 잠금이 활성화되어 있지 않습니다. 객체 잠금을 활성화하면 비용(CloudTrail 데이터 증가로 이어지는 추가 API 호출 필요)과 운영 복잡성이 증가할 수 있습니다. 특히 일반적인 작업의 일부로 객체를 자주 업데이트하거나 삭제해야 하는 버킷의 경우 더욱 그렇습니다. 그러나 규정 준수 또는 데이터 보존 요구 사항에 따라이 기능이 필요한 경우 이러한 버킷에서 객체 잠금을 수동으로 활성화할 수 있습니다. 이 구성에 도움이 필요한 경우 AMS에 문의하세요.

리소스:

- arn:aws:s3::ams-a<account_id>-patch-data-reporting-<region>
- arn:aws:s3::ams-a<account_id>-patch-data-reporting-<region>-audit

AWS 서비스 제한으로 인해 `ams-a<AccountID>-patch-data-reporting-<Region>` 및 `ams-a<AccountID>-patch-data-reporting-<Region>-audit` 버킷에서 객체 잠금을 활성화할 수 없습니다. patch-data-reporting 버킷은 S3 객체 잠금과 호환되지 않는 SSM 리소스 데이터 동기화를 통해 Systems Manager 인벤토리에서 데이터를 수신합니다. 감사 버킷은 객체 잠금을 활성화할 수 없는 S3 서버 액세스 로그 대상 역할을 합니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 인벤토리에 대한 리소스 데이터 동기화 생성을 참조하세요. 이러한 AWS 서비스 제약으로 인해 필수 기능을 유지하면서 객체 잠금이 기술적으로 불가능합니다.

Config.1 - 리소스 기록을 위해 서비스 연결 역할을 활성화하고 사용해야 AWS Config 합니다.

리소스:

- Config 레코더

온보딩 중에 AMS는 `AWSServiceRoleForConfig` 기본적으로 서비스 연결 역할을 AWS Config 사용하여 배포됩니다. 그러나 서비스 연결 AWS Identity and Access Management 역할을 사용하여 비용을 절감하는 AWS Config 대신에 사용자 지정 역할을 제공한 경우이 제어가 실패할 수 있습니다. 사용자 지정 역할은 작동할 수 있지만 수동 정책 관리가 필요하며가 새 리소스 유형 또는 기능에 대한 지원을 AWS Config 추가할 때 자동으로 업데이트를 받지 못할 수 있습니다.

서비스 연결 역할를 사용하도록 AWS Config 레코더를 업데이트하여이 결과를 자체 수정할 수 있습니다`AWSServiceRoleForConfig`. 이는 권장 구성이며 AWS 모범 사례에 부합합니다. AMS에서 배포한 AWS Config 인프라에 대한 자세한 지침은 인프라 보안 모니터링을 참조하세요.

Accelerate의 기타 Security Hub 제어

Accelerate에서 다음 보정 컨트롤을 사용할 수 있습니다.

주제

- Lambda.3 - Lambda 함수는 VPC에 있어야 합니다.
- S3.17 - S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys
- KMS.2 - IAM 보안 주체에 모든 KMS 키에 대한 복호화 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.

- S3.9 - S3 범용 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다.
- EC2.6 - 모든 VPC에서 VPCs 흐름 로깅을 활성화해야 합니다.

Lambda.3 - Lambda 함수는 VPC에 있어야 합니다.

리소스:

- AMSAlarmManagerDeploymentHandler
- AMSAlarmManagerOrphanedAlarmCleanup
- AMSAlarmManagerRemediation
- AMSAlarmManagerReporting
- AMSAlarmManagerTriggerEvaluation
- AMSAlarmManagerValidation
- AMSConfigExtensionDeploymentHandler
- AMSConfigFSXExtension
- AMSConfigOutpostExtension
- AMSConfigSyntheticCanaryExtension

AMS에서 배포한 AWS Lambda 함수는 계정의 리소스와 통신하지 않습니다. 따라서 전용 탄력적 네트워크 인터페이스(ENIs) 또는 VPC 배치가 필요하지 않습니다. VPC 외부에 이러한 함수를 배포하면 비용이 절감되고 배포 속도가 향상됩니다. 이 접근 방식은 리소스 내 통신에 대한 보안 문제를 일으키지 않습니다. 이러한 Lambda 함수는 독립적으로 작동하고 VPC 기반 리소스에 액세스하지 않으므로 VPC 배포는 추가 보안 이점 없이 불필요한 복잡성과 비용을 추가합니다.

S3.17 - S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys

리소스:

- arn:aws:s3::ams-a<account_id>-alarmmanager-<region>

AMS Alarm Manager 시스템에서 사용하는 Amazon Simple Storage Service 버킷은 고객 관리형 KMS 키(SSE-KMS) 대신 Amazon 관리형 암호화 키(SSE-S3)를 사용합니다. 고객 관리형 키를 구현하려면 키 정책을 통해 KMS 키를 사용할 수 있는 AMS 명시적 권한을 부여해야 합니다. 이로 인해 추가적인 운영 복잡성과 위험이 발생합니다. 이 제어를 사용하면 추가 비용과 운영 복잡성을 방지하면서 저장 시 강력한 암호화가 가능합니다.

키 정책을 수정하거나, 키를 부적절하게 교체하거나, 실수로 키를 삭제하거나 비활성화하면 AMS 모니터링이 즉시 실패합니다. 고객 관리형 키 가용성에 대한 이러한 종속성은 AMS 중요 모니터링 및 알림 인프라를 손상시킵니다. 실시간 모니터링 기능, 알림 전송, 인시던트 대응 및 서비스 상태 가시성이 잠재적으로 중단될 수 있습니다. Amazon 관리형 암호화 키는 키 정책, 교체 일정 또는 액세스 권한을 관리할 필요 없이 저장 데이터를 자동으로 암호화합니다. 이 구현은 AMS관리형 인프라의 비용 효율성과 운영 간소화를 유지하면서 암호화 요구 사항을 충족합니다.

리소스:

- arn:aws:s3::ams-a<account_id>-cloudtrail-log-<region>-audit

AWS CloudTrail 감사 로깅 버킷은 AWS 서비스 제한으로 인해 AWS KMS 암호화를 사용할 수 없습니다. 서버 액세스 로깅 대상으로 사용되는 S3 버킷에는 KMS 키 암호화가 활성화되어 있지 않아야 합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 기본 암호화 구성 및 서버 액세스 로깅 문제 해결을 참조하세요. 로깅 대상 버킷에서 AWS KMS 암호화를 활성화하면 로깅 실패가 발생하고 운영 문제가 발생할 수 있습니다. 이 버킷은 대신 Amazon S3-managed 암호화(SSE-S3)를 사용합니다. 이렇게 하면 S3 서버 액세스 로깅 기능과의 호환성을 유지하면서 저장 시 암호화를 제공합니다.

KMS.2 - IAM 보안 주체에 모든 KMS 키에 대한 복호화 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.

리소스:

- KMS 키: alias/ams/patchreporting

인라인 정책에는 특정 KMS 키(ams_ssm_inventory_bucket_kms_key)에 연결된 리소스 기반 정책인 KMS 키 정책에 "Resource": ["*"]가 포함되어 있습니다. 키 정책은 기본적으로 개별 키로 범위가 지정되며, 정책 범위가 이미 키 자체에 의해 제한되므로 리소스 요소에 *를 사용하는 것이 표준 AWS 관행입니다. 자세한 내용은 AWS KMS keys 개발자 안내서의 키 정책 생성 및 기본 키 정책을 참조하세요. 이 구성은 계정의 모든 키가 아닌 단일 KMS 키로 액세스가 제한되므로 보안 위험이 없습니다.

S3.9 - S3 범용 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다.

리소스:

- ams-config-recorder-bucket-<account_id>-audit

이러한 S3 버킷은 AWS Config 레코더 버킷의 액세스 로깅 대상 버킷입니다. S3는 이러한 버킷에 대한 액세스 로깅을 설정하지 않는 것이 좋습니다. 그러면 로깅 루프가 무한하게 생성되어 비용이 불필요하

게 증가합니다. AWS Security Hub 대신는이 시나리오의 리소스에 조사 결과가 표시되지 않도록 할 것을 권장합니다.

문제 해결:

결과는 유용하지 않으므로 영향을 받는 이러한 버킷에 대해이 결과를 숨겨야 합니다. 조사 결과를 억제하지 않으려면 선택적으로 버킷에서 자체 로깅을 구성할 수 있습니다. AMS가 버킷을 업데이트하면 자체 로깅이 제거될 위험이 있습니다.

EC2.6 - 모든 VPC에서 VPCs 흐름 로깅을 활성화해야 합니다.

리소스:

- 계정 생성 시 기본 vpc

기본적으로 AMS는 기본 VPC에 대해 VPC 흐름 로그를 활성화하지 않습니다.

문제 해결:

`ams:managed=true` 태그 키/값을 추가하고, 구성 규칙의 상태를 지우고, 규칙 평가를 다시 실행하여 제어를 자체 수정할 수 있습니다. AMS의 자동 수정 구성 요소는 vpc에서 VPC 흐름 로그를 활성화합니다.

AMS Accelerate 시작하기

AWS Managed Services(AMS)에서 아직 계정을 운영하지 않는 경우 먼저 AWS Managed Services - 판매 문의 페이지를 사용하여 Amazon Web Services(AWS) 영업 담당자에게 문의하세요. AWS Managed Services

AMS에 가입하면 AMS Accelerate 팀이 각에 대해 다음과 같은 온보딩 프로세스를 안내합니다 AWS 계정.

AWS AWS Managed Services 기능에서 기능 세트 검토

> **Note**
>
> AMS Accelerate는 GovCloud 리전을 지원합니다. 서비스가에 상주하는 경우 시작하기를 AWS GovCloud (US) Region참조하세요. AWS GovCloud (US)

Accelerate의 계정 온보딩 프로세스

AMS Accelerate에 계정을 온보딩하는 단계는 4단계로 구성됩니다.

1. 1단계. Accelerate의 계정 검색는 계정의 현재 상태를 평가하고 계정 온보딩을 위한 기술적 차단기를 식별합니다.
2. 2단계. Accelerate의 온보딩 관리 리소스는 이용 약관에 동의하고, 보안 기준을 설정하고 필요에 따라 문제를 해결하는 데 도움이 되는 AMS Accelerate 클라우드 아키텍트(CAs)의 온보딩 역할을 생성하도록 요청합니다.
3. 3단계. 기본 정책을 사용하여 AMS 기능 온보딩 모니터링, 패치 적용 및 백업과 같은 Accelerate 기능을 위한 입니다.
4. 4단계. Accelerate의 기능 사용자 지정는 EC2 인스턴스를 포함한 리소스가 애플리케이션에 맞게 올바르게 구성되도록 합니다.

온보딩 사전 조건 가속화

온보딩 프로세스를 시작하기 전에 Accelerate 구성 요소가 의존하는 기술적 종속성을 이해하는 것이 중요합니다.

> **Note**
>
> AMS Accelerate를 사용하려면 Enterprise On-Ramp 또는 Enterprise라는 두 가지 지원되는 지원 플랜 중 하나에 있어야 합니다. 개발자 및 비즈니스 플랜은 AMS Accelerate 자격이 없습니다. 다양한 플랜에 대한 자세한 내용은 지원 플랜 비교를 참조하세요.

AMS Accelerate VPC 엔드포인트

VPC 엔드포인트는 VPC와 지원되는 AWS 서비스 및 기반 VPC 엔드포인트 서비스 간의 프라이빗 연결을 활성화합니다 AWS. 아웃바운드 인터넷 연결을 필터링해야 하는 경우 AMS Accelerate가 서비스 종속성과 연결되도록 다음 VPC 서비스 엔드포인트를 구성합니다.

> **Note**
>
> 다음 목록에서 *region*은 미국 동부(오하이오) AWS 리전과 같은 리전us-east-2의 식별자를 나타냅니다.

```
com.amazonaws.region.logs
com.amazonaws.region.monitoring
com.amazonaws.region.ec2
com.amazonaws.region.ec2messages
com.amazonaws.region.ssm
com.amazonaws.region.ssmmessages
com.amazonaws.region.s3
com.amazonaws.region.events
```

AWS VPC 엔드포인트를 구성하는 방법에 대한 자세한 내용은 VPC 엔드포인트를 참조하세요.

> **Note**
>
> 위에서 언급한 모든 서비스에 대해 계정에 VPC 엔드포인트를 생성하는 경우이 샘플 CloudFormation 템플릿을 참조하세요. 이 템플릿을 업데이트하고 사용 사례에 따라 VPC 엔드포인트 정의를 제거하거나 추가할 수 있습니다.

Accelerate의 아웃바운드 인터넷 연결

1. egressMgmt.zip를 다운로드합니다.
2. **ams-egress.json** 파일을 엽니다.
3. JSON 속성에서 URLs을 찾습니다.
   - `WindowsPatching`
   - `RedHatPatching`
   - `AmazonLinuxPatching`
   - `EPELRepository`
4. 이러한 URLs에 대한 액세스를 허용합니다.

Accelerate에서 아웃바운드 연결 테스트

다음 방법 중 하나를 사용하여 아웃바운드 연결을 테스트합니다.

> **Note**
>
> 스크립트/명령을 실행하기 전에 빨간색 *##*을와 같은 리전 식별자로 바꿉니다`us-east-1`.

Windows PowerShell 스크립트

```
$region = 'region'
@('logs','monitoring','ec2','ec2messages','ssm','ssmmessages','s3','events') | `
ForEach-Object { `
Test-NetConnection ("$_" + '.' + "$region" + '.amazonaws.com') -Port 443 } | `
Format-Table ComputerName,RemotePort,RemoteAddress,PingSucceeded,TcpTestSucceeded -
AutoSize
```

Linux 명령

```
for endpoint in logs monitoring ec2 ec2messages ssm ssmmessages s3 events; do nc -zv
 $endpoint.region.amazonaws.com 443; done
```

Accelerate의 Amazon EC2 Systems Manager

AMS에서 관리하려는 모든 EC2 인스턴스에 AWS Systems Manager 에이전트(SSM 에이전트)를 설치해야 합니다. 또한 SSM 에이전트에 필요한 버킷 권한을 추가해야 합니다. Amazon EC2가 포함된 개요는 섹션을 참조하세요3단계. 기본 정책을 사용하여 AMS 기능 온보딩.

Accelerate의 IAM

사용자가 AMS 콘솔 액세스 또는 백업 구성과 같은 AMS Accelerate 기능을 읽고 구성할 수 있도록 하려면 AWS Identity and Access Management (IAM)에서 이러한 작업을 수행할 수 있는 명시적 권한을 부여해야 합니다. IAM 정책의 예는 AMS 기능을 사용할 수 있는 권한을 참조하세요.

1단계. Accelerate의 계정 검색

AMS는 계정 검색 중에 사용자와 협력하여 계정의 현재 상태를 평가하고 계정 온보딩을 위한 기술적 차단기를 식별합니다. AMS는 계정 검색 단계에서 운영 서비스를 제공하지 않습니다. AMS는 `AWSServiceRoleForSupport` 서비스 연결 역할을 사용하여 기술 차단기를 식별한 다음 계정 수준 온보딩 단계로 이동하기 전에 사용자와 협력하여 문제를 해결합니다.

Accelerate의 계정 검색 프로세스

계정의 분석 및 검색에 도움이 되도록 AMS는 운영 검사를 수행하여 읽기 전용 API 호출을 통해 기술적 차단기를 식별합니다. 계정이 AMS에 온보딩된 후 이러한 검사는 계정 태세를 유지하기 위해 온디맨드로 수행됩니다. AMS는 사용자와 협력하여 필요한 경우 이러한 검사와 관련된 모든 결과를 해결합니다. AMS는 계정 검색의 일부로 다음과 같은 운영 검사 및 읽기 전용 API 작업을 사용합니다.

운영 확인	용도	AWS 사용된 API 호출
AWS Control Tower 버전 평가	AWS Control Tower 버전을 식별하여 온보딩에 지원되는 최소 버전인지 확인합니다 AWS 계정.	• `ControlTower:GetLandingZone` • `ControlTower:ListEnabledControls` • `ControlTower:ListLandingZones`
AWS CloudTrail 평가	CloudTrail AWS CloudTrail 추적 비용을 최소화하기 위해 온	• `CloudTrail:GetTrail` • `CloudTrail:ListTrails`

운영 확인	용도	AWS 사용된 API 호출
	보딩 AWS 계정 을 위한 추적 및 해당 구성을 식별합니다.	• S3:GetBucketOwnershipControls • S3:GetBucketPolicy • KMS:GetKeyPolicy • CloudTrail:GetEventSelectors • S3:GetBucketLogging • S3: GetBucketLifecycleConfiguration • S3: GetBucketEncryption
CloudFormation 후크 평가	에서 AMS 서비스 배포를 차단 AWS 계정 하는 온보딩의 CloudFormation 후크를 식별합니다 AWS 계정.	• CloudFormation:ListTypes
Amazon EC2 인스턴스 평가	AWS Systems Manager 에이전트(SSM 에이전트) AWS 계정 를 실행하지 않고 AMS에서 지원하지 않는의 EC2 인스턴스를 식별합니다.	• EC2:DescribeInstances • EC2:DescribeImages • SSM:DescribeInstanceInformation

AMS Accelerate는 규정 준수 자격을 충족하고 유지하기 위해 업계 모범 사례를 따릅니다. 계정에 대한 AMS Accelerate Discovery 액세스는 AWSServiceRoleForSupport 서비스 연결 역할을 AWS CloudTrail 통해에 기록됩니다. 이를 통해 요구 사항을 모니터링하고 감사할 수 있습니다. 에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 AWS CloudTrail참조하세요.

2단계. Accelerate의 온보딩 관리 리소스

다음은 관리 리소스 온보딩 프로세스에 대한 개요입니다.

약관에 동의합니다.

클라우드 서비스 제공 관리자(CSDM)가 수락 프로세스를 안내합니다. 이용 약관, 선택, AWS 리전추가 기능 및 서비스 수준 계약(SLA)에 동의해야 합니다.

AMS 역할에 권한을 부여합니다.

AMS 프로세스 및 클라우드 아키텍트에 대한 액세스 권한을 부여해야 합니다. 이렇게 하려면 각 역할에 대한 CloudFormation 스택을 생성합니다. 단원AMS 역할을 생성하기 위한 템플릿을 참조한 다음 단원을 참조하십시오가속화 CloudFormation 를 위해 aws_managedservices_onboarding_role를 사용하여 생성. 자세한 내용은 AMS Accelerate의 액세스 관리 단원을 참조하십시오.

AMS가 구성을 검토합니다.

또한 Cloud Architect(CA)는 AMS가 AMS에 필요한 도구 및 리소스를 배포하지 못하게 할 수 있는 서비스 제어 정책(SCPs) 및 보안 조사 결과와 같은 계정의 가능한 구성 문제를 찾습니다. CA는 사용자와 협력하여 조사 결과를 수정하고 AMS 도구 및 리소스 배포에 대한 차단기를 제거하는 데 도움이 됩니다.

AMS가 AWS CloudTrail 추적 구성을 검토합니다.

Cloud Architect(CA)는 CloudTrail 추적 구성을 검토하고 AMS가 글로벌 CloudTrail 추적을 배포하거나 Accelerate를 CloudTrail 계정 또는 조직 추적 리소스와 통합할지 확인합니다. Accelerate를 CloudTrail 추적과 통합하도록 선택하면 CA가 CloudTrail 추적 리소스의 구성에 필요한 업데이트를 안내합니다.

AMS에서 관리 리소스 배포

AMS 팀은 도구와 AWS 리소스를 배포하여 AMS Accelerate의 다양한 서비스를 제공합니다. 완료되면 AMS는 AWS Managed Services 계정을 빌드하고 AMS는 계정이 활성 상태임을 알려줍니다.

이것으로 온보딩 관리 리소스 단계를 마칩니다. 온보딩 프로세스의 다음 단계인 로 바로 진행할 수 있습니다3단계. 기본 정책을 사용하여 AMS 기능 온보딩.

> **Note**
>
> 이제 계정이 활성화되었으므로 다음 작업 중 하나를 수행할 수 있습니다.
>
> - 지원 센터 콘솔을 사용하여 AWS 인프라에 대한 인시던트 및 서비스 요청을 생성합니다. AMS Accelerate의 인시던트 보고서, 서비스 요청 및 결제 질문을(를) 참조하세요.
> - AMS에서 배포한 AWS Config 규칙의 계정에서 적합성 상태를 확인합니다Accelerate의 구성 규정 준수.
> - GuardDuty 및 Macie(선택 사항) 조사 결과를 찾아 분석합니다. GuardDuty로 모니터링을(를) 참조하세요.

- CloudTrail 로그 액세스 및 감사
- AMS Accelerate 계정의 변경 사항을 추적합니다. AMS Accelerate 계정의 변경 사항 추적을(를) 참조하세요.
- Resource Tagger를 사용하여 태그를 생성합니다. 리소스 태거 가속화을(를) 참조하세요.
- 패치, 백업 및 AWS Config 보고서를 요청합니다. 보고서 및 옵션을(를) 참조하세요.

구성을 검토하고 업데이트하여 AMS Accelerate가 CloudTrail 추적을 사용할 수 있도록 합니다.

AMS Accelerate는 계정의 모든 리소스에 대한 감사 및 규정 준수를 관리하기 위해 AWS CloudTrail 로깅을 사용합니다. 온보딩 중에 Accelerate가 기본 AWS 리전에 CloudTrail 추적을 배포할지 아니면 기존 CloudTrail 계정에서 생성된 이벤트를 사용할지 선택합니다. 계정에 추적이 구성되어 있지 않은 경우 Accelerate는 온보딩 중에 관리형 CloudTrail 추적을 배포합니다.

Important

CloudTrail 로그 관리 구성은 AMS Accelerate를 CloudTrail 계정 또는 조직 추적과 통합하도록 선택한 경우에만 필요합니다.

Cloud Architect(CA)를 사용하여 CloudTrail 이벤트 전송 대상에 대한 CloudTrail 추적 구성, Amazon S3 버킷 정책 및 AWS KMS 키 정책 검토

Accelerate가 CloudTrail 추적을 사용하려면 먼저 Cloud Architect(CA)와 협력하여 Accelerate 요구 사항을 충족하도록 구성을 검토하고 업데이트해야 합니다. Accelerate를 CloudTrail Organization 추적과 통합하기로 선택한 경우 CA는 사용자와 협력하여 CloudTrail 이벤트 전송 대상 Amazon S3 버킷 및 AWS KMS 키 정책을 업데이트하여 Accelerate 계정에서 교차 계정 쿼리를 활성화합니다. Amazon S3 버킷은 Accelerate에서 관리하는 계정 또는 사용자가 관리하는 계정에 있을 수 있습니다. 온보딩 중에 Accelerate는 CloudTrail Organization 추적 이벤트 전송 대상에 쿼리를 수행할 수 있는지 확인하고 쿼리가 실패하면 온보딩을 일시 중지합니다. 온보딩을 재개할 수 있도록 CA와 협력하여 이러한 구성을 수정합니다.

CloudTrail 계정 또는 조직 추적 구성 검토 및 업데이트

CloudTrail 계정 또는 조직 추적 리소스의 Accelerate CloudTrail 로그 관리를 통합하려면 다음 구성이 필요합니다.

- CloudTrail 추적은 모든의 이벤트를 로깅하도록 구성됩니다 AWS 리전.
- CloudTrail 추적에 글로벌 서비스 이벤트가 활성화되어 있습니다.
- CloudTrail 계정 또는 조직 추적은 읽기 및 쓰기 이벤트를 포함한 모든 관리 이벤트를 로깅하며, AWS KMS Amazon RDS Data API 이벤트 로깅이 활성화됩니다. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-management-events-with-cloudtrail.html#read-write-events-mgmt
- CloudTrail 추적에 로그 파일 무결성 검증이 활성화되어 있습니다.
- CloudTrail 추적이 이벤트를 전달하는 Amazon S3 버킷은 SSE-S3 또는 SSE-KMS 암호화를 사용하여 이벤트를 암호화합니다.
- CloudTrail 추적이 이벤트를 전달하는 Amazon S3 버킷에는 서버 액세스 로깅이 활성화되어 있습니다.
- CloudTrail 추적이 이벤트를 전달하는 Amazon S3 버킷은 CloudTrail 추적 데이터를 최소 18개월 동안 유지하는 수명 주기 구성을 갖습니다.
- CloudTrail 추적이 이벤트를 전달하는 Amazon S3 버킷에는 객체 소유권이 버킷 소유자 적용으로 설정되어 있습니다.
- CloudTrail 추적이 이벤트를 전달하는 Amazon S3 버킷은 Accelerate에서 액세스할 수 있습니다.

CloudTrail 이벤트 전송 대상에 대한 Amazon S3 버킷 정책 검토 및 업데이트

온보딩 중에 Cloud Architect(CA)와 협력하여 CloudTrail 이벤트 전송 대상에 Amazon S3 버킷 정책 설명을 추가합니다. 사용자가 Accelerate 계정에서 CloudTrail 이벤트 전송 대상 Amazon S3 버킷의 변경 사항을 쿼리할 수 있도록 하려면 Accelerate가 관리하는 조직의 각 계정에 균일하게 이름이 지정된 IAM 역할을 배포하고 모든 Amazon S3 버킷 정책 설명의 `aws:PrincipalArn` 목록에 추가할 수 있습니다. 이 구성을 사용하면 사용자는 Athena를 사용하여 Accelerate에서 계정의 CloudTrail Organization 추적 이벤트를 쿼리하고 분석할 수 있습니다. Amazon S3 버킷 정책을 업데이트하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 콘솔을 사용하여 버킷 정책 추가를 참조하세요.

> **Important**
>
> Amazon S3 버킷 정책 업데이트는 Accelerate가 중앙 집중식 S3 버킷에 이벤트를 전달하는 CloudTrail 추적과 통합되는 경우에만 필요합니다. Accelerate는 중앙 집중식 버킷으로 전송하는 CloudTrail 추적과의 통합을 지원하지 않지만 AWS 조직 아래에 계정이 없습니다.

> **Note**
>
> Amazon S3 버킷 정책을 업데이트하기 전에 *###* 필드를 해당 값으로 바꿉니다.
>
> - *amzn-s3-demo-bucket*을 계정의 추적 이벤트가 포함된 Amazon S3 버킷의 이름으로 바꿉니다.
> - *your-organization-id*는 계정이 속한 AWS 조직의 ID입니다.
> - *your-optional-s3-log-delievery-prefix*와 CloudTrail 추적의 Amazon S3 버킷 전송 접두사. 예를 들어 `my-bucket-prefix`CloudTrail 추적을 생성할 때를 설정했을 수 있습니다.
>
> 추적에 대해 Amazon S3 버킷 전송 접두사를 구성하지 않은 경우 다음 Amazon S3 버킷 정책 설명에서 "*your-optional-s3-log-delievery-prefix*"와 진행 중인 슬래시(/)를 제거합니다.

다음 세 가지 Amazon S3 버킷 정책 설명은 Accelerate 계정에서 이벤트 전송 대상 Amazon S3 버킷의 CloudTrail 이벤트를 분석하기 위해의 구성을 검색하고 AWS Athena 쿼리를 실행할 수 있는 Accelerate 액세스 권한을 부여합니다.

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWBUCKETCONFIGAUDIT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
```

```
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWLISTBUCKET",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringLike": {
            "s3:prefix": "your-optional-s3-log-delievery-prefix/AWSLogs/*"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWGETOBJECT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/your-optional-s3-log-delievery-
prefix/AWSLogs/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
```

```
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

CloudTrail 이벤트 전송 대상에 대한 AWS KMS 키 정책 검토 및 업데이트

온보딩 중에 Cloud Architect(CA)와 협력하여 Amazon S3 버킷에 전달되는 CloudTrail 추적 이벤트를 암호화하는 데 사용되는 AWS KMS 키 정책을 업데이트합니다. 참조 AWS KMS 키 정책 설명을 기존 AWS KMS 키에 추가해야 합니다. 이렇게 하면 기존 CloudTrail 추적 이벤트 전송 대상 Amazon S3 버킷과 통합하고 이벤트를 복호화하도록 Accelerate가 구성됩니다. 사용자가 Accelerate 계정에서 CloudTrail 이벤트 전송 대상 Amazon S3 버킷의 변경 사항을 쿼리할 수 있도록 하려면 Accelerate가 관리하는 조직의 각 계정에 균일하게 이름이 지정된 IAM 역할을 배포하고 "aws:PrincipalArn" 목록에 추가할 수 있습니다. 이 구성을 사용하면 사용자가 이벤트를 쿼리할 수 있습니다.

고려해야 할 다양한 AWS KMS 주요 정책 업데이트 시나리오가 있습니다. 모든 이벤트를 암호화하도록 CloudTrail 추적에 구성된 AWS KMS 키만 있을 수 있으며 Amazon S3 버킷의 객체를 암호화하는 AWS KMS 키는 없을 수 있습니다. 또는 CloudTrail에서 제공하는 이벤트를 암호화하는 AWS KMS 키 하나와 Amazon S3 버킷에 저장된 모든 객체를 암호화하는 다른 AWS KMS 키 하나가 있을 수 있습니다. AWS KMS 키가 두 개 있는 경우 각 AWS KMS 키의 키 정책을 업데이트하여 CloudTrail 이벤트에 대한 Accelerate 액세스 권한을 부여합니다. 정책을 업데이트하기 전에 참조 AWS KMS 키 정책 설명을 기존 AWS KMS 키 정책으로 수정해야 합니다. AWS KMS 키 정책을 업데이트하는 방법에 대한 자세한 내용은 AWS Key Management Service 사용 설명서의 키 정책 변경을 참조하세요.

> **Important**
>
> Accelerate가 로그 파일 SSE-KMS 암호화가 활성화된 CloudTrail 추적과 통합되는 경우에만 AWS KMS 키 정책을 업데이트해야 합니다.

> **Note**
>
> Amazon S3 버킷에 전달된 AWS CloudTrail 이벤트를 암호화하는 데 사용되는 AWS KMS 키에 이 AWS KMS 키 정책 설명을 적용하기 전에 다음 ### 필드를 해당 값으로 바꿉니다.

- 계정이 속한 AWS 조직의 ID가 인 *YOUR-ORGANIZATION-ID*입니다.

이 AWS KMS 키 정책 설명은 Accelerate가 CloudTrail 이벤트를 쿼리하고 분석하는 데 사용하는 Athena에 대한 액세스 권한이 제한된 조직의 각 계정에서 Amazon S3 버킷으로 전송된 추적 이벤트를 해독하고 쿼리할 수 있는 액세스 권한을 Accelerate에 부여합니다. CloudTrail

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWTRAILOBJECTDECRYPTION",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "YOUR-ORGANIZATION-ID"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

AMS 역할을 생성하기 위한 템플릿

다음 AMS 역할은 AMS 클라우드 아키텍트(CA)에 권한을 부여합니다. 다음 zip 파일에는 IAM 역할, 권한 정책 및 신뢰 정책 생성을 간소화하는 Terraform 코드와 CloudFormation 템플릿이 포함되어 있습니다. 자세한 내용은 CA에 문의하세요.

역할 이름	에 필요	샘플 템플릿
`aws_managedservices_onboarding_role`	AMS personnel during onboarding only	onboarding_role_minimal.zip

> **Note**
>
> 샘플 템플릿(역할당 하나)을 선택하고 다운로드한 후 이를에서 CloudFormation 스택의 정의로 업로드합니다가속화 CloudFormation 를 위해 `aws_managedservices_onboarding_role`를 사용하여 생성.

가속화 CloudFormation 를 위해 **`aws_managedservices_onboarding_role`**를 사용하여 생성

에서 `aws_managedservices_onboarding_role`를 사용하여 AWS Identity and Access Management 역할을 생성할 수 CloudFormation 있습니다 AWS Management Console. 또는의 명령을 사용하여 역할을 AWS CloudShell 배포할 수 있습니다.

사용 AWS Management Console

> **Note**
>
> 시작하기 전에 각 역할에 대한 JSON 또는 YAML 파일을 업로드할 준비가 되어 있어야 합니다. 자세한 내용은 AMS 역할을 생성하기 위한 템플릿 단원을 참조하십시오.

에서 역할을 생성하려면 다음 단계를 AWS Management Console완료합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudformation CloudFormation 콘솔을 엽니다.

2. 스택 생성 > 새 리소스 사용(표준)을 선택합니다. 다음 페이지가 표시됩니다.

3. 템플릿 파일 업로드를 선택하고 IAM 역할의 JSON 또는 YAML 파일을 업로드한 후 다음을 선택합니다. 다음 페이지가 표시됩니다.

4. 스택 이름 필드에 스택 이름 "**ams-onboarding-role**"을 입력합니다. "YYYY-MM-DDT00:00:00Z" 형식을 사용하여 DateOfExpiry를 입력합니다(현재 날짜로부터 30일이 권장됨). 이 페이지에 도달할 때까지 아래로 스크롤하여 다음을 선택합니다.

5. 확인란이 선택되어 있는지 확인한 다음 스택 생성을 선택합니다.
6. 스택이 성공적으로 생성되었는지 확인합니다.

의 명령 사용 AWS CloudShell

`aws_managedservices_onboarding_role` IAM 역할을 배포하려면에서 다음 명령을 실행합니다. AWS CloudShell

AWS CLI

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/onboarding_role_minimal.zip" -o "onboarding_role_minimal.zip"
unzip -q -o onboarding_role_minimal.zip
aws cloudformation create-stack \
    --stack-name "aws-managedservices-onboarding-role" \
    --capabilities CAPABILITY_NAMED_IAM \
    --template-body file://onboarding_role_minimal.json \
    --parameters ParameterKey=DateOfExpiry,ParameterValue="`date -d '+30 days' -u '+
%Y-%m-%dT%H:%M:%SZ'`"
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/
latest/accelerate-guide/samples/onboarding_role_minimal.zip' -OutFile
 'onboarding_role_minimal.zip'
Expand-Archive -Path 'onboarding_role_minimal.zip' -DestinationPath . -Force
New-CFNStack `
    -StackName 'aws-managedservices-onboarding-role' `
    -Capability CAPABILITY_NAMED_IAM `
    -TemplateBody (Get-Content 'onboarding_role_minimal.json' -Raw) `
```

```
    -Parameter @{ParameterKey = "DateOfExpiry"; ParameterValue = (Get-
Date).AddDays(30).ToString('yyyy-MM-ddTHH:mm:ssZ')}
```

역할을 생성한 후 Cloud Architect(CA)와 협력하여 2단계. Accelerate의 온보딩 관리 리소스 프로세스를 완료합니다. AMS에서 계정이 활성 상태임을 알리면 인스턴스를 온보딩할 준비가 된 것입니다.

3단계. 기본 정책을 사용하여 AMS 기능 온보딩

이 단계에서는 기본 정책을 사용하여 AMS 기능을 온보딩합니다. 여기에는 Amazon EC2 인스턴스 추가 및 기본 설정에 따라 모니터링, 백업, AWS Config 수정 및 패치 구성(해당하는 경우 AMS 패치 오케스트레이터는 특별히 요청해야 하는 추가 기능)이 포함됩니다. 이 작업을 직접 수행하거나 AMS가 입력에 따라 기능을 온보딩하도록 요청할 수 있습니다. AMS에 도움을 요청하려면 서비스 요청을 생성하고 작업을 완료하는 데 필요한 모든 입력을 제공합니다. 서비스 요청은 즉시 해결되지 않습니다.

> **Note**
>
> 계정이 백업, 패치 또는 모니터링에 기본 정책을 사용할 수 있지만 적절한 정책을 적용하려면 리소스에 태그를 지정해야 합니다.

주제

- (선택 사항) Accelerate의 빠른 시작 템플릿
- 온보딩 가속화 모니터링
- 가속화할 EC2 인스턴스 온보딩
- Accelerate AWS Backup 의 온보딩
- Accelerate의 온보딩 패치
- Accelerate에서 규정 미준수 보고서 검토

(선택 사항) Accelerate의 빠른 시작 템플릿

Quick Start 템플릿은 Accelerate 지원 AWS 계정에서 AMS Resource Tagger의 배포 및 구성을 자동화합니다. 이 템플릿은 수동 설정에 비해 시간과 노력을 절약합니다. 이 템플릿을 있는 그대로 사용하여 하나의 계정에서 모니터링, 패치 적용 및 백업 기본 사항을 정의합니다. 또는 StackSet로 사용하여 Organizations 단위 전체에 설정을 적용하여 여러 계정에 대한 설정을 표준화합니다.

또한 이를 시작점으로 사용하여 사용자 지정 AMS 리소스 태거 프로파일을 빌드하고 설명서의 코드 조각을 사용하여 태그 지정을 위한 보다 복잡한 정의를 생성할 수 있습니다.

빠른 시작 템플릿 기능

퀵 스타트 템플릿은 다음 작업을 완료합니다.

- AMS Resource Tagger에 대한 구성 버전을 생성하고 배포합니다.
- AMS 관리 및 모니터링 리소스 생성을 지원하는 Amazon EC2 인스턴스에 태그를 적용합니다.
- (선택 사항) 원하는 일정에 따라 패치할 수 있는 관리형 EC2 인스턴스에 태그를 적용하고 패치 적용 유지 관리 기간을 생성하여 패치 적용을 용이하게 합니다.

  > **Warning**
  >
  > 기본적으로 인스턴스는 재부팅되고 중지된 인스턴스는 패치 설치를 위해 자동으로 시작됩니다.

- (선택 사항) 기본 AMS 백업 계획에 정의된 대로 백업할 수 있는 관리형 EC2 인스턴스에 태그를 적용합니다.
- (선택 사항) 향상된 백업 계획에 따라 백업할 수 있는 관리형 Amazon Relational Database Service(Amazon RDS) 리소스에 태그를 적용합니다. 또한 백업 계획은 Amazon RDS에 대해 시점 복구(PITR)를 활성화합니다. Amazon RDS 자동 백업이 활성화되지 않은 경우 데이터베이스는 다음 백업 기간에 가깝게 다시 시작됩니다.

빠른 시작 템플릿 재정의 및 제외

이 템플릿을 사용하여 퀵 스타트 스택을 생성한 후 다음 단계에 따라 관리/모니터링, 패치 또는 백업에서 특정 인스턴스를 제외합니다.

- 관리 및 모니터링: EC2 인스턴스가 AMS에 의해 관리 및 모니터링되지 않도록 제외하려면 인스턴스에이 태그를 추가합니다`ExcludeFromAMSQuickStartMonitoring=true`.
- 패치: Auto Scaling 그룹, Amazon Elastic Container Service 또는 Amazon Elastic Kubernetes Service 클러스터의 멤버인 EC2 인스턴스는이 Quick Start 템플릿에 의해 패치 적용에서 제외됩니다.

  패치 기간 생성 및 EC2 인스턴스의 패치 관련 태그 지정을 비활성화하려면 CloudFormation 스택 파라미터를 로 설정합니다`EnablePatching=false`.

에서 EC2 인스턴스가 퀵 스타트 패치 기간의 대상이 되지 않도록 제외하려면 인스턴스에이 태그를 `EnablePatching=true`추가합니다`ExcludeFromAMSQuickStartPatching=true`.

- 백업: Auto Scaling 그룹, ECS 또는 EKS 클러스터의 멤버인 EC2 인스턴스는이 퀵 스타트 템플릿에 의해 백업에서 제외됩니다.

  EC2 인스턴스가 기본 AMS 백업 계획의 대상이 되지 않도록 제외하려면에서이 태그를 해당 인스턴스에 `EnableBackup=true`추가합니다`ExcludeFromAMSQuickStartBackup=true`.

> **Tip**
>
> EC2 인스턴스에 대량으로 태그를 지정할 수 있습니다. Tag Editor를 사용하여의 한 단계에서 리소스를 대량 선택하고 태그를 지정합니다 AWS Management Console.

빠른 시작 템플릿 파라미터

이 Quick Start 템플릿은 태그를 추가하는 인스턴스를 제외하고 계정의 `ams:rt:ams-managed=true` 모든 EC2 인스턴스에 `ExcludeFromAMSQuickStartMonitoring=true` 태그를 추가하도록 Resource Tagger를 구성합니다. 다음 파라미터를 사용하여 요구 사항에 따라이 스택의 선택적 부분을 제어합니다.

CFN 파라미터	값	Effect
EnableBackup	'true'(기본값)	모든 AMS 관리형 EC2 인스턴스 (`ams:rt:ams-managed=true`) 는 기본 AMS 백업 계획에 따라 매일 4AM시 UTC에 백업을 `ams:rt:backup-orchestrator=true` 위해 로 태그가 지정됩니다. 모든 RDS 인스턴스 및 클러스터에 대해 템플릿은 향상된 백업 계획에 따라 최대 보존 기간(31일)으로 `ams:rt:backup-orchestrator-enhanced=true` "연속 백업"을 적용합니다. https://

CFN 파라미터	값	Effect
		docs.aws.amazon.com/aws-backup/latest/devguide/point-in-time-recovery.html#point-in-time-recovery-rds https://docs.aws.amazon.com/managedservices/latest/accelerate-guide/acc-backup-select-plan.html#acc-backup-plan-enhanced 이렇게 하면 PITR 보존 기간이 변경되는 경우 보류 중인 다른 구성 업데이트가 있는 경우와 같이 데이터베이스가 다시 시작될 수 있습니다.
	'false'	이 빠른 시작 템플릿의 백업 대상으로 지정된 인스턴스가 없습니다.
EnablePatching	'false'(기본값)	이 퀵 스타트 템플릿의 패치를 대상으로 하는 인스턴스는 없습니다.
	'true'	모든 AMS 관리형 인스턴스(`ams:rt:ams-managed=true`)에 태그가 `ams:rt:Patch Group=AMSQuickStartPatchWindow` 지정되고에 정의된 일정에 따라 패치 적용을 용이하게 하기 위한 기본 SSM 유지 관리 기간 리소스가 생성됩니다`CronExpression` . EC2 인스턴스에 `ams:rt:Patch Group` 태그를 적용하려면 해당 인스턴스의 인스턴스 메타데이터에 있는 태그에 대한 액세스를 꺼야 합니다.

CFN 파라미터	값	Effect
CronExpression	-	의 기본값은 Timezone 파라미터에 따라 매월 두 번째 토요일을 오후 7시 30분으로 cron(0 30 19 ? * SAT#2 *) 설정합니다. cron 구문을 사용합니다.
시간대	-	대상 인스턴스는에 따라 패치됩니다CronExpression . IANA 형식을 사용합니다.

빠른 시작 템플릿 다운로드

AMSQuickStart.zip 파일을 다운로드합니다.

또는에서 다음 명령을 실행AWS CloudShell하여를 배포합니다AMSQuickStart.yaml.

AWS Command Line Interface

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/AMSQuickStart.zip" -o "AMSQuickStart.zip"
unzip -q -o AMSQuickStart.zip
for region in region1 region2 ;
do
aws cloudformation create-stack \
    --region $region \
    --stack-name "AMSQuickStart" \
    --template-body file://AMSQuickStart.yaml \
    --parameters \
        ParameterKey=EnableBackup,ParameterValue="true" \
        ParameterKey=EnablePatching,ParameterValue="false" \
        ParameterKey=Timezone,ParameterValue="US/Eastern" \
        ParameterKey=CronExpression,ParameterValue="cron(0 30 19 ? * SAT#2 *)" \
;
done
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/latest/
accelerate-guide/samples/AMSQuickStart.zip' -OutFile 'AMSQuickStart.zip'
```

```
Expand-Archive -Path 'AMSQuickStart.zip' -DestinationPath . -Force
@('region1', 'region2') | `
ForEach-Object { `
New-CFNStack `
    -Region $_ `
    -StackName 'AMSQuickStart' `
    -TemplateBody (Get-Content 'AMSQuickStart.yaml' -Raw) `
    -Parameter @(
        @{ParameterKey = "EnableBackup"; ParameterValue = "true"},
        @{ParameterKey = "EnablePatching"; ParameterValue = "false"},
        @{ParameterKey = "Timezone"; ParameterValue = "US/Eastern"},
        @{ParameterKey = "CronExpression"; ParameterValue = "cron(0 30 19 ? * SAT#2
 *)"}
    )
}
```

각 파라미터에 대한 설명은 이전 단원인 단원을 참조하십시오빠른 시작 템플릿 파라미터.

온보딩 가속화 모니터링

Amazon EC2 인스턴스를 제외한 모든 새 리소스에 대해 기본적으로 모니터링이 활성화됩니다. 인스턴스에 태그를 지정하여 Amazon EC2 인스턴스 모니터링을 시작할 수 있습니다.

모니터링을 온보딩하려면 먼저 구성이 AMS가 모니터링할 리소스를 모니터링하고 무시할 리소스를 무시해야 합니다.

다음 CloudWatch 대시보드를 사용하여 AMS 모니터링 및 태그 지정의 대상이 되는 리소스 수와 그렇지 않은 리소스 수를 탐색할 수 있습니다. 계정에서 CloudWatch 대시보드 콘솔로 이동하여 다음 중 하나를 선택합니다.

- AMS-Alarm-Manager-Reporting-Dashboard
- AMS-Resource-Tagger-Reporting-Dashboard

대시보드 지표에 대한 전체 설명은 다음을 참조하세요.

- Resource Tagger에서 관리하는 리소스 수 보기

Accelerate에서 모니터링할 온보딩 리소스

예를 들어 non-EC2 리소스에 대한 기본 모니터링을 비활성화하려면 사용자 지정 구성 프로파일을 사용하여 해당 리소스의 태그를 해제해야 합니다. 모니터링을 위한 태그 지정에 대한 자세한 내용은 섹션을 참조하세요Accelerate의 모니터링.

사용자 지정 구성 프로파일을 사용하여 인스턴스에 태그를 지정하는 것을 포함하여 인스턴스를 온보딩할 때까지 EC2 인스턴스에 대한 모니터링이 비활성화됩니다. 다음 섹션에서는 EC2 인스턴스 온보딩에 대해 설명합니다.

Accelerate에서 모니터링 구성 프로파일 생성

- 기본 구성 사용에 대한 자세한 내용은 섹션을 참조하세요경보 관리자 가속화.
- 사용자 지정 구성 사용에 대한 자세한 내용은 섹션을 참조하세요Accelerate 경보 기본 구성 수정.

가속화할 EC2 인스턴스 온보딩

EC2 인스턴스는 자동 인스턴스 구성이라는 프로세스를 통해 AMS Accelerate에 온보딩되므로 각 인스턴스가 올바른 로그를 작성하고 AMS가 인스턴스를 올바르게 관리할 수 있도록 올바른 지표를 내보냅니다. AMS가 일부 인스턴스를 무시하도록 하려는 경우가 아니면 모든 EC2 인스턴스를 온보딩해야 합니다. 자동 인스턴스 구성을 사용하려면 AMS가 인스턴스를 구성할 수 있는 특정 조건을 충족해야 합니다(자세한 내용은 참조Accelerate의 자동 인스턴스 구성을 위한 사전 조건). 가장 중요한 조건은 AMS에서 관리할 각 Amazon EC2 인스턴스에 AWS Systems Manager 에이전트(SSM 에이전트)를 설치해야 한다는 것입니다. SSM 에이전트에 대한 자세한 내용은 SSM 에이전트 작업을 참조하세요.

Accelerate용 표준 AMIs에 사전 설치된 SSM

SSM 에이전트는 다음 운영 체제에 대해 이미 AWS제공 AMIs에 설치되어 있습니다.

- Amazon Linux and Amazon Linux 2
- SUSE Linux Enterprise Server(SLES) 12 및 15
- Microsoft Windows Server 2019, 2016, 2012 R2, 2012
- Ubuntu Linux 18.04 및 20.04

이러한 AWS제공 AMIsAccelerate에서 인스턴스 태그 지정.

Accelerate에서 SSM의 수동 SSM 설치

다음 운영 체제의 경우 또는 사용자 지정 AMI를 사용하는 경우 SSM 에이전트를 수동으로 설치할 수 있습니다. 또는 AMS SSM 에이전트 자동 설치 기능을 사용할 수 있습니다. SSM 자동 설치에 대한 자세한 내용은 섹션을 참조하세요SSM 에이전트 자동 설치. 수동 설치에 대한 지침은 운영 체제의 링크를 선택합니다.

- CentOS SSM 설치
- Oracle SSM 설치
- Red Hat SSM 설치
- SUSE Linux Enterprise Server SSM 설치
- Windows SSM 설치

Accelerate에서 인스턴스 태그 지정

SSM 에이전트를 설치한 후에는 인스턴스에 태그를 지정해야 합니다. AMS Accelerate의 태그 지정을(를) 참조하세요.

Accelerate의 자동 인스턴스 구성

인스턴스에 태그가 지정되면 AMS는 다음을 포함하는 자동 인스턴스 구성을 수행합니다.

- 운영 체제 로그 및 지표 기록
- AMS 엔지니어를 위한 원격 액세스 활성화
- 인스턴스에서 원격 명령 실행

이러한 작업은 AMS 모니터링, 패치 및 로그 서비스와 AMS가 인시던트에 대응하는 데 필수적입니다. 자동 인스턴스 구성 설정에 대한 자세한 내용은 섹션을 참조하세요AMS Accelerate의 자동 인스턴스 구성.

자동 인스턴스 구성이 완료되면 다음을 수행할 수 있습니다.

- 지원 센터 콘솔을 사용하여 Amazon EC2 인스턴스 및 운영 체제에 대한 인시던트 및 서비스 요청을 생성합니다. 자세한 내용은 AMS Accelerate의 인시던트 보고서, 서비스 요청 및 결제 질문 단원을 참조하십시오.
- Amazon EC2 로그 액세스 및 감사
- 패치 보고서 가져오기

Accelerate AWS Backup 의 온보딩

백업을 구성하려면 백업 계획이라고 하는 백업 정책을 생성해야 합니다. 백업 계획은 백업할 AWS 리소스, 백업 빈도 및 백업 보존 기간을 지정합니다. 조직의 연속성, 보안 및 규정 준수 요구 사항을 평가하여 필요한 백업 계획을 결정하는 것이 좋습니다.

옵트인

- 다음 단계에 따라 각 계정, 리전 및 리소스 유형에 대해 AWS Backup 가 활성화되어 있는지 확인합니다.

  시작하기 1: 서비스 옵트인.

  선택적으로 시작하기 2: 온디맨드 백업에서 생성.

백업 계획 선택

- 백업 계획을 선택하려면 섹션을 참조하세요AMS 백업 계획 선택.

리소스 추가

리소스는 기본적으로 백업 계획과 연결되지 않습니다. 백업 계획에 추가해야 합니다.

- 백업 계획에 리소스를 추가하려면 섹션을 참조하세요리소스에 태그를 지정하여 AMS 백업 계획 적용.
- 태그를 사용하여 모든 리소스에서 백업을 활성화하려면 섹션을 참조하세요Accelerate에서 백업 태그 관리.

Accelerate의 온보딩 패치

소프트웨어가 up-to-date 상태이고 규정 준수 정책을 충족하도록 패치 적용을 구성해야 합니다.

AWS Backup 사전 조건: 패치 유지 관리 기간 동안 루트 볼륨 스냅샷 생성을 허용하려면 시작하기 1: 서비스 옵트인 단계에 따라 Amazon EBS 리소스 유형의 각 계정 및 리전에 대해 AWS Backup 가 활성화되어 있는지 확인합니다. (시작 2: 온디맨드 백업 생성을 계속할 필요는 없습니다.)

패치 적용 시기: 패치 적용은 유지 관리 기간 중에 발생합니다. 패치가 사전 설정된 시간 동안에만 적용되도록 유지 관리 기간을 예약할 수 있습니다.

패치할 내용: 패치할 Amazon EC2 인스턴스를 유지 관리 기간에 연결해야 합니다. 인스턴스를 유지 관리 기간에 연결하려면 Amazon EC2 인스턴스에 태그를 지정해야 하며 유지 관리 기간에 해당 태그가 대상으로 있어야 합니다.

설치할 패치: 패치 기준을 사용하여 운영 체제 또는 심각도가 높은 패치와 같은 특정 유형의 패치를 자동으로 승인하는 규칙을 설정합니다. 규칙의 예외, 예를 들어 항상 승인되거나 거부되는 패치 목록을 지정할 수도 있습니다.

Amazon EC2 패치 정책에 패치 적용 권장 사항 대한 지침은 섹션을 참조하세요.

- 패치 관리 구성을 시작하려면 섹션을 참조하세요. AMS Accelerate의 패치 관리 이해
- 사용자 지정 패치 구성을 생성하려면 섹션을 참조하세요AMS Accelerate를 사용한 사용자 지정 패치 기준.

Accelerate에서 규정 미준수 보고서 검토

AMS는 인터넷 보안 센터(CIS), 미국 국립 표준 기술 연구소(NIST) 클라우드 보안 프레임워크(CSF)에서 설정한 표준에 대한 위반을 식별하는 데 도움이 되는 AWS Config 규칙을 배포합니다. 계정이 규정 준수 상태로 기준이 되도록 문제 해결 작업의 우선순위를 지정하려면 전송 팀과 함께 규정 미준수 보고서를 검토하는 것이 좋습니다.

4단계. Accelerate의 기능 사용자 지정

이 단계에서는 기본 정책을 사용하여 모니터링, 패치 적용 및 백업을 이미 온보딩했습니다. 이제 필요에 맞게 정책을 사용자 지정할 수 있습니다.

패치, 백업 또는 모니터링에 기본 정책을 사용하도록 선택하거나 필요에 따라 사용자 지정 정책을 선택할 수 있습니다. AMS는 태그를 사용하여 리소스를 운영 정책에 연결합니다. AMS는 애플리케이션 그룹화 또는 기타 그룹화 로직을 기반으로 리소스에 태그를 적용하는 방법에 대한 규칙을 지정할 수 있는 AWS Resource Tagger를 제공합니다. 자세한 내용은 섹션을 참조하세요리소스 태거 가속화.

고객 제공 태그 기능을 사용하면 AMS 리소스에 사용자 지정 태그를 추가하고 삭제할 수 있습니다. 자세한 내용은 Accelerate의 고객 제공 태그 단원을 참조하십시오.

주제

- Accelerate에서 모니터링 사용자 지정
- Accelerate에서 백업 사용자 지정
- Accelerate에서 패치 적용 사용자 지정

Accelerate에서 모니터링 사용자 지정

애플리케이션 요구 사항에 따라 클라우드 리소스 모니터링을 사용자 지정하려면:

1. 사용자 지정 모니터링 정책을 생성합니다. Accelerate 경보 기본 구성 수정을(를) 참조하세요.
2. 태그를 사용하여 리소스에 사용자 지정 정책을 적용합니다. Accelerate의 모니터링 섹션을 참조하세요
3. 리소스 소유자에게 알림을 라우팅합니다. 태그 기반 알림을(를) 참조하세요.

다음 CloudWatch 대시보드를 사용하여 AMS 모니터링 및 태그 지정의 대상이 되는 리소스 수와 그렇지 않은 리소스 수를 탐색할 수 있습니다. 계정에서 CloudWatch 대시보드 콘솔로 이동하여 다음 중 하나를 선택합니다.

- AMS-Alarm-Manager-Reporting-Dashboard
- AMS-Resource-Tagger-Reporting-Dashboard

대시보드 지표에 대한 전체 설명은 다음을 참조하세요.

- Resource Tagger에서 관리하는 리소스 수 보기

Accelerate에서 백업 사용자 지정

AMS 기본 백업 계획은 사용자 지정할 수 없습니다. 대신 애플리케이션 요구 사항에 따라 새 백업 계획을 생성한 다음 태그를 사용하여 사용자 지정 계획에 리소스를 연결합니다. AMS가 백업해야 하는 리소스, 빈도 및 보존 기간을 선택하는 것은 사용자의 몫입니다. 조직의 연속성, 보안 및 규정 준수 요구 사항을 평가하여 필요한 백업 계획을 결정하는 것이 좋습니다.

- 백업 계획을 생성하려면 백업 계획 생성을 참조하세요.
- 백업 계획에 리소스를 할당하려면 백업 계획에 리소스 할당을 참조하세요.

Accelerate에서 패치 적용 사용자 지정

패치를 적용하면 소프트웨어가 up-to-date 상태이고 규정 준수 정책을 충족할 수 있습니다.

패치 적용 시기: 패치 적용은 유지 관리 기간 중에 발생합니다. 패치가 사전 설정된 시간 동안에만 적용되도록 유지 관리 기간을 예약할 수 있습니다.

패치할 내용: 패치할 Amazon EC2 인스턴스를 유지 관리 기간에 연결해야 합니다. 인스턴스를 유지 관리 기간에 연결하려면 Amazon EC2 인스턴스에 태그를 지정해야 하며 유지 관리 기간에 해당 태그가 대상으로 있어야 합니다.

설치할 패치: 패치 기준을 사용하여 운영 체제 또는 심각도가 높은 패치와 같은 특정 유형의 패치를 자동으로 승인하는 규칙을 설정합니다. 규칙의 예외, 예를 들어 항상 승인되거나 거부되는 패치 목록을 지정할 수도 있습니다.

- 일반적인 패치 권장 사항은 섹션을 참조하세요패치 적용 권장 사항.
- 사용자 지정 유지 관리 기간을 생성하려면 섹션을 참조하세요AMS에서 패치 유지 관리 기간 생성.
- 사용자 지정 패치 기준을 생성하려면 섹션을 참조하세요AMS Accelerate를 사용한 사용자 지정 패치 기준.
- 패치 알림을 리소스 소유자에게 라우팅하려면 섹션을 참조하세요AMS Accelerate의 패치 알림 및 패치 실패 이해.

AMS 콘솔 사용

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

> **Note**
>
> 계정 역할에 따라 AMS Advanced 콘솔 또는 AMS Accelerate 콘솔에 액세스합니다.

AMS 콘솔을 사용할 때는 다음 주의 사항에 유의하세요.

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

AMS Accelerate 콘솔에는 다음과 같은 기능이 있습니다.

- 시작 페이지: 시작 페이지에는 인시던트, 서비스 요청 및 보고서에 쉽게 액세스할 수 있는 정보 상자와 링크가 있습니다.
- 기능 페이지, 왼쪽 탐색 창의 링크:
  - 대시보드: 다음을 포함하여 계정의 현재 상태에 대한 개요를 제공합니다.
    - 리소스의 인시던트: AWS Support Center에서 인시던트 사례를 열기 위한 버튼과 승인을 기다리고 있으며 주의가 필요한 인시던트 사례 수 및 미해결 상태 수
    - 규정 준수 상태: 규정 미준수 또는 규정 준수 규칙 및 리소스에 대한 링크
    - 서비스 요청: AWS Support Center에서 서비스 요청 사례를 여는 버튼과 승인 대기 중이며 주의가 필요한 수 및 열려 있는 수
    - 계정 수준 보안: 실시간 위협 탐지 GuardDuty 조사 결과 및 데이터 보안 및 개인 정보 Macie 조사 결과에 대한 세부 정보 링크
    - 빠른 작업: 백업 볼트 또는 패치 인스턴스 구성 페이지 열기
  - 보고서: 보고서 페이지와 기본 보고서, 일별 백업, 일별 패치 및 월별 청구를 엽니다.
  - 구성: 리소스가 사양에 따라 성공적으로 관리되고 있는지 확인합니다.
    - SSM 에이전트 설치: SSM 에이전트가 필요합니다.
    - 태그 지정 규칙 구성: AMS 리소스 태거를 엽니다.
    - 경보 구성: AMS CloudWatch 경보 구성을 엽니다.
    - 패치 일정 구성: AWS Systems Manager 콘솔을 엽니다.
    - 패치 기준 구성: AWS Patch Manager 콘솔을 엽니다.
    - 백업 계획 구성: AWS Backup 콘솔을 엽니다.
- 기능 스포트라이트: 콘솔의 최신 업데이트에 대한 정보
- 설명서: AWS Managed Services 설명서 랜딩 페이지

AMS 패턴

AWS Managed Services(AMS) 패턴은 AMS 관리형 환경의 사용 사례 패밀리를 해결하는 일반화된 솔루션입니다.

AMS 플랫폼에서 운영할 때 AMS 클라우드 아키텍트(CAs 비즈니스 및 운영 요구 사항을 충족하기 위해 고객과 협력합니다. AMS 고객은 고유한 방식으로 운영되지만 고객의 사용 사례는 비슷합니다. 이러한 경우 CAs는 구성 및 배포 작업을 최소화하면서 여러 고객 환경에서 사용되는 일반 솔루션 템플릿 또는 "패턴"을 생성합니다.

AMS 패턴은 AMS 고객에게 기능을 제공하는 데 도움이 되도록 구축되었으며 일반적으로 이를 요청하는 고객의 계정 CA에 의해 구축됩니다.

AMS 패턴 작동 방식

패턴을 배포할 수 있도록 필요한 Cloudformation 템플릿을 포함하여 각 패턴에 대한 자세한 내용을 요청하려면 제목 "Request for additional details about pattern *`Pattern_Name`*"(원하는 패턴 대체)을 사용하여 AMS 서비스 요청을 제출하고 AMS 클라우드 아키텍트(CA)를 추가 연락처 옵션에 추가합니다.

AMS 패턴은 다음 두(2) 가지 범주로 분류됩니다.

- 일반 사용: 패턴은 여러 AMS 고객이 배포하고 사용하므로 안정적인 것으로 간주됩니다.
- 미리 보기 모드: AMS는 검증을 위해 비프로덕션 환경에 미리 보기 모드 패턴을 배포하고 배포 전에 Cloud Architect와 협력하여 사용 사례를 논의하는 것이 좋습니다.

> **Important**
>
> AMS 패턴은 기본 AMS 서비스 수준 계약 서비스 수준 계약(SLAs) 및 서비스 수준 목표(SLOs)를 준수하지 않습니다. 패턴에 대한 지원 및 업데이트는 최선을 다해 수행됩니다.
> 이 AWS 콘텐츠는 AWS 고객과 Amazon Web Services, Inc. 또는 Amazon Web Services EMEA SARL("AWS 유럽") 또는 둘 다 간의 고객 계약 또는 기타 서면 계약의 약관에 따라 제공됩니다.
> 이 소프트웨어에 구현된 자료는 "있는 그대로" 제공되며 특정 용도에 대한 적합성 보증을 포함하되 이에 국한되지 않는 명시적, 묵시적 또는 기타 어떠한 종류의 보증도 제공하지 않습니다.

AMS 패턴

AMS 패턴.

AMS 패턴

이름	개요	이점	범주
CloudWatch 경보 알림 사용자 지정	인스턴스 이름, 애플리케이션 ID 등과 같은 인스턴스 태그의 정보를 포함하도록	경보 알림에 컨텍스트 정보를 추가하면 경보 알림이 더 의미 있고	모니터링

이름	개요	이점	범주
	CloudWatch 경보 알림을 사용자 지정합니다.	실행 가능한 정보를 제공합니다.	
디스크 사용 보고	디스크 사용 보고 패턴은 여러 앱 계정에서 볼륨의 소비 공간을 수집하여 Athena 테이블 쿼리 기능을 사용하여 Amazon S3에 중앙 집중식 보고서로 결과를 제공합니다.	계정 볼륨의 실제 사용량에 대한 인사이트를 제공하여 비용 절감 기회를 결정합니다.	비용 최적화
Prowler 스택	CloudShell을 사용할 수 없는 Amazon EC2를 사용하여 계정에 대해 Prowler 검사를 실행합니다.	현재 보안 태세에 영향을 주지 않고 권한 또는 제한 시간 문제로 인해 CloudShell을 사용할 수 없는 경우 Accelerate 온보딩(Prowler)의 차단을 해제할 수 있습니다.	[Security]
사용자 지정 객체 키를 사용한 AMS Amazon S3 복제	Amazon S3 객체를 복사하고 모든 메타데이터 및 객체 키(폴더)를 유지합니다. 소스 객체 키의 일부를 제거하거나 복제 중에 사용자 지정 대상 객체 키를 생성합니다.	객체를 필요한 폴더로 이동하는 데 추가 스크립트가 필요 없이 Amazon S3 복제 중에 객체 키(폴더)를 사용자 지정합니다.	신뢰성

이름	개요	이점	범주
Amazon EBS 스냅샷 삭제	Lambda 및 CloudWatch Events를 기반으로 하는 자동화를 통해 보존을 AWS Backup기반으로 외부에서 생성된 Amazon EBS 스냅샷의 삭제를 자동화합니다.	AWS Backup 오케스트레이터 외부에서 생성된 개별 스냅샷을 제거하여 시간이 지남에 따라 추가 비용을 절감할 수 있습니다.	비용 최적화
AMS Amazon RDS 보안 암호 교체	CloudFormation 템플릿을 사용하여 지원되는 Amazon RDS 데이터베이스, Redshift 및 DocumentDB의 보안 암호를 교체하는 데 필요한 모든 리소스(Lambda 함수, 보안 그룹, 탄력적 네트워크 인터페이스 또는 ENIs)를 자동으로 배포합니다.	데이터베이스 보안 암호 교체를 자동화하고 교체 실패 시 알림 메커니즘을 제공합니다.	[Security]
자동 키 교체	CloudWatch Events 및 Lambda를 기반으로 IAM 사용자의 액세스 및 보안 키를 자동으로 교체합니다.	IAM 사용자의 액세스 및 보안 키를 더 쉽게 교체할 수 있습니다.	[Security]

이름	개요	이점	범주
Amazon EBS 볼륨 스냅샷 태거	Amazon EC2 인스턴스의 태그를 사용하여 모든 Amazon EBS 볼륨 및 스냅샷에 태그를 지정합니다.	의미 있고 관련성 있는 비즈니스 정보로 비용을 분류하고 추적할 수 있으므로 비용이 지출되는 위치를 더 쉽게 검증하고 태그가 지정된 볼륨 및 스냅샷에 자동화를 사용할 수 있습니다. AWS Cost Optimization 원칙에서 권장하는 모범 사례입니다.	태그 지정(비용 최적화, 보안, 인시던트 관리 및 자동화)

AMS Accelerate의 자동 인스턴스 구성

AMS Accelerate는 자동화된 인스턴스 구성 서비스를 제공합니다. 이 서비스는 인스턴스가 AMS가 인스턴스를 올바르게 관리할 수 있도록 올바른 로그와 지표를 내보내도록 합니다. 자동 인스턴스 구성에는이 섹션의 뒷부분에서 설명하는 온보딩을 위한 자체 사전 조건과 단계가 있습니다.

주제

- Accelerate에서 자동화된 인스턴스 구성의 작동 방식
- SSM 에이전트 자동 설치
- 자동 인스턴스 구성 변경

Accelerate에서 자동화된 인스턴스 구성의 작동 방식

자동 인스턴스 구성을 사용하면 AMS Accelerate가 특정 에이전트 및 태그를 추가하여 표시하는 인스턴스에 대해 매일 특정 구성을 수행할 수 있습니다.

Accelerate의 자동 인스턴스 구성을 위한 사전 조건

AMS Accelerate가 관리형 인스턴스에서 이전에 설명한 자동화된 작업을 수행할 수 있도록 하려면 이러한 조건을 충족해야 합니다.

SSM 에이전트가 설치됨

AMS Accelerate 자동 인스턴스 구성을 사용하려면 AWS Systems Manager SSM 에이전트가 설치되어 있어야 합니다.

AMS SSM 에이전트 자동 설치 기능 사용에 대한 자세한 내용은 섹션을 참조하세요SSM 에이전트 자동 설치.

SSM 에이전트를 수동으로 설치하는 방법에 대한 자세한 내용은 다음을 참조하세요.

- Linux: Linux용 Amazon EC2 인스턴스에 SSM 에이전트 수동 설치 - AWS Systems Manager
- Windows: Windows Server용 Amazon EC2 인스턴스에 SSM Agent 수동 설치 - AWS Systems Manager

SSM 에이전트가 관리형 상태입니다.

AMS Accelerate 자동 인스턴스 구성에는 운영 SSM 에이전트가 필요합니다. SSM 에이전트가 설치되어 있어야 하며 Amazon EC2 인스턴스는 관리형 상태여야 합니다. 자세한 내용은 SSM 에이전트 작업 AWS 설명서를 참조하세요.

자동 인스턴스 구성 설정

사전 조건이 충족되었다고 가정하면 특정 Amazon EC2 인스턴스 태그를 추가하면 AMS Accelerate 자동 인스턴스 구성이 자동으로 시작됩니다. 다음 방법 중 하나를 사용하여이 태그를 추가합니다.

1. (매우 권장) AMS Accelerate 리소스 태거 사용

   계정에 대한 태그 지정 로직을 구성하려면 섹션을 참조하세요태그 지정 작동 방식. 태그 지정이 완료되면 태그 및 자동 인스턴스 구성이 자동으로 처리됩니다.

2. 수동으로 태그 추가

   Amazon EC2 인스턴스에 다음 태그를 수동으로 추가합니다.

   Key:ams:rt:ams-managed, Value:true.

> **Note**
>
> 인스턴스 구성 서비스는 ams:rt:ams 관리형 태그가 인스턴스에 적용되면 필요한 AMS 구성을 적용하려고 시도합니다. 서비스는 인스턴스가 시작될 때마다, 그리고 AMS 일일 구성 검사가 발생할 때마다 AMS 필수 구성을 어설션합니다.

SSM 에이전트 자동 설치

> **Important**
>
> SSM 에이전트 자동 설치는 아시아 태평양(말레이시아) 리전을 지원하지 않습니다.

AMS가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하도록 하려면 각 인스턴스에 AWS Systems Manager SSM 에이전트를 설치해야 합니다. 인스턴스에 SSM 에이전트가 설치되어 있지 않은 경우 AMS SSM 에이전트 자동 설치 기능을 사용할 수 있습니다.

> **Note**
>
> - 6/03/2024 이후에 계정이 AMS Accelerate에 온보딩되면이 기능이 기본적으로 활성화됩니다. 이 기능을 끄려면 CA 또는 CSDM에 문의하십시오.
> - 6/03/2024 이전에 온보딩된 계정에서이 기능을 켜려면 CA 또는 CSDM에 문의하십시오.
> - 이 기능은 Auto Scaling 그룹에 없고 AMS에서 지원하는 Linux 운영 체제를 실행하는 EC2 인스턴스에서만 사용할 수 있습니다.

SSM 에이전트 사용을 위한 사전 조건

- 대상 인스턴스와 연결된 인스턴스 프로파일에 다음 정책(또는 허용 목록에 있는 것과 동등한 권한) 중 하나가 있는지 확인합니다.
  - AmazonSSMManagedEC2InstanceDefaultPolicy
  - AmazonSSMManagedInstanceCore
- 이전 정책에 나열된 권한을 명시적으로 거부하는 AWS Organizations 수준의 서비스 제어 정책이 없는지 확인합니다.

  자세한 내용은 Systems Manager에 필요한 인스턴스 권한 구성을 참조하세요.

- 아웃바운드 트래픽을 차단하려면 대상 인스턴스가 있는 VPC에서 다음 인터페이스 엔드포인트가 활성화되어 있는지 확인합니다(URL에서 "리전"을 적절히 바꿉니다).
  - ssm.<region>.amazonaws.com
  - ssmmessages.<region>.amazonaws.com
  - ec2messages.<리전>.amazonaws.com

  자세한 내용은 Systems Manager용 VPC 엔드포인트를 사용하여 EC2 인스턴스의 보안 개선을 참조하세요.

관리형 노드 가용성 활성화 또는 문제 해결에 대한 일반적인 팁은 솔루션 2: 인스턴스에 IAM 인스턴스 프로파일이 지정되었는지 확인(EC2 인스턴스만 해당)을 참조하세요.

> **Note**
>
> AMS는 자동 설치 프로세스의 일부로 각 인스턴스를 중지하고 시작합니다. 인스턴스가 중지되면 인스턴스 스토어 볼륨에 저장된 데이터와 RAM에 저장된 데이터가 손실됩니다. 자세한 내용은 인스턴스를 중지하면 어떻게 되는지를 참조하세요.

인스턴스에 SSM 에이전트 자동 설치 요청

계정이 AMS Accelerate 패치 추가 기능에 온보딩된 경우 인스턴스에 대한 패치 유지 관리 기간(MW)을 구성합니다. 패치 프로세스를 완료하려면 작동 중인 SSM 에이전트가 필요합니다. 인스턴스에 SSM 에이전트가 없는 경우 AMS는 패치 유지 관리 기간 동안 인스턴스를 자동으로 설치하려고 시도합니다.

> **Note**
>
> AMS는 자동 설치 프로세스의 일부로 각 인스턴스를 중지하고 시작합니다. 인스턴스가 중지되면 인스턴스 스토어 볼륨에 저장된 데이터와 RAM에 저장된 데이터가 손실됩니다. 자세한 내용은 인스턴스를 중지하면 어떻게 되는지를 참조하세요.

SSM 에이전트 자동 설치 작동 방식

AMS는 EC2 사용자 데이터를 사용하여 인스턴스에서 설치 스크립트를 실행합니다. 사용자 데이터 스크립트를 추가하고 인스턴스에서 실행하려면 AMS가 각 인스턴스를 중지하고 시작해야 합니다.

인스턴스에 이미 기존 사용자 데이터 스크립트가 있는 경우 AMS는 자동 설치 프로세스 중에 다음 단계를 완료합니다.

1. 기존 사용자 데이터 스크립트의 백업을 생성합니다.
2. 기존 사용자 데이터 스크립트를 SSM 에이전트 설치 스크립트로 바꿉니다.
3. 인스턴스를 다시 시작하여 SSM 에이전트를 설치합니다.
4. 인스턴스를 중지하고 원래 스크립트를 복원합니다.
5. 원래 스크립트로 인스턴스를 다시 시작합니다.

자동 인스턴스 구성 변경

AMS Accelerate 인스턴스 구성 자동화는 계정에서 다음과 같이 변경합니다.

1. IAM 권한

   AMS Accelerate에서 설치한 에이전트를 사용할 수 있는 권한을 인스턴스에 부여하는 데 필요한 IAM 관리형 정책을 추가합니다.
2. Agents
   a. Amazon CloudWatch 에이전트는 OS 로그 및 지표를 내보낼 책임이 있습니다. 인스턴스 구성 자동화를 통해 CloudWatch 에이전트가 설치되고 AMS Accelerate 최소 버전을 실행할 수 있습니다.
   b. AWS Systems Manager SSM 에이전트는 인스턴스에서 원격 명령을 실행할 책임이 있습니다. 인스턴스 구성 자동화는 SSM 에이전트가 AMS Accelerate 최소 버전을 실행하고 있는지 확인합니다.
3. CloudWatch 구성
   a. 필요한 지표와 로그가 생성되도록 AMS Accelerate는 CloudWatch 구성을 사용자 지정합니다. 자세한 내용은 다음 CloudWatch 구성 변경 세부 정보 단원을 참조하세요.

자동 인스턴스 구성은 IAM 인스턴스 프로파일 및 CloudWatch 구성을 변경하거나 추가합니다.

IAM 권한 변경 세부 정보

각 관리형 인스턴스에는 다음과 같은 관리형 정책이 포함된 AWS Identity and Access Management 역할이 있어야 합니다.

- arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

- arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
- arn:aws:iam::aws:policy/AMSInstanceProfileBasePolicy

처음 두 정책은 AWS관리형 정책입니다. AMS 관리형 정책은 다음과 같습니다.

AMSInstanceProfileBasePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:/ams/byoa/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

인스턴스에 이미 연결된 IAM 역할이 있지만 이러한 정책이 누락된 경우 AMS는 누락된 정책을 IAM 역할에 추가합니다. 인스턴스에 IAM 역할이 없는 경우 AMS는 AMSOSConfigurationCustomerInstanceProfile IAM 역할을 연결합니다. AMSOSConfigurationCustomerInstanceProfile IAM 역할에는 AMS Accelerate에 필요한 모든 정책이 있습니다.

> **Note**
>
> 기본 인스턴스 프로파일 제한인 10에 도달하면 AMS는 제한을 20으로 늘려 필요한 인스턴스 프로파일을 연결할 수 있습니다.

CloudWatch 구성 변경 세부 정보

CloudWatch 구성에 대한 추가 세부 정보입니다.

- 인스턴스의 CloudWatch 구성 파일 위치:
  - Windows: %ProgramData%\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent.json
  - Linux: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/ams-accelerate-config.json
- Amazon S3의 CloudWatch 구성 파일 위치:
  - Windows: https://ams-configuration-artifacts-*REGION_NAME*.s3.*REGION_NAME*.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json
  - Linux: https://ams-configuration-artifacts-*REGION_NAME*.s3.*REGION_NAME*.amazonaws.com/configurations/cloudwatch/latest/linux-cloudwatch-config.json
- 수집된 지표:
  - Windows:
    - AWS Systems Manager SSM 에이전트(CPU_Usage)
    - CloudWatch 에이전트(CPU_Usage)
    - 모든 디스크의 디스크 공간 사용률(% 여유 공간)
    - 메모리(사용 중인 커밋 바이트 비율)
  - Linux:
    - AWS Systems Manager SSM 에이전트(CPU_Usage)
    - CloudWatch 에이전트(CPU_Usage)
    - CPU(cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system)
    - 디스크(used_percent, inodes_used, inodes_total)
    - Diskio(io_time, write_bytes, read_bytes, writes, reads)
    - Mem(mem_used_percent)
    - 스왑(swap_used_percent)

- 수집된 로그:
  - Windows:
    - AmazonSSMAgentLog
    - AmazonCloudWatchAgentLog
    - AmazonSSMErrorLog
    - AmazonCloudFormationLog
    - ApplicationEventLog
    - EC2ConfigServiceEventLog
    - MicrosoftWindowsAppLockerEXEAndDLLEventLog
    - MicrosoftWindowsAppLockerMSIAndScriptEventLog
    - MicrosoftWindowsGroupPolicyOperationalEventLog
    - SecurityEventLog
    - SystemEventLog
  - Linux:
    - /var/log/amazon/ssm/amazon-ssm-agent.log
    - /var/log/amazon/ssm/errors.log
    - /var/log/audit/audit.log
    - /var/log/cloud-init-output.log
    - /var/log/cloud-init.log
    - /var/log/cron
    - /var/log/dpkg.log
    - /var/log/maillog
    - /var/log/messages
    - /var/log/secure
    - /var/log/spooler
    - /var/log/syslog
    - /var/log/yum.log
    - /var/log/zypper.log

AMS Accelerate에서 오프보드

AMS Accelerate는 엔터프라이즈급 운영 환경을 쉽게 운영할 수 있는 방법을 제공합니다. 또한 AMS Accelerate는 AWS 마이그레이션 및 사용에 대한 지원 인프라 운영 모델을 제공합니다. 그러나 AMS Accelerate를 사용한 후 인소스를 결정하거나 AWS 인프라 운영 책임을 다른 팀에 재할당할 수 있습니다. 이렇게 하려면 AMS 서비스에서 계정을 오프보드해야 합니다.

AMS Accelerate에서 계정을 오프보딩하면 AMS는 서비스 설명에 정의된 모든 책임을 다시 사용자에게 이전합니다. 예를 들어 AMS에 대한 인시던트 또는 서비스 요청을 잘라낼 수 없습니다. 마찬가지로 운영 엔지니어와 자동화는 더 이상 Accelerate 계정에 액세스할 수 없으므로 상태, 가용성, 보안 및 규정 준수 조사 결과를 해결할 수 없습니다. AWS 워크로드는 AMS가 작동하는 계정과 동일한 계정에서 계속 실행될 수 있습니다.

앞으로 인프라 운영 서비스를 수행할 팀이 포함되어 Accelerate 오프보딩 후 사용할 인력, 도구 및 프로세스를 정의해야 합니다. AMS는 "to be" 운영 환경 및 모델을 개발할 수 있도록 가드레일 및 로그와 같은 일부 AMS 도구를 남겨 둡니다. 다음 설명서를 주의 깊게 검토하여 계속 사용할 수 있는 도구와 계정 오프보딩을 요청하는 방법을 이해합니다.

AMS Accelerate 오프보딩 효과

Accelerate에서 오프보딩을 준비하는 동안 다음 고려 사항을 염두에 두세요.

- 액세스: `ams-access-management` AWS Identity and Access Management 역할을 정의하는 `ams-access-management` CloudFormation 스택은 삭제되지 않습니다. 오프보딩 후 이러한 리소스는 남아 있지만 남아 있는 다른 구성 요소에서는 사용되지 않습니다. 편한 시간에 스택과 역할을 삭제할 수 있습니다.
- AMS 리소스 보존: 오프보딩 후 일부 AMS 리소스는 계정에 남아 있습니다. 보존되는 리소스와 이를 사용하여 수행할 수 있는 작업을 확인하려면 `resource_inventory.zip` 스프레드시트(압축됨)를 참조하세요.
- 자동화: 오프보딩 후에는 AMS에서 선별한 AWS SSM 자동화 런북과 AWS Lambda 함수를 더 이상 사용할 수 없습니다.
- 백업 관리: AMS는 백업 관리를 사용하여 리소스의 스냅샷을 생성합니다. 오프보딩 후 AMS 백업 계획을 AWS Backup 제외하고에 정의된 백업 일정, 빈도 및 보존 기간을 계속 사용할 수 있습니다. 섹션을 참조하세요AMS 백업 계획 선택. AMS Backup Orchestrator에서 생성한 AWS Identity and Access Management 리소스는 제거되지만 AMS에서 작성한 백업 볼트 및 해당 AWS KMS 키는 제거되지 않습니다. Accelerate는 더 이상 백업 작업을 모니터링하거나 인시던트 발생 시 복원 작업을 수행하지 않습니다.

- 비용 최적화: 오프보딩 후 AMS Resource Scheduler가 삭제됩니다. AMS Resource Scheduler를 사용하면 사용하지 않는 리소스를 중지하고 용량이 필요할 때 다시 시작하여 운영 비용을 절감할 수 있습니다. AMS는 비용 최적화 권장 사항을 계속 제공하지 않습니다. Resource Scheduler에 대한 자세한 내용은 AMS Resource Scheduler를 사용한 비용 최적화를 참조하세요.
- 지정된 전문가: 오프보딩 후 지정된 Cloud Service Delivery Manager(CSDM) 및 Cloud Architect(CA)는 더 이상 오프보딩된 Accelerate 계정에 대한 지침, 보고 또는 운영 및 보안 우수성을 제공하지 않습니다.
- 인시던트 관리: 인시던트 관리는 AMS 서비스가 보고된 인시던트에 대응하는 데 사용하는 프로세스입니다. 오프보딩 후 Accelerate는 더 이상 인시던트를 감지 및 대응하지 않거나 팀이 문제를 해결할 수 있도록 지원합니다. Accelerate 계정에 대한 Accelerate 및 Accelerate 콘솔 액세스가 비활성화된 상태에서는 인시던트 및 서비스 요청 통신을 교환할 수 없습니다.
- 로깅 및 보고: 오프보딩 후 CloudWatch, CloudTrail 및 VPC 흐름 로그의 결과로 저장된 로그를 유지합니다. 이러한 서비스의 구성을 그대로 두어 로그를 계속 생성할 수 있지만 AMS는 더 이상 이러한 구성을 모니터링하지 않습니다. Accelerate는 더 이상 AMS의 주요 성능 지표를 요약하는 월별 서비스 보고서를 제공하지 않습니다. 셀프 서비스 보고(SSR)(참조)에서 생성된 데이터는 유지셀프 서비스 보고서하지만 Accelerate는 새 데이터를 생성하지 않습니다.
- 모니터링: 모니터링은 AMS 서비스가 리소스를 추적하는 데 사용하는 프로세스입니다. 오프보딩 중에 AMS는 경보 관리자 및 리소스 태거와 같은 AMS별 도구와 AMS 모니터링 기준의 일부로 AMS가 배포한 EventBridge 이벤트 규칙 및 CloudWatch 경보를 제거합니다. Accelerate는 오프보딩 후 더 이상 경보에 응답하거나 새 경보를 구성하지 않습니다. 경보 관리자 및 리소스 태거에 대한 자세한 내용은 태그 기반 경보 관리자 및 리소스 태거를 참조하세요.
- 운영 도구: AMS Accelerate는 AWS에서 워크로드의 인프라에 대한 지속적인 운영을 제공할 수 있습니다. Accelerate 계정을 오프보딩한 후에는 규칙에 따라 리소스에 태그를 지정하는 데 도움이 되는 Resource Tagger와 같은 도구 또는 EC2 인스턴스에 필요한 에이전트를 설치하기 위한 자동화된 인스턴스 구성에 더 이상 액세스할 수 없습니다. 인스턴스의 CloudWatch 및 SSM 에이전트는 기존 구성과 함께 그대로 유지됩니다. `AMSOSConfigurationCustomerInstanceRole` IAM 프로파일과 `AMSInstanceProfileBasePolicy`는 인스턴스에서 분리되고 Accelerate 계정에서 제거됩니다.
- 패치 관리: 패치 관리는 AMS 서비스가 EC2 인스턴스를 업데이트하는 데 사용하는 프로세스입니다. 오프보딩 후 AMS는 더 이상 패치 적용 전에 인스턴스의 스냅샷을 생성하지 않고, 더 이상 패치 설치를 설치 및 모니터링하지 않으며, 더 이상 결과를 알리지 않습니다. 과거에 생성된 패치 기준 및 스냅샷은 유지됩니다. 또한 패치 유지 관리 기간의 구성은 유지되지만 패치는 더 이상 Accelerate에서 설치되지 않습니다.
- 문제 관리: 오프보딩 후 Accelerate는 더 이상 문제를 식별 및 조사하고 근본 원인을 식별하기 위한 분석을 수행하지 않습니다.

- 보안: 보안 관리는 AMS 서비스가 리소스를 보호하는 데 사용하는 프로세스입니다. 오프보딩 후 Amazon GuardDuty 탐지기 및 결과를 유지하면 Accelerate에서 AWS Config 배포한 AWS Config 규칙이 제거됩니다. 더 이상 이러한 도구의 결과를 모니터링, 수정 또는 보고하지 않도록 가속화합니다.
- 서비스 종료 날짜: 서비스 종료 날짜는 30일의 필수 종료 알림 기간이 끝나는 달의 마지막 날입니다. 필수 종료 알림 기간이 해당 월의 20일 이후인 경우 서비스 종료 날짜는 다음 달의 마지막 날입니다. 다음은 종료 날짜에 대한 예제 시나리오입니다.
  - 종료 알림이 4월 12일에 제공된 경우 30일 알림은 5월 12일에 종료됩니다. 서비스 종료 날짜는 5월 31일입니다.
  - 종료 알림이 4월 29일에 제공된 경우 30일 알림은 5월 29일에 종료됩니다. 서비스 종료 날짜는 6월 30일입니다.

경보 관리자 및 리소스 태거에 대한 종속성을 사용하여 AMS Accelerate에서 오프보딩

AMS에서 제공하는 경보 관리자 및 리소스 태거 구성 CloudFormation 스택과 함께 경보 관리자 또는 리소스 태거와 관련된 구성을 배포하는 사용자 지정 스택은 AWS Managed Services에서 오프보드할 때 계정에 남아 있습니다.

오프보딩 프로세스 중에 AMS 구성 스택을 삭제하려면 오프보딩 프로세스를 시작하기 전에 사용자 지정 CloudFormation 템플릿에서 경보 관리자 또는 리소스 태거에 대한 종속성과 참조를 제거해야 합니다. 참조를 제거하면 AMS에서 오프보드할 때 계정에서 스택이 올바르게 제거됩니다.

> **Important**
>
> 오프보딩 프로세스를 시작하기 전에 CloudFormation 템플릿을 주의 깊게 검토하고 경보 관리자 및 리소스 태거에 대한 참조를 제거합니다. 이렇게 하지 않으면 AMS에서 오프보딩한 후에도 계정에 이러한 스택이 보존될 수 있습니다. 이러한 스택에는 경보 관리자 및 리소스 태거와 관련된 구성 정보가 포함되어 있지만 이러한 스택의 존재로 인해 지속적인 요금이나 요금이 발생하지는 않습니다.

Accelerate 계정에 대한 오프보딩 지원 받기

AMS는 AMS 계정 서비스 종료 요청을 통해 최소 30일 전에 알림을 받은 후 계정을 오프보딩합니다. 서비스 종료 날짜는 30일 필수 종료 알림 기간이 끝나는 달의 마지막 날입니다. 단, 필수 종료 알림 기간이 20일 이후인 경우 서비스 종료 날짜는 다음 달의 마지막 날이 됩니다.

계정 오프보딩을 요청하려면 다음을 수행해야 합니다.

1. 서비스 요청을 사용하여 계정을 오프보딩하려면 공식 요청을 제출합니다. 오프보딩하려는 모든 계정을 문서화하는 서비스 요청(SR) 1개 또는 계정당 SR 1개.

   요청에서 오프보딩할 계정 IDs 목록, 오프보딩 이유 및 추가 고려 사항을 제공합니다.
2. 오프보딩하려는 계정에 대해 CSDM에 알리고 오프보딩 프로세스 실행에 도움을 요청합니다.

Accelerate의 알림 설정

사용자와 AMS 간의 통신은 다음과 같은 여러 가지 이유로 발생합니다.

- 모니터링 알림으로 생성된 이벤트
- 패치 추가 기능에 옵트인한 경우 서비스 알림 패치 적용
- 서비스 요청 및 인시던트 보고서
- 가끔 중요한 AWS 공지 사항(사용자 측에 조치가 필요한 경우 CSDM에서 연락)

모든 알림은 온보딩 시 패치 알림에 제공한 이메일을 사용하여 전송됩니다. 그렇지 않으면 온보딩 시 AMS에 제공한 기본 이메일로 알림이 전송됩니다. 개별 이메일을 최신 상태로 유지하기 어렵기 때문에 나중에 업데이트할 수 있는 그룹 이메일을 사용하는 것이 좋습니다. 사용자에게 전송된 모든 알림은 AMS 작업에서도 수신되며 응답을 하기 전에 분석됩니다.

GuardDuty 또는 AWS Config 기반 알림과 같은 리소스 기반이 아닌 알림에 명명된 연락처 목록을 사용할 수 있습니다. 예를 들어 이름이 인 목록`SecurityContacts`과 이름이 인 다른 목록이 있을 수 있습니다`OperationsContacts`. AMS는 경보와 알림을 이러한 목록에 전송합니다.

자세한 내용은 AWS Config 제어 규정 준수 보고서 섹션을 참조하세요.

AMS Accelerate의 태그 지정

대부분의 Accelerate 기능(패치, 백업, 모니터링)은 태그와 구성 프로파일을 사용하여 관리할 리소스, 적용할 작업, 적용할 시기를 결정합니다. 태그는 리소스에 적용하는 레이블입니다. 구성 프로필에는 해당 태그를 기반으로 하는 규칙이 포함됩니다.

각 Accelerate 기능에는 고유한 태그 지정 요구 사항이 있습니다. 일부 기능을 사용하려면 특정 태그를 사용해야 하지만 다른 기능을 사용하면 원하는 태그를 사용할 수 있습니다.

필수 태그에 대한 자세한 내용은 섹션을 참조하세요Accelerate의 고객 관리형 태그.

고객을 정의할 수 있는 태그에 대한 자세한 내용은 섹션을 참조하세요. Accelerate의 고객 제공 태그

목차

- AMS Accelerate의 태그
  - 태그란 무엇입니까?
  - 태그 지정 작동 방식
  - Accelerate의 고객 관리형 태그
    - Accelerate의 모니터링
    - Accelerate에서 EC2 인스턴스에 대한 태그 구성
    - Accelerate에서 백업 태그 관리
  - Accelerate 관리형 태그
  - Accelerate의 고객 제공 태그
- Accelerate용 태그 관리 도구
  - 리소스 태거 가속화
    - Resource Tagger란 무엇입니까?
    - Resource Tagger 작동 방식
    - AMS Accelerate의 리소스 태거 구성 프로파일
      - 구문 및 구조
    - AMS Accelerate의 Resource Tagger 사용 사례
      - Resource Tagger에서 적용한 태그 보기
      - Resource Tagger를 사용하여 태그 생성
      - Resource Tagger의 리소스 수정 방지

        - 예제 구성 프로필
        - 기본 구성 병합
        - 기본 구성 비활성화
        - Resource Tagger에서 적용한 태그 제거
        - Resource Tagger 구성 보기 또는 변경
        - 구성 변경 사항 배포
        - Resource Tagger 태그를 무시하도록 Terraform 구성
        - Resource Tagger에서 관리하는 리소스 수 보기
- CloudFormation을 사용하여 AMS Accelerate에 대한 태그 생성
    - CloudFormation AMS Accelerate 사용 사례
        - CloudFormation Accelerate용를 사용하여 EC2 인스턴스에 태그 지정
        - 가속화를 CloudFormation 위해를 사용하여 AutoScaling 그룹(ASG)에 태그 지정
        - CloudFormation for Accelerate를 사용하여 구성 프로파일 배포
- Terraform을 사용하여 AMS Accelerate용 태그 생성

AMS Accelerate의 태그

목차

- 태그란 무엇입니까?
- 태그 지정 작동 방식
- Accelerate의 고객 관리형 태그
    - Accelerate의 모니터링
    - Accelerate에서 EC2 인스턴스에 대한 태그 구성
    - Accelerate에서 백업 태그 관리
- Accelerate 관리형 태그
- Accelerate의 고객 제공 태그

태그란 무엇입니까?

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 사용자가 정의하는 키와 선택적 값으로 구성됩니다.

태그를 사용하여 용도, 소유자 또는 환경 등 다양한 방식으로 AWS 리소스를 분류합니다. 예를 들어 계정의 Amazon EC2 인스턴스에 대한 태그 세트를 정의하여 각 인스턴스의 소유자 및 스택 수준을 추적할 수 있습니다.

태그는 Amazon EC2에는 의미가 없으며 엄격하게 문자열로 해석됩니다.

자세한 내용은 AWS 리소스 태그 지정을 참조하세요.

태그 지정 작동 방식

리소스에 태그를 적용하는 방법에는 여러 가지가 있습니다. 리소스를 생성할 때 각 AWS 서비스의 콘솔에서 직접 리소스에 태그를 지정하거나, AWS 태그 편집기를 사용하여 여러 리소스에 대한 태그를 추가, 제거 또는 편집하거나, 리소스 태그와 같은 CloudFormation 프로비저닝 도구를 사용할 수 있습니다. https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-resource-tags.html 또한 AMS Accelerate는 자동화된 태그 수명 주기 관리자에 대한 규칙을 정의하는 데 사용하는 AMS Accelerate 리소스 태거도 제공합니다. AMS Accelerate에서 Resource Tagger를 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요리소스 태거 가속화. 또한 AMS Accelerate는 AMS 리소스에 사용자 지정 태그를 추가 및 제거할 수 있는 고객 제공 태그를 제공합니다. 고객 제공 태그에 대한 자세한 내용은 섹션을 참조하세요Accelerate의 고객 제공 태그.

Accelerate의 고객 관리형 태그

다양한 AMS Accelerate 작업을 트리거하려면 특정 태그가 필요합니다.

목차

- Accelerate의 모니터링
- Accelerate에서 EC2 인스턴스에 대한 태그 구성
- Accelerate에서 백업 태그 관리

Accelerate의 모니터링

AMS Accelerate는 지원되는 리소스의 상태, 가용성 및 신뢰성을 모니터링합니다. 이 서비스 상품에 대한 자세한 내용은 섹션을 참조하세요AMS Accelerate의 모니터링 및 이벤트 관리.

AMS Accelerate는 기준 모니터링 AWS 서비스 에 추가로 주기적으로 온보딩합니다. Resource Tagger 기본 구성을 사용하는 경우 이러한 업데이트가 계정에 자동으로 배포되고 변경 사항이 지원되는 리소스에 반영됩니다.

AMS Accelerate에서 Amazon EC2 인스턴스를 관리하도록 옵트인하려면 AppConfig의 사용자 지정 프로파일을 통해 다음 태그를 적용해야 합니다. 자세한 내용은 3단계: 구성 및 구성 프로파일 생성을 참조하세요.

리소스에 다음 태그를 적용합니다.

키	값
ams:rt:ams-managed	true

예를 들어 다음과 같은 사용자 지정 구성 문서를 생성하여 모든 AMS 지원 EC2 리소스에 태그를 적용할 수 있습니다.

```
{
    "AWS::EC2::Instance": {
        "AllEC2": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Important

구성 변경 사항을 적용한 후에는 배포해야 합니다. SSM AppConfig에서는 구성을 생성한 후 새 버전의 구성을 배포해야 합니다.

Amazon EC2 이외의 서비스에는 기본 기준 모니터링이 있습니다. AMS Accelerate에서 모니터링할 리소스를 옵트아웃하려면 사용자 지정 구성 프로파일을 사용하여 특정 리소스 또는를 제외할 수 있습니

다 AWS 서비스. 이를 통해 기준 경보 정의를 배포하기 위해 모니터링 태그가 있어야 하는 리소스를 제어할 수 있습니다. AMS Accelerate의 Resource Tagger 사용 사례을(를) 참조하세요.

Resource Tagger 사용

계정의 AMS Accelerate Resource Tagger 구성은이 하나의 태그(ams:rt:ams-managed)를 적용하는 경우 다음 태그가 자동으로 배포되도록 하는 데 도움이 됩니다.

기준 모니터링을 위해 지원되는 리소스에 다음 태그가 적용되는 것을 확인할 수 있습니다.

키	값	규칙
ams:rt:ams-monitoring-policy	ams-monitored	AMS에서 지원하는 모든 EC2 리소스에 적용됩니다.
ams:rt:ams-monitoring-policy-platform	ams-monitored-linux	Linux OS를 실행하는 모든 Amazon EC2 인스턴스에 적용됩니다.
ams:rt:ams-monitoring-policy-platform	ams-monitored-windows	Windows OS를 실행하는 모든 Amazon EC2 인스턴스에 적용됩니다.

기타 지원되는 서비스의 경우

지정된 규칙에 따라 리소스에 다음 태그를 적용합니다.

키	값	규칙
ams:rt:ams-monitoring-policy	ams-monitored	AMS Accelerate 모니터링에서 지원하는 모든 리소스에 적용됩니다.
ams:rt:ams-monitoring-with-kms	ams-monitored-with-kms	KMS를 사용하는 OpenSearch 도메인
ams:rt:ams-monitoring-with-master	ams-monitored-with-master	전용 마스터 노드가 있는 OpenSearch 도메인

Resource Tagger를 사용하지 않는 경우

AMS Resource Tagger 사용 이외의 방법을 사용하여 올바른 모니터링 태그를 적용하는 방법에 Resource Tagger 없이 태그 가속화 대한 도움말은 섹션을 참조하세요.

Accelerate에서 EC2 인스턴스에 대한 태그 구성

AMS Accelerate는 SSM 에이전트 및 CloudWatch 에이전트와 같은 Amazon EC2 인스턴스에서 에이전트를 관리합니다. 이 서비스 상품에 대한 자세한 내용은 섹션을 참조하세요. AMS Accelerate의 자동 인스턴스 구성

Amazon EC2 인스턴스를 AMS Accelerate에서 관리하도록 옵트인하려면 Amazon EC2 인스턴스에 다음 태그를 적용해야 합니다.

키	값
ams:rt:ams-managed	true

Accelerate에서 백업 태그 관리

AMS Accelerate는 지원되는 리소스의 백업을 관리합니다. 이 서비스 상품에 대한 자세한 내용은 섹션을 참조하세요AMS Accelerate의 연속성 관리.

AMS Accelerate 백업 관리는 태그를 사용하여 자동으로 백업해야 하는 리소스를 식별합니다(수동 백업 기능도 제공). 태그 키:값 조합을 사용하여 리소스를 백업 계획과 연결할 수 있습니다. ams-default-backup-plan AWS Backup 계획을 사용하여 자동 백업을 옵트인하려면 지원되는 리소스에 다음 태그를 적용해야 합니다.

키	값
ams:rt:backup-orchestrator	true

> **Note**
>
> 온보딩 중에 AMS Accelerate는 짧은 간격, 짧은 보존 스냅샷에 대해 값이 true인 ams:rt:backup-orchestrator-onboarding으로 모든 리소스에 태그를 지정합니다. 이는 ams-

onboarding-backup-plan 백업 계획에 의해 관리됩니다. AMS Accelerate 관리형 AWS Backup 플랜에 대한 자세한 내용은 섹션을 참조하세요AMS 백업 계획 선택.

Accelerate 관리형 태그

AMS Accelerate에 온보딩하는 동안 계정에 여러 AWS 리소스가 배포됩니다. 이를 식별할 수 있도록 이러한 리소스에는 다음과 같은 태그가 지정됩니다.

키	값
ams:resourceOwner	AMS
ams:resourceOwnerService	이 리소스를 제공하는 AMS Accelerate 서비스의 출처는 AMS Deployment, Backup, Controls, Monitoring, Patch 등입니다.
AppId	AMSInfrastructure
AppName	
Environment	

Note

이러한 태그는 CloudFormation 스택 수준 태그를 사용하여 적용되며 생성된 리소스에 태그를 CloudFormation 전파하는 데 의존합니다. 자세한 내용은 리소스 태그를 참조하세요.

Accelerate의 고객 제공 태그

고객 제공 태그란 무엇입니까?

고객 제공 태그는 계정에서 AMS 리소스에 태그를 지정하는 방법을 제어하는 규칙을 지정하는 데 사용되는 AMS Accelerate 서비스 기능입니다. 고객 제공 태그를 사용하면 계정에 배포된 AMS 리소스에 사용자 정의 사용자 지정 태그를 추가할 수 있습니다. 자동화된 서비스를 사용하여 Cloud Service Delivery Manager(CSDM)에 요청할 때 고객 제공 태그 기능이 요청된 계정에 자동으로 추가됩니다. AMS 태그는 재정의할 수 없습니다. AMS 태그는 'ams:'로 시작합니다.

자체 태그(레이블)를 정의하고 모든 AMS Accelerate 리소스에 대해 이러한 태그의 기능을 지정할 수 있습니다. AMS에 온보딩하기 전에 이러한 태그를 제공하여 AMS 태그와 사용자 지정 태그가 온보딩 프로세스 중에 적용되도록 할 수 있습니다. 또는 온보딩 후 태그를 제공할 수 있습니다.

고객 제공 태그를 추가하려면 어떻게 해야 하나요?

리소스에 이러한 태그를 추가하도록 요청하려면 CSDM에 문의하십시오. 이러한 태그는 계정의 AMS 리소스에 적용됩니다.

태그의 범위는 어떻게 됩니까?

이 기능은 현재 Accelerate 고객 및 AWS 상용 리전에서만 사용할 수 있습니다. 소유한 모든 계정 또는 특정 계정 목록에 태그를 추가할 수 있습니다.

> **Note**
>
> 이러한 태그는 AMS 리소스에만 적용되며 자체 리소스에는 영향을 주지 않습니다.

Accelerate용 태그 관리 도구

목차

- 리소스 태거 가속화
- CloudFormation을 사용하여 AMS Accelerate에 대한 태그 생성
- Terraform을 사용하여 AMS Accelerate용 태그 생성

리소스 태거 가속화

Resource Tagger를 사용하면 계정에서 AWS 리소스에 태그를 지정하는 방법을 제어하는 규칙을 지정할 수 있습니다. 계정을 온보딩하는 동안 AMS Accelerate는 태그 지정 정책을 배포하여 관리형 계정 내의 리소스에 태그가 지정되도록 합니다.

목차

- Resource Tagger란 무엇입니까?
- Resource Tagger 작동 방식
- AMS Accelerate의 리소스 태거 구성 프로파일

- 구문 및 구조
- AMS Accelerate의 Resource Tagger 사용 사례
  - Resource Tagger에서 적용한 태그 보기
  - Resource Tagger를 사용하여 태그 생성
  - Resource Tagger의 리소스 수정 방지
  - 예제 구성 프로필
  - 기본 구성 병합
  - 기본 구성 비활성화
  - Resource Tagger에서 적용한 태그 제거
  - Resource Tagger 구성 보기 또는 변경
  - 구성 변경 사항 배포
  - Resource Tagger 태그를 무시하도록 Terraform 구성
  - Resource Tagger에서 관리하는 리소스 수 보기

Resource Tagger란 무엇입니까?

Resource Tagger는 계정에서 AWS 리소스에 태그를 지정하는 방법을 제어하는 규칙을 지정하는 데 사용하는 AMS Accelerate 서비스입니다. 이는 태그가 리소스에 적용되는 방식에 대한 완전한 가시성을 제공하는 것을 목표로 합니다 AWS .

Resource Tagger는 구성 프로필에서 지정한 태그 지정 규칙에 따라 지원되는 AWS 리소스에 태그를 자동으로 생성, 업데이트 및 삭제합니다. 예를 들어 Amazon EC2 인스턴스 컬렉션에 태그를 적용하는 규칙을 지정하여 AMS Accelerate에서 관리해야 함을 나타내면 인스턴스가 모니터링되거나 백업됩니다. 이와 같은 태그를 사용하여 AWS AppConfig 구성 프로필에 정의된 정책을 기반으로 리소스의 규정 준수 상태를 AWS 식별할 수 있습니다. 자세한 내용은 AWS AppConfig 단원을 참조하십시오.

AMS Accelerate는 기본 관리형 태그 지정 구성을 제공하므로 AMS Accelerate에서 리소스를 모니터링할 수 있습니다. AMS Accelerate에서 관리해야 하는 리소스를 정의하면 관리형 태그 지정 규칙을 통해 AMS Accelerate에서 적절한 태그를 가진 리소스를 모니터링할 수 있습니다.

Resource Tagger를 사용하면 기본 AMS Accelerate 관리형 태그를 재정의하거나 비활성화하고, 정책에 맞는 자체 태그 지정 규칙을 제공하고, 드리프트를 방지하기 위해 Terraform과 같은 다른 메커니즘을 사용할 수 있습니다. 작업에 따라 확장할 예외를 정의할 수 있습니다. 예를 들어 지원되는 플랫폼(예: Windows 및 Linux)이 있는 모든 Amazon EC2 인스턴스에 태그를 적용하고 특정 인스턴스 IDs.

> **Important**
>
> Resource Tagger는 ams:rt: 접두사가 있는 계정의 모든 태그를 제어합니다. 이 접두사로 시작하는 모든 태그는 Resource Tagger의 구성 규칙에 없는 한 삭제됩니다. 요약하자면 ams:rt:로 시작하는 지원되는 리소스의 모든 태그는 Resource Tagger가 소유한 것으로 간주됩니다. ams:rt:와 같이 수동으로 태그를 지정하면 Resource Tagger 구성 프로필 중 하나에 지정되지 않은 태그가 자동으로 제거됩니다.

Resource Tagger 작동 방식

계정이 AMS Accelerate에 온보딩되면의 계정에 두 개의 JSON 구성 문서가 배포됩니다 AWS AppConfig. 구성 프로필이라고 하는 두 문서는 기본 구성 프로필이라고 하는 AMSManagedTags와 사용자 지정 구성 프로필이라고 하는 CustomerManagedTags입니다. 사용자 지정 구성 프로파일을 사용하여 계정에 대한 자체 정책 및 규칙을 정의하면 AMS Accelerate에서 이를 덮어쓰지 않습니다.

두 프로파일 모두 AMSResourceTagger 애플리케이션과 AMSInfrastructure 환경에 있습니다. 리소스 태거가 적용하는 모든 태그에는 키 접두사 ams:rt:가 있습니다.

사용자 지정 구성 프로필:

사용자 지정 구성 프로필은 처음에 계정 온보딩 시 비어 있지만, 프로필 문서에 배치된 모든 규칙은 기본 구성 프로필의 규칙 외에도 적용됩니다. 사용자 지정 구성 프로필의 모든 구성은 전적으로 사용자가 관리하며 요청을 제외하고 AMS Accelerate에서 덮어쓰지 않습니다.

지원되는 AWS 리소스의 사용자 지정 구성 프로필에서 원하는 사용자 지정 태그 지정 규칙을 지정할 수 있으며, 여기에서 AMS Accelerate 관리형 기본 구성에 대한 수정을 지정할 수도 있습니다. 섹션을 참조하세요AMS Accelerate의 Resource Tagger 사용 사례.

> **Important**
>
> 이 프로필을 업데이트하면 Resource Tagger는의 모든 관련 리소스에 변경 사항을 자동으로 적용합니다 AWS 계정. 변경 사항은 자동으로 적용되지만 적용되는 데 최대 60분이 걸릴 수 있습니다.

를 사용하거나 AWS CLI/SDK 도구를 AWS Management Console통해이 프로파일을 업데이트할 수 있습니다. 사용자 지정 구성 프로필 업데이트에 대한 자세한 내용은 AWS AppConfig 사용 설명서:란 무엇입니까 AWS AppConfig?를 참조하세요.

기본 구성 프로필:

기본 구성 프로필 문서는 AMS Accelerate의 내부 문서이며 영구적으로 수정하거나 삭제할 수 없는 AMS Accelerate 제공 기본 규칙을 포함합니다. 이 프로필은 AMS Accelerate에서 언제든지 업데이트할 수 있으며 검토할 수 있습니다. 프로필을 변경하면 자동으로 삭제됩니다. 사용자 지정 구성 프로파일을 사용하는 기본 구성 규칙을 수정하거나 비활성화하려면 섹션을 참조하세요AMS Accelerate의 Resource Tagger 사용 사례.

AMS Accelerate의 리소스 태거 구성 프로파일

구성 프로필을 사용하면 리소스 수명 주기 동안 리소스에 태그를 균일하게 적용할 수 있습니다.

구문 및 구조

구성 프로필은 다음 구조의 JSON 객체입니다.

```
{
   "Options": {
      "ReadOnly": false
   },
   "ResourceType": {
      "ConfigurationID": {
      "Enabled": true,
      "Filter": { ... },
      "Tags": [  ...  ]
      },
      "ConfigurationID": {
      ...
      }
   },
   "ResourceType": {
     ...
   }
}
```

옵션: (선택 사항) ResourceTagger의 작동 방식에 대한 옵션을 지정합니다. 블록을 생략하는 것은 모든 옵션을 기본값으로 설정하는 것과 같습니다. 사용 가능한 옵션 설정은 아래를 참조하세요.

- ReadOnly: (선택 사항, 기본값은 false): Resource Tagger에 대한 ReadOnly 모드를 지정합니다. AWS 리소스에서 태그를 생성하거나 제거하는 Resource Tagger를 비활성화하려면 ReadOnly를 true로 설정합니다. 자세한 내용은 Resource Tagger의 리소스 수정 방지 단원을 참조하십시오.

ResourceType:이 키는 다음 지원되는 문자열 중 하나여야 하며 표시된 리소스 유형과 관련된 모든 구성을 나타냅니다.

- AWS::AutoScaling::AutoScalingGroup
- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::NatGateway
- AWS::EC2::VPNConnection
- AWS::EFS::FileSystem
- AWS::EKS::Cluster
- AWS::ElasticLoadBalancing::LoadBalancer
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::Elasticsearch::Domain
- AWS::FSx::FileSystem
- AWS::OpenSearch::Domain
- AWS::RDS::DBCluster
- AWS::RDS::DBInstance
- AWS::Redshift::Cluster
- AWS::S3::Bucket
- AWS::Synthetics::Canary

ConfigurationID:이 키는 프로파일 문서에서 고유해야 하며 다음 구성 블록의 이름을 고유하게 지정해야 합니다. 동일한 ResourceType 블록에 있는 두 구성 블록의 ConfigurationID가 동일한 경우 프로파일에 마지막으로 나타나는 구성 블록이 적용됩니다. 사용자 지정 프로파일에서 기본 문서에 지정된 것과 동일한 ConfigurationID를 지정하면 사용자 지정 프로파일에 정의된 구성 블록이 적용됩니다.

> **Important**
>
> ConfigurationID는 AMS Accelerate 프로파일과 겹치지 **###** 합니다. 예를 들어 AMSMonitoringLinux 또는 AMSMonitoringWindows가 아니어야 합니다. 그렇지 않으면 AMSManagedTags 구성 프로파일의 각 구성을 비활성화합니다.

활성화됨(선택 사항, 기본값은 true): 구성 블록이 적용되는지 여부를 지정합니다. 구성 블록을 비활성화하려면 false로 설정합니다. 비활성화된 구성 블록은 효과가 없습니다.

필터: 구성이 적용되는 리소스를 지정합니다. 각 필터 객체에는 다음 필드 중 하나(하나만)가 있을 수 있습니다.

- AWS::AutoScaling::AutoScalingGroup:
  - AutoScalingGroupName: Autoscaling 그룹 이름입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::DynamoDB::Table:
  - TableName: DynamoDB 테이블의 이름입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::EC2::Instance:
  - AvailabilityZone: 필터가 지정된 가용 영역의 EC2 인스턴스와 일치합니다. 이 필드는 와일드카드 일치를 지원하므로 *a는 us-east-1a, ap-northeast-1a 등과 일치합니다.
  - InstanceId: 필터가 지정된 인스턴스 ID를 가진 EC2 인스턴스와 일치합니다. 이 필드는 와일드카드 일치를 지원하므로 i-00000*은 인스턴스 ID가 i-00000으로 시작하는 모든 인스턴스와 일치합니다.
  - 플랫폼: 필터가 지정된 플랫폼과 EC2 인스턴스를 일치시킵니다. 유효한 값은 창, Linux 또는 와일드카드 *(모든 플랫폼과 일치)입니다.
- AWS::EC2::NatGateway:
  - NatGatewayId: NAT 게이트웨이의 ID입니다. 이 필드는 와일드카드 일치를 지원합니다.
  - 상태: NAT 게이트웨이의 상태(보류 중 | 실패 | 사용 가능 | 삭제 | 삭제됨 또는 와일드카드 "*")
  - VpcId: NAT 게이트웨이가 있는 VPC의 ID입니다. 이 필드는 와일드카드 일치를 지원합니다.
  - SubnetId: NAT 게이트웨이가 있는 서브넷의 ID입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::EC2::VPNConnection:
  - VpnConnectionId: 연결의 ID입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::EFS::FileSystem:
  - FileSystemId: EFS 파일 시스템의 ID입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::EKS::Cluster:
  - ClusterName: 클러스터의 이름입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::ElasticLoadBalancing::LoadBalancer(Classic Load Balancer):
  - LoadBalancerName: LoadBalancer 이름입니다. 이 필드는 와일드카드 일치를 지원합니다.
  - 스키마: "인터넷 경계", "내부" 또는 와일드카드 "*"일 수 있습니다.
  - VPCId: 로드밸런서가 배포되는 VPCId로, 와일드카드 "*"일 수 있습니다.

- AWS::ElasticLoadBalancingV2::LoadBalancer(Application Load Balancer(ALB)):
  - LoadBalancerArn: LoadBalancer Amazon 리소스 이름(ARN).
  - DNSName: LoadBalancer의 DNSName입니다. 이 필드는 와일드카드 일치를 지원합니다.
  - LoadBalancerName: LoadBalancer 이름입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::Elasticsearch::Domain:
  - DomainId: ElasticSearch 리소스의 DomainId입니다. 이 필드는 와일드카드 일치를 지원합니다.
  - DomainName: ElasticSearch 리소스의 DomainName입니다. 이 필드는 와일드카드 일치를 지원합니다.
  - HasMasterNode: true 또는 false의 부울 값입니다. 도메인에 전용 마스터 노드가 있는 경우 일치합니다.
  - HasKmsKey 부울 값이 true 또는 false입니다. 도메인에 저장 시 암호화를 위한 KMS 키가 있는 경우 일치합니다.
- AWS::FSx::FileSystem:
  - FileSystemId: FSx 파일 시스템의 ID입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::OpenSearch::Domain:
  - DomainId: OpenSearch 리소스의 DomainId입니다. 이 필드는 와일드카드 일치를 지원합니다.
  - DomainName: OpenSearch 리소스의 DomainName입니다. 이 필드는 와일드카드 일치를 지원합니다.
  - HasMasterNode: 부울, 도메인에 전용 마스터 노드가 있는 경우 true로 설정할 수 있습니다.
  - HasKmsKey: 도메인에 저장 시 암호화를 위한 KMS 키가 있는 경우 true로 설정할 수 있습니다.
- AWS::RDS::DBCluster:
  - DBClusterIdentifier: 필터가 RDS 클러스터 식별자와 지정된 식별자를 일치시킵니다. 이 필드는 와일드카드 일치를 지원하지 않으므로 클러스터 식별자를 지정해야 합니다.
  - 엔진: RDS 인스턴스에서 사용 중인 엔진입니다. 이 필드는 와일드카드 일치를 지원합니다.
  - EngineVersion: 엔진 버전입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::RDS::DBInstance:
  - DBInstanceIdentifier: 필터가 지정된 인스턴스 ID를 가진 RDS 인스턴스와 일치합니다. 이 필드는 와일드카드 일치를 지원하지 않으므로 인스턴스 식별자를 지정해야 합니다.
  - 엔진: RDS 인스턴스에서 사용 중인 엔진입니다. 이 필드는 와일드카드 일치를 지원합니다.
  - EngineVersion: 엔진 버전입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::Redshift::Cluster:

  - ClusterIdentifier: 클러스터 식별자입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::S3::Bucket:
  - BucketName: S3 버킷의 이름입니다. 이 필드는 와일드카드 일치를 지원합니다.
- AWS::Synthetics::Canary:
  - CanaryName: Synthetics canary의 이름입니다.

기타 필터 속성:

- 태그: 필터는 지정된 태그가 이미 적용된 모든 리소스에 적용됩니다. 이 속성의 값은 다음 필드가 있는 JSON 객체여야 합니다.
  - 키: 정확한 문자열이어야 하며 리소스에 정확한 키가 있는 태그가 있도록 지정합니다.
  - 값: 태그의 일치하는 값을 지정합니다. 와일드카드를 지원하므로 샘플 값은 문자열 샘플로 끝나는 모든 값과 일치합니다.
- Fn::AND: JSON 객체의 JSON 배열입니다. 각 객체는 필터 구성 블록과 동일한 규칙을 따릅니다. 이는 필터가 모든 하위 필터와 일치하는 모든 리소스와 일치하도록 지정합니다.
- Fn::OR: JSON 객체의 JSON 배열입니다. 각 객체는 필터 구성 블록과 동일한 규칙을 따릅니다. 이는 필터가 하위 필터와 일치하는 모든 리소스와 일치하도록 지정합니다.
- Fn::NOT: 필터 구성 블록과 동일한 규칙을 따르는 JSON 객체입니다. 이는 필터가 하위 필터와 일치하는 리소스와 명시적으로 일치하지 않도록 지정합니다. 이를 사용하여 태그 지정 규칙에 대한 제외 항목을 지정합니다.

태그: 일치하는 리소스에 적용할 태그입니다. (태그 이름 지정 및 사용 규칙 참조) 이 필드는 키-값 페어의 배열입니다.

- 키: 적용할 태그의 키입니다.
- 값: 적용할 태그의 값입니다.

> **Note**
>
> Resource Tagger에서 적용하는 태그에는 항상 ams:rt:로 시작하는 키가 있습니다. 프로필에 이 접두사를 지정하지 않으면 Resource Tagger가 이를 삽입합니다. 이렇게 하면 Resource Tagger가 소유 및 관리하는 태그를 다른 도구에서 다른 목적으로 사용하는 태그와 구별할 수 있습니다.

AMS Accelerate의 Resource Tagger 사용 사례

이 섹션에서는 Resource Tagger에서 일반적으로 수행되는 작업을 나열합니다.

Resource Tagger에서 적용한 태그 보기

Resource Tagger에서 적용하는 모든 태그에는 ams:rt:라는 키 접두사가 있습니다. 예를 들어 다음 태그 정의는 키 ams:rt:sampleKey 및 값 sampleValue가 있는 태그를 생성합니다. 이 접두사가 있는 모든 태그는 Resource Tagger의 일부로 취급됩니다.

```
{
 "Key": "sampleKey",
 "Value": "sampleValue"
}
```

> **Important**
>
> ams:rt: 접두사를 사용하여 자체 태그를 수동으로 생성하는 경우 Resource Tagger에서 관리하는 것으로 간주됩니다. 즉, Resource Tagger에서 리소스를 관리하지만 구성 프로필에 태그를 적용해야 한다고 표시되지 않는 경우 Resource Tagger는 수동으로 추가된 태그를 제거합니다. Resource Tagger에서 관리하는 리소스에 수동으로 태그를 지정하는 경우 태그 키에 ams:rt: 접두사를 사용하지 마십시오.

Resource Tagger를 사용하여 태그 생성

AMS Accelerate 리소스 태거는 AMS Accelerate 온보딩 중에 계정에 배포되는 구성 요소입니다. Resource Tagger에는 리소스에 태그를 지정하는 방법을 정의하는 구성 가능한 규칙 세트가 있습니다. 그런 다음 해당 규칙을 적용하여 리소스에 태그를 자동으로 추가 및 제거하여 규칙을 준수하는지 확인합니다.

Resource Tagger를 사용하여 리소스에 태그를 지정하려면 섹션을 참조하세요리소스 태거 가속화.

다음은 모든 Amazon EC2 인스턴스에 값이 true인 ams:rt:ams-managed 태그를 추가하는 Resource Tagger 구성 코드 조각의 예입니다. ams:rt:ams-managed 태그는 AMS Accelerate에서 리소스를 모니터링하도록 옵트인합니다.

```
{
    "AWS::EC2::Instance": {
        "SampleConfigurationBlock": {
            "Enabled": true,
```

```
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> 새 구성의 이름(SampleConfigurationBlock제공된 예의)을 지정할 때는 AMS 관리형 구성을 동일한 이름으로 실수로 재정의할 수 있으므로 주의해야 합니다.

Resource Tagger의 리소스 수정 방지

Resource Tagger는 리소스에 태그를 추가하거나 제거하지 못하도록 읽기 전용 모드로 설정할 수 있습니다. 이는 자체 태그 지정 메커니즘을 제공하려는 경우에 유용합니다.

읽기 전용 모드인 경우에도 Resource Tagger는 관리형 및 고객 구성 프로필에 지정된 태그 지정 규칙을 검사하고 이러한 태그 지정 규칙을 충족하지 않는 리소스를 검사합니다. 규정을 준수하지 않는 리소스는 모두 표시됩니다 AWS Config. 찾을 수 AWS Config 규칙 있는 에는 AMSResourceTagger- 접두사가 있습니다. 예를 들어 AMSResourceTagger-EC2Instance AWS Config 규칙은 구성 프로파일을 기반으로 AWS::EC2::Instance 리소스에 대한 적절한 태그가 생성되었는지 평가합니다.

Resource Tagger는이 시점에서 중지되며 리소스를 변경하지 않습니다(태그를 추가하거나 제거하지 않음).

옵션 블록에 ReadOnly 키를 포함하도록 고객 구성 프로필을 수정하여 읽기 전용 모드를 활성화할 수 있습니다. 예를 들어 다음 구성 프로파일 코드 조각은이 모양이 어떻게 보일 수 있는지 보여줍니다.

```
{
    "Options": {
        "ReadOnly": true
    },
    "AWS::EC2::Instance": {
```

```
        [... the rest of your configuration ...]
    }
}
```

Resource Tagger는 배포가 완료되는 즉시이 새 구성에 반응하고 리소스에 대한 태그 추가 및 제거를 중지합니다.

> **Note**
>
> 태그 수정을 다시 활성화하려면 기본값이 false이므로 ReadOnly 값을 false로 변경하거나 키를 모두 제거합니다.

옵션 설정에 대한 자세한 내용은 구문 및 구조다음 단원을 참조하십시오.

예제 구성 프로필

다음 예제 프로파일 문서는 스택-* CloudFormation 스택의 일부인 모든 Windows EC2 인스턴스를 AMS Accelerate에서 관리하도록 지정하지만 ID가 i-00000000000000001인 특정 EC2 인스턴스는 명시적으로 제외합니다.

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "Windows"
                    },
                    {
                        "Tag": {
                            "Key": "aws:cloudformation:stack-name",
                            "Value": "stack-*"
                        }
                    },
                    {
                        "Fn::NOT": {
                            "InstanceId": "i-00000000000000001"
                        }
                    }
                ]
```

```
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> 새 구성의 이름(SampleConfigurationBlock제공된 예의)을 지정할 때는 AMS 관리형 구성을 동일한 이름으로 실수로 재정의할 수 있으므로 주의해야 합니다.

기본 구성 병합

기본 구성 프로필은 계정 온보딩 시 AMS Accelerate에서 제공합니다. 이 프로필은 계정에 배포된 기본 규칙을 제공합니다.

기본 구성 프로필은 수정할 수 없지만 기본 구성 블록과 동일한 ConfigurationID를 사용하여 사용자 지정 구성 프로필에 구성 블록을 지정하여 기본값에 대한 재정의를 제공할 수 있습니다. 이렇게 하면 구성 블록이 기본 구성 블록을 덮어씁니다.

예를 들어 다음과 같은 기본 구성 문서를 고려합니다.

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

여기에 적용된 태그 값을에서 SampleValueA로 변경SampleValueB하고 Windows 인스턴스뿐만 아니라 모든 인스턴스에 태그를 적용하려면 다음과 같은 사용자 지정 구성 프로파일을 제공합니다.

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "*"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueB"
   }]
  }
 }
}
```

> **Important**
>
> 구성 변경 사항을 적용한 후에는 배포해야 합니다. 자세한 내용은 구성 변경 사항 배포 단원을 참조하십시오. SSM AppConfig에서는 구성을 생성한 후 새 버전의 구성을 배포해야 합니다.

기본 구성 비활성화

사용자 지정 구성 프로필에 동일한 ConfigurationID가 있는 구성 블록을 추가하고 값에 대해 활성화됨 필드를 false로 지정하여 기본 구성 규칙을 비활성화할 수 있습니다.

예를 들어 기본 구성 프로필에 다음 구성이 있는 경우:

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
```

```
  }
 }
}
```

사용자 지정 구성 프로필에 다음을 포함하여이 태그 지정 규칙을 비활성화할 수 있습니다.

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": false
  }
 }
}
```

> **Important**
>
> 구성 변경 사항을 적용한 후에는 배포해야 합니다. 자세한 내용은 섹션을 참조하세요구성 변경 사항 배포. SSM AppConfig에서는 구성을 생성한 후 새 버전의 구성을 배포해야 합니다.

Resource Tagger에서 적용한 태그 제거

ams:rt 접두사가 붙은 태그가 구성 프로필에 없거나 태그가 있는 경우 필터가 일치하지 않는 경우 Resource Tagger에서 제거합니다. 즉, 다음 중 하나를 수행하여 Resource Tagger에서 적용한 태그를 제거할 수 있습니다.

- 태그를 정의하는 사용자 지정 구성 섹션 수정.
- 특정 리소스가 더 이상 필터와 일치하지 않도록 해당 리소스에 대한 예외를 추가합니다.

예: Linux 인스턴스에 다음 태그가 있는 경우:

```
"Tags": [{
    "Key": "ams:rt:MyOwnTag",
    "Value": true
},{
    "Key": "myTag",
    "Value": true
}]
```

그리고 다음 Resource Tagger 구성 프로파일을 배포합니다.

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Platform": "Windows"
            },
            "Tags": [{
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }]
        }
    }
}
```

Resource Tagger는 새 구성 변경에 반응하며 인스턴스의 유일한 태그는 다음과 같습니다.

```
"Tags": [{
    "Key": "myTag",
    "Value": true
}]
```

Warning

새 구성의 이름(SampleConfigurationBlock제공된 예의)을 지정할 때는 AMS 관리형 구성을 동일한 이름으로 실수로 재정의할 수 있으므로 주의해야 합니다.

Important

구성 변경 사항을 적용한 후에는 배포해야 합니다. 자세한 내용은 섹션을 참조하세요구성 변경 사항 배포. SSM AppConfig에서는 구성을 생성한 후 새 버전의 구성을 배포해야 합니다.

Resource Tagger 구성 보기 또는 변경

AMSManagedTags 및 AMSInfrastructure 환경에서 온보딩 및 상주 시 AWS AppConfig의 계정에 배포된 두 가지 JSON 구성 프로파일인 AMSManagedTags 및 CustomerManagedTags는 AppConfig의 GetConfiguration API를 통해 검토할 수 있습니다. AMSResourceTagger

다음은이 GetConfiguration 호출의 예입니다.

```
aws appconfig get-configuration
 --application AMSResourceTagger
 --environment AMSInfrastructure
 --configuration AMSManagedTags
 --client-id ANY_STRING
 outfile.json
```

애플리케이션: 기능을 제공하는 AppConfig 논리 단위입니다. Resource Tagger의 경우 AMSResourceTagger입니다.

- 환경: AMSInfrastructure.
- 구성: AMS Accelerate 기본 태그 정의를 보려면 값은 AMSManagedTags이고, 고객 태그 정의를 보려면 CustomerManagedTags입니다.
- 클라이언트 ID: 고유한 애플리케이션 인스턴스 식별자로, 모든 문자열일 수 있습니다.
- 그런 다음 지정된 출력 파일,이 경우 outfile.json에서 태그 정의를 볼 수 있습니다.

그런 다음 지정된 출력 파일,이 경우 outfile.json에서 경보 정의를 볼 수 있습니다.

AMSInfrastructure 환경에서 과거 배포를 확인하여 계정에 배포된 구성 버전을 확인할 수 있습니다.

태그 규칙을 재정의하려면:

CloudFormation CloudFormation for Accelerate를 사용하여 구성 프로파일 배포 또는를 사용하여 사용자 지정 프로필을 업데이트하거나 AppConfig의 CreateHostedConfigurationVersion API를 사용하여 직접 기존 태그 규칙을 재정의할 수 있습니다. 동일한 ConfigurationID를 기본 구성 태그 규칙으로 사용하면 기본 규칙이 재정의되고 사용자 지정 규칙이 대신 적용됩니다.

CustomerManagedTags 문서에 대한 변경 사항을 배포하려면

사용자 지정 구성 프로필을 변경한 후에는 변경 사항을 배포해야 합니다. 새 변경 사항을 배포하려면 AWS AppConfig 콘솔 또는 CLI를 사용하여 AppConfig의 StartDeployment API를 실행해야 합니다.

구성 변경 사항 배포

사용자 지정이 완료되면 이러한 변경 사항을 StartDeployment API를 AWS AppConfig 통해 배포해야 합니다. 다음 지침은를 사용하여를 배포하는 방법을 보여줍니다 AWS CLI. 또한 AWS Management Console 를 사용하여 이러한 변경을 수행할 수 있습니다. 자세한 내용은 5단계: 구성 배포를 참조하세요.

```
aws appconfig start-deployment
--application-id <application_id>
--environment-id <environment_id>
--deployment-strategy-id <deployment_strategy_id>
--configuration-profile-id <configuration_profile_id>
--configuration-version 1
```

- 애플리케이션 ID: 애플리케이션 AMSResourceTagger의 애플리케이션 ID입니다. ListApplications API 호출을 통해 이를 가져옵니다.
- 환경 ID: 환경 ID입니다. ListEnvironments API 호출을 통해 이를 가져옵니다.
- 배포 전략 ID: 배포 전략 ID입니다. ListDeploymentStrategies API 호출을 통해 이를 가져옵니다.
- 구성 프로필 ID: CustomerManagedTags의 구성 프로필 ID입니다. ListConfigurationProfiles API 호출을 통해 이를 가져옵니다.
- 구성 버전: 배포하려는 구성 프로필의 버전입니다.

Important

Resource Tagger는 구성 프로필에 지정된 대로 태그를 적용합니다. 리소스 태그에 대한 모든 수동 수정 사항(AWS Management Console또는 CloudWatch CLI/SDK 사용)은 자동으로 되돌려지므로 Resource Tagger를 통해 변경 사항을 정의해야 합니다. Resource Tagger에서 생성되는 태그를 확인하려면 접두사가 붙은 태그 키를 찾습니다`ams:rt:`.

StartDeployment 및 StopDeployment API 작업을 사용하여 배포에 대한 액세스를 대상에 새 구성을 배포할 때의 책임과 결과를 이해하는 신뢰할 수 있는 사용자로 제한합니다.

AWS AppConfig 기능을 사용하여 구성을 생성하고 배포하는 방법에 대한 자세한 내용은 AWS AppConfig 작업의 설명서를 참조하세요.

Resource Tagger 태그를 무시하도록 Terraform 구성

Terraform을 사용하여 리소스를 프로비저닝하고 Resource Tagger를 사용하여 리소스에 태그를 지정하려는 경우 Resource Tagger 태그는 Terraform에 의해 드리프트로 식별될 수 있습니다.

수명 주기 구성 블록 또는 ignore_tags 글로벌 구성 블록을 사용하여 모든 Resource Tagger 태그를 무시하도록 Terraform을 구성할 수 있습니다. 자세한 내용은 리소스 태그 지정의 리소스 태그 지정에 대한 Terraform 설명서를 참조하세요.

다음 예제에서는 Resource Tagger 태그 접두사 로 시작하는 모든 태그를 무시하도록 전역 구성을 생성하는 방법을 보여줍니다`ams:rt:`.

```
provider "aws" {
  # ... potentially other configuration ...

  ignore_tags {
    key_prefixes = ["ams:rt:"]
  }
}
```

Resource Tagger에서 관리하는 리소스 수 보기

Resource Tagger는 매시간 `AMS/ResourceTagger` 네임스페이스의 Amazon CloudWatch로 지표를 전송합니다. 지표는 Resource Tagger에서 지원하는 리소스 유형에 대해서만 내보내집니다.

지표 이름	측정기준	설명
ResourceCount	구성 요소, ResourceType	이 리전에 배포된 리소스 수(지정된 리소스 유형)입니다. 단위: 개
ResourcesMissingManagedTags	구성 요소, ResourceType	구성 프로필에 따라 관리형 태그가 필요하지만 아직 Resource Tagger에서 태그를 지정하지 않은 리소스 수(지정된 리소스 유형)입니다. 단위: 개
UnmanagedResources	구성 요소, ResourceType	Resource Tagger에서 관리형 태그를 적용하지 않은 리소스 수(지정된 리소스 유형)입니다. 일반적으로 이러한 리소스는 Resource Tagger 구성 블록과 일치하지 않거나 구성 블록에서 명시적으로 제외됩니다. 단위: 개
MatchingResourceCount	구성 요소, ResourceType, ConfigClauseName	Resource Tagger 구성 블록과 일치하는 리소스 수(지정된 리소스 유형)입니다. 리소스가 구성 블

지표 이름	측정기준	설명
		록과 일치하려면 블록을 활성화하고 리소스가 블록의 필터와 일치해야 합니다. 단위: 개

이러한 지표는 AMS-Resource-Tagger-Reporting-Dashboard에서 그래프로도 볼 수 있습니다. 대시보드를 보려면 Amazon CloudWatch 관리 콘솔에서 AMS-Resource-Tagger-Reporting-Dashboard를 선택합니다. 기본적으로이 대시보드의 그래프에는 이전 12시간 동안의 데이터가 표시됩니다.

AMS Accelerate는 계정에 CloudWatch 경보를 배포하여 AMS Resource Tagger의 관리에서 제외된 리소스와 같은 비관리형 리소스 수의 상당한 증가를 감지합니다. AMS Operations는 동일한 유형의 리소스 3개를 초과하거나 동일한 유형의 모든 리소스에 대해 50% 증가를 초과하는 비관리형 리소스의 증가를 조사합니다. 변경 사항이 의도적으로 표시되지 않는 경우 AMS Operations에서 변경 사항을 검토하기 위해 사용자에게 연락할 수 있습니다.

CloudFormation을 사용하여 AMS Accelerate에 대한 태그 생성

CloudFormation 를 사용하여 스택 수준(CloudFormation 설명서, 리소스 태그 참조) 또는 개별 리소스 수준(예: Amazon EC2 리소스 태그 지정 참조)에서 태그를 적용할 수 있습니다.

> **Important**
>
> 일부 AMS Accelerate 서비스 구성 요소에는 ams:rt: 접두사가 있는 태그가 필요합니다. Resource Tagger는 이러한 태그를 소유하고 있다고 생각하며 Resource Tagger 구성 규칙에서 허용하는 태그가 없는 경우 태그를 삭제합니다. CloudFormation 또는 Terraform을 사용하는 경우에도 항상 이러한 태그에 대한 Resource Tagger 구성 프로파일을 배포해야 합니다.

CloudFormation AMS Accelerate 사용 사례

이 섹션에서는를 사용하여 일반적으로 수행되는 작업을 나열합니다 CloudFormation.

주제

- CloudFormation Accelerate용를 사용하여 EC2 인스턴스에 태그 지정
- 가속화를 CloudFormation 위해를 사용하여 AutoScaling 그룹(ASG)에 태그 지정
- CloudFormation for Accelerate를 사용하여 구성 프로파일 배포

CloudFormation Accelerate용를 사용하여 EC2 인스턴스에 태그 지정

다음은 ams:rt:ams-managed 태그와 true 값을에서 관리하는 Amazon EC2 인스턴스에 적용하는 방법의 예입니다 CloudFormation. ams:rt:ams-managed 태그는 AMS Accelerate에서 리소스를 모니터링하도록 옵트인합니다.

```
 Type: AWS::EC2::Instance

Properties:
  InstanceType: "t3.micro"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

가속화를 CloudFormation 위해를 사용하여 AutoScaling 그룹(ASG)에 태그 지정

다음은 ams:rt:ams-managed 태그와 true 값을에서 관리하는 Auto Scaling 그룹에 적용하는 방법의 예입니다 CloudFormation. Auto Scaling 그룹은 자신이 생성한 Amazon EC2 인스턴스에 태그를 전파합니다. ams:rt:ams-managed 태그는 AMS Accelerate에서 리소스를 모니터링하도록 옵트인합니다.

```
  Type: AWS::AutoScaling::AutoScalingGroup
Properties:
  AutoScalingGroupName: "SampleASG"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

CloudFormation for Accelerate를 사용하여 구성 프로파일 배포

를 사용하여 `CustomerManagedTags` 구성 프로필을 배포하려는 경우 다음 CloudFormation 템플릿을 사용할 CloudFormation수 있습니다. `AMSResourceTaggerConfigurationVersion.Content` 필드에 원하는 JSON 구성을 입력합니다.

CloudFormation 스택 또는 스택 세트에 템플릿을 배포하면 구성에 필요한 JSON 형식을 따르지 않으면 `AMSResourceTaggerDeployment` 리소스 배포가 실패합니다. 예상 형식에 대한 구문 및 구조 자세한 내용은 섹션을 참조하세요.

이러한 템플릿을 CloudFormation 스택 또는 스택 세트로 배포하는 방법에 대한 도움말은 아래 관련 AWS CloudFormation 설명서를 참조하세요.

- AWS CloudFormation 콘솔에서 스택 생성
- 를 사용하여 스택 생성 AWS CLI
- 스택 세트 생성

> **Note**
>
> 이러한 템플릿 중 하나를 사용하여 구성 버전을 배포한 다음 CloudFormation 스택/스택 세트를 삭제하면 템플릿 구성 버전이 현재 배포된 버전으로 유지되며 추가 배포가 이루어지지 않습니다. 기본 구성으로 되돌리려면 스택을 삭제하는 대신 수동으로 빈 구성(즉, 만{})을 배포하거나 스택을 빈 구성으로 업데이트해야 합니다.

JSON

```
{
  "Description": "Custom configuration for the AMS Resource Tagger.",
  "Resources": {
    "AMSResourceTaggerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "Content": "{\"Options\": {\"ReadOnly\": false}}",
        "ContentType": "application/json"
      }
    },
    "AMSResourceTaggerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
```

```
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSResourceTaggerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Resource Tagger.
Resources:
  AMSResourceTaggerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      Content: |
        {
          "Options": {
            "ReadOnly": false
          }
        }
      ContentType: application/json
  AMSResourceTaggerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
```

```
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      ConfigurationVersion:
        !Ref AMSResourceTaggerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-ResourceTagger-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-ResourceTagger-Configuration-EnvironmentId
```

Terraform을 사용하여 AMS Accelerate용 태그 생성

AMS Accelerate Resource Tagger를 사용하지 않으려면 Terraform을 사용하여 자체 태그를 적용할 수 있습니다. 그러나 Terraform 정의의 드리프트로 인해 Resource Tagger를 사용하지 않으려는 경우 Resource Tagger를 사용하고 Resource Tagger가 유발하는 드리프트를 무시할 수 있는 방법이 있습니다. 섹션을 참조하세요Resource Tagger 태그를 무시하도록 Terraform 구성.

> **Important**
>
> 일부 AMS Accelerate 서비스 구성 요소에는 ams:rt: 접두사가 있는 태그가 필요합니다. Resource Tagger는 이러한 태그를 소유하고 있다고 생각하며 Resource Tagger 구성 규칙에서 허용하는 태그가 없는 경우 태그를 삭제합니다. CloudFormation 또는 Terraform을 사용하는 경우에도 이러한 태그에 대한 Resource Tagger 구성 프로파일을 배포해야 합니다.

다음은 Terraform에서 관리하는 Amazon EC2 인스턴스에 값으로 ams:rt:ams-managed 태그를 적용하는 방법의 예입니다. ams:rt:ams-managed 태그는 AMS Accelerate에서 리소스를 모니터링하도록 옵트인합니다.

```
  resource "aws_instance" "sample_linux_instance" {
    # ...ami and other properties...

    instance_type = "t3.micro"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

다음은 Terraform에서 관리하는 Auto Scaling 그룹에 값이 true인 ams:rt:ams-managed 태그를 적용하는 방법의 예입니다. Auto Scaling 그룹은 태그를 자신이 생성한 Amazon EC2 인스턴스로 전파합니다. ams:rt:ams-managed 태그는 AMS Accelerate에서 리소스를 모니터링하도록 옵트인합니다.

```
  resource "aws_autoscaling_group" "sample_asg" {
    # ...other properties...

    name = "terraform-sample"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Terraform에서 생성한 리소스 태그를 관리하는 방법에 대한 설명은 섹션을 참조하세요Resource Tagger 태그를 무시하도록 Terraform 구성.

AMS Accelerate의 인시던트 보고서, 서비스 요청 및 결제 질문

AMS Accelerate를 사용하면의 AWS 지원 센터를 통해 언제든지 운영 문제 및 요청에 대한 도움을 요청할 수 있습니다 AWS Management Console. AMS Accelerate 운영 엔지니어는 서비스에 대한 응답 시간 서비스 수준 계약(SLAs)을 사용하여 인시던트 및 서비스 요청에 round-the-clock 응답할 수 있습니다. AMS Accelerate 운영 엔지니어는 동일한 메커니즘을 사용하여 중요한 알림 및 질문을 사전에 알립니다.

AMS Accelerate는 운영 우수성을 달성하는 데 도움이 되는 다양한 운영 서비스를 제공합니다 AWS. round-the-clock 헬프데스크, 사전 모니터링, 보안, 패치 적용, 로깅 및 백업을 포함한 몇 가지 주요 운영 기능을 AWS 클라우드 통해 AMS가 팀이에서 전반적인 운영 우수성을 달성하는 데 어떻게 도움이 되는지 빠르게 이해하려면 AMS 참조 아키텍처 다이어그램을 참조하세요.

주제

- AMS Accelerate의 인시던트 관리
- Accelerate의 서비스 요청 관리
- Accelerate의 인시던트 보고서 및 서비스 요청 테스트
- AMS Accelerate에 대한 결제 질문

AMS Accelerate의 인시던트 관리

AMS Accelerate에서는 AWS Support Center Console를 사용하여 인시던트 보고서를 제출합니다. 인시던트는 AMS Accelerate 또는 사용자의 결정에 따라 관리형 환경에 영향을 미치는 AWS 서비스 성능 문제입니다. AMS Accelerate 팀이 식별한 인시던트는 먼저 이벤트(모니터링으로 캡처된 시스템 상태 변경)로 수신됩니다. 구성된 임계값이 위반되면 이벤트는 알림이라고도 하는 경보를 트리거합니다. AMS Accelerate 운영 팀은 이벤트가 영향을 미치지 않는지, 인시던트(서비스 중단 또는 성능 저하) 또는 문제(하나 이상의 인시던트의 근본 원인)인지 확인합니다.

> **Note**
>
> 또한 AMS Accelerate 팀은 서비스 코드와 함께 AWS Support API를 사용하여 사용자가 생성한 인시던트를 프로그래밍 방식으로 수신합니다`service-ams-operations-report-incident`.

사용에 대한 자세한 내용은 시작하기를 지원참조하세요. 지원

인시던트 관리가 무엇인가요?

인시던트 관리는 AMS가 활성 인시던트를 기록, 조치, 진행 상황 전달 및 알림을 제공하는 데 사용하는 프로세스입니다.

인시던트 관리 프로세스의 목표는 관리형 서비스의 정상 운영을 최대한 빨리 복원하고, 비즈니스 영향을 최소화하고, 모든 관련 당사자에게 정보를 제공하는 것입니다.

인시던트의 예로는 네트워크 연결의 손실 또는 성능 저하, 응답하지 않는 프로세스 또는 API 또는 예약된 작업이 수행되지 않는 경우(예: 백업 실패) 등이 있습니다(이에 국한되지 않음).

다음 그림은 사용자가 AMS에 보고한 인시던트의 워크플로를 보여줍니다.

이 그래픽은 AMS에서 보고하는 인시던트의 워크플로를 보여줍니다.

인시던트 우선 순위

AWS 지원 센터, 콘솔 또는 지원 API(SAPI)에서 생성된 인시던트는 AMS 콘솔에서 생성된 인시던트와 분류가 다릅니다.

- 낮음: AWS 또는 AMS 리소스와 관련된 비즈니스 서비스 또는 애플리케이션의 중요하지 않은 기능에 영향을 미칩니다.
- 중간: AWS 및/또는 AMS 리소스와 관련된 비즈니스 서비스 또는 애플리케이션이 중간 정도로 영향을 받고 성능이 저하된 상태에서 작동합니다.
- 높음: 비즈니스에 큰 영향을 미칩니다. AWS 및/또는 AMS 리소스와 관련된 애플리케이션의 중요한 기능은 사용할 수 없습니다. 프로덕션 시스템에 영향을 미치는 가장 중요한 중단에 대해 예약됩니다.

> **Note**
>
> AWS 지원 콘솔은 세 가지 AMS 수준으로 변환되는 다섯 가지 수준의 인시던트 우선 순위를 제공합니다.

인시던트 대응 및 해결 방법

AMS Accelerate는 IT 서비스 관리(ITSM) 인시던트 관리 모범 사례를 사용하여 필요한 경우 최대한 빨리 서비스를 복원합니다.

모니터링 대시보드와 인시던트 대기열을 적극적으로 감시하는 전담 운영자와 함께 전 세계 운영 센터를 통해 연중무휴 follow-the-sun 제공합니다.

운영 엔지니어는 내부 인시던트 추적 도구를 사용하여 인시던트를 식별, 로그, 분류, 우선 순위 지정, 진단, 해결 및 종료합니다. AWS Support Center 및 AWS Support API를 통해 이러한 모든 활동에 대한 업데이트를 제공합니다. 운영자는 다양한 내부 AWS 지원 도구를 활용하여 이러한 모든 활동을 지원합니다. 이러한 운영자는 AMS Accelerate 지원 인프라에 대해 깊이 숙지하고 식별된 지원 문제를 해결할 수 있는 전문가 수준의 기술 역량을 갖추고 있습니다. 운영자에게 지원이 필요한 경우 Premium Support 및 AWS 서비스 팀을 이용할 수 있습니다.

AMS Accelerate 운영 팀에서 인시던트를 수신한 후 명확한 설명이 필요한 경우 우선순위 및 분류를 검증합니다. 예를 들어 인시던트 보고서가 서비스 요청으로 더 잘 분류되는 경우 재분류되고 AMS Accelerate 서비스 요청 팀이 인계하고 알림을 받습니다. 수신 운영자가 인시던트를 해결할 수 있는 경우 인시던트를 신속하게 해결하기 위한 조치가 취해집니다. AMS Accelerate 운영자는 해결 방법은 내부 설명서를 참조하고 필요한 경우 인시던트가 해결될 때까지 다른 지원 리소스로 인시던트를 에스컬레이션합니다. 해결된 후 AMS Accelerate 운영 팀은 나중에 사용할 수 있도록 인시던트와 해결 방법을 문서화합니다.

중요한 심각도 인시던트가 중요한 워크로드에 영향을 미치는 경우 AMS Accelerate는 인프라 복원을 권장할 수 있습니다. 문제 해결과 알려진 기능 백업에서 단순히 복원하는 것 사이에는 절충점이 있는 경우가 많으며, 서비스 가동 중지로 인한 위험과 영향이 결정 요인입니다. 문제 해결에 전념할 시간이 있는 경우 AMS Accelerate가 도와드릴 것이며 클라우드 서비스 제공 관리자(CSDM)가 관여할 수 있지만, 복원 긴급성이 높으면 AMS Accelerate가 즉시 복원을 시작할 수 있습니다.

AMS Accelerate에서 인시던트 작업

AWS 지원 센터에서 다음 작업을 수행할 수 있습니다.

- 인시던트를 보고하고 업데이트합니다. AMS Accelerate 인시던트를 보고하려면 서비스 메뉴에서 AMS 운영 -- 인시던트 보고를 선택합니다.
- 제출된 모든 인시던트의 목록과 자세한 정보를 가져옵니다.
- 상태 및 기타 필터별로 인시던트 검색 범위를 좁힙니다.
- 인시던트에 커뮤니케이션 및 파일 첨부 파일을 추가하고 사례 대응을 위해 이메일 수신자를 추가합니다.

- 실시간 채팅을 시작하거나 인시던트에 대한 콜백을 요청합니다.

> **Note**
>
> 실시간 채팅 기능은 보안 이벤트용이 아니며, 보안 문제의 경우 우선 순위가 높은(P1 또는 P2) 지원 사례를 생성합니다.

- 인시던트를 해결합니다.
- 인시던트 커뮤니케이션을 평가합니다.

다음 예제에서는 지원 센터를 사용하여 인시던트를 제출하는 방법을 설명합니다. 제출 후 AMS Accelerate 팀은 표준 AMS Accelerate SLA에 따라 인시던트를 해결하기 위해 고객과 협력합니다.

Accelerate를 위한 인시던트 제출

지원 센터를 사용하여 인시던트를 보고하려면 지원 설명서: 지원 사례 생성을 참조하세요.

지원 센터를 사용하여 인시던트를 보고하려면:

1. 사례 생성을 클릭합니다. 인시던트 사례 생성 페이지가 열립니다.
2. 기술 지원 문제 유형 메뉴를 열고 AMS 작업 -- 인시던트 보고를 선택합니다. 인시던트에 대한 정보를 입력하고 생성을 선택합니다.
3. 인시던트 해결 프로세스의 각 단계에서 이메일로 알림을 받으려면 CC 이메일 옵션을 작성해야 합니다. 페더레이션으로 연결하는 경우 AMS Accelerate가 인시던트에 대해 보내는 이메일의 링크를 따르기 전에 로그인합니다.

> **Note**
>
> 설명을 가능한 상세히 작성해야 합니다. 문제를 이해하는 데 도움이 되는 다른 자료와 함께 관련 리소스 정보를 포함해야 합니다. 예를 들어, 성능 문제를 해결하려면 타임스탬프 및 로그를 포함합니다. 기능 요청이나 일반 지침 질문에 대해서는 환경 및 목적에 대한 설명을 포함합니다. 모든 사례에서 사례 제출 양식에 표시되는 설명 지침(Description Guidance)을 준수하세요. 최대한 자세하게 설명하면 사례가 빨리 해결될 가능성이 커집니다.

AWS Support API를 서비스 코드와 함께 사용하여 인시던트`service-ams-operations-report-incident`를 보고할 수도 있습니다.

Accelerate 인시던트 모니터링 및 업데이트

지원 센터를 사용하거나 지원 API, `DescribeCases` 작업을 프로그래밍 방식으로 사용하여 사례라고 하는 인시던트 보고서 및 서비스 요청을 업데이트, 모니터링 및 검토할 수 있습니다.

지원 Center를 사용하여 사례, 인시던트 또는 서비스 요청을 모니터링하려면 다음 단계를 따릅니다.

1. AWS 관리 콘솔에서 지원을 찾습니다.
2. 왼쪽 탐색에서 지원 사례를 선택하고 사례로 이동한 다음 Subjectlink를 선택하여 현재 상태 및 서신이 포함된 세부 정보 페이지를 엽니다.

   이 시점에서 전화 또는 채팅을 사용하려면 지원 센터에서 사례 열기를 클릭하여 AMS 서비스 유형으로 자동 채워진 지원 센터에서 사례 생성 페이지를 엽니다.

   Accelerate 운영 팀에서 보고된 인시던트 또는 서비스 요청 사례를 업데이트하면 대응이 가능하도록 지원 센터에서 인시던트에 대한 이메일과 링크를 받게 됩니다.

   > **Note**
   >
   > 이메일에 회신하여 사례 대응 서신에 응답할 수 없습니다.

   대시보드에 사례가 많은 경우 필터 옵션을 사용할 수 있습니다.

   - 제목:이 필터를 사용하여 사례 제목의 키워드를 검색합니다.
   - 심각도: 목록에서 심각도를 선택하여 심각도별로 사례를 필터링하는 데 사용합니다.
   - 사례 유형: 특정 사례 유형의 모든 사례를 보려면이 옵션을 사용합니다. 가속화 인시던트 및 서비스 요청은 서비스별 사례와 함께 기술 지원 사례 유형 아래에 표시됩니다.
   - 상태: 목록에서 특정 상태를 선택하여 상태별로 사례를 필터링하는 데 사용합니다.
3. 최신 상태를 확인하려면 페이지를 새로 고칩니다.
4. 모든 서신이 페이지에 표시되지 않는 서신이 너무 많으면 더 보기를 선택합니다.
5. 사례 상태를 업데이트하려면 회신을 선택하고 새 서신을 입력한 다음 제출을 선택합니다.
6. 만족스럽게 해결된 후 사례를 종료하려면 사례 종료를 선택합니다.

   AMS에 진행 상황을 알리려면 별점 1~5점을 기준으로 서비스를 평가해야 합니다.

지원 API를 사용하여 Accelerate 인시던트 관리

지원 API를 사용하여 인시던트를 생성하고 문제에 대한 조사 중에 지원 직원과 서신을 추가할 수 있습니다. 지원 API는 AWS 지원 센터의 대부분의 동작을 모델링합니다.

이 AWS 지원 서비스를 사용할 수 있는 방법에 대한 자세한 내용은 AWS 지원 사례의 수명 프로그래밍을 참조하세요.

> **Note**
>
> AMS Accelerate 팀은 서비스 코드와 함께를 사용하여 사용자가 생성한 인시던트를 프로그래밍 방식으로 수신합니다`service-ams-operations-report-incident`.

AMS Accelerate 생성 인시던트에 대응

AMS Accelerate는 리소스를 사전에 모니터링합니다. 자세한 정보는 AMS Accelerate의 모니터링 및 이벤트 관리을 참조하십시오. AMS Accelerate가 인시던트를 식별하고 생성하는 경우가 있으며, 가장 자주 이벤트를 알립니다. 인시던트를 해결하기 위해 사용자 측의 조치가 필요한 경우 AMS Accelerate 팀이 계정에 제공한 연락처 정보로 알림을 보냅니다. 일반적으로 지원 센터를 통해 다른 인시던트와 동일한 방식으로이 알림에 응답하지만 경우에 따라 이메일 또는 전화를 통해 문의해야 합니다.

> **Important**
>
> 인시던트 사례 또는 서비스 요청에 대한 상태 변경 알림을 받으려면 주소 필드에 이메일 주소를 입력합니다.

Akshay의 비디오를 보고 자세히 알아보기(4:15)

Accelerate의 서비스 요청 관리

주제

- Accelerate에 대한 서비스 요청을 사용해야 하는 경우
- Accelerate에서 서비스 요청 관리 작동 방식
- Accelerate에서 서비스 요청 생성
- Accelerate에 대한 서비스 요청 모니터링 및 업데이트

- Accelerate용 지원 API를 사용하여 서비스 요청 관리
- AMS Accelerate에서 생성한 서비스 요청에 응답

AMS Accelerate는 서비스 요청 관리를 사용하여 활성 서비스 요청을 기록하고, 조치를 취하고, 진행 상황을 전달하고, 알림을 제공합니다.

서비스 요청 관리 프로세스의 목표는 관리형 서비스가 필요한 것을 제공하는지 확인하는 것입니다.

결제 관련 쿼리의 경우 서비스 요청을 생성합니다.

> **Note**
>
> AMS Accelerate 팀은 서비스 코드와 함께 AWS Support API를 사용하여 사용자가 생성한 서비스 요청을 프로그래밍 방식으로 수신합니다`service-ams-operations-service-request`.

AWS 지원 센터를 사용하여 다음 작업을 수행할 수 있습니다.

- 서비스 요청을 보고하고 업데이트합니다. AMS Accelerate 서비스 요청을 하려면 서비스 메뉴에서 AMS 작업 -- 서비스 요청을 선택합니다.
- 제출된 모든 서비스 요청의 목록과 세부 정보를 가져옵니다.
- 상태 및 기타 필터별로 서비스 요청 검색 범위를 좁힙니다.
- 요청에 커뮤니케이션 및 파일 첨부 파일을 추가하고 사례 대응을 위해 이메일 수신자를 추가합니다.
- 서비스 요청을 해결합니다.
- 서비스 요청 통신을 평가합니다.

Accelerate에 대한 서비스 요청을 사용해야 하는 경우

다음 예제에서는 서비스 요청을 설명합니다. 서비스 요청을 제출한 후 AMS Accelerate 팀은 사용자와 협력하여 AMS SLA에 따라 요청을 해결합니다.

- AMS 또는 AWS 일반 지침
- 패치 MW 관련 질문
- 백업 일정 관련 질문
- AWS 서비스 기능에 대한 질문

다음은 서비스 요청에서 발생해서는 안 되는 사항의 예입니다.

- 액세스 문제
- 패치 실패
- 백업 실패

Accelerate에서 서비스 요청 관리 작동 방식

서비스 요청은 대기 중인 AMS Accelerate 운영 팀에서 처리합니다.

AMS Accelerate 운영 팀에서 서비스 요청을 수신한 후 서비스 요청이 서비스 요청 또는 인시던트로 올바르게 분류되었는지 검토합니다. 인시던트로 재분류되면 AMS Accelerate 인시던트 관리 프로세스가 시작되고 알림이 전송됩니다.

AMS Accelerate 운영자가 서비스 요청을 해결할 수 있는 경우 이를 위한 단계가 즉시 수행됩니다. 예를 들어 서비스 요청이 아키텍처 조언 또는 기타 정보용인 경우 운영자는 적절한 리소스를 참조하거나 질문에 직접 답변합니다.

서비스 요청 분석에서 버그 또는 기능 요청이 식별되면 AMS는 서비스 요청을 통해 알림을 보냅니다. 기능 요청 또는 버그 수정에 대한 ETA가 없으므로 원래 서비스 요청이 종료됩니다. 원래 서비스 요청과 관련된 후속 질문은 CSDM에 문의하십시오.

서비스 요청이 AMS Accelerate 작업 범위를 벗어나는 경우 운영자는 요청을 클라우드 서비스 제공 관리자에게 전송하여 진행 중인 단계에 대한 이메일과 함께 사용자 또는 적절한 AWS 지원 팀과 통신할 수 있도록 합니다.

결과에 만족한다고 표시할 때까지 서비스 요청은 해결되지 않습니다.

> **Note**
>
> 원활한 커뮤니케이션을 위해 모든 경우에 연락처 이메일, 이름 및 전화번호를 제공하는 것이 좋습니다.

Accelerate에서 서비스 요청 생성

서비스 요청을 생성하려면 다음 단계를 따릅니다.

1. AMS Accelerate 콘솔에서 대시보드로 이동합니다.

2. 서비스 요청 열기를 선택하면 AMS - 서비스 요청이 미리 선택됩니다.
3. aCategory를 선택합니다.
4. 심각도를 선택합니다(Plus 또는 Premium 티어만 해당).
5. 다음에 대한 정보를 입력합니다.

   - 제목: 서비스 요청에 대한 설명 제목입니다.
   - 설명: 서비스 요청, 영향을 받는 시스템 및 해결의 예상 결과에 대한 포괄적인 설명입니다.
6. 첨부 파일을 추가하려면 파일 연결을 선택하고 원하는 첨부 파일로 이동한 다음 열기를 선택합니다. 첨부 파일을 삭제하려면 삭제 아이콘을 선택합니다.
7. 문의처: 웹을 통한 기본 연락처 AMS입니다. 다른 옵션을 선택하려면:

   - 선호하는 연락 언어: 영어는 AMS Accelerate 서비스 요청에 지원되는 언어입니다.
   - 웹: 서비스 요청은 웹을 통해 제출되고 AMS 운영 팀에서 처리합니다.
   - 채팅: AMS Accelerate 운영 담당자와 온라인으로 채팅합니다. 이 옵션은 채팅 대기열에 사용자를 추가합니다.
   - 전화: AMS 작업 담당자가 다시 전화를 겁니다. 해당하는 경우 AWS 리전, 전화번호 및 확장을 입력합니다.
   - 추가 연락처: 서비스 요청에 복사하려는 추가 이메일 주소를 입력합니다.
8. 제출을 선택합니다.

   Type,Subject,Created, ID 및Status와 같은 서비스 요청에 대한 정보가 포함된 사례 세부 정보 페이지가 열립니다. 또한 생성한 요청에 대한 설명이 포함된 aCorrespondencearea입니다.

   대응 영역을 열고 상태에 추가 세부 정보 또는 업데이트를 제공하려면 회신을 선택합니다.

   서비스 요청이 해결된 후 사례 해결을 선택합니다.

   모든 서신이 페이지에 표시되지 않는 서신이 너무 많으면 더 보기를 선택합니다.

   AMS에 진행 상황을 알리려면 별점 1~5점을 통해 서비스를 평가해야 합니다.

> **Note**
>
> 서비스 요청 기능을 테스트하려는 경우와 같이 서비스 요청의 제목에 작업 없음 플래그를 추가하는 것이 좋습니다`AMSTestNoOpsActionRequired`. 그런 다음 서비스 요청 해결 프로세스를 시작하지 않고 테스트할 수 있습니다.

AMS Accelerate 팀은 서비스 코드와 함께 AWS Support API를 사용하여 사용자가 생성한 서비스 요청을 프로그래밍 방식으로 수신합니다`service-ams-operations-service-request`.

Accelerate에 대한 서비스 요청 모니터링 및 업데이트

지원 Center를 사용하여 사례, 인시던트 또는 서비스 요청을 모니터링하려면 다음 단계를 따릅니다.

1. AWS 관리 콘솔에서 지원을 찾습니다.
2. 왼쪽 탐색에서 지원 사례를 선택하고 사례로 이동한 다음 Subjectlink를 선택하여 현재 상태 및 서신이 포함된 세부 정보 페이지를 엽니다.

   이 시점에서 전화 또는 채팅을 사용하려면 지원 센터에서 사례 열기를 클릭하여 AMS 서비스 유형으로 자동 채워진 지원 센터에서 사례 생성 페이지를 엽니다.

   Accelerate 운영 팀이 보고된 인시던트 또는 서비스 요청 사례를 업데이트하면 대응이 가능하도록 지원 센터에서 인시던트에 대한 이메일과 링크를 받게 됩니다.

   > **Note**
   >
   > 이메일에 회신하여 사례 대응 서신에 응답할 수 없습니다.

   대시보드에 사례가 많은 경우 필터 옵션을 사용할 수 있습니다.

   - 제목:이 필터를 사용하여 사례 제목의 키워드를 검색합니다.
   - 심각도: 목록에서 심각도를 선택하여 심각도별로 사례를 필터링하는 데 사용합니다.
   - 사례 유형: 특정 사례 유형의 모든 사례를 보려면이 옵션을 사용합니다. 가속화 인시던트 및 서비스 요청은 서비스별 사례와 함께 기술 지원 사례 유형 아래에 표시됩니다.
   - 상태: 목록에서 특정 상태를 선택하여 상태별로 사례를 필터링하는 데 사용합니다.
3. 최신 상태를 확인하려면 페이지를 새로 고칩니다.
4. 모든 서신이 페이지에 표시되지 않는 서신이 너무 많으면 더 보기를 선택합니다.
5. 사례 상태를 업데이트하려면 회신을 선택하고 새 서신을 입력한 다음 제출을 선택합니다.
6. 만족스럽게 해결된 후 사례를 종료하려면 사례 종료를 선택합니다.

   AMS에 진행 상황을 알리려면 별점 1~5점을 통해 서비스를 평가해야 합니다.

Accelerate용 지원 API를 사용하여 서비스 요청 관리

AWS Support API를 사용하여 문제 조사 및 AWS 지원 담당자와의 상호 작용 전반에 걸쳐 서비스 요청을 생성하고 이에 대한 서신을 추가할 수 있습니다. AWS 지원 API는 AWS 지원 센터의 대부분의 동작을 모델링합니다.

또한 AMS 팀은 서비스 코드 serviceservice-ams-operations-service-request.

이 AWS 지원 서비스를 사용하는 방법에 대한 자세한 내용은 AWS 지원 사례의 수명 프로그래밍을 참조 하세요.

AMS Accelerate에서 생성한 서비스 요청에 응답

AMS Accelerate는 리소스를 사전에 모니터링합니다. 자세한 내용은 섹션을 참조하세요AMS Accelerate의 모니터링 및 이벤트 관리. 일반적으로 서비스 요청을 해결하기 위해 사용자 측의 조치가 필요한 경우 AMS Accelerate가 서비스 요청 또는 서비스 알림을 생성하는 경우가 있습니다. 이 경우 AMS Accelerate 팀은 계정에 제공한 연락처로 알림을 보냅니다. 일반적으로 지원 센터를 통해 다른 경우와 동일한 방식으로이 서비스 요청에 응답하지만 경우에 따라 이메일 또는 전화 통신이 필요합니다.

> **Important**
>
> 서비스 요청 또는 인시던트 사례에 대한 상태 변경 알림을 받으려면 주소 필드에 이메일 주소를 입력해야 합니다. 알림은 생성 시 사례에 추가된 이메일 주소로만 전송됩니다.

알림 이메일의 링크는 AMS Accelerate 페더레이션 네트워크에서 이메일 서버를 사용하는 경우에만 작동합니다. 그렇지 않으면 AMS Accelerate 콘솔로 이동하여 사례 세부 정보 페이지를 사용하여 서신에 응답할 수 있습니다.

> **Note**
>
> AMS Accelerate는 AWS 계정의 기본 이메일 주소로 통신을 전송합니다. 서비스 요청/알림 관리 프로세스를 용이하게 하기 위해 대체 작업 연락처 이메일 별칭을 추가하는 것이 좋습니다. 이는 AMS Accelerate 온보딩 프로세스 및 관련 온보딩 설명서에서 다룹니다.

Accelerate의 인시던트 보고서 및 서비스 요청 테스트

인시던트 보고서 또는 서비스 요청을 테스트할 때는 제목 텍스트에 AMSTestNoOpsActionRequired를 포함해야 합니다. 이를 통해 AMS는 인시던트 또는 요청이 테스트용임을 알 수 있습니다. AMS 운영 엔지니어는 이를 볼 때 어떤 식으로도 응답하지 않습니다.

AMS Accelerate에 대한 결제 질문

결제 관련 질문을 제출하려면 다음 단계를 완료하세요.

1. https://console.aws.amazon.com/support/home AWS Support 센터를 엽니다.
2. 계정 및 결제를 선택합니다.
3. 사례 생성을 선택합니다.
4. 계정 및 결제를 선택한 다음 프롬프트에 따라 사례를 제출합니다.

AWS Managed Services의 계획된 이벤트 관리

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

AMS PEM 기준

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

PEM 유형

사용 가능한 PEM 유형은 다음과 같습니다.

- 게임데이
  - 운영 게임데이: 프로세스, 사람 및 시스템의 통합을 검증하는 것을 목표로 운영 대응에 대한 시나리오 기반 게임 접근 방식입니다.
  - Security Gameday: 시나리오 기반 게임 접근 방식을 사용하여 시스템, 프로세스 및 인력의 통합을 평가하는 보안 인시던트 대응 전략입니다.
- 고객 보안 이벤트: 계획된 보안 이벤트. 예를 들어 침투 테스트입니다.
- 마이그레이션 지원: 계획된 온보딩 및 마이그레이션 활동을 지원합니다.

이 워크플로는 AMS 지원과 관련하여 계획된 이벤트 및 마이그레이션 활동을 조정하기 위해 AMS와의 협업을 용이하게 합니다. 특정 요구 사항에 대한 도움이 필요하면 CSDM에 문의하십시오.

AMS PEM 프로세스

PEM 프로세스는 다음 단계로 구성됩니다.

- PEM 시작: CSDM과 협력하여 계획된 이벤트에 대한 목표를 정의하고 AMS 작업에 필요한 사항을 결정합니다. AMS CAs PEM 계획의 기술적 측면을 검토합니다. CAs는 AMS 보안 및 운영 부서와 협

력하여 규정 준수, 실행 최적화 및 자동화를 수행하고 사전 PEM 실행 작업 및 결과물을 정의합니다. 그런 다음 CSDM이 PEM 티켓을 생성하고 AMS에 프로젝트 정보와 기술 세부 정보를 제공합니다. AMS 운영 팀이 리소스를 계획하고, 기술 검토를 제공하고, 할당하는 데 걸리는 리드 타임은 14일입니다.

- PEM 검토: AMS 운영 팀이 PEM 요청을 검토하고 CSDM과 협력하여 PEM 계획의 정보가 정확하고 완전한지 확인합니다.
- PEM 수락: AMS는 제공된 정보를 검토하고 PEM 활동 중에 지원 수준이 무엇인지 CSDM에 전달합니다. PEM에 전체 정보가 포함되어 있고 CSDM이 작업 범위에 동의하는 경우 PEM이 승인됩니다.
- 준비 및 실행: AMS는 PEM이 시작되기 전에 필요한 작업이 완료되었는지 확인하고 내부 및 고객 커뮤니케이션을 용이하게 합니다. AMS는 PEM 계획이 올바르게 실행되고 상태 및 진행 상황 보고를 제공하는지 확인합니다.

PEM FAQs

PEM 이벤트 중에 사례: 서비스 요청(SRs)/사고를 통해 AMS를 참여시키려면 어떻게 해야 합니까?

- 형식의 RFC/SR 제목 줄에서 CSDM이 공유하는 PEM ID를 사용합니다*PEM-ID*.

  해당하는 경우 라이브 연락처 옵션을 사용할 수 있습니다.
- 서비스 요청(SR)을 생성하여 사용 사례를 논의하거나 계획된 이벤트에 대한 질문을 할 수도 있습니다. SR을 사용하는 경우 PEM이 유효하지 않아도 됩니다.

PEM 관련 사례가 제출되면 어떤 검증이 수행되나요?

- 계정 ID가 PEM에 나열되어 있는지 확인합니다.
- 제공된 시작일과 종료일 사이에 PEM 상태가 승인되고 활성 상태인지 확인합니다.
- PEM 세부 정보에 대한 링크는 내부적으로 AMS 엔지니어에게 제공됩니다.

PEM 요청에 대한 SLAs 또는 SLOs 있습니까?

- PEMs은 SLAs 또는 SLOs와 연결되지 않습니다.
- PEM 관련 작업 항목(서비스 요청, 인시던트)에 SLOs 대한 SLAs 및 SLO는 AMS SLOs에서 정의합니다.

  자세한 내용은 AMS Accelerate의 인시던트 보고서, 서비스 요청 및 결제 질문을 참조하세요.

서비스 요청(SR)을 통해 PEM을 생성할 수 있나요?

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

온디맨드 작업

OOD(Otions on Demand)는 현재 AMS 운영 계획 또는에서 기본적으로 제공하지 않는 운영 서비스를 제공하여 AMS 운영 계획의 표준 범위를 확장하는 AWS Managed Services(AMS) 기능입니다 AWS. https://aws.amazon.com/managed-services/features/ 선택하면 자동화와 고도로 숙련된 AMS 리소스의 조합으로 카탈로그 오퍼링이 제공됩니다. 장기 약정이나 추가 계약이 없으므로 필요에 따라 기존 AMS와 AWS 운영 및 기능을 확장할 수 있습니다. 사용자는 매월 블록당 20시간의 시간 블록(OOD 블록)을 구매하는 데 동의합니다.

표준화된 상품 카탈로그에서 선택하고 서비스 요청을 통해 새 OOD 참여를 시작할 수 있습니다. OOD 상품의 예로는 Amazon EKS 유지 관리, SAP 클러스터 운영 AWS Control Tower및 관리 지원이 있습니다. 새로운 카탈로그 상품은 수요와 가장 자주 볼 수 있는 운영 사용 사례에 따라 정기적으로 추가됩니다.

OOD는 AMS Advanced 및 AMS Accelerate 운영 계획 모두에 사용할 수 있으며 AMS를 사용할 수 AWS 리전 있는 모든에서 사용할 수 있습니다.

AMS는 요청된 변경 사항을 구현하는 동안 고객 보안 위험 관리(CSRM)를 수행합니다. CSRM 프로세스에 대한 자세한 내용은 변경 요청 보안 검토를 참조하세요.

오퍼링의 온디맨드 작업 카탈로그

OOD(Otions on Demand)는 다음 표에 설명된 서비스를 제공합니다.

> **Note**
>
> 키 용어에 대한 정의는 AWS Managed Services 설명서 키 용어를 참조하세요.

운영 계획	제목	설명	예상 결과
AMS Advanced 및 AMS Accelerate	Amazon EKS 클러스터 유지 관리	AMS는 Amazon Elastic Kubernetes Service(Amazon EKS) 배포의 지속적인 유지 관리를 처리하여 컨테이너 개발자를 확보합니다. AMS는 컨트롤 플레인, 추가 기능 및 노드의 구성 요소를 처리하는 클러스터를 업데이트하는 데 필요한 end-to-en	고객 팀은 Amazon EKS 클러스터 업데이트의 기본 작업을 지원했습니다.

		d 절차를 수행합니다. AMS는 관리형 노드 유형과 큐레이션된 Amazon EKS 및 Kubernetes 추가 기능에 대한 업데이트를 수행합니다.	
AMS Accelerate	AMI 구축 및 판매	AMS는 고객을 위한 AMI 구축 및 판매를 지속적으로 관리합니다. 엔지니어는 구독한 AMIs의 월간 릴리스를 수행하고, 긴급 패치 작업에 대한 온디맨드 AMIs를 릴리스하고, 실행서를 사용하여 변경 사항을 관리하고, CloudWatch Monitoring을 사용하여 AMI 빌드를 모니터링합니다. 또한 지정된 계정에서 사용되는 모든 AMIs에 대한 문제 해결 지원 및 자세한 보고를 제공합니다. 이 서비스를 사용하려면 EC2 이미지 빌더를 통해 AMI 빌드 파이프라인을 배포해야 합니다. AMS는 EC2 Image 빌더와 상호 작용하는 다른 자동화 또는 서비스를 지원하지 않습니다.	고객 보안 태세가 개선되고 AMIs 단축되었습니다.

AMS Accelerate	큐레이션된 변경 실행	숙련된 운영 엔지니어와 협력하여 비즈니스 요구 사항을 AWS 환경 내에서 안전하게 실행할 수 있는 검증된 변경 요청으로 변환합니다. 자동화에 대한 고유한 접근 방식과 운영 모범 사례(예: 영향 평가, 롤백, 2인 규칙)에 대한 지식을 활용합니다. 이는 규모에 따른 간단한 변경이든 다운스트림 영향이 있는 복잡한 작업이든 상관없습니다.	고객은 사용자 지정 변경 요청의 정의, 생성 및 실행을 지원했습니다. 변경 사항은 수동 또는 자동(CloudFormation, SSM)일 수 있습니다. 필요한 경우 구성 지침에 지원 대한 와의 상담을 포함합니다. 애플리케이션 코드, 애플리케이션 설치/배포, 데이터 마이그레이션 또는 OS 구성 변경을 위한 것이 아닙니다.
AMS Accelerate	AWS Network Firewall 운영	AMS는 고객과 협력하여 방화벽을 온보딩하고 지속적인 방화벽 작업에 대한 정책 및 규칙을 구현하고 관리합니다. 엔지니어는 운영 모범 사례와 자동화를 활용하여 표준화된 정책 및 규칙을 구성하고 모니터링을 활성화하여 자동화 프로세스 외부에서 이루어진 변경 사항을 감지함으로써 이를 수행합니다. AMS는 원치 않는 변경 사항을 신속하게 알리고 요청 시 이를 포함하거나 이전 구성으로 계정을 복원하여 시스템의 전반적인 안정성을 보장할 수 있는 옵션을 제공합니다.	고객 팀은 의도하지 않은 네트워크 방화벽 변경을 신속하게 감지하여 관리 오버헤드를 줄이는 데 도움을 주었으며, 이로 인해 인시던트 해결이 개선되고 예상 및 예상치 못한 문제에 대한 근본 원인 분석 시간이 단축되었습니다.

AMS Accelerate	AWS Control Tower 작업	AWS Transit Gateway 및를 포함한 AWS Control Tower 랜딩 존의 지속적인 운영 및 관리 AWS Organizations - 포괄적인 랜딩 존 솔루션을 제공합니다. 사용자 지정 제어 및 가드레일 라이브러리를 사용하여 계정 벤딩, SCP 및 OU 관리, 드리프트 문제 해결, SSO 사용자 관리 및 AWS Control Tower 업그레이드를 처리합니다.	고객 팀은 일부 기본 운영 작업인 AWS Control Tower, AWS Transit Gateway 및 관리를 지원했습니다 AWS Organizations.
AMS Accelerate	AWS 랜딩 존 Accelerate 작업	AMS는 AWS Landing Zone Accelerator(LZA)를 통해 배포된 AWS 랜딩 존의 지속적인 작업을 제공합니다. 엔지니어는 구성 파일 변경, AWS Control Tower (CT) 환경 관리(계정 벤딩, OU 생성, CT 가드레일), 서비스 제어 정책(SCP) 관리, CT 드리프트 감지 및 수정, 네트워크 구성 관리, CT 및 LZA 프레임워크 업데이트 등을 처리합니다. AWS LZA는와 같은 운영 모범 사례와 서비스를 사용하여 안전한 다중 계정 AWS 환경을 설정하고 관리할 수 있는 수단을 제공합니다 AWS Control Tower.	고객 팀은 AWS Landing Zone Accelerator 솔루션의 지속적인 운영 및 관리를 지원했습니다.
AMS Accelerate	SAP 클러스터 지원	SAP 클러스터에 대한 전용 경보, 모니터링, 클러스터 패치 적용, 백업 및 인시던트 수정. 이 카탈로그 항목을 사용하면 SAP 운영 팀에서 진행 중인 운영 작업 중 일부를 오프로드하여 용량 관리 및 성능 튜닝에 집중할 수 있습니다.	고객 또는 파트너 SAP 팀이 일부 기본 작업을 지원했습니다. 여전히 고객은 용량 관리, 성능 튜닝, DBA 및 SAP 기본 관리와 같은 다른 SAP 기능을 제공해야 합니다.

AMS 고급	우선 순위 RFC 실행	지정된 AMS 운영 엔지니어 용량은 변경 요청(RFC) 실행의 우선순위를 정합니다. 모든 제출은 더 높은 수준의 응답을 받으며 Amazon Chime 회의실을 통해 엔지니어와 직접 상호 작용하여 우선 순위 순서를 조정할 수 있습니다.	고객은 RFCs에 대해 8시간의 응답 SLO를 받습니다.

AMS Advanced 및 AMS Accelerate	레거시 OS 업그레이드	지원되는 운영 체제 버전으로 인스턴스를 업그레이드하여 인스턴스 마이그레이션을 방지합니다. 선택한 인스턴스에서 소프트웨어 공급업체의 자동화 및 업그레이드 기능을 활용하여 현재 위치 업그레이드를 수행할 수 있습니다(예: Microsoft Windows 2008 R2에서 Microsoft Windows 2012 R2로). 이 접근 방식은 새 인스턴스에 쉽게 다시 설치할 수 없는 레거시 애플리케이션에 이상적이며 이전 OS 버전에서 알려진 보안 위협과 완화되지 않은 보안 위협으로부터 추가 보호를 제공합니다. 현재 위치 업그레이드에는 다음 운영 체제가 지원됩니다. • Microsoft Windows 2012 R2에서 Microsoft Windows 2016 이상으로 • Microsoft Windows 2016에서 Microsoft Windows 2022 이상으로 • Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로 • Red Hat Enterprise Linux 8에서 Red Hat Enterprise Linux 9로 • Oracle Linux 7에서 Oracle Linux 8로	이 솔루션은 새 인스턴스에 더 이상 다시 설치할 수 없는 애플리케이션(예: 소스 코드 손실, ISV 업무 중단 등)에 제공됩니다. 실패한 업그레이드를 원래 상태로 롤백할 수 있습니다. 운영 관점에서 롤백을 사용하는 것이 좋습니다. 최신 보안 패치를 사용하면 인스턴스가 더 지원 가능한 상태로 전환되기 때문입니다.

주제

- 온디맨드 AMS 작업 요청
- Operations on Demand 오퍼링 변경

온디맨드 AMS 작업 요청

AWS Managed Services(AMS) OOD(Otions on Demand)는 AMS에 온보딩된 모든 AWS 계정 에서 사용할 수 있습니다. Operations on Demand를 활용하려면 클라우드 서비스 제공 관리자(CSDM), 솔루션 아키텍트(SA), 계정 관리자 또는 클라우드 아키텍트(CA)에 추가 정보를 요청합니다. 사용 가능한 OOD 오퍼링은 위의 오퍼링 테이블의 Operations on Demand 카탈로그에 나열되어 있습니다. 참여 범위 조정이 완료되면 AMS Operations에 서비스 요청을 제출하여 OOD에 대한 참여를 시작합니다.

각 OOD 서비스 요청에는 참여와 관련된 다음과 같은 세부 정보가 포함되어야 합니다.

- 요청된 특정 OOD 제품 및 각 특정 OOD 제품:
  - 특정 OOD 상품에 할당할 블록 수(블럭 1개는 해당 역월의 운영 리소스 시간 20시간과 동일하며, 해당 Operations on Demand 상품에 대해 AWS당시의 표준 요금으로 청구됨)입니다.
  - 특정 OOD 오퍼링이 요청되는 각 AWS Managed Services 계정의 계정 ID입니다.

OOD 서비스 요청은 다음 중 하나를 통해 제출해야 합니다.

- 해당 Operations on Demand 오퍼링을 수신하는 AWS Managed Services 계정 또는
- AWS Managed Services 계정인 멤버 계정을 대신하여 모든 기능 모드의 AWS Organizations 관리 계정인 AWS Managed Services 계정입니다.

OOD 서비스 요청이 수신되면 AMS Operations는 승인, 부분 승인 또는 거부로 계정을 검토하고 업데이트합니다.

OOD 오퍼링 서비스 요청이 승인되면 AMS와 사용자가 계약을 시작하도록 조정합니다. 서비스 요청이 승인되고 참여 시작 날짜가 합의될 때까지 OOD 오퍼링이 시작되지 않습니다.

AMS는 OOD 블록의 월별 구독 할당을 사용합니다. 새 서비스 요청을 통해 옵트아웃을 요청할 때까지 계약 시작 날짜부터 매월 승인된 블록 수를 할당합니다. OOD 블록은 한 달 동안 유효합니다. 미사용 블록 또는 블록 부분은 롤오버되거나 향후 달로 이월되지 않습니다.

실제로 사용한 시간에 관계없이 매월 최소 1개의 OOD 블록이 청구됩니다. 사용한 시간이 없는 추가 할당된 OOD 블록에는 요금이 청구되지 않습니다.

Operations on Demand 오퍼링 변경

OOD(Otions on Demand) 오퍼링에 대한 지속적인 참여 변경을 요청하려면 다음 정보가 포함된 서비스 요청을 제출합니다.

- 요청 중인 수정(들) 및
- 수정 사항이 적용되는 요청 날짜입니다.

OOD 서비스 요청을 수신한 후 AMS Operations는 요청을 검토하고 승인 또는 할당된 CSDM이 사용자와 협력하여 수정의 범위와 영향을 결정하는 요청으로 업데이트합니다. 수정에 CSDM의 범위 조정 작업이 필요하다고 판단되면 범위 조정 연습이 완료된 후 수정된 참여를 시작하기 위해 두 번째 OOD 서비스 요청을 제출해야 합니다.

승인되면 가장 최근에 수정된 블록 할당은 활성 상태가 되고 계속 활성 상태로 유지되며, AWS 와 사용자가 달리 합의하지 않는 한 이전 블록 할당을 대체합니다.

보고서 및 옵션

AWS Managed Services(AMS)는 다양한 네이티브 AWS 서비스의 데이터를 수집하여 주요 AMS 제품에 대한 부가가치 보고서를 제공합니다.

AMS는 두 가지 유형의 세부 보고를 제공합니다.

- 요청 보고서: Cloud Service Delivery Manager(CSDM)를 통해 특정 보고서를 임시로 요청할 수 있습니다. 온보딩 또는 중요한 이벤트 중에 보고서를 여러 번 요청해야 할 수 있으므로 이러한 보고서에는 제한이 없습니다. 그러나 이러한 보고서는 주간 보고서와 같은 일정에 따라 제공되도록 설계되지 않았습니다. 요구 사항을 더 잘 이해하거나 셀프 서비스 보고 사용에 대한 자세한 내용은 CSDM에 문의하십시오.
- 셀프 서비스 보고서: AMS 셀프 서비스 보고서를 사용하면 필요한 만큼 자주 데이터를 직접 쿼리하고 분석할 수 있습니다. 셀프 서비스 보고서를 사용하여 AMS 콘솔에서 보고서에 액세스하고 S3 버킷(계정당 버킷 1개)을 통해 데이터 세트를 보고합니다. 이를 통해 원하는 비즈니스 인텔리전스(BI) 도구에 데이터를 통합하여 요구 사항에 맞게 보고서를 사용자 지정할 수 있습니다.

주제

- 요청 시 보고서
- 셀프 서비스 보고서

요청 시 보고서

주제

- AMS 호스트 관리 보고서
- AMS 백업 보고서
- AWS Config 제어 규정 준수 보고서
- AMS Config 규칙 응답 구성 보고서
- 인시던트 방지 및 상위 화자 보고서 모니터링
- 결제 요금 세부 정보 보고서
- 신뢰할 수 있는 수정자 보고서

AMS는 다양한 네이티브 AWS 서비스의 데이터를 수집하여 주요 AMS 제품에 대한 부가가치 보고서를 제공합니다. 이러한 보고서의 사본을 보려면 Cloud Service Delivery Manager(CSDM)에 요청합니다.

AMS 호스트 관리 보고서

사용 가능한 보고서

- SSM 에이전트 담당률 보고서

SSM 에이전트 담당률 보고서

AMS SSM 에이전트 적용 범위 보고서는 계정의 EC2 인스턴스에 SSM 에이전트가 설치되어 있는지 여부를 알려줍니다.

필드 이름	정의
고객 이름	하위 고객이 여러 명 있는 상황의 고객 이름
리소스 리전	AWS 리소스가 위치한 리전
계정 이름	계정의 이름입니다.
AWS 계정 ID	AWS 계정의 ID
Resource Id	EC2 인스턴스의 ID
Resource Name	EC2 인스턴스의 이름
규정 준수 플래그	리소스에 SSM 에이전트가 설치되어 있는지("규정 준수") 또는 설치되어 있지 않은지("NON_COMPLIANT") 나타냅니다.

AMS 백업 보고서

사용 가능한 보고서

- 백업 작업 성공/실패 보고서
- 백업 요약 보고서
- 백업 요약/보장 보고서

백업 작업 성공/실패 보고서

백업 작업 성공/실패 보고서는 지난 몇 주 동안 실행된 백업에 대한 정보를 제공합니다. 보고서를 사용자 지정하려면 데이터를 검색할 주 수를 지정합니다. 기본 주 수는 12입니다. 다음 표에는 보고서에 포함된 데이터가 나열되어 있습니다.

필드 이름	정의
AWS 계정 ID	리소스가 속한 AWS 계정 ID
계정 이름	AWS 계정 이름
백업 작업 ID	백업 작업의 ID
리소스 ID	백업된 리소스의 ID
리소스 유형	백업 중인 리소스 유형
리소스 리전	백업된 리소스의 AWS 리전
백업 상태	백업의 상태입니다. 자세한 내용은 백업 작업 상태를 참조하세요.
복구 시점 ID	복구 시점의 고유 식별자입니다.
상태 메시지	백업 작업 중에 발생한 오류 또는 경고에 대한 설명
백업 크기	GB 단위의 백업 크기
복구 시점 ARN	생성된 백업의 ARN
일 단위의 복구 시점 기간	복구 시점이 생성된 이후 경과한 일수
30일 미만	30일 미만의 백업 지표

백업 요약 보고서

필드 이름	정의
고객 이름	여러 하위 고객이 인 상황의 고객 이름
백업 월	백업 월
백업 연도	백업 연도
리소스 유형	백업 중인 리소스 유형
리소스 수	백업된 리소스 수
복구 시점 수	고유한 스냅샷 수
30일 미만의 백업	30일 미만의 백업 수
최대 복구 시점 수명	일 단위의 가장 오래된 복구 시점 수명
최소 복구 시점 수명	일 단위의 가장 최근 복구 시점 기간

백업 요약/보장 보고서

백업 요약/보장 보고서에는 현재 어떤 AWS Backup 계획으로도 보호되지 않는 리소스 수가 나열됩니다. 가능한 경우 적용 범위를 늘리고 데이터 손실 위험을 줄이기 위한 적절한 계획을 CDSM과 논의합니다.

필드 이름	정의
고객 이름	여러 하위 고객이 인 상황의 고객 이름
리전	AWS 리소스가 위치한 리전
계정 이름	계정의 이름입니다.
AWS 계정 ID	AWS 계정의 ID

필드 이름	정의
리소스 유형	리소스의 유형입니다. 리소스는 AWS Backup (Aurora, DocumentDB, DynamoDB, EBS, EC2, EFS, FSx, RDS 및 S3)에서 지원됩니다.
리소스 ARN	리소스의 ARN
리소스 ID	리소스의 ID
충당률	리소스가 포함되는지 여부를 나타냅니다("COVERED" 또는 "NOT_COVERED").
리소스 수	계정에서 지원되는 리소스 수
perc_coverage	지난 30일 동안 실행된 백업이 있는 지원되는 리소스의 백분율입니다.

AWS Config 제어 규정 준수 보고서

AWS Config 제어 규정 준수 보고서는 AMS 계정의 리소스 및 AWS Config 규칙 규정 준수를 심층적으로 살펴봅니다. Config 규칙 심각도를 기준으로 보고서를 필터링하여 가장 중요한 조사 결과의 우선순위를 지정합니다. 다음 표에는이 보고서에서 제공하는 데이터가 나열되어 있습니다.

필드	설명
날짜	보고서 날짜
고객 이름	고객 이름
AWS 계정 ID	고객의 연결된 AWS 계정 ID
소스 식별자	AWS Config 규칙 고유 소스 식별자
규칙 설명	AWS Config 규칙 설명
규칙 유형	AWS Config 규칙 유형
규정 준수 플래그	AWS Config 규칙 규정 준수 상태

필드	설명
리소스 유형	AWS 리소스 유형
Resource Name	AWS 리소스 이름
심각도	AWS Config 규칙에 대해 AMS에서 정의한 기본 권장 심각도
문제 해결 범주	AWS Config 규칙에 연결된 문제 해결 응답 범주
문제 해결 설명	AWS Config 규칙을 준수하도록 하기 위한 해결 작업 설명
고객 작업	AWS Config 규칙을 준수하는 데 필요한 고객 작업
델타 지표 보고서	지정된 두 날짜 사이의 규칙 준수에 대한 변경 사항

AMS Config 규칙 응답 구성 보고서

AMS Config 규칙 응답 구성 보고서는 현재 규정을 준수하지 않는 AMS 구성 규칙에 응답하도록 Accelerate를 구성한 방법을 자세히 살펴봅니다. AMS 구성 규칙에 대한 응답을 변경하는 방법에 대한 자세한 내용은 AMS Accelerate 사용자 지정 결과 응답을 참조하세요.

이 보고서는 변경한 구성만 표시하며 AMS Config 규칙 라이브러리에 나열된 AMS 기본 구성은 제외합니다. 보고서는 다음을 포함하여 AMS 계정의 리소스 및 AMS 구성 규칙 응답 구성에 대한 데이터를 제공합니다.

- AMS 구성 규칙에 대한 기본 응답을 변경한 AWS 계정 목록입니다.
- AMS 구성 규칙에 대한 응답을 연결한 태그 목록입니다.
- 각 규칙, 계정 및 태그에 대한 응답 구성 목록입니다.
- AMS 구성 규칙에 대한 기본 응답을 변경한 리소스 목록입니다.

최신 응답 구성 보고서

필드	설명
Date	보고서가 생성된 날짜
고객 이름	고객 이름
AWS 계정 ID	구성과 연결된 AWS 계정 ID
계정 이름	AWS 계정 수준 리소스 그룹의 계정 이름
결과 유형	식별된 조사 결과 유형입니다. 이 경우 AWS Config
소스 식별자	AWS Config 규칙 고유 소스 식별자
리소스 그룹 ID	응답 구성과 연결된 리소스 그룹 ID
구성된 응답 작업	AMS에서 트리거한 작업 유형
SSM 런북 연결됨	실행될 문제 해결 런북이 있는 경우
리소스 그룹 유형	계정 또는 태그일 수 있습니다.

Config 규칙의 사용자 지정 기본 응답이 있는 리소스

필드 이름	정의
고객 이름	고객 이름
Date	보고서가 생성된 날짜
AWS 계정 이름	AWS 계정 이름
계정 ID	연결된 AWS 계정 ID
AMS Config 규칙	리소스를 대상으로 하고 구성으로 적용하는 AMS 구성 규칙

필드 이름	정의
리소스 ID	AMS 구성 규칙의 대상이 되는 고객 계정의 리소스 ID
리소스 리전	구성이 적용되는 AWS 리전
리소스 유형	AWS 리소스 유형
리소스 그룹 ID	응답 구성과 연결된 리소스 그룹 ID
리소스 AMS 플래그	AMS에서 AWS 리소스를 배포하는 경우이 필드는 로 설정됩니다. `True`
트리거 유형	리소스에 대해 구성된 응답 유형
규정 준수 플래그	AMS 구성 규칙 규정 준수 상태

인시던트 방지 및 상위 화자 보고서 모니터링

사용 가능한 보고서

- 인시던트 방지 보고서
- 상위 화자 보고서 모니터링

인시던트 방지 보고서

Incidents Prevented 보고서에는 자동으로 해결되어 발생할 수 있는 인시던트를 방지하는 Amazon CloudWatch 경보가 나열됩니다. 자세한 내용은 자동 문제 해결을 참조하세요. 다음 표에는이 보고서에 포함된 정보가 나열되어 있습니다.

필드 이름	정의
실행_시작_시간_utc	자동화가 실행된 날짜
customer_name	계정 고객 이름
account_name	계정의 이름입니다.

필드 이름	정의
AwsAccountId	AWS 계정의 ID
document_name	실행된 SSM 문서 또는 자동화의 이름
duration_in_분	분 단위의 자동화 길이
리전	AWS 리소스가 위치한 리전
automation_execution_id	실행의 ID입니다.
automation_execution_status	실행 상태

상위 화자 보고서 모니터링

상위 화자 모니터링 보고서는 특정 기간 동안 생성된 Amazon CloudWatch 알림 수를 표시하고 가장 많은 수의 알림을 생성하는 리소스에 대한 시각화를 제공합니다. 이 보고서는 가장 많은 수의 알림을 생성하는 리소스를 식별하는 데 도움이 됩니다. 이러한 리소스는 근본 원인 분석을 수행하여 문제를 해결하거나 실제 문제가 없을 때 불필요한 트리거를 방지하기 위해 경보 임계값을 수정하는 데 적합할 수 있습니다. 다음 표에는이 보고서에 포함된 정보가 나열되어 있습니다.

필드 이름	정의
고객 이름	고객 이름
AccountId	AWS 계정의 ID
알림 범주	트리거된 알림 유형
설명	알림에 대한 설명
리소스 ID	알림을 트리거한 리소스의 ID
Resource Name	알림을 트리거한 리소스의 이름
리전	AWS리소스가 위치한 리전
인시던트 상태	경보에서 생성된 인시던트의 최신 상태

필드 이름	정의
첫 번째 발생	알림이 처음 트리거된 경우
최근 발생	알림이 트리거된 가장 최근 시간
알림 수	첫 번째 발생과 최근 발생 사이에 생성된 알림 수

결제 요금 세부 정보 보고서

AWS Managed Services(AMS) 결제 요금 세부 정보 보고서는 다음을 포함하여 연결된 계정 및 각 AWS 서비스의 AMS 결제 요금에 대한 세부 정보를 제공합니다.

- AMS 서비스 수준 요금, 증가 비율, 계정 수준 AMS 서비스 티어 및 AMS 요금.
- 연결된 계정 및 AWS 사용 요금

필드 이름	정의
결제 월	청구된 서비스의 월 및 연도
지급인 계정 ID	AMS 요금 지불을 담당하는 계정을 식별하는 12자리 ID
연결된 계정 ID	비용을 생성하는 서비스를 사용하는 AMS 계정을 식별하는 12자리 ID
AWS 서비스 이름	사용된 AWS 서비스
AWS 요금	AWS 서비스 이름에 나열된 AWS 서비스 이름에 대한 AWS 요금
요금제	연결된 계정과 연결된 요금제의 이름입니다.
상승 비율	pricing_plan, SLA 및 AWS 서비스를 기반으로 한 상승 비율(10진수 V.WXYZ)
조정된 AWS 요금	AWS AMS에 맞게 조정된 사용량

필드 이름	정의
업리프팅된 AWS 요금	AMS에 대해 청구되는 AWS 요금의 비율입니다. adjusted_aws_charges * uplift_percent
인스턴스 EC2 RDS 지출	EC2 및 RDS 인스턴스에 대한 지출
AMS 요금	제품에 대한 총 AMS 요금, uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
비례 할당 최소 요금	계약 최소값을 충족하기 위해 청구되는 금액
최소 요금	AMS 최소 요금(해당하는 경우)
연결된 계정 총 AMS 요금	linked_account에 대한 모든 요금의 합계
지급인 계정 총 AMS 요금	지급인 계정에 대한 모든 요금의 합계

신뢰할 수 있는 수정자 보고서

사용 가능한 보고서

- 신뢰할 수 있는 수정자 수정 요약 보고서
- 신뢰할 수 있는 수정자 구성 요약 보고서
- Trusted Advisor 요약 보고서 확인

신뢰할 수 있는 수정자 수정 요약 보고서

신뢰할 수 있는 문제 해결자 문제 해결 상태 보고서는 이전 문제 해결 주기 동안 발생한 문제 해결에 대한 정보를 제공합니다. 기본 주 수는 1입니다. 보고서를 사용자 지정하려면 수정 일정에 따라 주 수를 지정합니다.

필드 이름	정의
날짜	데이터가 수집된 날짜입니다.
계정 ID	리소스가 속한 AWS 계정 ID

필드 이름	정의
계정 이름	AWS 계정 이름
범주 확인	AWS Trusted Advisor 검사 범주
이름 확인	수정 Trusted Advisor 검사의 이름입니다.
검사 ID	수정 Trusted Advisor 검사의 ID입니다.
실행 모드	특정 Trusted Advisor 검사에 대해 구성된 실행 모드
OpsItem ID	문제 해결을 Trusted Advisor 위해에서 생성한 OpsItem의 ID
OpsItem 상태	보고 Trusted Advisor 시에서 생성한 OpsItem의 상태
리소스 ID	문제 해결을 위해 생성된 리소스의 ARN

신뢰할 수 있는 수정자 구성 요약 보고서

신뢰할 수 있는 수정자 구성 요약 보고서는 각 Trusted Advisor 검사에 대한 현재 신뢰할 수 있는 수정자 수정자 구성에 대한 정보를 제공합니다.

필드 이름	정의
날짜	데이터가 수집된 날짜입니다.
계정 ID	구성이 적용되는 AWS 계정 ID입니다.
계정 이름	AWS 계정 이름
범주 확인	AWS Trusted Advisor 검사 범주
이름 확인	구성이 적용되는 수정 Trusted Advisor 검사의 이름입니다.

필드 이름	정의
검사 ID	구성이 적용되는 수정 Trusted Advisor 검사의 ID입니다.
실행 모드	특정 Trusted Advisor 검사에 대해 구성된 실행 모드
자동으로 재정의	구성된 경우 실행 모드를 자동화로 재정의하는 태그 패턴
수동 재정의	구성된 경우 실행 모드를 수동으로 재정의하는 태그 패턴

Trusted Advisor 요약 보고서 확인

Trusted Advisor 검사 요약 보고서는 현재 Trusted Advisor 검사에 대한 정보를 제공합니다. 이 보고서는 매주 문제 해결 일정 이후에 데이터를 수집합니다. 기본 주 수는 1입니다. 보고서를 사용자 지정하려면 문제 해결 주기에 따라 주 수를 지정합니다.

필드 이름	정의
날짜	데이터가 수집된 날짜입니다.
계정 ID	구성이 적용되는 AWS 계정 ID입니다.
고객 이름	AWS 계정 이름
범주 확인	AWS Trusted Advisor 검사 범주
이름 확인	구성이 적용되는 수정 Trusted Advisor 검사의 이름입니다.
검사 ID	구성이 적용되는 수정 Trusted Advisor 검사의 ID입니다.
상태	검사의 알림 상태입니다. 가능한 상태는 정상(녹색), 경고(노란색), 오류(빨간색) 또는 not_available입니다.

필드 이름	정의
플래그가 지정된 리소스	Trusted Advisor 검사에 의해 플래그가 지정된 (목록에 있는) AWS 리소스 수입니다.
무시된 리소스	가 숨김으로 표시 Trusted Advisor 하여 무시한 AWS 리소스 수입니다.
중요 상태의 리소스	중요 상태의 리소스 수
경고 상태의 리소스	경고 상태의 리소스 수

셀프 서비스 보고서

AWS Managed Services(AMS) 셀프 서비스 보고서(SSR)는 다양한 네이티브 AWS 서비스에서 데이터를 수집하고 주요 AMS 제품에 대한 보고서에 대한 액세스를 제공하는 기능입니다. SSR은 운영, 구성 관리, 자산 관리, 보안 관리 및 규정 준수를 지원하는 데 사용할 수 있는 정보를 제공합니다.

SSR을 사용하여 AMS 콘솔에서 보고서에 액세스하고 Amazon S3 버킷(계정당 버킷 1개)을 통해 데이터 세트를 보고합니다. 선호하는 비즈니스 인텔리전스(BI) 도구에 데이터를 연결하여 고유한 요구 사항에 따라 보고서를 사용자 지정할 수 있습니다. AMS는 기본 AWS 리전에서이 S3 버킷(S3 버킷 이름: (ams-reporting-data-a<Account_ID>)을 생성하고 us-east-1 리전에서 호스팅되는 AMS 컨트롤 플레인에서 데이터를 공유합니다.

사용자가 AMS 콘솔에서 AMS Accelerate 보고서를 볼 수 있도록 허용하려면 AWS Identity and Access Management (IAM)에서 이러한 작업을 수행할 수 있는 명시적 권한을 부여해야 합니다. IAM 정책의 예는 AMS 기능을 사용할 수 있는 권한을 참조하세요.

Important

에서 사용자 지정 키 사용 AWS Glue
고객 관리형 KMS 키로 AWS Glue 메타데이터를 암호화하려면 AMS가 계정의 데이터를 집계할 수 있도록 다음 추가 단계를 수행해야 합니다.

1. https://console.aws.amazon.com/kms AWS Key Management Service 콘솔을 연 다음 고객 관리형 키를 선택합니다.
2. AWS Glue 메타데이터를 암호화하는 데 사용할 키 ID를 선택합니다.
3. 별칭 탭을 선택한 다음 별칭 생성을 선택합니다.

4. 텍스트 상자에 AmsReportingFlywheelCustomKey를 입력한 다음 별칭 생성을 선택합니다.

주제

- 내부 API 작업
- 패치 보고서(일별)
- 백업 보고서(일별)
- 인시던트 보고서(주별)
- 결제 보고서(월별)
- 집계된 보고서
- AMS 셀프 서비스 보고서 대시보드
- 데이터 보존 정책
- SSR에서 오프보드

내부 API 작업

API 작업을 모니터링하는 경우 다음 내부 전용 작업에 대한 호출이 표시될 수 있습니다.

- `GetDashboardUrl`
- `ListReportsV2`

내부 API 작업: GetDashboardUrl

이 작업은 AMS 콘솔에서 호출할 때 시스템 로그에 표시됩니다. 다른 사용 사례는 없습니다. 직접 사용할 수 없습니다.

해당 보고서에 대한 임베디드 대시보드 URL을 반환합니다. 이 작업은에서 `dashboardName` 반환한를 수락합니다`ListReports`.

요청 구문

```
HTTP/1.1 200
Content-type: application/json
{
    "dashboardName": "string"
}
```

요청 요소

dashboardName: URL이 요청되는 빠른 대시보드의 이름입니다. 대시보드 이름은 ListReportsV2에 반환됩니다.

유형: 문자열

응답 구문

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다. 다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

url: 요청된에 대한 빠른 URL을 반환합니다dashboardName.

유형: 문자열

오류

모든 작업에 공통적인 오류에 대한 자세한 내용은 공통 오류를 참조하세요.

BadRequestException:

제출된 요청이 유효하지 않습니다. 예를 들어 입력이 불완전하거나 잘못된 경우입니다. 자세한 내용은 함께 제공되는 오류 메시지를 참조하세요.

HTTP 상태 코드: 400

NotFoundException:

요청된 리소스를 찾을 수 없습니다. 요청 URI가 올바른지 확인합니다.

HTTP 상태 코드: 404

TooManyRequestsException:

요청이 제한 한도에 도달했습니다. 지정된 기간 후에 재시도합니다.

HTTP 상태 코드: 429

UnauthorizedException:

호출자에게 권한이 부족하기 때문에 요청이 거부됩니다.

HTTP 상태 코드: 401

내부 API 작업: ListReportsV2

이 API는 AMS 콘솔에서 호출할 때 시스템 로그에 나타납니다. 다른 사용 사례는 없습니다. 직접 사용할 수 없습니다.

지정된 계정에 사용할 수 있는 운영 보고서 목록을 반환합니다.

요청 구문

요청에 요청 본문이 없습니다.

응답 구문

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
        "dashboard": "string",
        "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다. 다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

reportsList: 사용 가능한 운영 보고서 목록입니다.

유형: Dashboard 객체 배열

reportsType: 보고서가 여러 계정에 걸쳐 집계되는지 여부를 나타냅니다.

유형: 문자열

오류

모든 작업에 공통적인 오류에 대한 자세한 내용은 공통 오류를 참조하세요.

BadRequestException:

제출된 요청이 유효하지 않습니다. 예를 들어 입력이 불완전하거나 올바르지 않습니다. 자세한 내용은 함께 제공되는 오류 메시지를 참조하세요.

HTTP 상태 코드: 400

NotFoundException:

요청된 리소스를 찾을 수 없습니다. 요청 URI가 올바른지 확인합니다.

HTTP 상태 코드: 404

TooManyRequestsException:

요청이 제한 한도에 도달했습니다. 지정된 기간 후에 재시도합니다.

HTTP 상태 코드: 429

UnauthorizedException:

호출자에게 권한이 부족하기 때문에 요청이 거부됩니다.

HTTP 상태 코드: 401

패치 보고서(일별)

사용 가능한 보고서

- AMS 패치에 대한 인스턴스 세부 정보 요약
- 패치 세부 정보
- 패치를 놓친 인스턴스

AMS 패치에 대한 인스턴스 세부 정보 요약

AMS 패치에 온보딩된 모든 인스턴스, 계정 상태, 인스턴스 세부 정보, 유지 관리 기간 적용 범위, 유지 관리 기간 실행 시간, 스택 세부 정보 및 플랫폼 유형을 식별하는 데 도움이 되는 정보 보고서입니다.

이 데이터 세트는 다음을 제공합니다.

- 계정의 프로덕션 및 비프로덕션 인스턴스에 대한 데이터입니다. 프로덕션 및 비프로덕션 단계는 인스턴스 태그가 아닌 계정 이름에서 파생됩니다.
- 플랫폼 유형별 인스턴스 배포에 대한 데이터입니다. 'N/A' 플랫폼 유형은 AWS Systems Manager(SSM)가 플랫폼 정보를 가져올 수 없을 때 발생합니다.
- 인스턴스 상태 분포, 실행, 중지 또는 종료 중인 인스턴스 수에 대한 데이터입니다.

콘솔 필드 이름	데이터 세트 필드 이름	정의
액세스 제한	access_restrictions	액세스가 제한된 리전
계정 ID	aws_account_id	AWS 인스턴스 ID가 속한 계정 ID
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
계정 이름	account_name	AWS 계정 이름
계정 상태	account_status	AMS 계정 상태
	account_sla	AMS 계정 서비스 약정
계정 유형	malz_role	MALZ 역할
오토 스케일링 그룹 이름	instance_asg_name	인스턴스가 포함된 Auto Scaling 그룹(ASG)의 이름
인스턴스 ID	instance-id	EC2 인스턴스의 ID
인스턴스 이름	instance_name	EC2 인스턴스의 이름
인스턴스 패치 그룹	instance_patch_group	인스턴스를 그룹화하고 동일한 유지 관리 기간을 적용하는 데 사용되는 패치 그룹 이름
인스턴스 패치 그룹 유형	instance_patch_group_type	패치 그룹 유형
인스턴스 플랫폼 유형	instance_platform_type	운영 체제(OS) 유형

콘솔 필드 이름	데이터 세트 필드 이름	정의
인스턴스 플랫폼 이름	instance_platform_name	운영 체제(OS) 이름
인스턴스 상태	instance_state	EC2 인스턴스 수명 주기 내의 상태
인스턴스 태그	ec2_tags	Amazon EC2 인스턴스 ID와 연결된 태그
랜딩 존	malz_flag	MALZ 관련 계정에 대한 플래그
유지 관리 기간 범위	mw_covered_flag	인스턴스에 향후 실행 날짜가 있는 활성화된 유지 관리 기간이 하나 이상 있는 경우 해당 기간이 적용되는 것으로 간주되고 그렇지 않으면 적용되지 않습니다.
유지 관리 기간 실행 날짜/시간	earliest_window_execution_time	다음에 유지 관리 기간이 실행될 것으로 예상되는 경우
유지 관리 기간 실행 날짜/시간	earliest_window_execution_time	다음에 유지 관리 기간이 실행될 것으로 예상되는 경우
프로덕션 계정	prod_계정	계정 이름에 'PROD', 'NONPROD' 값이 포함되는지 여부에 따라 AMS prod, 비prod 계정의 식별자입니다.
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간입니다.
[Stack Name]	인스턴스_스택_이름	인스턴스가 포함된 스택의 이름

콘솔 필드 이름	데이터 세트 필드 이름	정의
스택 유형	인스턴스_스택_유형	AMS 스택(고객 계정 내 AMS 인프라) 또는 고객 스택(고객 애플리케이션을 지원하는 AMS 관리형 인프라)

패치 세부 정보

이 보고서는 다양한 인스턴스의 패치 세부 정보와 유지 관리 기간 범위를 제공합니다.

이 보고서는 다음을 제공합니다.

- 패치 그룹 및 해당 유형에 대한 데이터입니다.
- 유지 관리 기간, 기간, 마감, 향후 유지 관리 기간 실행 날짜(일정) 및 각 기간의 영향을 받는 인스턴스에 대한 데이터입니다.
- 계정의 모든 운영 체제에 대한 데이터와 운영 체제가 설치된 인스턴스 수입니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간입니다.
계정 ID	aws_account_id	AWS 인스턴스 ID가 속한 계정 ID
계정 이름	account_name	AWS 계정 이름
계정 상태	account_status	AMS 계정 상태
규정 준수 - 중요	compliant_critical	심각도가 "중요"인 규정 준수 패치 수
규정 준수 - 높음	규정 준수_높음	심각도가 "높음"인 규정 준수 패치 수

필드 이름	데이터 세트 필드 이름	정의
규정 준수 - 중간	compliant_medium	심각도가 "중간"인 규정 준수 패치 수
규정 준수 - 낮음	compliant_low	심각도가 "낮음"인 규정 준수 패치 수
규정 준수 - 정보 제공	규정 준수_정보	"정보" 심각도의 규정 준수 패치 수
규정 준수 - 지정되지 않음	compliant_unspecified	심각도가 “지정되지 않음”인 규정 준수 패치 수
규정 준수 - 합계	compliant_total	규정 준수 패치 수(모든 심각도)
인스턴스 ID	instance-id	EC2 인스턴스의 ID
인스턴스 이름	instance_name	EC2 인스턴스의 이름
	account_sla	AMS 계정 서비스 티어
인스턴스 플랫폼 유형	instance_platform_type	운영 체제(OS) 유형
인스턴스 플랫폼 이름	instance_platform_name	운영 체제(OS) 이름
인스턴스 패치 그룹 유형	instance_patch_group_type	DEFAULT: 인스턴스의 AMSDefaultPatchGroup:True 태그로 결정되는 기본 유지 관리 기간이 있는 기본 패치 그룹 고객: 고객이 생성한 패치 그룹 NOT_ASSIGNED: 할당된 패치 그룹이 없음
인스턴스 패치 그룹	instance_patch_group	인스턴스를 그룹화하고 동일한 유지 관리 기간을 적용하는 데 사용되는 패치 그룹 이름

필드 이름	데이터 세트 필드 이름	정의
인스턴스 상태	instance_state	EC2 인스턴스 수명 주기 내의 상태
인스턴스 태그	ec2_tags	Amazon EC2 인스턴스 ID와 연결된 태그
마지막 실행 유지 관리 기간	last_execution_window	유지 관리 기간이 실행된 최근 시간
유지 관리 기간 ID	window_id	유지 관리 기간 ID
유지 관리 기간 상태	window_state	유지 관리 기간 상태
유지 관리 기간 유형	window_type	유지 관리 기간 유형
유지 관리 기간 다음 실행 날짜/시간	window_next execution_time	다음에 유지 관리 기간이 실행될 것으로 예상되는 경우
유지 관리 기간(시간)	window_duration	유지 관리 기간의 지속 시간
유지 관리 기간 범위	mw_covered_flag	인스턴스에 향후 실행 날짜가 있는 활성화된 유지 관리 기간이 하나 이상 있는 경우 해당 기간이 적용되는 것으로 간주되고 그렇지 않으면 적용되지 않습니다.
규정 미준수 - 중요	noncompliant_critical	심각도가 "중요"인 규정 미준수 패치 수
규정 미준수 - 높음	규정 미준수_높음	심각도가 "높음"인 규정 미준수 패치 수
규정 미준수 - 중간	규정 미준수_중간	심각도가 "중간"인 규정 미준수 패치 수

필드 이름	데이터 세트 필드 이름	정의
규정 미준수 - 낮음	규정 미준수_낮음	심각도가 "낮음"인 규정 미준수 패치 수
규정 미준수 - 정보 제공	규정 미준수 _정보	심각도가 "정보"인 규정 미준수 패치 수
규정 미준수 - 지정되지 않음	규정 미준수 _지정되지 않음	심각도가 “지정되지 않음”인 규정 미준수 패치 수
규정 미준수 - 합계	noncompliant_total	규정 미준수 패치 수(모든 심각도)
패치 기준 ID	patch_Baseline_id	현재 인스턴스에 연결된 패치 기준
패치 상태	patch_status	전체 패치 규정 준수 상태입니다. 누락된 패치가 하나 이상 있는 경우 인스턴스는 규정을 준수하지 않는 것으로 간주되고, 그렇지 않으면 규정을 준수하는 것으로 간주됩니다.
프로덕션 계정	prod_계정	계정 이름에 'PROD', 'NONPROD' 값이 포함되는지 여부에 따라 AMS prod, 비prod 계정의 식별자입니다.
스택 유형	인스턴스_스택_유형	AMS 스택(고객 계정 내 AMS 인프라) 또는 고객 스택(고객 애플리케이션을 지원하는 AMS 관리형 인프라)
	window_next_exec_yyyy	window_next_execution_time의 연도 부분

필드 이름	데이터 세트 필드 이름	정의
	window_next_exec_mm	window_next_execution_time의 월 부분
	window_next_exec_D	window_next_execution_time의 요일 부분
	window_next _exec_HHMI	window_next_execution_time의 시간:분 부분

패치를 놓친 인스턴스

이 보고서는 마지막 유지 관리 기간 실행 중에 패치를 놓친 인스턴스에 대한 세부 정보를 제공합니다.

이 보고서는 다음을 제공합니다.

- 패치 ID 수준에서 누락된 패치에 대한 데이터입니다.
- 패치가 하나 이상 누락된 모든 인스턴스의 데이터 및 패치 심각도, 패치가 적용되지 않은 날짜, 범위 및 패치 릴리스 날짜와 같은 속성.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간
계정 ID	aws_account_id	AWS 인스턴스 ID가 속한 계정 ID
계정 이름	account_name	AWS 계정 이름
고객 이름 상위	customer_name_parent	
고객 이름	customer_name	
프로덕션 계정	prod_계정	계정 이름에 'PROD' 또는 'NONPROD' 값이 포함되는지

필드 이름	데이터 세트 필드 이름	정의
		여부에 따라 AMS prod 또는 비 prod 계정의 식별자입니다.
계정 상태	account_status	AMS 계정 상태
계정 유형	account_type	
	account_sla	AMS 계정 서비스 티어
인스턴스 ID	instance-id	EC2 인스턴스의 ID
인스턴스 이름	instance_name	EC2 인스턴스의 이름
인스턴스 플랫폼 유형	instance_platform_type	운영 체제(OS) 유형
인스턴스 상태	instance_state	EC2 인스턴스 수명 주기 내의 상태
인스턴스 태그	ec2_tags	Amazon EC2 인스턴스 ID와 연결된 태그
패치 ID	patch_id	릴리스된 패치의 ID
패치 심각도	patch_sev	게시자당 패치 심각도
패치 분류	patch_class	패치 게시자당 패치 분류
패치 릴리스 날짜/시간(UTC)	release_dt_utc	게시자당 패치 릴리스 날짜
패치 설치 상태	install_state	SSM당 인스턴스에 패치 상태 설치
패치되지 않은 일수	days_unpatched	마지막 SSM 스캔 이후 인스턴스가 패치되지 않은 일수
패치되지 않은 일수 범위	days_unpatched_bucket	패치되지 않은 일수의 버킷팅

백업 보고서(일별)

백업 보고서는 기본 및 보조(해당하는 경우) 리전을 다룹니다. 백업 상태(성공/실패)와 생성된 스냅샷에 대한 데이터를 다룹니다.

이 보고서는 다음을 제공합니다.

- 백업 상태
- 생성된 스냅샷 수
- 복구 시점
- 백업 계획 및 볼트 정보

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간입니다.
계정 ID	aws_account_id	인스턴스 ID가 속한 AWS 계정 ID
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
계정 이름	account_name	AWS 계정 이름
계정 SLA	account_sla	AMS 계정 서비스 약정
	malz_flag	MALZ 관련 계정에 대한 플래그
	malz_role	MALZ 역할
	access_restrictions	액세스가 제한된 리전
백업 스냅샷 예약 시작 날짜/시간	시작_바이_dt_utc	스냅샷이 시작되도록 예약된 시점의 타임스탬프

필드 이름	데이터 세트 필드 이름	정의
백업 스냅샷 실제 시작 날짜/시간	생성_dt_utc	스냅샷이 실제로 시작될 때의 타임스탬프
백업 스냅샷 완료 날짜/시간	completion_dt_utc	스냅샷 완료 시 타임스탬프
백업 스냅샷 만료 날짜/시간	expiration_dt_utc	스냅샷 만료 시 타임스탬프
백업 작업 상태	backup_job_status	스냅샷의 상태
백업 유형	backup_type	백업 유형
백업 작업 ID	backup_job_id	백업 작업의 고유 식별자
바이트 단위의 백업 크기	backup_size_in_바이트	바이트 단위의 백업 크기
백업 계획 ARN	backup_plan_arn	백업 계획 ARN
백업 계획 ID	backup_plan_id	백업 계획 고유 식별자
백업 계획 이름	backup_plan_이름	백업 계획 이름
백업 계획 버전	backup_plan_버전	백업 계획 버전
백업 규칙 ID	backup_rule_id	백업 규칙 ID
백업 볼트 ARN	backup_vault_arn	백업 볼트 ARN
백업 볼트 이름	backup_vault_이름	백업 볼트 이름
IAM 역할 ARN	iam_role_arn	IAM 역할 ARN
인스턴스 ID	instance-id	고유 인스턴스 ID
인스턴스 상태	instance_state	인스턴스 상태
인스턴스 태그	ec2_tags	EC2 인스턴스 ID와 연결된 태그
리소스 ARN	resource_arn	Amazon 리소스 이름

필드 이름	데이터 세트 필드 이름	정의
Resource Id	resource_id	고유한 리소스 식별자
리소스 리전	resource_region	리소스의 기본(및 해당하는 경우 보조) 리전입니다.
리소스 유형	resource_type	리소스 유형
복구 시점 ARN	recovery_point_arn	복구 시점의 ARN
복구 시점 ID	recovery_point_id	복구 시점의 고유 식별자입니다.
복구 시점 상태	recovery_point_status	복구 시점 상태
일 후 복구 시점 삭제	recovery_point_delete_after_days	일 후 복구 시점 삭제
며칠 후 콜드 스토리지로 복구 시점 이동	recovery_point_move_to_cold_storage_after_days	백업 스냅샷이 콜드 스토리지로 이동된 완료 날짜 이후의 일수
복구 시점 암호화 상태	recovery_point_is_encrypted	복구 시점 암호화 상태
복구 시점 암호화 키 ARN	recovery_point_encryption_key_arn	복구 시점 암호화 키 ARN
스택 ID	stack_id	Cloudformation 스택 고유 식별자
[Stack Name]	stack_name	[Stack Name]
태그: AMS 기본 패치 그룹	tag_ams_default_patch_group	태그 값: AMS 기본 패치 그룹
태그: 앱 ID	tag_app_id	태그 값: 앱 ID
태그: 앱 이름	tag_app_name	태그 값: 앱 이름
태그: 백업	tag_backup	태그 값: 백업

필드 이름	데이터 세트 필드 이름	정의
태그: 규정 준수 프레임워크	tag_compliance_framework	태그 값: 규정 준수 프레임워크
태그: 비용 센터	tag_cost_center	태그 값: 비용 센터
태그: 고객	태그_고객	태그 값: 고객
태그: 데이터 분류	tag_data_classification	태그 값: 데이터 분류
태그: 환경 유형	tag_environment_type	태그 값: 환경 유형
태그: 운영 시간	작업_시간_태그	태그 값: 운영 시간
태그: 소유자 팀	tag_owner_team	태그 값: 소유자 팀
태그: 소유자 팀 이메일	tag_owner_team_email	태그 값: 소유자 팀 이메일
태그: 패치 그룹	tag_patch_group	태그 값: 패치 그룹
태그: 지원 우선 순위	tag_support_priority	태그 값: 지원 우선 순위
볼륨 상태	volume_state	볼륨 상태

인시던트 보고서(주별)

이 보고서는 다음을 포함하여 우선순위, 심각도 및 최신 상태와 함께 집계된 인시던트 목록을 제공합니다.

- 관리형 계정에서 인시던트로 분류된 지원 사례에 대한 데이터
- 관리형 계정의 인시던트 지표를 시각화하는 데 필요한 인시던트 정보
- 모든 인시던트의 인시던트 범주 및 문제 해결 상태에 대한 데이터

주간 인시던트 보고서에는 시각화와 데이터를 모두 사용할 수 있습니다.

- 시각화는 보고서 페이지를 통해 계정의 AMS 콘솔을 통해 액세스할 수 있습니다.
- 다음 스키마가 있는 데이터 세트는 관리형 계정의 S3 버킷을 통해 액세스할 수 있습니다.

- 제공된 날짜 필드를 사용하여 인시던트가 생성되거나 해결된 월, 분기, 주 및/또는 날짜를 기준으로 인시던트를 필터링합니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜와 시간입니다.
계정 ID	aws_account_id	AWS 인시던트가 속한 계정 ID입니다.
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
계정 이름	account_name	AWS 계정 이름입니다.
사례 ID	case_id	인시던트의 ID입니다.
생성된 월	생성_월	인시던트가 생성된 달입니다.
우선순위	priority	인시던트의 우선 순위입니다.
심각도	severity	인시던트의 심각도입니다.
상태	status	인시던트의 상태입니다.
범주	yuma_category	인시던트의 범주입니다.
생성된 날짜	생성_일	인시던트가 YYYY-MM-DD 형식으로 생성된 날짜입니다.
생성된 주	created_wk	인시던트가 YYYY-WW 형식으로 생성된 주입니다. 일요일부터 토요일까지는 일주일의 시작과 끝으로 계산됩니다. 주 단위는 01~52입니다. 01주차는 항상 연도의 첫날이 포함된 주입니다. 예를 들어 2023-12-31

필드 이름	데이터 세트 필드 이름	정의
		및 2024-01-01은 2024년 1주차입니다.
생성된 분기	created_qtr	인시던트가 YYYY-Q 형식으로 생성된 분기입니다. 01/01~03/31은 Q1 등으로 정의됩니다.
해결된 날짜	resolved_day	인시던트가 YYYY-MM-DD 형식으로 해결된 날짜입니다.
해결된 주	Resolve_wk	인시던트가 YYYY-WW 형식으로 해결된 주입니다. 일요일부터 토요일까지는 일주일의 시작과 끝으로 계산됩니다. 주 단위는 01~52입니다. 01주차는 항상 연도의 첫날이 포함된 주입니다. 예를 들어, 2023-12-31 및 2024-01-01은 2024년 1월에 있습니다.
해결된 월	resolved_month	인시던트가 YYYY-MM 형식으로 해결된 달입니다.
해결된 분기	해석됨_qtr	인시던트가 YYYY-Q 형식으로 해결된 분기입니다. 01/01~03/31은 Q1 등으로 정의됩니다.
생성된 그룹화 규칙	그룹화_규칙	인시던트에 적용되는 그룹화 규칙입니다. "no_grouping" 또는 "instance_grouping".
인스턴스 ID	instance_ids	인시던트와 연결된 인스턴스입니다.

필드 이름	데이터 세트 필드 이름	정의
알림 수	number_of_alerts	해당 인시던트와 연결된 알림 수입니다. 그룹화를 활성화한 경우이 숫자는 1보다 클 수 있습니다. 그룹화를 활성화하지 않은 경우 항상 1이 됩니다.
생성 시간	created_at	인시던트가 생성된 시점의 타임스탬프입니다.
경보 ARNs	alarm_arns	인시던트와 관련된 경보의 Amazon 리소스 이름("arn")입니다.
관련 경보	related_alarms	인시던트와 관련된 모든 경보의 사람이 읽을 수 있는 이름입니다.

결제 보고서(월별)

결제 요금 세부 정보

이 보고서는 연결된 계정 및 각 AWS 서비스의 AMS 청구 요금에 대한 세부 정보를 제공합니다.

이 보고서는 다음을 제공합니다.

- AMS 서비스 수준 요금, 증가율, 계정 수준 AMS 서비스 티어 및 AMS 요금에 대한 데이터입니다.
- 연결된 계정 및 AWS 사용 요금에 대한 데이터입니다.

> **Important**
>
> 월별 결제 보고서는 Management Payer Account(MPA) 또는 정의된 요금 계정에서만 사용할 수 있습니다. AMS 월별 청구서가 전송되는 계정입니다. 이러한 계정을 찾을 수 없는 경우 Cloud Service Delivery Manager(CSDM)에 문의하여 지원을 받으세요.

필드 이름	데이터 세트 필드 이름	정의
결제 날짜	date	청구된 서비스의 월 및 연도
지급인 계정 ID	payer_account_id	AMS 요금 지불을 담당하는 계정을 식별하는 12자리 ID
연결된 계정 ID	linked_account_id	확장을 생성하는 서비스를 사용하는 AMS 계정을 식별하는 12자리 ID
AWS 서비스 이름	product_name	사용된 AWS 서비스
AWS 요금	aws_charges	AWS 서비스 이름의 AWS 서비스 이름에 대한 AWS 요금
요금제	요금제	연결된 계정과 연결된 요금제
AMS 서비스 그룹	tier_uplifting_groups	업리프트 비율을 결정하는 AMS 서비스 그룹 코드
상승 비율	uplift_percent	pricing_plan, SLA 및 AWS 서비스를 기반으로 한 상승 비율(10진수 V.WXYZ)
조정된 AWS 요금	adjusted_aws_usage	AWS AMS에 맞게 조정된 사용량
업리프팅된 AWS 요금	uplifted_aws_charges	AMS에 대해 청구되는 AWS 요금의 비율입니다. adjusted_aws_charges * uplift_percent
인스턴스 EC2 RDS 지출	인스턴스_ec2_rds_spend	EC2 및 RDS 인스턴스에 대한 지출
예약 인스턴스 요금	ris_charges	예약 인스턴스 요금

필드 이름	데이터 세트 필드 이름	정의
업그레이드된 예약 인스턴스 요금	uplifted_ris	AMS에 대해 청구할 예약 인스턴스 요금의 백분율입니다. ris_charges * uplift_percent
Savings Plan 요금	sp_charges	SavingsPlan 사용 요금
업리프팅된 Savings Plan 요금	uplifted_sp	AMS에 대해 청구되는 절감형 플랜 요금의 비율, sp_charges * uplift_percent
AMS 요금	ams_charges	제품에 대한 총 ams 요금, uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
비례 할당 최소 요금	비례 할당_최소	계약 최소값을 충족하기 위해 청구되는 금액
연결된 계정 총 AMS 요금	linked_account_total ams_charges	linked_account에 대한 모든 요금의 합계
지급인 계정 총 AMS 요금	지급인_계정_총계 ams_charges	지급인 계정에 대한 모든 요금의 합계
최소 요금	minimum_fees	AMS 최소 요금(해당하는 경우)
예약 인스턴스 및 Savings Plan 할인	adj_ri_sp_charges	RI/SP 요금에 적용되는 RI/SP 할인(특정 상황에서 적용)

집계된 보고서

집계된 셀프 서비스 보고(SSR)를 사용하면 조직 수준, 교차 계정에서 집계된 기존 셀프 서비스 보고서를 볼 수 있습니다. 이를 통해 내 AMS 관리 중인 모든 계정에서 패치 규정 준수, 백업 적용 범위 및 인시던트와 같은 주요 운영 지표를 파악할 수 있습니다 AWS Organizations.

집계된 SSR은 AWS Managed Services를 사용할 수 AWS 리전 있는 모든 상용에서 사용할 수 있습니다. 사용 가능한 리전의 전체 목록은 리전 표를 참조하세요.

집계된 보고서 활성화

AWS Organizations 관리 계정에서 집계된 SSR을 관리해야 합니다. 관리 계정은 조직을 생성하는 데 사용한 AWS 계정입니다.

AMS에 온보딩된 AWS Organizations 관리 계정에 대해 집계된 SSR을 활성화하려면 AMS 콘솔에 액세스하고 보고서로 이동합니다. top-right-hand 모서리에서 조직 액세스를 선택하여 AWS Managed Services 콘솔: 조직 보기 창을 엽니다. 이 창에서 집계된 SSR 기능을 관리할 수 있습니다.

AWS Organizations AMS에 온보딩되지 않은 관리 계정은 AMS 콘솔에 액세스할 수 없습니다. AMS에 온보딩되지 않은 AWS Organizations 관리 계정에 대해 집계된 SSR을 활성화하려면 먼저에 인증한 AWS 계정다음 AWS 콘솔로 이동하여 관리형 서비스를 검색합니다. 그러면 AMS Marketing 페이지가 열립니다. 이 페이지에서 탐색 모음의 조직 액세스 링크를 선택하여 집계된 SSR 기능을 관리할 수 있는 AWS Managed Services 콘솔: 조직 보기를 엽니다.

AWS Managed Services 콘솔: Organization View에 처음 액세스할 때 다음 단계를 완료합니다.

1. 아직 설정하지 않은 경우 콘솔에서 활성화 AWS Organizations를 AWS Organizations선택합니다. 설정에 대한 자세한 내용은 AWS Organizations 사용 설명서를 AWS Organizations참조하세요. 이미를 사용하고 있는 경우이 단계를 건너뛸 수 있습니다 AWS Organizations.
2. 집계된 셀프 서비스 보고 서비스를 활성화하려면 콘솔에서 신뢰할 수 있는 액세스 활성화를 선택합니다.
3. (선택 사항) 조직 보기에 대한 읽기 액세스 권한을 갖도록 위임된 관리자를 등록합니다.

위임된 관리자로 집계된 보고서 보기

위임된 관리자는 집계된 보고서에 대한 읽기 액세스 권한을 갖도록 선택한 계정입니다. 위임된 관리자는 AMS에 온보딩된 계정이어야 하며 집계된 보고서에 대한 읽기 액세스 권한이 있는 유일한 계정이어야 합니다.

위임된 관리자를 선택하려면 AWS Managed Services 콘솔: 조직 보기의 3단계에 계정 ID를 입력합니다. 한 번에 하나의 위임된 관리자 계정만 등록할 수 있습니다. 위임된 관리자 계정은 AMS 관리 계정이어야 합니다.

위임된 관리자 계정을 업데이트하려면 AWS Managed Services 콘솔: 조직 보기로 이동하여 위임된 관리자 제거를 선택합니다. 콘솔에 위임된 관리자로 등록할 새 계정 ID를 삽입하라는 메시지가 표시됩니다.

집계된 보고서 읽기

위임된 관리자를 등록하지 않고 AWS Organizations 관리 계정이 AMS에 온보딩된 경우 AWS Organizations 관리 계정은 기본적으로 집계된 보고서에 대한 읽기 액세스 권한을 갖게 됩니다. AWS Organizations 관리 계정이 AMS에서 관리되지 않는 경우 집계된 보고서에 대한 읽기 액세스 권한을 가질 위임된 관리자 계정을 선택해야 합니다.

언제든지 AMS에 온보딩된 단일 계정만 AWS Organizations 관리 계정 또는 등록된 위임된 관리자인 집계된 보고서에 대한 읽기 액세스 권한을 가집니다. 조직 내(및 AMS에 온보딩된) 다른 모든 멤버 계정은 여전히 각 개별 계정의 단일 계정 보고서에만 액세스할 수 있습니다.

집계된 SSR을 활성화한 후 보고서로 이동합니다. 모든 기존 셀프 서비스 보고서가이 섹션에 나열되고 파란색 태그는 보고서가 집계되었음을 나타냅니다. 집계된 보고서에 대한 읽기 액세스 권한을 갖도록 선택한 계정에서 AMS 콘솔에 액세스해야 합니다. 관리 AWS Organizations 계정 또는 위임된 관리자 계정입니다.

집계된 SSR을 활성화하면 다음 보고 주기부터 집계된 보고서를 사용할 수 있습니다.

집계된 보고서 비활성화

집계된 SSR을 비활성화하려면 AWS Managed Services 콘솔: 조직 보기를 엽니다. 신뢰할 수 있는 액세스 비활성화를 선택합니다. 집계된 SSR에 대해 신뢰할 수 있는 액세스를 비활성화하면 AMS 셀프 서비스 보고서가 조직 수준에서 계정 간에 집계되지 않습니다. 또한 비활성화는 다음 보고 주기부터 적용됩니다.

집계된 SSR을 비활성화한 후 AMS 콘솔의 보고서가 단일 계정 보고서로 나타나기까지 대기합니다. 이 지연은 다음 보고 주기부터 기능 비활성화가 적용되기 때문에 발생합니다.

AMS 셀프 서비스 보고서 대시보드

AMS 셀프 서비스 보고서는 Resource Tagger 대시보드 및의 두 가지 대시보드를 제공합니다보안 구성 규칙 대시보드.

Resource Tagger 대시보드

AMS 리소스 태거 대시보드는 Resource Tagger에서 지원하는 리소스에 대한 자세한 정보와 Resource Tagger가 해당 리소스에 적용하도록 구성된 태그의 현재 상태를 제공합니다.

리소스 유형별 리소스 태거 적용 범위

이 데이터 세트는 Resource Tagger에서 관리하는 태그가 있는 리소스 목록으로 구성됩니다.

리소스 유형별 리소스 적용 범위는 다음 지표를 설명하는 네 줄 차트로 시각화됩니다.

- 리소스 수: 리소스 유형별 리전의 총 리소스 수입니다.
- 관리형 태그가 누락된 리소스: 관리형 태그가 필요하지만 Resource Tagger에서 태그가 지정되지 않은 리소스 유형별 리전의 총 리소스 수입니다.
- 비관리형 리소스: Resource Tagger에서 관리형 태그를 적용하지 않은 리전의 리소스 유형별 총 수입니다. 이는 일반적으로 이러한 리소스가 Resource Tagger 구성과 일치하지 않거나 구성에서 명시적으로 제외됨을 의미합니다.
- 관리형 리소스: 비관리형 리소스 지표(리소스 수 - 비관리형 리소스)와 상응합니다.

다음 표에는이 보고서에서 제공하는 데이터가 나열되어 있습니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간(UTC 시간)
AWS 계정 ID	aws_account_id	AWS 계정 ID
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
리전	리전	AWS 리전
리소스 유형	resource_type	이 필드는 리소스 유형을 식별합니다. Resource Tagger에서 지원하는 리소스 유형만 포함됩니다.
리소스 수	resource_count	이 리전에 배포된 리소스 수(지정된 리소스 유형)입니다.
ResourcesMissingManagedTags	resource_missing_managed_tags_count	구성 프로필에 따라 관리형 태그가 필요하지만 아직

필드 이름	데이터 세트 필드 이름	정의
		Resource Tagger에서 태그를 지정하지 않은 리소스 수(지정된 리소스 유형)입니다.
UnmanagedResources	unmanaged_resource_count	Resource Tagger에서 관리형 태그를 적용하지 않은 리소스 수(지정된 리소스 유형)입니다. 일반적으로 이러한 리소스는 Resource Tagger 구성 블록과 일치하지 않거나 구성 블록에서 명시적으로 제외됩니다.

Resource Tagger 구성 규칙 규정 준수

이 데이터 세트는 리소스 유형 AWS 리전별로 특정 구성 프로필이 적용된의 리소스 목록으로 구성됩니다. 선 차트로 시각화됩니다.

다음 표에는이 보고서에서 제공하는 데이터가 나열되어 있습니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간(UTC 시간)
AWS 계정 ID	aws_account_id	AWS 계정 ID
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
리전	리전	AWS 리전
리소스 유형	resource_type	이 필드는 리소스 유형을 식별합니다. Resource Tagger에서 지원하는 리소스 유형만 포함됩니다.

필드 이름	데이터 세트 필드 이름	정의
구성 프로필 ID	configuration_profile_id	Resource Tagger 구성 프로필의 ID입니다. 구성 프로파일은 리소스에 태그를 지정하는 데 사용되는 정책 및 규칙을 정의하는 데 사용됩니다.
MatchingResourceCount	resource_count	Resource Tagger 구성 프로필 ID와 일치하는 리소스 수(지정된 리소스 유형)입니다. 리소스가 구성 프로필과 일치하려면 프로필을 활성화하고 리소스가 프로필의 규칙과 일치해야 합니다.

Resource Tagger 규정 미준수 리소스

이 데이터 세트는 단일 Resource Tagger 구성에 대해 규정을 준수하지 않는 리소스 목록으로 구성됩니다. 이 데이터는 리소스 규정 준수의 일일 스냅샷으로, 이러한 보고서가 고객 계정에 전달되는 시점의 고객 리소스 상태를 보여줍니다(기록 보기는 없음). 지정된 구성에 대해 불만이 없는 리소스로 구성된 피벗 테이블로 시각화됩니다.

다음 표에는이 보고서에서 제공하는 데이터가 나열되어 있습니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간(UTC 시간)
AWS 계정 ID	aws_account_id	AWS 계정 ID
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
리전	리전	AWS 리전

필드 이름	데이터 세트 필드 이름	정의
리소스 유형	resource_type	이 필드는 리소스 유형을 식별합니다. Resource Tagger에서 지원하는 리소스 유형만 포함됩니다.
리소스 ID	resource_id	Resource Tagger에서 지원하는 리소스의 고유 식별자입니다.
적용 범위 상태	coverage_state	이 필드는 리소스가 Resource Tagger 구성 ID로 구성된 대로 태그가 지정되었는지 여부를 나타냅니다.
구성 프로필 ID	configuration_profile_id	Resource Tagger 구성 프로필의 ID입니다. 구성 프로파일은 리소스에 태그를 지정하는 데 사용되는 정책 및 규칙을 정의하는 데 사용됩니다.

보안 구성 규칙 대시보드

보안 구성 규칙 대시보드는 AMS 계정의 리소스 및 AWS Config 규칙 규정 준수를 자세히 살펴봅니다. 보고서를 규칙 심각도별로 필터링하여 가장 중요한 조사 결과의 우선순위를 지정할 수 있습니다. 다음 표에는이 보고서에서 제공하는 데이터가 나열되어 있습니다.

필드 이름	데이터 세트 필드 이름	정의
AWS 계정 ID	AWS 계정 ID	관련 리소스에 연결된 계정 ID입니다.
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	보고서 날짜	보고서가 생성된 날짜 및 시간입니다.
customer_name	고객 이름	고객 이름입니다.
account_name	계정 이름	계정 ID와 연결된 이름
resource_id	리소스 ID	리소스의 식별자입니다.
resource_region	리소스 리전	리소스가 AWS 리전 있는 입니다.
resource_type	리소스 유형	AWS 서비스 또는 리소스 유형입니다.
resource_name	리소스 이름	리소스의 이름입니다.
resource_ams_flag	리소스 AMS 플래그	리소스가 AMS 소유인 경우이 플래그는 TRUE로 설정됩니다. 리소스가 고객 소유인 경우이 플래그는 FALSE로 설정됩니다. 소유권을 알 수 없는 경우이 플래그는 UNKNOWN으로 설정됩니다.
config_rule	Config 규칙	구성 규칙의 사용자 지정할 수 없는 이름입니다.
config_rule_description	구성 규칙 설명	구성 규칙에 대한 설명입니다.
source_identifier	소스 식별자	관리형 구성 규칙의 고유 식별자이며 사용자 지정 구성 규칙의 식별자는 없습니다.
규정 준수_플래그	규정 준수 플래그	리소스가 구성 규칙을 준수하는지 또는 준수하지 않는지를 표시합니다.

필드 이름	데이터 세트 필드 이름	정의
rule_type	규칙 유형	규칙이 사전 정의 또는 사용자 지정 빌드되었는지 여부를 나타냅니다.
exception_flag	예외 플래그	리소스 예외 플래그는 규정 미준수 리소스에 대한 위험 수락을 보여줍니다. 리소스에 대한 리소스 예외 플래그가 TRUE인 경우 리소스는 제외됩니다. 예외 플래그가 NULL인 경우 리소스는 제외되지 않습니다.
cal_dt	Date	규칙의 평가 날짜입니다.
remediation_description	문제 해결 설명	규칙 규정 준수를 해결하는 방법에 대한 설명입니다.
severity	심각도	구성 규칙 심각도는 규정 미준수의 영향을 나타냅니다.
customer_action	고객 작업	따라서 규칙을 수정하는 데 필요한 작업입니다.
recommendation	권장 사항	구성 규칙이 확인하는 항목에 대한 설명입니다.
문제 해결_범주	문제 해결 범주	이 규칙을 준수하지 않을 때 AMS가 수행하는 기본 작업입니다.

데이터 보존 정책

AMS SSR에는 보고된 기간, 데이터가 지워지고 더 이상 사용할 수 없게 된 후 보고서당 데이터 보존 정책이 있습니다.

보고서 이름	데이터 보존 SSR 콘솔	데이터 보존 SSR S3 버킷
AMS 패치에 대한 인스턴스 세부 정보 요약	2개월	2년
패치 세부 정보	2개월	2년
유지 관리 기간 실행 중에 패치를 놓친 인스턴스	2개월	2년
AMS 결제 요금 세부 정보	2년	2년
일별 백업 보고서	1개월	2년
주간 인시던트 보고서	2개월	2년
보안 구성 규칙 대시보드	3개월	2년
Resource Tagger 대시보드	1년	2년

SSR에서 오프보드

SSR 서비스에서 오프보드하려면 AMS 콘솔을 통해 서비스 요청(SR)을 생성합니다. SR을 제출하면 AMS 운영 엔지니어가 SSR에서 오프보딩하는 데 도움을 줍니다. SR에서 오프보딩하려는 이유를 입력합니다.

계정을 오프보딩하고 리소스 정리를 수행하려면 AMS 콘솔을 통해 SR을 생성합니다. SR을 제출하면 AMS 운영 엔지니어가 SSR Amazon S3 버킷을 삭제하는 데 도움을 줍니다.

AMS에서 오프보딩하면 AMS SSR 콘솔에서 자동으로 오프보딩됩니다. AMS는 자동으로 사용자 계정으로 데이터 전송을 중지합니다. AMS는 오프보딩 프로세스의 일부로 SSR S3 버킷을 삭제합니다.

AMS Accelerate의 액세스 관리

액세스 관리는 권한 있고 인증된 액세스만 허용하여 리소스를 보호하는 방법입니다. AMS Accelerate를 사용하면 액세스 관리 솔루션, 액세스 정책 및 관련 프로세스와 같은 AWS 계정 및 기본 리소스에 대한 액세스를 관리할 책임이 있습니다. 액세스 솔루션을 관리하는 데 도움이 되도록 AMS Accelerate는 일반적인 IAM 구성 오류를 감지한 다음 문제 해결 알림을 전송하는 AWS Config 규칙을 배포합니다. 일반적인 IAM 구성 오류는 루트 사용자에게 액세스 키가 있다는 것입니다. `iam-root-access-key-check` 구성 규칙은 루트 사용자 액세스 키를 사용할 수 있고 규정을 준수하는지 또는 액세스 키가 없는지 확인합니다. AMS에서 배포한 구성 규칙 목록은 AMS AWS Config 규칙 라이브러리를 참조하세요.

주제

- Accelerate 콘솔에 액세스
- AMS 기능을 사용할 수 있는 권한
- AMS가 계정에 액세스하는 이유와 시간
- AMS가 계정에 액세스하는 방법
- AMS에서 루트 사용자 계정을 사용하는 방법 및 시기

Accelerate 콘솔에 액세스

Accelerate로 온보딩하면 Accelerate 콘솔에 자동으로 액세스할 수 있습니다. AWS 관리 콘솔에서 관리형 서비스를 검색하여 콘솔에 액세스할 수 있습니다. Accelerate 콘솔은 Accelerate의 기능에 대한 요약된 보기를 제공합니다. 이 보기에는 대시보드와 구성 페이지에 표시되는 개별 구성 요소가 포함됩니다.

AMS 기능을 사용할 수 있는 권한

사용자가 AMS 콘솔 액세스 또는 백업 구성과 같은 AMS Accelerate 기능을 읽고 구성할 수 있도록 하려면 IAM 역할에 이러한 작업을 수행할 수 있는 명시적 권한을 부여해야 합니다. 다음 CloudFormation 템플릿에는 IAM 역할에 할당할 수 있도록 AMS와 연결된 서비스를 읽고 구성하는 데 필요한 정책이 포함되어 있습니다. 관리자 또는 읽기 전용 권한이 필요한 IT 업계의 일반적인 직무 책임과 밀접하게 일치하도록 설계되었습니다. 그러나 사용자에게 다른 권한을 부여해야 하는 경우 정책을 편집하여 특정 권한을 포함하거나 제외할 수 있습니다. 또한 사용자 고유의 사용자 지정 정책을 만들 수도 있습니다.

템플릿은 두 가지 정책을 제공합니다. 이 AMSAccelerateAdminAccess 정책은 AMS Accelerate 구성 요소를 설정하고 운영하는 데 사용됩니다. 이 정책은 일반적으로 IT 관리자가 수임하며 패치 및 백업과 같은 AMS 기능을 구성할 수 있는 권한을 부여합니다. 는 AMS Accelerate 관련 리소스를 보는 데 필요한 최소 권한을 AMSAccelerateReadOnly 부여합니다.

```
AWSTemplateFormatVersion: 2010-09-09
Description: AMSAccelerateCustomerAccessPolicies

Resources:
  AMSAccelerateAdminAccess:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateAdminAccess
      Path: /
      PolicyDocument:
        Fn::Sub:
        - |
          {
            "Version": "2012-10-17",
            "Statement": [
              {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
              {
                "Sid": "AmsBackupPolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/ams-backup-iam-role"
              },
              {
                "Sid": "AmsChangeRecordKMSPolicy",
                "Effect": "Allow",
                "Action": [
                  "kms:Encrypt",
                  "kms:Decrypt",
                  "kms:GenerateDataKey"
                ],
                "Resource": [
                  "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
                ],
```

```
                "Condition": {
                  "ForAnyValue:StringLike": {
                    "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                  }
                }
              },
              {
                "Sid": "AmsChangeRecordAthenaReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "athena:BatchGetNamedQuery",
                  "athena:Get*",
                  "athena:List*",
                  "athena:StartQueryExecution",
                  "athena:UpdateWorkGroup",
                  "glue:GetDatabase*",
                  "glue:GetTable*",
                  "s3:GetAccountPublicAccessBlock",
                  "s3:ListAccessPoints",
                  "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AmsChangeRecordS3ReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:Get*",
                  "s3:List*"
                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/
*",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
                ]
              },
              {
                "Sid": "AmsChangeRecordS3WritePolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:PutObject",
                  "s3:PutObjectLegalHold",
```

```
            "s3:PutObjectRetention"

          ],
          "Resource": [
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
          ]
        },
        {
          "Sid": "MaciePolicy",
          "Effect": "Allow",
          "Action": [
            "macie2:GetFindingStatistics"
          ],
          "Resource": "*"
        },
        {
          "Sid": "GuardDutyPolicy",
          "Effect": "Allow",
          "Action": [
            "guardduty:GetFindingsStatistics",
            "guardduty:ListDetectors"
          ],
          "Resource": "*"
        },
        {
          "Sid": "SupportPolicy",
          "Effect": "Allow",
          "Action": "support:*",
          "Resource": "*"
        },
        {
          "Sid": "ConfigPolicy",
          "Effect": "Allow",
          "Action": [
            "config:Get*",
            "config:Describe*",
            "config:Deliver*",
            "config:List*",
            "config:StartConfigRulesEvaluation"
          ],
          "Resource": "*"
        },
        {
          "Sid": "AppConfigReadPolicy",
```

```
                "Effect": "Allow",
                "Action": [
                  "appconfig:List*",
                  "appconfig:Get*"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AppConfigPolicy",
                "Effect": "Allow",
                "Action": [
                  "appconfig:StartDeployment",
                  "appconfig:StopDeployment",
                  "appconfig:CreateHostedConfigurationVersion",
                  "appconfig:ValidateConfiguration"
                ],
                "Resource": [
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/configurationprofile/
${AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/environment/*",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/configurationprofile/
${AMSResourceTaggerConfigurationCustomerManagedTagsProfileID}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/environment/*",
                  "arn:aws:appconfig:*:${AWS::AccountId}:deploymentstrategy/*"
                ]
              },
              {
                "Sid": "CloudFormationStacksPolicy",
                "Effect": "Allow",
                "Action": [
                  "cloudformation:DescribeStacks"
                ],
                "Resource": "*"
              },
              {
                "Sid": "EC2Policy",
```

```
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "SSMPolicy",
      "Effect": "Allow",
      "Action": [
        "ssm:AddTagsToResource",
        "ssm:CancelCommand",
        "ssm:CancelMaintenanceWindowExecution",
        "ssm:CreateAssociation",
        "ssm:CreateAssociationBatch",
        "ssm:CreateMaintenanceWindow",
        "ssm:CreateOpsItem",
        "ssm:CreatePatchBaseline",
        "ssm:DeleteAssociation",
        "ssm:DeleteMaintenanceWindow",
        "ssm:DeletePatchBaseline",
        "ssm:DeregisterPatchBaselineForPatchGroup",
        "ssm:DeregisterTargetFromMaintenanceWindow",
        "ssm:DeregisterTaskFromMaintenanceWindow",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "ssm:PutConfigurePackageResult",
        "ssm:RegisterDefaultPatchBaseline",
        "ssm:RegisterPatchBaselineForPatchGroup",
        "ssm:RegisterTargetWithMaintenanceWindow",
        "ssm:RegisterTaskWithMaintenanceWindow",
        "ssm:RemoveTagsFromResource",
        "ssm:SendCommand",
        "ssm:StartAssociationsOnce",
        "ssm:StartAutomationExecution",
        "ssm:StartSession",
        "ssm:StopAutomationExecution",
        "ssm:TerminateSession",
        "ssm:UpdateAssociation",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateMaintenanceWindow",
        "ssm:UpdateMaintenanceWindowTarget",
        "ssm:UpdateMaintenanceWindowTask",
```

```
            "ssm:UpdateOpsItem",
            "ssm:UpdatePatchBaseline"
          ],
          "Resource": "*"
        },
        {
          "Sid": "AmsPatchRestrictAMSResources",
          "Effect": "Deny",
          "Action": [
            "ssm:DeletePatchBaseline",
            "ssm:UpdatePatchBaseline"
          ],
          "Resource": [
            "arn:aws:ssm:${AWS::Region}:${AWS::AccountId}:patchbaseline/*"
          ],
          "Condition": {
            "StringLike": {
              "aws:ResourceTag/ams:resourceOwner": "*"
            }
          }
        },
        {
          "Sid": "AmsPatchRestrictAmsTags",
          "Effect": "Deny",
          "Action": [
            "ssm:AddTagsToResource",
            "ssm:RemoveTagsFromResource"
          ],
          "Resource": "*",
          "Condition": {
            "ForAnyValue:StringLike": {
              "aws:TagKeys": [
                "AMS*",
                "Ams*",
                "ams*"
              ]
            }
          }
        },
        {
          "Sid": "TagReadPolicy",
          "Effect": "Allow",
          "Action": [
            "tag:GetResources",
```

```
                "tag:GetTagKeys"
              ],
              "Resource": "*"
            },
            {
              "Sid": "CloudtrailReadPolicy",
              "Effect": "Allow",
              "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
              ],
              "Resource": "*"
            },
            {
              "Sid": "EventBridgePolicy",
              "Effect": "Allow",
              "Action": [
                "events:Describe*",
                "events:List*",
                "events:TestEventPattern"
              ],
              "Resource": "*"
            },
            {
              "Sid": "IAMReadOnlyPolicy",
              "Action": [
                  "iam:ListRoles",
                  "iam:GetRole"
              ],
              "Effect": "Allow",
              "Resource": "*"
            },
            {
              "Sid": "AmsResourceSchedulerPassRolePolicy",
              "Effect": "Allow",
              "Action": "iam:PassRole",
              "Resource": "arn:aws:iam::${AWS::AccountId}:role/
ams_resource_scheduler_ssm_automation_role",
              "Condition": {
                  "StringEquals": {
                      "iam:PassedToService": "ssm.amazonaws.com"
                  }
              }
```

```
              }
            ]
          }
        - AMSAlarmManagerConfigurationApplicationId: !ImportValue "AMS-Alarm-Manager-
Configuration-ApplicationId"
          AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID: !ImportValue
 "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID"
          AMSResourceTaggerConfigurationApplicationId: !ImportValue "AMS-
ResourceTagger-Configuration-ApplicationId"
          AMSResourceTaggerConfigurationCustomerManagedTagsProfileID: !ImportValue
 "AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID"

  AMSAccelerateReadOnly:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateReadOnly
      Path: /
      PolicyDocument: !Sub |
        {
          "Version": "2012-10-17",
          "Statement": [
          {
                "Sid": "AmsSelfServiceReport",
                "Effect": "Allow",
                "Action": "amsssrv:*",
                "Resource": "*"
             },
           {
              "Sid": "AmsBackupPolicy",
              "Effect": "Allow",
              "Action": [
                "backup:Describe*",
                "backup:Get*",
                "backup:List*"
              ],
              "Resource": "*"
           },
           {
               "Action": [
                   "rds:DescribeDBSnapshots",
                   "rds:ListTagsForResource",
                   "rds:DescribeDBInstances",
                   "rds:describeDBSnapshots",
                   "rds:describeDBEngineVersions",
```

```
                "rds:describeOptionGroups",
                "rds:describeOrderableDBInstanceOptions",
                "rds:describeDBSubnetGroups",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBInstanceAutomatedBackups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "dynamodb:ListBackups",
                "dynamodb:ListTables"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "elasticfilesystem:DescribeFilesystems"
            ],
            "Resource": "arn:aws:elasticfilesystem:*:*:file-system/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:describeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
```

```
            {
                "Action": [
                    "tag:GetTagKeys",
                    "tag:GetTagValues",
                    "tag:GetResources"
                ],
                "Effect": "Allow",
                "Resource": "*"
            },
            {
                "Effect": "Allow",
                "Action": [
                    "storagegateway:DescribeCachediSCSIVolumes",
                    "storagegateway:DescribeStorediSCSIVolumes"
                ],
                "Resource": "arn:aws:storagegateway:*:*:gateway/*/volume/*"
            },
            {
                "Effect": "Allow",
                "Action": [
                    "storagegateway:ListGateways"
                ],
                "Resource": "arn:aws:storagegateway:*:*:*"
            },
            {
                "Effect": "Allow",
                "Action": [
                    "storagegateway:DescribeGatewayInformation",
                    "storagegateway:ListVolumes",
                    "storagegateway:ListLocalDisks"
                ],
                "Resource": "arn:aws:storagegateway:*:*:gateway/*"
            },
            {
                "Action": [
                    "iam:ListRoles",
                    "iam:GetRole"
                ],
                "Effect": "Allow",
                "Resource": "*"
            },
            {
                "Effect": "Allow",
                "Action": "organizations:DescribeOrganization",
```

```
            "Resource": "*"
        },
        {
            "Action": "fsx:DescribeBackups",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:backup/*"
        },
        {
            "Action": "fsx:DescribeFileSystems",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:file-system/*"
        },
        {
            "Action": "ds:DescribeDirectories",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
          "Sid": "AmsChangeRecordKMSPolicy",
          "Effect": "Allow",
          "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:GenerateDataKey"
          ],
          "Resource": [
            "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
          ],
          "Condition": {
            "ForAnyValue:StringLike": {
              "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
            }
          }
        },
        {
          "Sid": "AmsChangeRecordAthenaReadPolicy",
          "Effect": "Allow",
          "Action": [
            "athena:BatchGetNamedQuery",
            "athena:Get*",
            "athena:List*",
            "athena:StartQueryExecution",
            "athena:UpdateWorkGroup",
            "glue:GetDatabase*",
```

```
            "glue:GetTable*",
            "s3:GetAccountPublicAccessBlock",
            "s3:ListAccessPoints",
            "s3:ListAllMyBuckets"
          ],
          "Resource": "*"
        },
        {
          "Sid": "AmsChangeRecordS3ReadPolicy",
          "Effect": "Allow",
          "Action": [
            "s3:Get*",
            "s3:List*"
          ],
          "Resource": [
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*",
            "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
            "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
          ]
        },
        {
          "Sid": "AmsChangeRecordS3WritePolicy",
          "Effect": "Allow",
          "Action": [
            "s3:PutObject",
            "s3:PutObjectLegalHold",
            "s3:PutObjectRetention"
          ],
          "Resource": [
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
          ]
        },
        {
          "Sid": "MaciePolicy",
          "Effect": "Allow",
          "Action": [
            "macie2:GetFindingStatistics"
          ],
          "Resource": "*"
        },
        {
          "Sid": "GuardDutyReadPolicy",
          "Effect": "Allow",
```

```
            "Action": [
              "guardduty:GetFindingsStatistics",
              "guardduty:ListDetectors"
            ],
            "Resource": "*"
          },
          {
            "Sid": "SupportReadPolicy",
            "Effect": "Allow",
            "Action": "support:Describe*",
            "Resource": "*"
          },
          {
            "Sid": "ConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "config:Get*",
              "config:Describe*",
              "config:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "AppConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "appconfig:List*",
              "appconfig:Get*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudFormationReadPolicy",
            "Effect": "Allow",
            "Action": [
              "cloudformation:DescribeStacks"
            ],
            "Resource": "*"
          },
          {
            "Sid": "EC2ReadPolicy",
            "Effect": "Allow",
            "Action": [
              "ec2:DescribeInstances"
```

```
            ],
            "Resource": "*"
          },
          {
            "Sid": "SSMReadPolicy",
            "Effect": "Allow",
            "Action": [
              "ssm:Describe*",
              "ssm:Get*",
              "ssm:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "TagReadPolicy",
            "Effect": "Allow",
            "Action": [
              "tag:GetResources",
              "tag:GetTagKeys"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudtrailReadPolicy",
            "Effect": "Allow",
            "Action": [
              "cloudtrail:DescribeTrails",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
          },
          {
            "Sid": "EventBridgePolicy",
            "Effect": "Allow",
            "Action": [
              "events:Describe*",
              "events:List*",
              "events:TestEventPattern"
            ],
            "Resource": "*"
          }
        ]
```

```
        }
```

AMS가 계정에 액세스하는 이유와 시간

AMS Accelerate(Accelerate) 운영자는 특정 상황에서 리소스 관리를 위해 계정 콘솔 및 인스턴스에 액세스할 수 있습니다. 이러한 액세스 이벤트는 AWS CloudTrail (CloudTrail) 로그에 문서화됩니다. AMS Accelerate Operations 팀 및 AMS Accelerate 자동화를 통해 계정의 활동을 검토하는 방법에 대한 자세한 내용은 섹션을 참조하세요AMS Accelerate 계정의 변경 사항 추적.

AMS가 계정에 액세스하는 이유, 시기 및 방법은 다음 주제에 설명되어 있습니다.

AMS 고객 계정 액세스 트리거

AMS 고객 계정 액세스 활동은 트리거에 의해 구동됩니다. 오늘 트리거는 Amazon CloudWatch(CloudWatch) 경보 및 이벤트에 대한 응답으로 문제 관리 시스템에서 생성된 AWS 티켓과 제출한 인시던트 보고서 또는 서비스 요청입니다. 각 액세스에 대해 여러 서비스 호출 및 호스트 수준 활동을 수행할 수 있습니다.

액세스 근거, 트리거 및 트리거의 이니시에이터는 다음 표에 나열되어 있습니다.

액세스 트리거

액세스	시작한 사용자	트리거
패치 적용	AMS	패치 문제
내부 문제 조사	AMS	문제 문제(시스템적으로 식별된 문제)
알림 조사 및 문제 해결	AMS	AWS Systems Manager 운영 작업 항목(SSM OpsItems)
인시던트 조사 및 해결	사용자	인바운드 지원 사례(제출한 인시던트 또는 서비스 요청)
인바운드 서비스 요청 이행	사용자	

AMS 고객 계정 액세스 IAM 역할

AMS 운영자가 계정을 서비스하려면 다음 역할이 필요합니다.

> **Note**
>
> AMS 액세스 역할을 사용하면 AMS 운영자가 리소스에 액세스하여 AMS 기능을 제공할 수 있습니다(참조서비스 설명). 이러한 역할을 변경하면 이러한 기능을 제공할 수 없게 될 수 있습니다. AMS 액세스 역할을 변경해야 하는 경우 Cloud Architect에 문의하세요.

고객 계정에 대한 AMS 액세스를 위한 IAM 역할

역할 이름	설명
ams-access-admin	이 역할에는 제한 없이 계정에 대한 전체 관리 액세스 권한이 있습니다. AMS 서비스는 AMS 인프라를 배포하고 계정을 운영하기 위한 액세스를 제한하는 제한적인 세션 정책과 함께이 역할을 사용합니다.
ams-access-admin-operations	이 역할은 AMS 운영자에게 계정을 운영할 수 있는 관리 권한을 부여합니다. 이 역할은 Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift, Amazon ElastiCache와 같이 데이터 스토어로 일반적으로 사용되는 AWS 서비스의 고객 콘텐츠에 대한 읽기, 쓰기 또는 삭제 권한을 부여하지 않습니다. 액세스 관리에 대한 이해와 배경 지식을 갖춘 적격 AMS 운영자만이 역할을 수임할 수 있습니다. 이러한 연산자는 액세스 관리 문제 및 계정에 대한 에스컬레이션 지점 역할을 하여 AMS 연산자 액세스 문제를 해결합니다.
ams-access-management	온보딩 중에 수동으로 배포됩니다. AMS Access 시스템에서 `ams-access-roles` 및 `ams-access-managed-policies` 스택을 관리하려면이 역할이 필요합니다.
ams-access-operations	이 역할에는 계정에서 관리 작업을 수행할 수 있는 권한이 있습니다. 이 역할에는 Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift, Amazon ElastiCache와 같이 데이터 스토어로 일반적으로 사

역할 이름	설명
	용되는 AWS 서비스의 고객 콘텐츠에 대한 읽기, 쓰기 또는 삭제 권한이 없습니다. AWS Identity and Access Management 쓰기 작업을 수행할 수 있는 권한도이 역할에서 제외됩니다. AMS Accelerate 운영 직원 및 클라우드 아키텍트(CAs)가이 역할을 맡을 수 있습니다.
ams-access-read-only	이 역할에는 계정에 대한 읽기 전용 액세스 권한이 있습니다. AMS Accelerate 운영 직원 및 클라우드 아키텍트(CAs)가이 역할을 맡을 수 있습니다. Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift, ElastiCache와 같이 데이터 스토어로 일반적으로 사용되는 AWS 서비스의 고객 콘텐츠에 대한 읽기 권한은이 역할에 부여되지 않습니다.
ams-access-security-analyst	이 AMS 보안 역할은 AMS 계정에 전용 보안 알림 모니터링 및 보안 인시던트 처리를 수행할 수 있는 권한이 있습니다. 일부 AMS 보안 담당자만이 역할을 수임할 수 있습니다.
ams-access-security-analyst-read-only	이 AMS 보안 역할은 전용 보안 알림 모니터링 및 보안 인시던트 처리를 수행할 수 있는 AMS 계정의 읽기 전용 권한으로 제한됩니다.

> **Note**
>
> ams-access-management 역할의 템플릿입니다. 온보딩 시 클라우드 아키텍트(CAs)가 계정에 수동으로 배포하는 스택은 management-role.yaml입니다.
> ams-access-read-only, ams-access-operations, ams-access-admin-operations, ams-access-admin: accelerate-roles.json 등 다양한 액세스 수준에 대한 다양한 액세스 역할을 위한 템플릿입니다.

AMS가 계정에 액세스하는 방법

AMS Accelerate 운영자는 특정 상황에서 계정 콘솔 및 인스턴스에 액세스할 수 있습니다.

AMS 운영자는 내부 AMS Accelerate 액세스 서비스를 사용하여 안전하고 감사된 방식으로 계정에 액세스합니다. 인스턴스에 액세스하기 위해 AMS 운영자는 브로커와 동일한 내부 AMS 액세스 서비스를 사용하고 액세스 권한이 부여되면 AMS Accelerate 운영자는 SSM 세션 관리자를 사용하여 세션 자격 증명을 사용하여 액세스 권한을 얻습니다. Windows 인스턴스에 대한 RDP 액세스는 인스턴스로 포트 전달을 설정하고 SSM을 사용하여 로컬 사용자를 생성하여 제공됩니다. 로컬 사용자 자격 증명은 RDP 액세스에 사용되며 세션이 끝날 때 제거됩니다.

AMS에서 루트 사용자 계정을 사용하는 방법 및 시기

루트 사용자는 계정 AWS 내의 수퍼유저입니다. AMS는 루트 사용량을 모니터링합니다. 계정 설정 변경, 결제 및 비용 관리에 대한 (IAM) 액세스 활성화 AWS Identity and Access Management , 루트 암호 변경, 멀티 팩터 인증(MFA) 활성화 등 필요한 몇 가지 작업에만 루트를 사용하는 것이 좋습니다. AWS Identity and Access Management 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하세요.

AMS Accelerate를 사용한 루트:

AMS는 루트 사용자 계정 사용을 금지하지 않습니다. 그러나 AMS Operations and Security는 사용량을 조사할 문제로 취급하며, 사용할 때마다 보안 팀에 연락할 것입니다.

24시간 전에 CSDM 및 CA에 문의하여 수행하려는 루트 액세스 작업에 대해 알리는 것이 좋습니다.

AMS 작업 및 루트 사용에 대한 보안 응답:

AMS는 루트 사용자 계정이 사용될 때 경보를 수신합니다. 루트 자격 증명 사용이 예약되지 않은 경우 AMS 보안 팀 및 계정 팀에 문의하여 예상되는 활동인지 확인합니다. 예기치 않은 활동인 경우 AMS는 보안 팀과 협력하여 문제를 조사합니다.

AMS Accelerate의 보안 관리

AWS Managed Services는 여러 제어를 사용하여 정보 자산을 보호하고 AWS 인프라를 안전하게 유지할 수 있도록 지원합니다. AMS Accelerate는 모든 계정이 보안 AWS Config 규칙 및 운영 무결성에 대한 업계 표준을 준수하도록 및 수정 작업 라이브러리를 유지 관리합니다.는 기록된 리소스 간의 구성 변경을 AWS Config 규칙 지속적으로 추적합니다. 변경 사항이 규칙 조건을 위반하는 경우 AMS는 결과를 보고하고 위반의 심각도에 따라 위반을 자동으로 또는 요청으로 해결할 수 있습니다. 인터넷 보안 센터(CIS), 미국 국립 표준 기술 연구소(NIST) 클라우드 보안 프레임워크(CSF), 건강 보험 양도 및 책임에 관한 법률(HIPAA) 및 결제 카드 산업(PCI) 데이터 보안 표준(DSS)에서 설정한 표준을 AWS Config 규칙 쉽게 준수할 수 있습니다.

또한 AMS는 Amazon GuardDuty를 활용하여 AWS 환경에서 잠재적으로 승인되지 않았거나 악의적인 활동을 식별합니다. AMS는 GuardDuty 결과를 연중무휴 모니터링합니다. AMS는 고객과 협력하여 조사 결과의 영향을 이해하고 모범 사례 권장 사항을 기반으로 문제 해결을 식별합니다. 또한 AMS는 Amazon Macie를 사용하여 개인 건강 정보(PHI), 개인 식별 정보(PII) 및 금융 데이터와 같은 민감한 데이터를 보호합니다.

> **Note**
>
> Amazon Macie는 선택적 서비스이며 기본적으로 활성화되어 있지 않습니다.

AMS Accelerate는 운영 우수성을 달성하는 데 도움이 되는 다양한 운영 서비스를 제공합니다 AWS. 연중무휴 24시간 헬프데스크, 사전 모니터링, 보안, 패치 적용, 로깅 및 백업을 포함한 AMS 주요 운영 기능을 AWS 클라우드 통해 팀이에서 전반적인 운영 우수성을 달성하는 데 AMS가 어떻게 도움이 되는지 자세히 알아보려면 AMS 참조 아키텍처 다이어그램을 참조하세요.

주제

- Log4j SSM 문서를 사용하여 Accelerate에서 발생 항목 검색
- AMS의 인프라 보안 모니터링
- Accelerate의 데이터 보호
- AWS Identity and Access Management AMS Accelerate의
- AMS의 보안 인시던트 대응
- Accelerate의 보안 이벤트 로깅 및 모니터링
- Accelerate의 구성 규정 준수

- Accelerate의 인시던트 대응
- Accelerate의 복원력
- end-of-support 운영 체제에 대한 보안 제어
- Accelerate의 보안 모범 사례
- 변경 요청 보안 검토
- 보안 FAQ

Log4j SSM 문서를 사용하여 Accelerate에서 발생 항목 검색

Log4j AWS Systems Manager 문서(SSM 문서)는 수집된 워크로드 내에서 Apache Log4j2 라이브러리를 검색하는 데 도움이 됩니다. 자동화 문서는 Log4j2 라이브러리가 활성화된 Java 애플리케이션(들)의 프로세스 ID에 대한 보고서를 제공합니다.

보고서에는 JndiLookup 클래스가 포함된 지정된 환경 내에 있는 Java 아카이브(JAR 파일)에 대한 정보가 포함되어 있습니다. 검색된 라이브러리를 사용 가능한 최신 버전으로 업그레이드하는 것이 가장 좋습니다. 이 업그레이드는 CVE-2021-44228을 통해 식별된 원격 코드 실행(RCE)을 완화합니다. Apache에서 최신 버전의 Log4j 라이브러리를 다운로드합니다. 자세한 내용은 Apache Log4j 2 다운로드를 참조하세요.

문서는 Accelerate에 온보딩된 모든 리전과 공유됩니다. 문서에 액세스하려면 다음 단계를 완료합니다.

1. https://console.aws.amazon.com/systems-manager/ AWS Systems Manager 콘솔을 엽니다.
2. 탐색 창에서 Documents를 선택합니다.
3. 나와 공유를 선택합니다.
4. 검색 상자에 AWSManagedServices-GatherLog4jInformation을 입력합니다.
5. 속도 제어를 사용하여 문서를 대규모로 실행합니다.

AWSManagedServices-GatherLog4jInformation 문서는 다음 파라미터를 수집합니다.

- InstanceId: EC2 인스턴스의 (필수) ID입니다.
- S3Bucket: (선택 사항) 결과를 업로드할 S3 미리 서명된 URL 또는 S3 URI(s3://BUCKET_NAME)입니다.
- AutomationAssumeRole: (필수) 자동화가 사용자를 대신하여 작업을 수행하도록 허용하는 역할의 ARN입니다.

속도 제어를 사용하여이 문서를 실행하는 것이 가장 좋습니다. 속도 제어 파라미터를 InstanceId로 설정하고 인스턴스 목록을 할당하거나 태그 키 조합을 적용하여 특정 태그가 있는 모든 EC2 인스턴스를 대상으로 지정할 수 있습니다. 또한 AWS Managed Services는 Amazon S3S3) 버킷을 제공할 것을 권장합니다. S3에서 결과를 집계하는 방법의 예는 EC2 인스턴스 스택 | Log4j 정보 수집을 참조하세요.

패키지를 업그레이드할 수 없는 경우 AWS 보안 서비스 사용에 나와 있는 AWS 보안 지침에 따라 Log4j 취약성을 방지, 탐지 및 대응합니다. JndiLookup 클래스 기능을 제거하여 취약성을 완화하려면 Java 애플리케이션(들)과 인라인으로 Log4j 핫 패치를 실행합니다. 핫 패치에 대한 자세한 내용은 Hotpatch for Apache Log4j를 참조하세요.

자동화의 출력 또는 추가 완화 조치를 진행하는 방법에 대한 질문은 서비스 요청을 제출하세요.

AMS의 인프라 보안 모니터링

AMS Accelerate에 온보딩하면가 다음과 같은 AWS Config 기준 인프라와 규칙 세트를 AWS 배포합니다. AMS Accelerate는 이러한 규칙을 사용하여 계정을 모니터링합니다.

- AWS Config 서비스 연결 역할: AMS Accelerate는 AWSServiceRoleForConfig라는 서비스 연결 역할을 배포합니다.이 역할은에서 다른 AWS 서비스의 상태를 쿼리 AWS Config 하는 데 사용됩니다. AWSServiceRoleForConfig 서비스 연결 역할은 AWS Config 서비스를 신뢰하여 역할을 수임합니다. AWSServiceRoleForConfig 역할에 대한 권한 정책에는 AWS Config 리소스에 대한 읽기 전용 및 쓰기 전용 권한과가 AWS Config 지원하는 다른 서비스의 리소스에 대한 읽기 전용 권한이 포함되어 있습니다. AWS Config 레코더로 구성된 역할이 이미 있는 경우 AMS Accelerate는 기존 역할에 AWS Config 관리형 정책이 연결되어 있는지 확인합니다. 그렇지 않은 경우 AMS Accelerate는 역할을 서비스 연결 역할 AWSServiceRoleForConfig로 바꿉니다.
- AWS Config 레코더 및 전송 채널: 구성 레코더를 AWS Config 사용하여 리소스 구성의 변경 사항을 감지하고 이러한 변경 사항을 구성 항목으로 캡처합니다. AMS Accelerate는 모든 리소스의 지속적인 기록 AWS 리전과 함께 모든 서비스에 구성 레코더를 배포합니다. 또한 AMS Accelerate는 AWS 리소스에서 발생하는 변경 사항을 기록하는 데 사용되는 Amazon S3 버킷인 구성 전송 채널을 생성합니다. 구성 레코더는 전송 채널을 통해 구성 상태를 업데이트합니다. 가 작동 AWS Config 하려면 구성 레코더 및 전송 채널이 필요합니다. AMS Accelerate는 모든에 레코더를 AWS 리전생성하고 단일에 전송 채널을 생성합니다 AWS 리전. 에 이미 레코더 및 전송 채널이 있는 경우 AWS 리전 AMS Accelerate는 기존 AWS Config 리소스를 삭제하지 않고 대신 AMS Accelerate는 기존 레코더 및 전송 채널이 제대로 구성되었는지 확인한 후 기존 레코더 및 전송 채널을 사용합니다. AWS Config 비용 절감 방법에 대한 자세한 내용은 섹션을 참조하세요Accelerate에서 AWS Config 비용 절감.
- AWS Config 규칙: AMS Accelerate는 보안 AWS Config 규칙 및 운영 무결성에 대한 업계 표준을 준수하는 데 도움이 되는 및 수정 작업 라이브러리를 유지 관리합니다.는 기록된 리소스 간의 구성 변경을 AWS Config 규칙 지속적으로 추적합니다. 변경 사항이 규칙 조건을 위반하는 경우 AMS는 조

사 결과를 보고하고 위반의 심각도에 따라 위반을 자동으로 또는 요청으로 해결할 수 있습니다.는 인터넷 보안 센터(CIS), 미국 국립 표준 기술 연구소(NIST) 클라우드 보안 프레임워크(CSF), 건강 보험 양도 및 책임에 관한 법률(HIPAA), 결제 카드 산업(PCI) 데이터 보안 표준(DSS)에서 설정한 표준을 AWS Config 규칙 쉽게 준수할 수 있습니다.

- AWS Config 애그리게이터 권한 부여: 애그리게이터는 여러 계정 및 여러 리전에서 AWS Config 구성 및 규정 준수 데이터를 수집하는 AWS Config 리소스 유형입니다. AMS Accelerate는 계정을 구성 애그리게이터에 온보딩하여 AMS Accelerate가 계정의 리소스 구성 정보를 집계하고 규정 준수 데이터를 구성하고 규정 준수 보고서를 생성합니다. AMS 소유 계정에 구성된 기존 애그리게이터가 있는 경우 AMS Accelerate는 추가 애그리게이터를 배포하고 기존 애그리게이터는 수정되지 않습니다.

> **Note**
>
> Config 애그리게이터는 계정에 설정되지 않고 AMS 소유 계정에 설정되며 계정(들)이 계정에 온보딩됩니다.

에 대한 자세한 내용은 다음을 AWS Config참조하세요.

- AWS Config: Config란 무엇입니까?
- AWS Config 규칙: 규칙을 사용하여 리소스 평가
- AWS Config 규칙: 동적 규정 준수 확인: AWS Config 규칙 - 클라우드 리소스에 대한 동적 규정 준수 확인
- AWS Config 집계자: 다중 계정 다중 리전 데이터 집계

보고서에 대한 자세한 내용은 단원을 참조하십시오AWS Config 제어 규정 준수 보고서.

AMS Accelerate에 서비스 연결 역할 사용

AMS Accelerate는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할(SLR)은 AMS Accelerate에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AMS Accelerate에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할을 사용하면 AMS Accelerate를 더 쉽게 설정할 수 있습니다. AMS Accelerate는 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않은 한 AMS Accelerate만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 AWS IAM으로 작업하는 서비스를 참조하고 서비스 연결 역할 열에서 Yes가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

AMS Accelerate의 배포 툴킷 서비스 연결 역할

AMS Accelerate는 AWSServiceRoleForAWSManagedServicesDeploymentToolkit이라는 서비스 연결 역할(SLR)을 사용합니다.이 역할은 AMS Accelerate 인프라를 고객 계정에 배포합니다.

> **Note**
>
> 이 정책은 최근에 업데이트되었습니다. 자세한 내용은 섹션을 참조하세요서비스 연결 역할에 대한 업데이트 가속화.

AMS Accelerate 배포 툴킷 SLR

AWSServiceRoleForAWSManagedServicesDeploymentToolkit 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `deploymenttoolkit.managedservices.amazonaws.com`

AWSManagedServicesDeploymentToolkitPolicy라는 정책은 AMS Accelerate가 다음 리소스에 대한 작업을 수행하도록 허용합니다.

- `arn:aws*:s3:::ams-cdktoolkit*`
- `arn:aws*:cloudformation:*:*:stack/ams-cdk-toolkit*`
- `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`

이 SLR은 AMS가 CloudFormation 템플릿 또는 Lambda 자산 번들과 같은 리소스를 구성 요소 배포 계정에 업로드하는 데 사용하는 배포 버킷을 생성하고 관리할 수 있는 권한을 Amazon S3에 부여합니다. 이 SLR은 배포 버킷을 정의하는 CloudFormation 스택을 배포할 수 있는 권한을 CloudFormation에 부여합니다. 자세한 내용을 보거나 정책을 다운로드하려면 AWSManagedServices_DeploymentToolkitPolicy를 참조하세요.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AMS Accelerate용 배포 툴킷 SLR 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS CLI, 또는 AWS API에서 AMS AWS Management Console에 온보딩하면 AMS Accelerate가 서비스 연결 역할을 생성합니다.

> **Important**
>
> 이 서비스 연결 역할은 서비스 연결 역할을 지원하기 시작한 2022년 6월 9일 이전에 AMS Accelerate 서비스를 사용 중인 경우 계정에 표시될 수 있으며, AMS Accelerate는 계정에 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 역할을 생성했습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. AMS에 온보딩하면 AMS Accelerate가 서비스 연결 역할을 다시 생성합니다.

AMS Accelerate용 배포 툴킷 SLR 편집

AMS Accelerate에서는 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

AMS Accelerate용 배포 툴킷 SLR 삭제

AWSServiceRoleForAWSManagedServicesDeploymentToolkit 역할을 수동으로 삭제할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API의 AMS에서 오프보딩하면 AMS Accelerate가 리소스를 정리하고 서비스 연결 역할을 삭제합니다.

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 서비스 연결 역할을 수동으로 삭제할 수도 있습니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려고 할 때 AMS Accelerate 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForAWSManagedServicesDeploymentToolkit 서비스 연결 역할에서 사용하는 AMS Accelerate 리소스를 삭제하려면

계정이 온보딩된 모든 리전의 AMS에서 `ams-cdk-toolkit` 스택을 삭제합니다(먼저 S3 버킷을 수동으로 비워야 할 수 있음).

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

Detective는 AMS Accelerate의 서비스 연결 역할을 제어합니다.

AMS Accelerate는 AWSServiceRoleForManagedServices_DetectiveControlsConfig라는 서비스 연결 역할(SLR)을 사용합니다. AWS Managed Services는이 서비스 연결 역할을 사용하여 config-recorder, config 규칙 및 S3 버킷 탐지 제어를 배포합니다.

AWSServiceRoleForManagedServices_DetectiveControlsConfig 서비스 연결 역할에 연결된 관리형 정책은 AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy입니다. 이 정책에 대한 업데이트는 AWS 관리형 정책에 대한 업데이트 가속화 섹션을 참조하세요.

AMS Accelerate용 탐지 제어 SLR에 대한 권한

AWSServiceRoleForManagedServices_DetectiveControlsConfig 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `detectivecontrols.managedservices.amazonaws.com`

이 역할에는 `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS 관리형 정책이 연결되어 있습니다(서비스AWS 관리형 정책: AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy는 역할을 사용하여 계정에서 AMS Detective 제어 구성을 생성하므로 s3 버킷, 구성 규칙 및 애그리게이터와 같은 리소스를 배포해야 함을 참조하세요. IAM 엔터티(예: 사용자, 그룹 또는 역할)가 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 권한을 구성해야 합니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

AMS Accelerate용 탐지 제어 SLR 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS CLI, 또는 AWS API에서 AMS AWS Management Console에 온보딩하면 AMS Accelerate가 서비스 연결 역할을 생성합니다.

> **Important**
>
> 이 서비스 연결 역할은 서비스 연결 역할을 지원하기 시작한 후 AMS Accelerate가 계정에 AWSServiceRoleForManagedServices_DetectiveControlsConfig 역할을 생성한 2022년 6월 9일 이전에 AMS Accelerate 서비스를 사용하는 경우 계정에 나타날 수 있습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. AMS에 온보딩하면 AMS Accelerate가 서비스 연결 역할을 다시 생성합니다.

AMS Accelerate용 탐지 제어 SLR 편집

AMS Accelerate에서는 AWSServiceRoleForManagedServices_DetectiveControlsConfig 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

AMS Accelerate용 탐지 제어 SLR 삭제

AWSServiceRoleForManagedServices_DetectiveControlsConfig 역할을 수동으로 삭제할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API의 AMS에서 오프보딩하면 AMS Accelerate가 리소스를 정리하고 서비스 연결 역할을 삭제합니다.

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 서비스 연결 역할을 수동으로 삭제할 수도 있습니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려고 할 때 AMS Accelerate 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForManagedServices_DetectiveControlsConfig 서비스 연결 역할에서 사용하는 AMS Accelerate 리소스를 삭제하려면

AMS에서 계정이 온보딩된 모든 리전의 `ams-detective-controls-config-recorder` `ams-detective-controls-config-rules-cdk` 및 `ams-detective-controls-infrastructure-cdk` 스택을 삭제합니다(먼저 S3 버킷을 수동으로 비워야 할 수 있음).

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForManagedServices_DetectiveControlsConfig 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

AMS Accelerate에 대한 Amazon EventBridge 규칙 서비스 연결 역할

AMS Accelerate는 AWSServiceRoleForManagedServices_Events라는 서비스 연결 역할(SLR)을 사용합니다. 이 역할은 AWS Managed Services 서비스 보안 주체(events.managedservices.amazonaws.com) 중 하나를 신뢰하여 역할을 수임합니다. 서비스는 역할을 사용하여 Amazon EventBridge 관리형 규칙을 생성합니다. 이 규칙은 계정에서 AWS Managed Services로 경보 상태 변경 정보를 전달하는 데 필요한 인프라입니다.

AMS Accelerate용 EventBridge SLR에 대한 권한

AWSServiceRoleForManagedServices_Events 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `events.managedservices.amazonaws.com`

이 역할에는 `AWSManagedServices_EventsServiceRolePolicy` AWS 관리형 정책이 연결되어 있습니다(참조AWS 관리형 정책: AWSManagedServices_EventsServiceRolePolicy). 서비스는 역할을 사용하여 계정에서 AMS로 경보 상태 변경 정보를 전달합니다. IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

이 ZIP: EventsServiceRolePolicy.zip에서 JSON AWSManagedServices_EventsServiceRolePolicy를 다운로드할 수 있습니다. EventsServiceRolePolicy.zip

AMS Accelerate용 EventBridge SLR 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS CLI, 또는 AWS API에서 AMS AWS Management Console에 온보딩하면 AMS Accelerate가 서비스 연결 역할을 생성합니다.

> **Important**
>
> 이 서비스 연결 역할은 2023년 2월 7일 이전에 AMS Accelerate 서비스를 사용하던 경우 계정에 나타날 수 있습니다. 서비스 연결 역할을 지원하기 시작한 후 AMS Accelerate가 계정에

AWSServiceRoleForManagedServices_Events 역할을 생성했습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. AMS에 온보딩하면 AMS Accelerate가 서비스 연결 역할을 다시 생성합니다.

AMS Accelerate용 EventBridge SLR 편집

AMS Accelerate에서는 AWSServiceRoleForManagedServices_Events 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

AMS Accelerate용 EventBridge SLR 삭제

AWSServiceRoleForManagedServices_Events 역할은 수동으로 삭제할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API의 AMS에서 오프보딩하면 AMS Accelerate가 리소스를 정리하고 서비스 연결 역할을 삭제합니다.

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 서비스 연결 역할을 수동으로 삭제할 수도 있습니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

Note

리소스를 삭제하려고 할 때 AMS Accelerate 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForManagedServices_Events 서비스 연결 역할에서 사용하는 AMS Accelerate 리소스를 삭제하려면

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForManagedServices_Events 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

AMS Accelerate의 서비스 연결 역할에 문의

AMS Accelerate는 AWSServiceRoleForManagedServices_Contacts라는 서비스 연결 역할(SLR)을 사용합니다.이 역할은 서비스가 영향을 받는 리소스의 기존 태그를 읽고 적절한 연락처의 구성된 이메일을 검색하도록 허용하여 인시던트가 발생할 때 자동 알림을 용이하게 합니다.

이 서비스 연결 역할을 사용하는 유일한 서비스입니다.

AWSServiceRoleForManagedServices_Contacts 서비스 연결 역할에 연결된 관리형 정책은 AWSManagedServices_ContactsServiceRolePolicy입니다. 이 정책에 대한 업데이트는 AWS 관리형 정책에 대한 업데이트 가속화 섹션을 참조하세요.

AMS Accelerate에 대한 연락처 SLR 권한

AWSServiceRoleForManagedServices_Contacts 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `contacts-service.managedservices.amazonaws.com`

이 역할에는 `AWSManagedServices_ContactsServiceRolePolicy` AWS 관리형 정책이 연결되어 있습니다(참조AWS 관리형 정책: AWSManagedServices_ContactsServiceRolePolicy). 이 서비스는 역할을 사용하여 모든 AWS 리소스의 태그를 읽고 인시던트 발생 시 적절한 연락 지점의 태그에 포함된 이메일을 찾습니다. 이 역할은 AMS가 영향을 받는 리소스에서 해당 태그를 읽고 이메일을 검색하도록 허용하여 인시던트 발생 시 자동 알림을 용이하게 합니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

> **Important**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. AMS는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 개인 데이터나 민감한 데이터에 사용하기 위한 것이 아닙니다.

AWSManagedServices_ContactsServiceRolePolicy라는 역할 권한 정책은 AMS Accelerate가 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 작업: Contacts Service가 AMS가 모든 AWS 리소스에서 인시던트 알림을 보낼 수 있도록 이메일을 포함하도록 특별히 설정된 태그를 읽을 수 있도록 허용합니다.

이 ZIP: ContactsServicePolicy.zip에서 JSON AWSManagedServices_ContactsServiceRolePolicy를 다운로드할 수 있습니다. ContactsServicePolicy.zip

AMS Accelerate용 연락처 SLR 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS CLI, 또는 AWS API에서 AMS AWS Management Console에 온보딩하면 AMS Accelerate가 서비스 연결 역할을 생성합니다.

> **Important**
>
> 이 서비스 연결 역할은 2023년 2월 16일 이전에 AMS Accelerate 서비스를 사용하는 경우 계정에 나타날 수 있습니다. 서비스 연결 역할을 지원하기 시작한 후 AMS Accelerate는 계정에 AWSServiceRoleForManagedServices_Contacts 역할을 생성했습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. AMS에 온보딩하면 AMS Accelerate가 서비스 연결 역할을 다시 생성합니다.

AMS Accelerate에 대한 연락처 SLR 편집

AMS Accelerate에서는 AWSServiceRoleForManagedServices_Contacts 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

AMS Accelerate에 대한 연락처 SLR 삭제

AWSServiceRoleForManagedServices_Contacts 역할은 수동으로 삭제할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API의 AMS에서 오프보딩하면 AMS Accelerate가 리소스를 정리하고 서비스 연결 역할을 삭제합니다.

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 서비스 연결 역할을 수동으로 삭제할 수도 있습니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려고 할 때 AMS Accelerate 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForManagedServices_Contacts 서비스 연결 역할에서 사용하는 AMS Accelerate 리소스를 삭제하려면

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForManagedServices_Contacts 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

AMS Accelerate 서비스 연결 역할에 지원되는 리전

AMS Accelerate는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용을 알아보려면 AWS 리전 및 엔드포인트를 참조하세요.

서비스 연결 역할에 대한 업데이트 가속화

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Accelerate 서비스 연결 역할 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Accelerate AMS Accelerate 사용 설명서의 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경	설명	Date

업데이트된 정책 - 배포 도구 키트	• 리소스에 대해 `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` 다음과 같은 새 권한이 추가되었습니다.
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		2024년 4월 4일

업데이트된 정책 - 배포 도구 키트	• 리소스에 대해 `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` 다음과 같은 새 권한이 추가되었습니다.
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
		2023년 5월 9일

변경	설명	Date

	• 리소스에 대해 `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` 다음과 같은 새 권한이 추가되었습니다.
	
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
	`ecr:GetLifecyclePolicy`
	`ecr:ListTagsForResource`
	`ecr:PutImageTagMutability`
	`ecr:PutLifecyclePolicy`
	`ecr:SetRepositoryPolicy`
	`ecr:TagResource`
	`ecr:UntagResource`
	
	• 또한 와일드카드가 있는 일부 기존 작업은 개별 작업으로 범위가 축소되었습니다.
	
	`- s3:DeleteObject*`
	`+ s3:DeleteObject`
	`+ s3:DeleteObjectTagging`
	`+ s3:DeleteObjectVersion`
	`+ s3:DeleteObjectVersionTagging`
	
	`- s3:GetObject*`
	`+ s3:GetObject`
	`+ s3:GetObjectAcl`
	`+ s3:GetObjectAttributes`
	`+ s3:GetObjectLegalHold`
	`+ s3:GetObjectRetention`
	`+ s3:GetObjectTagging`
	`+ s3:GetObjectVersion`
	`+ s3:GetObjectVersionAcl`
	`+ s3:GetObjectVersionAttributes`
	`+ s3:GetObjectVersionForReplication`
	`+ s3:GetObjectVersionTagging`
	`+ s3:GetObjectVersionTorrent`
	
	`- cloudformation:UpdateTermination*`	

변경	설명	Date
	`+ cloudformation:UpdateTerminationProtection`	
업데이트된 정책 - 탐지 제어	• 보안 및 액세스 팀에 확인한 후 CloudFormation 작업의 범위가 더 축소되었습니다. • Lambda 작업은 온보딩/오프보딩에 영향을 주지 않으므로 정책에서 제거되었습니다.	2023년 4월 10일
업데이트된 정책 - 탐지 제어	정책을 업데이트하고 권한 경계 정책을 추가했습니다.	2023년 3월 21일
새 서비스 연결 역할 - SLR에 문의	Accelerate는 고객 응대 서비스에 대한 새 서비스 연결 역할을 추가했습니다. 이 역할은 서비스가 영향을 받는 리소스의 기존 태그를 읽고 적절한 연락 지점의 구성된 이메일을 검색할 수 있도록 하여 인시던트 발생 시 자동 알림을 용이하게 합니다.	2023년 2월 16일
새 서비스 연결 역할 - EventBridge	Accelerate는 Amazon EventBridge 규칙에 대한 새 서비스 연결 역할을 추가했습니다. 이 역할은 AWS Managed Services 서비스 보안 주체(events.managedservices.amazonaws.com) 중 하나를 신뢰하여 역할을 수임합니다. 서비스는 역할을 사용하여 Amazon EventBridge 관리형 규칙을 생성합니다. 이 규칙은 계정에서 AWS Managed Services로 경보 상태 변경 정보를 전달하는 데 AWS 계정에 필요한 인프라입니다.	2023년 2월 7일

변경	설명	Date
업데이트된 서비스 연결 역할 - 배포 도구 키트	새 S3 권한으로 업데이트된 AWSServiceRoleForAWSManagedServicesDeploymentToolkit를 가속화합니다. 이러한 새 권한이 추가되었습니다. `"s3:GetLifecycleConfiguration", "s3:GetBucketLogging", "s3:ListBucket", "s3:GetBucketVersioning", "s3:PutLifecycleConfiguration", "s3:GetBucketLocation", "s3:GetObject*"`	2023년 1월 30일
변경 사항 추적 가속화 시작	Accelerate는 서비스 연결 역할에 대한 변경 사항 추적을 시작했습니다.	2022년 11월 30일
새로운 서비스 연결 역할 - 탐지 제어	Accelerate는 탐지 제어 가속화를 배포하는 새로운 서비스 연결 역할을 추가했습니다. AWS Managed Services는이 서비스 연결 역할을 사용하여 config-recorder, config 규칙 및 S3 버킷 탐지 제어를 배포합니다.	2022년 10월 13일
새로운 서비스 연결 역할 - 배포 도구 키트	Accelerate는 Accelerate 인프라를 배포하기 위한 새로운 서비스 연결 역할을 추가했습니다. 이 역할은 AMS Accelerate 인프라를 고객 계정에 배포합니다.	2022년 6월 9일

AWS AMS Accelerate에 대한 관리형 정책

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 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 줍니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 될 때 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

변경 사항 표는 섹션을 참조하세요AWS 관리형 정책에 대한 업데이트 가속화.

AWS 관리형 정책: AWSManagedServices_AlarmManagerPermissionsBoundary

AWS Managed Services (AMS)는 `AWSManagedServices_AlarmManagerPermissionsBoundary` AWS 관리형 정책을 사용합니다. 이 AWS관리형 정책은 AWSManagedServices_AlarmManager_ServiceRolePolicy에서 AWSServiceRoleForManagedServices_AlarmManager에 의해 생성된 IAM 역할의 권한을 제한하는 데 사용됩니다.

이 정책은의 일부로 생성된 IAM 역할경보 관리자의 작동 방식, AWS Config 평가, Alarm Manager 구성을 가져오기 위한 AWS Config 읽기, 필요한 Amazon CloudWatch 경보 생성과 같은 작업을 수행할 수 있는 권한을 부여합니다.

`AWSManagedServices_AlarmManagerPermissionsBoundary` 정책은 `AWSServiceRoleForManagedServices_DetectiveControlsConfig` 서비스 연결 역할에 연결됩니다. 이 역할에 대한 업데이트는 섹션을 참조하세요서비스 연결 역할에 대한 업데이트 가속화.

이 정책을 IAM 자격 증명에 연결할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `AWS Config` - 구성 규칙을 평가하고 리소스 구성을 선택할 수 있는 권한을 허용합니다.
- `AWS AppConfig` - AlarmManager 구성을 가져올 수 있는 권한을 허용합니다.
- `Amazon S3` - AlarmManager 버킷 및 객체를 작동할 수 있는 권한을 허용합니다.
- `Amazon CloudWatch` - AlarmManager 관리형 경보 및 지표를 읽고 넣을 수 있는 권한을 허용합니다.
- `AWS Resource Groups and Tags` - 리소스 태그를 읽을 수 있는 권한을 허용합니다.
- `Amazon EC2` - Amazon EC2 리소스를 읽을 수 있는 권한을 허용합니다.
- `Amazon Redshift` - Redshift 인스턴스 및 클러스터를 읽을 수 있는 권한을 허용합니다.

- `Amazon FSx` - 파일 시스템, 볼륨 및 리소스 태그를 설명할 수 있는 권한을 허용합니다.
- `Amazon CloudWatch Synthetics` - Synthetics 리소스를 읽을 수 있는 권한을 허용합니다.
- `Amazon Elastic Kubernetes Service` - Amazon EKS 클러스터를 설명할 수 있는 권한을 허용합니다.
- `Amazon ElastiCache` - 리소스를 설명할 수 있는 권한을 허용합니다.

이 ZIP: RecommendedPermissionBoundary.zip.

AWS 관리형 정책: AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

AWS Managed Services (AMS)는 `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS 관리형 정책을 사용합니다. 이 AWS관리형 정책은 `AWSServiceRoleForManagedServices_DetectiveControlsConfig` 서비스 연결 역할에 연결됩니다(참조Detective는 AMS Accelerate의 서비스 연결 역할을 제어합니다.). `AWSServiceRoleForManagedServices_DetectiveControlsConfig` 서비스 연결 역할에 대한 업데이트는 섹션을 참조하세요서비스 연결 역할에 대한 업데이트 가속화.

이 정책을 통해 서비스 연결 역할이 사용자를 대신하여 작업을 완료할 수 있습니다.

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 정책을 IAM 엔터티에 연결할 수 있습니다.

자세한 내용은 AMS Accelerate에 서비스 연결 역할 사용 단원을 참조하십시오.

권한 세부 정보

이 정책에는 AWS Managed Services Detective Controls가 필요한 모든 리소스를 배포하고 구성할 수 있도록 허용하는 다음과 같은 권한이 있습니다.

- `CloudFormation` - AMS Detective Controls가 s3 버킷, 구성 규칙 및 config-recorder와 같은 리소스를 사용하여 CloudFormation 스택을 배포할 수 있도록 허용합니다.
- `AWS Config` - AMS Detective Controls가 AMS 구성 규칙을 생성하고 집계자 및 태그 리소스를 구성할 수 있도록 허용합니다.
- `Amazon S3` - AMS Detective Controls가 s3 버킷을 관리할 수 있도록 허용합니다.

이 ZIP: DetectiveControlsConfig_ServiceRolePolicy.zip에서 JSON 정책 파일을 다운로드할 수 있습니다.

AWS 관리형 정책: AWSManagedServicesDeploymentToolkitPolicy

AWS Managed Services (AMS)는 AWSManagedServicesDeploymentToolkitPolicy AWS 관리형 정책을 사용합니다. 이 AWS관리형 정책은 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 서비스 연결 역할에 연결됩니다(참조AMS Accelerate의 배포 툴킷 서비스 연결 역할). 이 정책을 통해 서비스 연결 역할이 사용자를 대신하여 작업을 완료할 수 있습니다. IAM 엔터티에 이 정책을 연결할 수 없습니다. 자세한 내용은 AMS Accelerate에 서비스 연결 역할 사용 단원을 참조하십시오.

AWSServiceRoleForManagedServicesDeploymentToolkitPolicy 서비스 연결 역할에 대한 업데이트는 섹션을 참조하세요서비스 연결 역할에 대한 업데이트 가속화.

권한 세부 정보

이 정책에는 AWS Managed Services Detective Controls가 필요한 모든 리소스를 배포하고 구성할 수 있도록 허용하는 다음과 같은 권한이 있습니다.

- CloudFormation - AMS Deployment Toolkit이 CDK에 필요한 S3 리소스를 사용하여 CFN 스택을 배포할 수 있도록 허용합니다.
- Amazon S3 -는 AMS Deployment Toolkit이 S3 버킷을 관리할 수 있도록 허용합니다.
- Elastic Container Registry -를 사용하면 AMS Deployment Toolkit이 AMS CDK 앱에 필요한 자산을 배포하는 데 사용되는 ECR 리포지토리를 관리할 수 있습니다.

이 ZIP: AWSManagedServicesDeploymentToolkitPolicy.zip.

AWS 관리형 정책: AWSManagedServices_EventsServiceRolePolicy

AWS Managed Services (AMS)는 AWSManagedServices_EventsServiceRolePolicy AWS 관리형 정책을 사용합니다. 이 AWS관리형 정책은 AWSServiceRoleForManagedServices_Events 서비스 연결 역할에 연결됩니다. 이 정책을 통해 서비스 연결 역할이 사용자를 대신하여 작업을 완료할 수 있습니다. IAM 엔터티에 이 정책을 연결할 수 없습니다. 자세한 내용은 AMS Accelerate에 서비스 연결 역할 사용 단원을 참조하십시오.

AWSServiceRoleForManagedServices_Events 서비스 연결 역할에 대한 업데이트는 섹션을 참조하세요서비스 연결 역할에 대한 업데이트 가속화.

권한 세부 정보

이 정책에는 Amazon EventBridge가 계정에서 AWS Managed Services로 경보 상태 변경 정보를 전달할 수 있도록 허용하는 다음과 같은 권한이 있습니다.

- `events` - Accelerate가 Amazon EventBridge 관리형 규칙을 생성할 수 있도록 허용합니다. 이 규칙은 계정에서 로 경보 상태 변경 정보를 전달하는 AWS 계정 데 필요한 인프라입니다 AWS Managed Services.

이 ZIP: EventsServiceRolePolicy.zip.

AWS 관리형 정책: AWSManagedServices_ContactsServiceRolePolicy

AWS Managed Services (AMS)는 `AWSManagedServices_ContactsServiceRolePolicy` AWS 관리형 정책을 사용합니다. 이 AWS관리형 정책은 `AWSServiceRoleForManagedServices_Contacts` 서비스 연결 역할에 연결됩니다(참조AMS Accelerate용 연락처 SLR 생성). 이 정책은 AMS Contacts SLR이 AWS 리소스에서 리소스 태그와 해당 값을 볼 수 있도록 허용합니다. IAM 엔터티에 이 정책을 연결할 수 없습니다. 자세한 내용은 AMS Accelerate에 서비스 연결 역할 사용 단원을 참조하십시오.

> **Important**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. AMS는 태그를 사용하여 관리 서비스를 제공합니다. 태그는 개인 데이터나 민감한 데이터에 사용하기 위한 것이 아닙니다.

`AWSServiceRoleForManagedServices_Contacts` 서비스 연결 역할에 대한 업데이트는 섹션을 참조하세요서비스 연결 역할에 대한 업데이트 가속화.

권한 세부 정보

이 정책에는 Contacts SLR이 리소스 태그를 읽고 미리 설정한 리소스 연락처 정보를 검색할 수 있도록 허용하는 다음과 같은 권한이 있습니다.

- `IAM` - Contacts 서비스가 IAM 역할 및 IAM 사용자의 태그를 볼 수 있도록 허용합니다.
- `Amazon EC2` - Contacts 서비스가 Amazon EC2 리소스의 태그를 볼 수 있도록 허용합니다.
- `Amazon S3` - Contacts Service가 Amazon S3 버킷의 태그를 볼 수 있도록 허용합니다. 이 작업은 조건을 사용하여 AMS가 HTTP 권한 부여 헤더, SigV4 서명 프로토콜 및 TLS 1.2 이상의 HTTPS를 사용하여 버킷 태그에 액세스하도록 합니다. 자세한 내용은 인증 방법 및 Amazon S3 서명 버전 4 인증별 정책 키를 참조하세요.
- `Tag` - Contacts 서비스가 다른 AWS 리소스의 태그를 볼 수 있도록 허용합니다.

- "iam:ListRoleTags", "iam:ListUserTags", "tag:GetResources", "tag:GetTagKeys", "tag:GetTagValues", "ec2:DescribeTags", "s3:GetBucketTagging"

이 ZIP: ContactsServicePolicy.zip에서 JSON 정책 파일을 다운로드할 수 있습니다.

AWS 관리형 정책에 대한 업데이트 가속화

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 Accelerate의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다.

변경 사항	설명	날짜

업데이트된 정책 - 배포 도구 키트	• 리소스에 대해 `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` 다음과 같은 새 권한이 추가되었습니다.
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		2024년 4월 4일

업데이트된 정책 - 배포 도구 키트	• 리소스에 대해 `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` 다음과 같은 새 권한이 추가되었습니다.
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• 리소스에 대해 `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` 다음과 같은 새 권한이 추가되었습니다.
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
		2023년 5월 9일

변경 사항	설명	날짜

```
ecr:DeleteRepositoryPolicy
ecr:DescribeRepositories
ecr:GetLifecyclePolicy
ecr:ListTagsForResource
ecr:PutImageTagMutability
ecr:PutLifecyclePolicy
ecr:SetRepositoryPolicy
ecr:TagResource
ecr:UntagResource
```

- 또한 와일드카드가 있는 일부 기존 작업의 범위가 개별 작업으로 축소되었습니다.

```
- s3:DeleteObject*

+ s3:DeleteObject
+ s3:DeleteObjectTagging
+ s3:DeleteObjectVersion
+ s3:DeleteObjectVersionTagging

- s3:GetObject*
+ s3:GetObject
+ s3:GetObjectAcl
+ s3:GetObjectAttributes
+ s3:GetObjectLegalHold
+ s3:GetObjectRetention
+ s3:GetObjectTagging
+ s3:GetObjectVersion
+ s3:GetObjectVersionAcl
+ s3:GetObjectVersionAttributes
+ s3:GetObjectVersionForReplication
+ s3:GetObjectVersionTagging
+ s3:GetObjectVersionTorrent

- cloudformation:UpdateTermination*
+ cloudformation:UpdateTerminationProt
ection
```

변경 사항	설명	날짜
업데이트된 정책 - 탐지 제어	• 보안 및 액세스 팀에 확인한 후 CloudFormation 작업의 범위가 더 축소되었습니다. • Lambda 작업은 온보딩/오프보딩에 영향을 주지 않으므로 정책에서 제거되었습니다.	2023년 4월 10일
업데이트된 정책 - 탐지 제어	`ListAttachedRolePolicies` 작업이 정책에서 제거됩니다. 작업에는 와일드카드(*)로 리소스가 있었습니다. "list"는 변경되지 않는 작업이므로 모든 리소스에 대한 액세스 권한이 부여되며 와일드카드는 허용되지 않습니다.	2023년 3월 28일
업데이트된 정책 - 탐지 제어	정책을 업데이트하고 권한 경계 정책을 추가했습니다.	2023년 3월 21일
새 정책 - Contacts Service	Accelerate는 리소스 태그에서 계정 연락처 정보를 확인하는 새 정책을 추가했습니다. Accelerate는 미리 설정한 리소스 연락처 정보를 검색할 수 있도록 리소스 태그를 읽는 새 정책을 추가했습니다.	2023년 2월 16일
새 정책 - Events Service	Accelerate는 계정에서 AWS Managed Services로 경보 상태 변경 정보를 전달하는 새 정책을 추가했습니다. 필요한 Amazon EventBridge 관리형 규칙을 생성할 수 있는 경보 관리자의 작동 방식 권한의 일부로 생성된 IAM 역할을 부여합니다.	2023년 2월 7일
업데이트된 정책 - 배포 도구 키트	Accelerate에서 고객 오프보딩을 지원하는 S3 권한이 추가되었습니다.	2023년 1월 30일
새 정책 - 탐지 제어	서비스 연결 역할인가 탐지 제어 가속화를 배포Detective는 AMS Accelerate의 서비스 연결 역할을 제어합니다.하는 작업을 완료하도록 허용합니다.	2022년 12월 19일

변경 사항	설명	날짜
새 정책 - 경보 관리자	Accelerate는 경보 관리자 작업을 수행할 수 있는 권한을 허용하는 새 정책을 추가했습니다. Config 평가, 경보 관리자 구성을 가져오기 위한 AWS AWS Config 읽기, 필요한 Amazon CloudWatch 경보 생성과 같은 작업을 수행할 수 있는 경보 관리자의 작동 방식 권한의 일부로 생성된 IAM 역할을 부여합니다.	2022년 11월 30일
변경 사항 추적을 가속화하기 시작	Accelerate는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2022년 11월 30일
새 정책 - 배포 도구 키트	Accelerate는 배포 작업에 대해이 정책을 추가했습니다. 서비스 연결 역할 AWSServiceRoleForAWSManagedServicesDeploymentToolkit에 배포 관련 Amazon S3 버킷 및 CloudFormation 스택에 액세스하고 업데이트할 수 있는 권한을 부여합니다.	2022년 6월 9일

Accelerate의 데이터 보호

AMS Accelerate는 Amazon GuardDuty, Amazon Macie(선택 사항) 및 기타 내부 독점 도구 및 프로세스와 AWS 서비스 같은 네이티브를 활용하여 관리형 계정을 지속적으로 모니터링합니다. 경보가 트리거된 후 AMS Accelerate는 경보에 대한 초기 분류 및 대응을 담당합니다. AMS 응답 프로세스는 NIST 표준을 기반으로 합니다. AMS Accelerate는 보안 인시던트 대응 시뮬레이션을 사용하여 정기적으로 대응 프로세스를 테스트하여 워크플로를 기존 고객 보안 대응 프로그램에 맞게 조정합니다.

AMS Accelerate가 AWS 또는 보안 정책의 위반 또는 위반에 대한 임박한 위협을 탐지하면 Accelerate는 영향을 받는 리소스 및 구성 관련 변경 사항을 포함한 정보를 수집합니다. AMS Accelerate는 모든 관리형 계정에서 모니터링 대시보드, 인시던트 대기열 및 서비스 요청을 적극적으로 검토하고 조사하는 전용 운영자와 함께 연중무휴 follow-the-sun 제공합니다. Accelerate는 내부 보안 전문가와 조사하여 활동을 분석하고 계정에 나열된 보안 에스컬레이션 연락처를 통해 사용자에게 알립니다.

조사 결과에 따라 Accelerate는 사전에 고객과 소통합니다. 활동이 무단이거나 의심스러운 경우 AMS는 사용자와 협력하여 문제를 조사 및 해결하거나 억제합니다. GuardDuty에서 생성한 특정 결과 유형은 Accelerate가 조치를 취하기 전에 영향을 확인해야 합니다. 예를 들어, GuardDuty 결과 유형 UnauthorizedAccess:IAMUser/ConsoleLogin은 사용자 중 한 명이 비정상적인 위치에서 로그인했음을

나타냅니다. AMS는 사용자에게 알리고이 동작이 합법적인지 확인하기 위해 결과를 검토하도록 요청합니다.

Amazon Macie로 모니터링

> **Important**
>
> AMS Accelerate는 아시아 태평양(말레이시아) 리전에서 Amazon Macie를 사용한 모니터링을 지원하지 않습니다.

AMS Accelerate는 개인 건강 정보(PHI), 개인 식별 정보(PII) 및 금융 데이터와 같은 크고 포괄적인 민감한 데이터 목록을 탐지하기 위해 Amazon Macie를 지원하고 사용하는 모범 사례입니다.

모든 Amazon S3 버킷에서 정기적으로 실행되도록 Macie를 구성할 수 있습니다. 이렇게 하면 시간이 지남에 따라 버킷 내의 새 객체 또는 수정된 객체에 대한 평가가 자동화됩니다. 보안 조사 결과가 생성되면 AMS는 사용자에게 알리고 사용자와 협력하여 필요에 따라 조사 결과를 수정합니다.

자세한 내용은 Amazon Macie 조사 결과 분석을 참조하세요.

GuardDuty로 모니터링

GuardDuty는 악성 IP 주소 및 도메인 목록과 같은 위협 인텔리전스 피드와 기계 학습을 사용하여 AWS 환경 내에서 예기치 않고 잠재적으로 승인되지 않은 악의적인 활동을 식별하는 지속적인 보안 모니터링 서비스입니다. 여기에는 권한 에스컬레이션, 노출된 자격 증명 사용 또는 악성 IP 주소 또는 도메인과의 통신과 같은 문제가 포함될 수 있습니다. GuardDuty는 무단 인프라 배포, 사용한 적이 없는 AWS 리전에 배포된 인스턴스와 같은 손상 징후가 있는지 AWS 계정 액세스 동작을 모니터링합니다. 또한 GuardDuty는 암호 강도 감소를 위한 암호 정책 변경과 같은 비정상적인 API 호출을 감지합니다. 자세한 내용은 GuardDuty 사용 설명서를 참조하세요.

GuardDuty 결과를 보고 분석하려면 다음 단계를 완료하세요.

1. https://console.aws.amazon.com/guardduty/에서 GuardDuty 콘솔을 엽니다.
2. 조사 결과를 선택한 다음 특정 조사 결과를 선택하여 세부 정보를 확인합니다. 각 결과에 대한 세부 정보는 결과 유형, 관련된 리소스 및 활동의 특성에 따라 다릅니다.

사용 가능한 결과 필드에 대한 자세한 내용은 GuardDuty 결과 세부 정보를 참조하세요.

GuardDuty 억제 규칙을 사용하여 결과 필터링

억제 규칙은 값과 페어링된 필터 속성으로 구성된 기준 집합입니다. 억제 규칙을 사용하여 거짓 긍정 조사 결과 또는 알려진 활동과 같이 조치를 취하지 않을 가치가 낮은 조사 결과를 필터링할 수 있습니다. 결과를 필터링하면 환경에 가장 큰 영향을 미칠 수 있는 보안 위협을 더 쉽게 인식할 수 있습니다.

결과를 필터링하기 위해 억제 규칙은 지정된 기준과 일치하는 새 결과를 자동으로 보관합니다. 보관된 결과는 AWS Security Hub, Amazon S3 또는 CloudTrail Events로 전송되지 않습니다. 따라서 Security Hub 또는 타사 SIEM 알림 및 티켓팅 애플리케이션을 통해 GuardDuty 조사 결과를 사용하는 경우 억제 필터는 실행 불가능한 데이터를 줄입니다.

AMS에는 관리형 계정에 대한 금지 규칙을 식별하기 위한 정의된 기준 집합이 있습니다. 관리형 계정이 이 기준을 충족하면 AMS는 필터를 적용하고 배포된 억제 필터를 자세히 설명하는 서비스 요청(SR)을 생성합니다.

SR을 통해 AMS와 통신하여 억제 필터를 수정하거나 되돌릴 수 있습니다.

보관된 조사 결과 보기

GuardDuty는 조사 결과가 억제 규칙과 일치하는 경우에도 조사 결과를 계속 생성합니다. 억제된 조사 결과는 아카이브된 것으로 표시됩니다. GuardDuty는 보관된 결과를 90일 동안 저장합니다. 결과 테이블에서 아카이브됨을 선택하여 해당 90일 동안 GuardDuty 콘솔에서 아카이브된 결과를 볼 수 있습니다. 또는 service.archived의 findingCriteria가 true인 ListFindings API를 사용하여 GuardDuty API를 통해 보관된 결과를 볼 수 있습니다.

억제 규칙의 일반적인 사용 사례

다음 검색 결과 유형에는 억제 규칙을 적용하는 일반적인 사용 사례가 있습니다.

- Recon:EC2/Portscan: 승인된 취약성 스캐너를 사용할 때 결과를 자동으로 보관하려면 억제 규칙을 사용합니다.
- UnauthorizedAccess:EC2/SSHBruteForce: Bastion 인스턴스를 대상으로 하는 경우 억제 규칙을 사용하여 결과를 자동으로 아카이브합니다.
- Recon:EC2/PortProbeUnprotectedPort: 의도적으로 노출된 인스턴스를 대상으로 하는 경우 억제 규칙을 사용하여 결과를 자동으로 아카이브합니다.

Amazon Route 53 Resolver DNS 방화벽을 사용하여 모니터링

Amazon Route 53 Resolver는 퍼블릭 레코드, Amazon VPC별 DNS 이름 및 Amazon Route 53 프라이빗 호스팅 영역에 대한 AWS 리소스의 DNS 쿼리에 재귀적으로 응답하며 기본적으로 모든 VPCs.

Route 53 Resolver DNS 방화벽을 사용하면 Virtual Private Cloud(VPC)에 대한 아웃바운드 DNS 트래픽을 필터링하고 제어할 수 있습니다. 이렇게 하려면 DNS 방화벽 규칙 그룹에 재사용 가능한 필터링 규칙 컬렉션을 생성하고 규칙 그룹을 VPC에 연결한 다음 DNS 방화벽 로그 및 지표 활동을 모니터링합니다. 활동에 따라 DNS 방화벽의 동작을 적절하게 조정할 수 있습니다. 자세한 내용은 DNS 방화벽을 사용하여 아웃바운드 DNS 트래픽 필터링을 참조하세요.

Route 53 Resolver DNS 방화벽 구성을 보고 관리하려면 다음 절차를 사용합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/vpc/ Amazon VPC 콘솔을 엽니다.
2. DNS 방화벽에서 규칙 그룹을 선택합니다.
3. 기존 구성을 검토, 편집 또는 삭제하거나 새 규칙 그룹을 생성합니다. 자세한 내용은 Route 53 Resolver DNS 방화벽 작동 방식을 참조하세요.

Amazon Route 53 Resolver DNS 방화벽 모니터링 및 보안

Amazon Route 53 DNS 방화벽은 규칙 연결, 규칙 작업 및 규칙 평가 우선 순위의 개념을 사용합니다. 도메인 목록(domain list)은 규칙 그룹 내부의 DNS 방화벽 규칙에서 사용하는 재사용 가능한 도메인 사양 집합입니다. 규칙 그룹을 VPC 와 연결하면 DNS 방화벽은 규칙에 사용되는 도메인 목록과 DNS 쿼리를 비교합니다. DNS 방화벽이 일치하는 항목을 찾으면 일치하는 규칙의 작업에 따라 DNS 쿼리를 처리합니다. 규칙 그룹 및 규칙에 대한 자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙을 참조하세요.

도메인 목록은 두 가지 주요 범주로 나뉩니다.

- 가 자동으로 AWS 생성하고 유지 관리하는 관리형 도메인 목록입니다.
- 생성 및 유지 관리하는 자체 도메인 목록입니다.

규칙 그룹은 연결 우선 순위 인덱스를 기반으로 평가됩니다.

기본적으로 AMS는 다음 규칙과 규칙 그룹으로 구성된 기준 구성을 배포합니다.

- 라는 규칙 그룹 1개`DefaultSecurityMonitoringRule`. 규칙 그룹은 활성화된 각의 각 기존 VPC에 대해 생성 시 사용할 수 있는 연결 우선 순위가 가장 높습니다 AWS 리전.
- 작업 `ALERT`와 함께 `DefaultSecurityMonitoringRule` `AWSManagedDomainsAggregateThreatList` 관리형 도메인 목록을 사용하여 규칙 그룹 내에서 우선순위가 1인 라는 하나의 `DefaultSecurityMonitoringRule` 규칙.

기존 구성이 있는 경우 기존 구성보다 우선 순위가 낮은 기준 구성이 배포됩니다. 기존 구성이 기본값입니다. 기존 구성이 쿼리 해결을 처리하는 방법에 대한 우선 순위가 더 높은 지침을 제공하지 않는 경우 AMS 기준 구성을 catch-all로 사용합니다. 기준 구성을 변경하거나 제거하려면 다음 중 하나를 수행합니다.

- Cloud Service Delivery Manager(CSDM) 또는 Cloud Architect(CA)에 문의하세요.
- 서비스 요청을 생성하십시오.

AMS Accelerate의 데이터 암호화

AMS Accelerate는 여러를 데이터 암호화 AWS 서비스 에 사용합니다.

Amazon Simple Storage Service는 전송 중 및 저장 데이터를 보호하는 여러 객체 암호화 옵션을 제공합니다. 서버 측 암호화는 데이터 센터의 디스크에 저장하기 전에 객체를 암호화하고 객체를 다운로드할 때 암호를 해독합니다. 요청을 인증하기만 하면 액세스 권한을 갖게 되며, 객체의 암호화 여부와 관계없이 액세스 방식에는 차이가 없습니다. 자세한 내용은 Amazon S3의 데이터 보호를 참조하세요.

AWS Identity and Access Management AMS Accelerate의

AWS Identity and Access Management 는 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 웹 서비스입니다. IAM을 사용하여 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 있음)된 대상을 제어합니다. AMS Accelerate 온보딩 중에 각 관리형 계정 내에서 교차 계정 IAM 관리자 역할을 생성할 책임은 사용자에게 있습니다.

AMS Accelerate에서는 액세스 관리 솔루션, 액세스 정책 AWS 계정 및 관련 프로세스와 같은 및 기본 리소스에 대한 액세스를 관리할 책임이 있습니다. 즉, 사용자 수명 주기, 디렉터리 서비스의 권한 및 페더레이션 인증 시스템을 관리하여 AWS 콘솔 또는 AWS APIs. 액세스 솔루션을 관리하는 데 도움이 되도록 AMS Accelerate는 일반적인 IAM 구성 오류를 감지하는 AWS Config 규칙을 배포하고 문제 해결 알림을 제공합니다. 자세한 내용은 AWS Config 관리형 규칙을 참조하세요.

AMS Accelerate에서 자격 증명으로 인증

AMS는 IAM 자격 증명의 한 유형인 IAM 역할을 사용합니다. IAM 역할은 자격 증명이 할 수 있는 것과 없는 것을 결정하는 권한 정책이 있는 자격 증명이라는 점에서 사용자와 유사합니다 AWS. 그러나 역할에는 자격 증명이 연결되어 있지 않으며, 역할이 필요한 사람은 한 사람과 고유하게 연결되는 대신 역할을 수임할 수 있습니다. IAM 사용자는 한 가지 역할을 맡음으로써 특정 작업을 위해 다른 권한을 임시로 얻을 수 있습니다.

액세스 역할은 Operations Management에서 관리하고 정기적으로 검토하는 내부 그룹 멤버십에 의해 제어됩니다. AMS는 다음 IAM 역할을 사용합니다.

> **Note**
>
> AMS 액세스 역할을 사용하면 AMS 운영자가 리소스에 액세스하여 AMS 기능을 제공할 수 있습니다(참조서비스 설명). 이러한 역할을 변경하면 이러한 기능을 제공할 수 없게 될 수 있습니다. AMS 액세스 역할을 변경해야 하는 경우 Cloud Architect에 문의하세요.

역할 이름	설명
(엔터티)에서 사용: AMS Access Service만 해당	
ams-access-management	온보딩 중에 사용자가 수동으로 배포합니다. 액세스 역할을 배포하거나 업데이트하기 위해 AMS 액세스에서만 수임합니다. 향후 액세스 역할에 대한 업데이트를 위해 온보딩 후에도 계정에 남아 있습니다.
(엔터티)에서 사용: AMS 작업	
ams-access-admin-operations	이 역할은 계정에서 작동할 수 있는 관리 권한이 있지만 Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift, Amazon ElastiCache와 같이 데이터 스토어로 일반적으로 사용되는 AWS 서비스의 고객 콘텐츠를 읽거나, 쓰거나, 삭제할 수 있는 권한은 없습니다. 일부 AMS 개인만이 역할을 수임할 수 있습니다.
ams-access-operations	이 AMS 작업 역할에는 계정에서 관리 작업을 수행할 수 있는 권한이 있습니다. 이 역할에는 Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift, Amazon ElastiCache와 같이 데이터 스토어로 일반적으로 사용되는 AWS 서비스의 고객 콘텐츠에 대

역할 이름	설명
	한 읽기, 쓰기 또는 삭제 권한이 없습니다. AWS Identity and Access Management 쓰기 작업을 수행할 수 있는 권한도이 역할에서 제외됩니다.
ams-access-read-only	이 AMS 읽기 전용 역할은 AMS 계정의 읽기 전용 권한으로 제한됩니다. Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift, ElastiCache와 같이 데이터 스토어로 일반적으로 사용되는 AWS 서비스의 고객 콘텐츠에 대한 읽기 권한은이 역할에서 부여하지 않습니다.
(엔터티)에서 사용: AMS 작업 및 AMS 서비스	
ams_ssm_automation_역할	계정 내에서 SSM 자동화 문서를 실행 AWS Systems Manager 하기 위해에서 가정합니다.
ams_ssm_automation_역할	
(엔터티)에서 사용: AMS 보안	
ams-access-security-analyst	이 AMS 보안 역할은 AMS 계정에 전용 보안 알림 모니터링 및 보안 인시던트 처리를 수행할 수 있는 권한이 있습니다. 일부 AMS 보안 담당자만이 역할을 수임할 수 있습니다. Amazon S3;, Amazon RDS;, Amazon DynamoDB, Amazon Redshift 및 ElastiCache와 같이 일반적으로 데이터 스토어로 사용되는 AWS 서비스의 고객 콘텐츠에 대한 읽기 권한은이 역할에서 부여하지 않습니다.
ams-access-security-analyst-read-only	이 AMS 보안 역할은 전용 보안 알림 모니터링 및 보안 인시던트 처리를 수행할 수 있는 AMS 계정의 읽기 전용 권한으로 제한됩니다. Amazon S3;, Amazon RDS;, Amazon DynamoDB, Amazon Redshift 및 ElastiCache와 같이 일반적으로 데이터 스토어로 사용되는 AWS 서비스의 고객 콘텐츠에 대한 읽기 권한은 이 역할에서 부여하지 않습니다.

역할 이름	설명
(엔터티)에서 사용: AWS 서비스	
ams-access-admin	이 AMS 관리자 역할에는 제한 없이 계정에서 작업할 수 있는 모든 권한이 있습니다. AMS 내부 서비스(범위 축소 세션 정책 포함)만 관리자 역할을 수임할 수 있습니다.
ams-opscenter-eventbridge-role	Amazon EventBridge에서 AMS별 AWS Config 규칙 문제 해결 워크플로의 일부로 AWS Systems Manager OpsItems를 생성한다고 가정합니다.
AMSOSConfigurationCustomerInstanceRole	이 IAM 역할은 AMS OS-Configuration 서비스가 필요한 IAM 정책이 누락된 것을 발견하면 Amazon EC2 인스턴스에 적용됩니다. 이를 통해 Amazon EC2 인스턴스가 AWS Systems Manager Amazon CloudWatch 및 Amazon EventBridge 서비스와 상호 작용할 수 있습니다. 또한 Windows 인스턴스에 대한 RDP 액세스를 활성화하기 위해 AMS 사용자 지정 관리형 정책을 연결했습니다.
mc-patch-glue-service-role	데이터 변환을 수행하고 AMS 패치 보고서 생성기를 준비하기 위해 AWS Glue ETL 워크플로에서 가정합니다.
(엔터티)에서 사용: AMS 서비스	
ams-alarm-manager-AWSManagedServicesAlarmManagerDe-<8자리 해시>	새 AWS AppConfig 배포에 대한 평가를 수행하기 AWS Config 규칙 위해 AMS 계정 내의 AMS 경보 관리자 인프라에서 가정합니다.
ams-alarm-manager-AWSManagedServicesAlarmManagerRe-<8자리 해시>	문제 해결을 위해 경보를 생성하거나 삭제할 수 있도록 AMS 계정 내의 AMS 경보 관리자 문제 해결 인프라에서 가정합니다.

역할 이름	설명
ams-alarm-manager-AWSManagedServices AlarmManagerSS-<8자리 해시>	가 AMS 계정 내에서 AMS 경보 관리자 문제 해결 서비스를 호출 AWS Systems Manager 하는 것으로 가정합니다.
ams-alarm-manager-AWSManagedServices AlarmManagerTr-<8자리 해시>	AWS 계정 내의 AMS 경보 관리자 인프라에서 정기적인 AMS AWS Config 규칙 평가를 수행하도록 가정합니다.
ams-alarm-manager-AWSManagedServices AlarmManagerVa-<8자리 해시>	필요한 경보가 AWS 계정에 존재하는지 확인하기 위해 AMS 계정 내의 AMS 경보 관리자 인프라에서 가정합니다.
ams-backup-iam-role	이 역할은 계정 AWS Backup 내에서를 실행하는 데 사용됩니다.
ams-monitoring-AWSManagedServicesLog GroupLimitLamb-<8자리 해시>	AMS 계정의 AMS 로깅 및 모니터링 인프라에서 Amazon CloudWatch Logs 그룹 제한을 평가하고 서비스 할당량과 비교한다고 가정합니다.
ams-monitoring-AWSManagedServicesRDS MonitoringRDSE-<8자리 해시>	Amazon RDS 이벤트를 Amazon CloudWatch Events에 전달하기 위해 AMS 계정의 AMS 로깅 및 모니터링 인프라에서 가정합니다.
ams-monitoring-AWSManagedServicesRed shiftMonitorin-<8자리 해시>	AMS 계정의 AMS 로깅 및 모니터링 인프라가 Amazon Redshift 이벤트(CreateCluster 및 DeleteCuster)를 Amazon CloudWatch Events로 전달한다고 가정합니다.
ams-monitoring-infrastruc-AWSManaged ServicesMonito-<8자리 해시>	AMS 계정의 AMS 로깅 및 모니터링 인프라에서 Amazon Simple Notification Service에 메시지를 게시하여 계정이 필요한 모든 데이터를 보고하고 있는지 검증하는 것으로 가정합니다.
ams-opscenter-role	계정의 알림과 관련된 AWS Systems Manager OpsItems 관리하기 위해 AMS 계정의 AMS 알림 관리 시스템에서 수임합니다.

역할 이름	설명
ams-opsitem-autoexecution-role	계정의 리소스와 관련된 알림을 모니터링하기 위해 SSM 문서를 사용하여 자동 문제 해결을 처리하도록 AMS 알림 관리 시스템에서 가정합니다.
ams-patch-infrastructure-amspatchconfigruleroleC1-<8자리 해시>	AMS 패치 리소스를 평가하고 스택의 드리프트를 CloudFormation 감지하기 AWS Config 위해에서 가정합니다.
ams-patch-infrastructure-amspatchcwruleopsitemams-<8자리 해시>	Amazon EventBridge에서 패치 실패에 대한 AWS Systems Manager OpsItems를 생성한다고 가정합니다.
ams-patch-infrastructure-amspatchservicebusamspat-<8자리 해시>	Amazon EventBridge에서 AWS Systems Manager Maintenance Windows 상태 변경 알림을 위해 이벤트를 AMS Patch 오케스트레이터 이벤트 버스로 보내는 것으로 가정합니다.
ams-patch-reporting-infra-amspatchreportingconfigr-<8자리 해시>	AMS 패치 보고 리소스를 평가하고 CloudFormation 스택의 드리프트를 감지하기 AWS Config 위해에서 가정합니다.
ams-resource-tagger-AWSManagedServicesResourceTagg-<8자리 해시>	새 AWS AppConfig 배포 시 AWS Config 규칙 평가를 수행하기 위해 AMS 계정 내의 AMS Resource Tagger 인프라에서 가정합니다.
ams-resource-tagger-AWSManagedServicesResourceTagg-<8자리 해시>	관리형 리소스에 필요한 AWS 태그가 있는지 확인하기 위해 AMS 계정 내의 AMS Resource Tagger 인프라에서 가정합니다.
ams-resource-tagger-AWSManagedServicesResourceTagg-<8자리 해시>	가 AMS 계정에서 AMS Resource Tagger 문제 해결 워크플로를 호출 AWS Systems Manager 하는 것으로 가정합니다.
ams-resource-tagger-AWSManagedServicesResourceTagg-<8자리 해시>	관리형 리소스에 대한 AWS 태그를 생성하거나 삭제하기 위해 AMS 계정 내의 AMS 리소스 태거 수정 인프라에서 가정합니다.

역할 이름	설명
ams-resource-tagger-AWSManagedServicesResourceTagg-<8자리 해시>	AWS 계정 내의 AMS Resource Tagger 인프라에서 정기적인 AMS Config 규칙 평가를 수행하는 것으로 가정합니다.
ams_os_configuration_event_rule_role-<AWS 리전>	Amazon EventBridge에서 계정의 이벤트를 올바른 리전의 AMS OS-Configuration 서비스 EventBus로 전달한다고 가정합니다.
mc-patch-reporting-service	AMS 패치 데이터 집계자 및 보고서 생성기가 가정합니다.

> **Note**
>
> ams-access-management 역할의 템플릿입니다. 온보딩 시 클라우드 아키텍트(CAs)가 계정에 수동으로 배포하는 스택은 management-role.yaml입니다.
> 이 템플릿은 ams-access-read-only, ams-access-operations, ams-access-admin-operations, ams-access-admin: accelerate-roles.yaml 등 다양한 액세스 역할 및 액세스 수준에 대한 템플릿입니다.

해시를 포함한 AWS Cloud Development Kit (AWS CDK) (AWS CDK) 식별자에 대한 자세한 내용은 UniqueIDs.

AMS Accelerate 기능 서비스는 계정에 프로그래밍 방식으로 액세스하기 위한 ams-access-admin 역할을 수임하지만 각 기능 서비스(예: 패치, 백업, 모니터링 등)에 대해 세션 정책 범위가 축소됩니다.

AMS Accelerate는 규정 준수 자격을 충족하고 유지하기 위해 업계 모범 사례를 따릅니다. 계정에 대한 AMS Accelerate 액세스는 CloudTrail에 기록되며 변경 사항 추적을 통해 검토할 수도 있습니다. 이 정보를 가져오는 데 사용할 수 있는 쿼리에 대한 자세한 내용은 섹션을 참조하세요AMS Accelerate 계정의 변경 사항 추적.

정책을 사용하여 액세스 관리

운영 엔지니어, 클라우드 아키텍트, 클라우드 서비스 제공 관리자(CSDMs)와 같은 다양한 AMS Accelerate 지원 팀이 서비스 요청 및 인시던트에 대응하기 위해 계정에 액세스해야 하는 경우가 있습니다. 액세스는 비즈니스 정당화, 서비스 요청, 운영 항목 및 지원 사례와 같은 제어를 적용하는 내부

AMS 액세스 서비스에 의해 관리됩니다. 기본 액세스는 읽기 전용이며 모든 액세스가 추적되고 기록됩니다. 단원도 참조하십시오AMS Accelerate 계정의 변경 사항 추적.

IAM 리소스 검증

AMS Accelerate 액세스 시스템은 계정의 역할을 주기적으로 수임하고(최소 24시간마다) 모든 IAM 리소스가 예상대로인지 확인합니다.

계정을 보호하기 위해 AMS Accelerate에는 위에서 언급한 IAM 역할의 존재 및 상태와 연결된 정책을 모니터링하고 경고하는 "canary"가 있습니다. 주기적으로 canary는 ams-access-read-only 역할을 수임하고 계정에 대해 CloudFormation 및 IAM API 호출을 시작합니다. canary는 AMS Accelerate 액세스 역할의 상태를 평가하여 항상 수정되지 않고 up-to-date 상태인지 확인합니다. 이 활동은 계정에 CloudTrail 로그를 생성합니다.

canary의 AWS Security Token Service (AWS STS) 세션 이름은 CloudTrail에 표시된 AMS-Access-Roles-Auditor-{uuid4()}이며 다음과 같은 API 호출이 발생합니다.

- Cloud Formation API 호출: `describe_stacks()`
- IAM API 호출:
  - `get_role()`
  - `list_attached_role_policies()`
  - `list_role_policies()`
  - `get_policy()`
  - `get_policy_version()`
  - `get_role_policy()`

AMS의 보안 인시던트 대응

AWS Managed Services(AMS)에서는 보안이 최우선 순위입니다. AMS는 리소스와 제어를 계정에 배포하여 관리합니다. AWS 에는 공동 책임 모델이 있습니다.는 클라우드의 보안을 AWS 관리하며 사용자는 클라우드의 보안을 책임집니다. AMS는 보안 제어 및 보안 문제에 대한 활성 모니터링을 사용하여 데이터와 자산을 보호하고 AWS 인프라를 안전하게 유지하는 데 도움이 됩니다. 이러한 기능은 AWS 클라우드에서 실행되는 애플리케이션의 보안 기준을 설정하는 데 도움이 됩니다. AMS는 보안 인시던트 대응을 통해 고객과 협력하여 효과를 평가한 다음 모범 사례 권장 사항에 따라 억제 및 수정을 수행합니다.

잘못된 구성이나 외부 요인의 변경으로 인해 기준에서 벗어나는 경우 대응하고 조사해야 합니다. 이를 성공적으로 수행하려면 AMS 환경 내에서 보안 인시던트 대응의 기본 개념을 이해해야 합니다. 또한 보안 문제가 발생하기 전에 클라우드 팀을 준비, 교육 및 훈련하기 위한 요구 사항을 이해해야 합니다. 사용할 수 있는 제어 및 기능을 파악하고, 사용자 계정 손상 또는 권한 있는 계정의 오용과 같은 일반적인 보안 문제에 대한 대응 계획을 준비하고, 자동화를 사용하여 대응 속도와 일관성을 개선하는 해결 방법을 식별하는 것이 중요합니다. 또한 이러한 요구 사항을 충족하기 위한 보안 인시던트 대응 프로그램 구축과 관련된 규정 준수 및 규제 요구 사항을 이해해야 합니다.

보안 인시던트 대응은 복잡할 수 있지만 반복적인 접근 방식을 구현하면 프로세스를 간소화하고 인시던트 대응 팀이 조기 및 지속적인 탐지 및 대응을 제공하여 자산 이해관계자를 만족시킬 수 있습니다. 이 가이드에서는 AMS가 인시던트 대응에 사용하는 방법론, AMS 책임 매트릭스(RACI), 보안 이벤트에 대비하는 방법, 보안 인시던트 발생 시 AMS를 참여시키는 방법, AMS가 사용하는 일부 인시던트 대응 런북을 제공합니다.

AMS 보안 인시던트 대응 작동 방식

AWS Managed Services는 보안 인시던트 대응을 위한 NIST 800-61 컴퓨터 보안 인시던트 처리 가이드에 부합합니다. 이 업계 표준에 따라 보안 이벤트 관리에 대한 일관된 접근 방식을 제공하고 클라우드의 보안 인시던트를 보호하고 이에 대응하는 모범 사례를 준수합니다.

인시던트 대응 수명 주기

탐지에서 보안 알림을 식별 및 생성하거나 사용자가 보안 지원을 요청할 때 AWS Managed Services Operations 팀은 적시에 조사하고, 자동화를 실행하여 데이터 수집을 수행하고, 분류 및 분석하고, 분석을 알리고, 조사 및 억제 활동을 수행하고, 이벤트 분석을 게시합니다.

인시던트 대응 중에 수행되는 데이터 수집, 분류, 분석 및 억제 활동은 조사 중인 보안 이벤트 유형에 따라 달라집니다. 일부 시나리오에 대한 보안 인시던트 대응 워크플로의 예는이 문서의 끝에 있습니다.

인시던트 발생 시 AMS는 올바른 조치를 동적으로 결정하므로 문서화된 단계를 적절하게 재정렬하거나 우회하여 올바른 결과가 발생하도록 할 수 있습니다.

준비

위협 환경이 발전함에 따라 AMS는 탐지 및 대응 기능을 계속 확장하고 있습니다. 새로운 탐지가 추가되면 AMS는 이러한 새로운 탐지의 알림을 탐지 및 대응 플랫폼에 통합합니다. AMS 보안 대응 담당자는 보안 인시던트 대응 수명 주기 전반에 걸쳐 조사하고 협력하도록 훈련됩니다.

이러한 파트너십 접근 방식 때문에 보안 및 애플리케이션 팀이 AMS와 협력하여 이러한 이벤트가 발생할 때 보안 이벤트를 처리할 준비가 되어 있어야 합니다. 이 설명서에서는 보안 이벤트 중에 예상되는 사항을 설명하고 보안 인시던트가 발생할 때 신속한 대응을 준비하는 데 도움이 됩니다.

이 설명서에서는 이벤트의 NIST 800-61 정의를 시스템 또는 네트워크에서 관찰 가능한 발생으로 사용하고 인시던트를 정책, 허용 가능한 사용 정책 또는 표준 보안 관행 위반의 위반 또는 임박한 위협으로 사용합니다.

준비 체크리스트

AMS 클라우드 솔루션 제공 관리자(CSDM) 및 AMS 클라우드 아키텍트(CA)와 함께 다음 체크리스트를 살펴봅니다.

- 어떤 워크로드가 어떤 계정에서 실행되고 있는지 이해합니다.
- 다양한 워크로드를 담당하는 내부 팀을 이해하고 워크로드에서 적절하게 태그를 지정합니다.
- 보안 이벤트 조사 중에 필요할 수 있는 다른 팀과 억제 결정을 위해 연락처 세부 정보를 내부적으로 유지 관리합니다.
- 보안 연락처가 최신 상태이고 모든 관리형 AWS 계정에 추가되었는지 확인합니다. 연락처는 계정별로 관리됩니다.
- 보안 인시던트를 AMS에 제기하는 방법을 알고 심각도와 예상 대응 시간을 숙지합니다.
- 보안 알림이 수신되면 페이저 또는 보안 운영 센터와 같은 적절한 사람과 시스템으로 라우팅되어야 합니다.
- 사용 가능한 로그 소스, 계정에 저장된 위치 및 액세스할 수 있는 사용자를 이해합니다.
- 조사 중에 CloudWatch Insights를 사용하여 로그를 쿼리하는 방법을 이해합니다.
- 리소스(EC2, IAM, S3, son on)별로 사용할 수 있는 격리 옵션과 격리 시 워크로드 가용성에 미치는 결과를 이해합니다.

감지

AWS 계정을 관리하는 동안 AMS는 Amazon CloudWatch, Amazon GuardDuty, VPC 흐름 로그, Amazon Macie 및 Amazon 내부 위협 인텔리전스 피드를 포함하되 이에 국한되지 않는 탐지 소스 및 제어에서 수집된 데이터를 사용하여 사용자 동작, 계정 활동 AWS Config 및 잠재적 보안 이벤트의 이상을 모니터링합니다.

AMS는 네이티브 AWS 서비스와 기타 탐지 기술을 모두 사용하여 다음에서 생성된 보안 이벤트에 대응합니다.

- Config 적합성 조사 결과 유형
- GuardDuty 결과 유형
- Macie 결과 유형
- Amazon Route 53 Resolver DNS 방화벽 이벤트
- AMS 보안 이벤트(클라우드 감시 경보)

서비스, 제품 및 위협 에코시스템이 발전함에 따라 추가 조사 결과가 추가됩니다.

AMS에 보안 이벤트 보고

AMS 지원 포털 또는 지원 센터를 통해 인시던트를 제기하여 AMS에 보안 인시던트를 알리거나 조사를 요청합니다.

분석

보안 이벤트를 식별하고 보고한 후 다음 단계는 보고된 이벤트가 거짓 긍정인지 실제 인시던트인지 분석하는 것입니다. AMS는 자동화 및 수동 조사 기술을 사용하여 보안 이벤트를 처리합니다. 분석에는 네트워크 트래픽 로그, 호스트 로그, CloudTrail 이벤트, AWS 서비스 로그 등과 같은 다양한 탐지 소스의 로그에 대한 조사가 포함됩니다. 또한이 분석에서는 상관관계를 기준으로 이상 동작을 보여주는 패턴을 찾습니다.

파트너십은 계정 환경과 관련된 컨텍스트를 이해하고 계정 및 워크로드에 일반적인 사항을 설정하는 데 필요합니다. 이를 통해 AMS는 이상을 더 빠르게 식별하고 인시던트 대응을 가속화할 수 있습니다.

보안 이벤트에 대한 AMS의 통신 처리

AMS는 인시던트 티켓을 통해 보안 담당자를 참여시켜 조사 중에 정보를 제공합니다. AMS 클라우드 서비스 제공 관리자(CSDM)와 AMS 클라우드 아키텍트(CA)는 활성 보안 조사 중에 통신을 위해에 문의할 수 있는 담당자입니다.

통신에는 보안 알림이 생성될 때의 자동 알림, 이벤트 분석 후의 통신, 통화 브리지 설정, 로그 파일, 감염된 리소스의 스냅샷, 보안 이벤트 중에 사용자에게 조사 결과 가져오기와 같은 아티팩트의 지속적인 전달이 포함됩니다.

AMS 보안 알림에 포함된 표준 필드는 다음과 같습니다. 이러한 필드는 문제 해결을 위해 조직 내 적절한 팀에 이벤트를 라우팅할 수 있도록 정보를 제공합니다.

- 결과 유형

- 결과 식별자(해당하는 경우)
- 심각도 찾기
- 결과 설명
- 생성된 날짜 및 시간 찾기
- AWS 계정 ID
- 리전(해당하는 경우)
- AWS 리소스(IAM user/role/policy, EC2, S3, EKS)

결과 유형에 따라 추가 필드가 제공됩니다. 예를 들어 EKS 결과에는 포드, 컨테이너 및 클러스터 세부 정보가 포함됩니다.

격리

AMS의 억제 접근 방식은 사용자와의 파트너십입니다. 네트워크 격리, IAM 사용자 또는 역할 프로비저닝 해제, 인스턴스 재구축 등과 같은 억제 활동으로 인해 발생할 수 있는 비즈니스 및 워크로드 영향을 이해합니다.

억제의 필수 부분은 의사 결정입니다. 예를 들어 시스템을 종료하거나, 네트워크에서 리소스를 격리하거나, 액세스 또는 종료 세션을 끕니다. 인시던트를 억제할 사전 결정된 전략과 절차가 있는 경우 이러한 결정을 더 쉽게 내릴 수 있습니다. AMS는 억제 전략을 제공한 다음 억제 작업 구현과 관련된 위험을 고려한 후 솔루션을 구현합니다.

분석 중인 리소스에 따라 다양한 억제 옵션이 있습니다. AMS는 인시던트 조사 중에 여러 유형의 억제가 동시에 배포될 것으로 예상합니다. 이러한 예에는 다음이 포함됩니다.

- 보호 규칙을 적용하여 무단 트래픽 차단(보안 그룹, NACL, WAF 규칙, SCP 규칙, 거부 목록, 격리 또는 차단으로 서명 작업 설정)
- 리소스 격리
- 네트워크 격리
- IAM 사용자, 역할 및 정책 비활성화
- IAM 사용자, 역할 권한 수정/축소
- 컴퓨팅 리소스 종료/일시 중지/삭제
- 영향을 받는 리소스에서 퍼블릭 액세스 제한
- 액세스 키, API 키 및 암호 교체

- 공개된 자격 증명 및 민감한 정보 스크러빙

AMS는 위험 선호도 내에 있는 각 주요 인시던트 유형에 대한 억제 전략 유형을 고려하는 것이 좋습니다. 인시던트 발생 시 의사 결정에 도움이 되는 기준이 명확하게 문서화되어 있습니다. 적절한 전략을 결정하기 위한 기준은 다음과 같습니다.

- 리소스의 잠재적 손상
- 증거 보존
- 서비스 사용 불가(예: 네트워크 연결, 외부 당사자에게 제공되는 서비스)
- 전략을 구현하는 데 필요한 시간 및 리소스
- 전략의 효율성(예: 부분 격리, 전체 격리)
- 솔루션의 영구성(예: 단방향 출입구와 양방향 출입구 결정)
- 솔루션 기간(예: 긴급 해결 방법은 4시간 내에 제거, 임시 해결 방법은 2주 내에 제거, 영구 솔루션).
- 켤 수 있는 보안 제어를 적용하여 위험을 낮추고 시간을 내어 보다 효과적인 억제를 정의하고 구현할 수 있습니다.

억제 속도가 매우 중요하므로 AMS는 단기 및 장기 접근 방식을 전략화하여 효율적이고 효과적인 억제를 달성하기 위해 단계적 접근 방식을 권장합니다.

이 가이드를 사용하여 리소스 유형에 따라 다양한 기법이 포함된 억제 전략을 고려하세요.

- 억제 전략
  - AMS가 보안 인시던트의 범위를 식별할 수 있습니까?
    - 그렇다면 모든 리소스(사용자, 시스템, 리소스)를 식별합니다.
    - 그렇지 않으면 식별된 리소스에 대해 다음 단계를 실행하는 것과 병행하여 조사합니다.
  - 리소스를 격리할 수 있나요?
    - 그렇다면 영향을 받는 리소스를 격리합니다.
    - 그렇지 않은 경우 시스템 소유자 및 관리자와 협력하여 문제를 격리하는 데 필요한 추가 조치를 결정합니다.
  - 영향을 받는 모든 리소스가 영향을 받지 않는 리소스로부터 격리되어 있나요?
    - 그렇다면 다음 단계로 계속 진행합니다.
    - 그렇지 않은 경우 인시던트가 더 이상 에스컬레이션되지 않도록 단기 격리가 완료될 때까지 영향을 받는 리소스를 계속 격리합니다.
- 시스템 백업

- 추가 분석을 위해 영향을 받는 시스템의 백업 복사본이 생성되었나요?
- 포렌식 사본은 암호화되어 안전한 위치에 저장되나요?
  - 그렇다면 다음 단계로 계속 진행합니다.
  - 그렇지 않으면 포렌식 이미지를 암호화한 다음 안전한 위치에 저장하여 우발적인 사용, 손상 및 변조를 방지합니다.

근절

인시던트가 억제된 후 다음 복구 단계로 진행하기 전에 시스템을 보호하기 위해 위협 원인을 완전히 제거하기 위해 근절이 필요할 수 있습니다. 제거 단계에는 멀웨어 삭제 및 손상된 사용자 계정 제거, 악용된 모든 취약성 식별 및 완화가 포함될 수 있습니다. 근절 중에는 환경 내에서 영향을 받는 모든 계정, 리소스 및 인스턴스를 식별하여 문제를 해결하는 것이 중요합니다.

문제 해결 단계가 우선시되도록 단계적 접근 방식으로 근절 및 복구를 수행하는 것이 모범 사례입니다. 대규모 인시던트의 경우 복구에 몇 개월이 걸릴 수 있습니다. 초기 단계의 의도는 향후 인시던트를 방지하기 위해 비교적 빠른(수일에서 수주) 고가치 변경으로 전반적인 보안을 강화하는 것이어야 합니다. 이후 단계에서는 엔터프라이즈를 최대한 안전하게 유지하기 위해 장기 변경(예: 인프라 변경)과 지속적인 작업에 중점을 두어야 합니다.

일부 인시던트의 경우 근절이 필요하지 않거나 복구 중에 수행됩니다.

다음을 고려하세요.

- 시스템을 다시 이미지화한 다음 패치 또는 기타 대응책으로 강화하여 공격 위험을 방지하거나 줄일 수 있습니까?
- 공격자가 남긴 모든 맬웨어 및 기타 아티팩트가 제거되고 영향을 받는 시스템이 추가 공격에 대해 강화되나요?

복구

AMS는 고객과 협력하여 시스템을 정상 작동으로 복원하고, 시스템이 정상적으로 작동하는지 확인하고, (해당하는 경우) 취약성을 해결하여 유사한 인시던트를 방지합니다.

다음을 고려하세요.

- 영향을 받는 시스템(들)이 최근 공격 및 가능한 향후 공격에 대해 패치되고 강화됩니까?
- 영향을 받는 시스템을 다시 프로덕션 환경으로 복원할 수 있는 날짜와 시간은 언제입니까?

- 프로덕션으로 복원하는 시스템이 초기 공격 기법에 취약하지 않은지 테스트, 모니터링 및 확인하는 데 사용할 도구는 무엇입니까?

사후 인시던트 보고서

이벤트 후 AMS는 모든 보안 인시던트에 대한 조사 검토 프로세스를 실행합니다. 또한 AMS는 시스템 또는 개선의 여지가 있을 수 있는 절차적 누락으로 인한 보안 인시던트를 해결하기 위해 오류 수정(COE) 프로세스를 시작합니다. AMS는 고객과 협력하여 보안 조사 경험을 지속적으로 개선합니다. COE 프로세스는 AMS가 고객에게 영향을 미치는 이벤트의 기여 요인을 식별하고 이러한 원인을 유사한 이벤트의 재발을 방지하거나 영향 기간 또는 수준을 완화할 수 있는 다음 조치 항목에 연결하는 데 도움이 됩니다.

보안 인시던트에 대한 조사 검토 프로세스는 개선 기회를 식별하기 위해 다음 항목을 다룹니다.

- 인시던트 시작부터 인시던트 검색, 초기 영향 평가, 인시던트 처리 프로세스의 각 단계(예: 억제, 복구)까지의 경과 시간은 얼마였나요?
- 인시던트 대응 팀이 인시던트의 초기 보고서에 응답하는 데 얼마나 걸렸나요?
- 초기 영향 분석을 수행하는 데 얼마나 걸렸나요?
- 이를 예방할 수 있었나요? 그리고 어떻게 했나요? 이를 방지할 수 있는 도구나 프로세스가 있나요?
- 이를 더 빨리, 그리고 어떻게 감지할 수 있었을까요?
- 조사 속도를 높일 수 있었던 이유는 무엇입니까?
- 문서화된 인시던트 대응 절차를 따랐습니까? 적절했나요?
- 다른 이해관계자와의 정보 공유가 적시에 이루어졌습니까? 어떻게 개선할 수 있습니까?
- 다른 팀(AWS 보안, 계정 팀, AWS 개발 팀 및 고객 보안 팀)과의 협업이 효과적이었나요? 그렇지 않다면 무엇을 개선할 수 있을까요?
- 도움이 될 수 있는 준비 단계, 에스컬레이션 매트릭스, RACI, 공동 책임 모델 등이 누락되었나요? 런북을 업데이트해야 하나요?
- 초기 영향 평가와 최종 영향 평가의 차이점은 무엇입니까? 인시던트 대응 초기에 평가의 정확도를 높이기 위해 무엇을 할 수 있습니까?
- 학습한 교훈의 작업 항목은 무엇입니까?

AMS의 보안 인시던트 대응 런북

이 섹션에는 두 개의 실행서가 포함되어 있습니다.

- 루트 사용자 활동에 대한 응답
- 맬웨어 이벤트에 대한 응답

루트 사용자 활동에 대한 응답

루트 사용자는 AWS 계정 내의 수퍼유저입니다. AMS는 루트 사용량을 모니터링합니다. 계정 설정을 변경하고, 결제 및 비용 관리에 대한 액세스를 활성화 AWS Identity and Access Management (IAM)하고, 루트 암호를 변경하고, 다중 인증(MFA)을 활성화하는 등 루트 사용자가 필요한 몇 가지 작업에만 루트 사용자를 사용하는 것이 좋습니다. 자세한 내용은 루트 사용자 자격 증명이 필요한 작업을 참조하세요.

AMS에 계획된 루트 사용량을 알리는 방법에 대한 자세한 내용은 AMS에서 루트 계정을 사용하는 시기와 방법을 참조하세요.

루트 사용자 활동이 감지되면 로그인 시도가 실패하여 로그인 성공 후 계정에서 무차별 대입 공격 또는 활동을 나타낼 수 있으며 이벤트가 생성되고 정의된 보안 연락처로 인시던트가 전송됩니다.

AWS Managed Services Operations는 계획되지 않은 루트 사용자 활동을 조사하고, 데이터 수집, 분류 및 분석을 수행하고, 지시에 따라 억제 활동을 수행한 다음 사후 이벤트 분석을 수행합니다.

AMS Advanced 운영 모델을 사용하는 경우 AMS CSDM 및 AMS Ops 엔지니어로부터 루트 사용자 자격 증명을 보호할 AMS의 책임으로 인해 계획되지 않은 루트 사용자 활동을 확인하는 추가 커뮤니케이션을 받게 됩니다. AMS는 경로를 확인할 때까지 루트 사용자 활동을 조사합니다.

준비

불필요한 인시던트 대응 활동을 방지하기 위해 계획된 이벤트의 데이터 및 시간과 함께 AMS 서비스 요청을 제출하여 계획된 루트 사용자 사용에 대해 AMS에 알립니다.

AMS로 GameDays를 정기적으로 수행하여 AMS의 고객 인시던트 대응 프로세스, 최신 사용자 및 시스템을 검증하고 책임 있는 개인과 함께 메모리를 구축하여 인시던트 대응 속도를 높입니다.

단계 A: 감지

AMS는 GuardDuty 및 AMS 모니터링을 포함한 탐지 소스를 통해 계정의 루트 활동을 모니터링합니다.

AMS Accelerate를 사용하는 경우 운영 모델은 예상치 못한 루트 사용자 활동에 대한 조사를 요청하는 인시던트에 응답합니다. 이 경우 AMS 작업은 손상된 계정 실행서를 시작합니다.

AMS Advanced가 있는 경우 운영 모델은 인시던트에 대응하거나 CSDM에 계획된 루트 사용자 활동을 알려 활성 계정 침해 조사를 종료합니다.

단계 B: 분석

AMS는 활동이 승인되지 않은 것으로 확인되면 루트 사용자 이벤트에 대한 철저한 조사를 수행합니다. 로그와 이벤트는 자동화와 AMS 보안 대응 팀을 모두 사용하여 루트 사용자의 이상 및 예상치 못한 동작에 대해 분석됩니다. 활동을 알 수 없는지, 권한이 부여된 루트 사용자 이벤트인지 또는 추가 조사가 필요한지 확인하는 데 도움이 되는 로그가 제공됩니다.

내부 검사를 지원하기 위해 조사 중에 제공되는 정보의 몇 가지 예는 다음과 같습니다.

- 계정 정보: 루트 계정이 사용된 계정은 무엇입니까?
- 루트 사용자의 이메일 주소: 각 루트 사용자는 조직의 이메일 주소와 연결됩니다.
- 인증 세부 정보: 루트 사용자는 어디에서 언제 환경에 액세스했습니까?
- 활동 레코드: 루트로 로그인할 때 사용자가 수행한 작업은 무엇입니까? 이러한 레코드는 CloudWatch 이벤트의 형태입니다. 이러한 로그를 읽는 방법을 이해하면 조사에 도움이 됩니다.

분석 정보를 수신하고 조직 내 계정의 승인된 연락 지점에 도달하는 방법을 계획할 준비가 되어 있는 것이 모범 사례입니다. 루트 사용자는 개인으로 이름이 지정되지 않으므로 조직 내 계정에 사용되는 루트 이메일 주소에 액세스할 수 있는 사람을 결정하면 질문을 내부적으로 빠르게 라우팅하는 데 도움이 됩니다.

단계 C: 포함 및 제거

AMS는 보안 팀과 협력하여 승인된 고객 보안 담당자의 지시에 따라 제한을 수행합니다. 억제 옵션은 다음과 같습니다.

- 적절한 자격 증명 및 키 교체.
- 계정 및 리소스에 대한 활성 세션을 종료합니다.
- 생성된 리소스 제거.

억제 활동 중에 AMS는 보안 팀과 긴밀하게 협력하여 워크로드 중단을 최소화하고 루트 자격 증명을 적절하게 보호합니다.

억제 계획이 완료되면 필요에 따라 AMS 운영 팀과 협력하여 복구 작업을 수행합니다.

사후 인시던트 보고서

필요에 따라 AMS는 조사 검토 프로세스를 시작하여 학습한 교훈을 식별합니다. COE 완료의 일환으로 AMS는 영향을 받는 고객에게 관련 조사 결과를 전달하여 인시던트 대응 프로세스를 개선하는 데 도움을 줍니다.

AMS는 조사의 모든 최종 세부 정보를 문서화하고 적절한 지표를 수집한 다음 할당된 CSDM 및 CA를 포함하여 정보가 필요한 모든 AMS 내부 팀에 인시던트를 보고합니다.

맬웨어 이벤트에 대한 응답

Amazon EC2 인스턴스는 조직 내 애플리케이션 팀이 배포한 타사 소프트웨어 및 사용자 지정 개발 소프트웨어를 비롯한 다양한 워크로드를 호스팅하는 데 사용됩니다. AMS는 AMS에서 패치를 적용하고 지속적으로 유지 관리하는 이미지에 워크로드를 배포하도록 권장하고 제공합니다.

인스턴스를 작동하는 동안 AMS는 Amazon GuardDuty, 네트워크 트래픽 및 Amazon 내부 위협 인텔리전스 피드를 비롯한 다양한 보안 탐지 제어를 통해 동작 또는 활동의 이상을 모니터링합니다.

또한 AMS는 GuardDuty 맬웨어 조사 결과를 모니터링합니다. 활성화된 경우 AMS Advanced와 AMS Accelerate 모두에서 사용할 수 있습니다. 자세한 내용은 Amazon GuardDuty의 맬웨어 보호를 참조하세요.

> **Note**
>
> Bring Your Own EPS를 선택한 경우 인시던트 대응 프로세스는이 페이지에 설명된 것과 다릅니다. 자세한 내용은 참조된 설명서를 참조하세요.

맬웨어가 감지되면 인시던트가 생성되고 이벤트에 대한 알림을 받게 됩니다. 이 알림 뒤에는 해결 활동이 발생합니다. AMS Operations는 데이터 수집, 분류 및 분석을 조사하고 수행한 다음 사용자 방향에 따라 억제 활동을 수행한 다음 사후 이벤트 분석을 수행합니다.

단계 A: 감지

AMS는 GuardDuty를 사용하여 인스턴스의 이벤트를 모니터링합니다. AMS는 조사 결과 또는 알림 유형에 따라 억제 또는 위험 수용 결정을 내리는 데 도움이 되는 적절한 보강 및 분류 활동을 결정합니다.

데이터 수집은 결과 유형에 따라 수행됩니다. 데이터 수집에는 영향을 받는 계정 내부 및 외부에서 여러 데이터 소스를 쿼리하여 관찰된 활동 또는 우려되는 구성에 대한 그림을 작성하는 작업이 포함됩니다.

AMS는 영향을 받는 계정 또는 AMS 위협 인텔리전스 플랫폼의 다른 경보 및 알림 또는 원격 측정과 결과의 상관 관계를 수행합니다.

B단계: 분석

데이터가 수집되면 데이터를 분석하여 우려되는 활동 또는 지표를 식별합니다. 이 조사 단계에서 AMS는 고객과 협력하여 인스턴스 및 워크로드에 대한 비즈니스 및 도메인 지식을 통합하여 무엇이 예상되고 무엇이 일반적이지 않은지 이해하는 데 도움을 줍니다.

내부 검사를 지원하기 위해 조사 중에 제공되는 정보의 몇 가지 예는 다음과 같습니다.

- 계정 정보: 맬웨어 활동이 관찰된 계정은 무엇입니까?
- 인스턴스 세부 정보: 맬웨어 이벤트와 관련된 인스턴스(들)는 무엇입니까?
- 이벤트 타임스탬프: 알림이 트리거된 시기는 언제입니까?
- 워크로드 정보: 인스턴스에서 실행 중인 것은 무엇입니까?
- 해당하는 경우 맬웨어 세부 정보: 맬웨어 패밀리 및 맬웨어에 대한 오픈 소스 정보.
- 사용자 또는 역할 세부 정보: 활동의 영향을 받고 활동에 관련된 사용자 또는 역할은 무엇입니까?
- 활동 레코드: 인스턴스에 기록되는 활동은 무엇입니까? 이는 CloudWatch 이벤트 및 인스턴스의 시스템 이벤트의 형태입니다. 이러한 로그를 읽는 방법을 이해하면 조사에 도움이 됩니다.
- 네트워크 활동: 인스턴스에 연결하는 엔드포인트, 인스턴스가 연결하는 엔드포인트, 트래픽 분석이란 무엇입니까?

조사 정보를 수신하고 조직 내 계정, 인스턴스 및 워크로드의 적절한 연락 지점에 연락하는 방법에 대한 계획을 세우는 것이 모범 사례입니다. 네트워크 토폴로지와 예상 연결을 이해하면 영향 분석을 가속화하는 데 도움이 될 수 있습니다. 환경에서 계획된 침투 테스트와 애플리케이션 소유자가 수행한 최근 배포에 대한 지식도 조사 속도를 높일 수 있습니다.

활동이 계획되고 승인되었다고 판단되면 인시던트가 업데이트되고 조사가 종료됩니다. 손상이 확인되면 사용자와 AMS가 적절한 억제 계획을 결정합니다.

속도 C: 포함 및 제거

AMS는 고객과 협력하여 수집된 데이터와 알려진 정보를 기반으로 적절한 억제 활동을 결정합니다. 억제 옵션은 다음을 포함하지만 이에 국한되지는 않습니다.

- 스냅샷을 통한 데이터 보존
- 인스턴스 내부 또는 외부의 트래픽을 제한하도록 네트워크 규칙 수정
- SCP, IAM 사용자 및 역할 정책을 수정하여 액세스 제한
- 인스턴스 종료, 일시 중지 또는 끄기
- 영구 연결 종료

- 적절한 자격 증명/키 교체

인스턴스에 대해 근절 활동을 수행하도록 선택하면 AMS가 이를 달성할 수 있도록 지원합니다. 옵션은 다음을 포함하지만 이에 국한되지는 않습니다.

- 원치 않는 소프트웨어 제거
- 완전히 패치된 깨끗한 이미지에서 인스턴스 재구축 및 애플리케이션 및 구성 재배포
- 이전 백업에서 인스턴스 복원
- 워크로드를 호스팅하는 데 적합할 수 있는 계정 내 다른 인스턴스에 애플리케이션 및 서비스를 배포합니다.

인스턴스에서 맬웨어가 다시 발생하지 않도록 추가 제어가 적용되도록 서비스를 복원하기 전에 인스턴스에서 맬웨어가 전달되고 실행되는 방법을 확인하는 것이 중요합니다. AMS는 포렌식을 지원하는 데 필요한 추가 인사이트 또는 정보를 포렌식 파트너 또는 팀에 제공합니다.

이 시점에서 복구 활동을 위해 AMS Operations와 협력합니다. AMS는 사용자와 긴밀하게 협력하여 워크로드 중단을 최소화하고 인스턴스를 보호합니다.

사후 인시던트 보고서

필요에 따라 AMS는 조사 검토 프로세스를 시작하여 학습한 교훈을 식별합니다. COE 완료의 일환으로 AMS는 인시던트 대응 프로세스를 개선하는 데 도움이 되도록 관련 조사 결과를 사용자에게 전달합니다.

AMS는 조사의 최종 세부 정보를 문서화하고, 적절한 지표를 수집하고, 할당된 CSDM 및 CA를 포함하여 정보가 필요한 AMS 내부 팀에 인시던트를 보고합니다.

Accelerate의 보안 이벤트 로깅 및 모니터링

AMS Accelerate에 등록된 계정은 노이즈를 줄이고 실제 인시던트의 징후를 식별하도록 최적화된 CloudWatch 이벤트 및 경보의 기본 배포로 구성됩니다. 또한 AMS Accelerate는 계정 모니터링에 GuardDuty를 사용합니다. 자세한 내용은 GuardDuty로 모니터링 단원을 참조하십시오.

Accelerate의 구성 규정 준수

AMS Accelerate를 사용하면 보안 및 운영 무결성에 대한 높은 표준에 맞게 리소스를 구성하고 다음 업계 표준을 준수할 수 있습니다.

- 인터넷 보안 센터(CIS)
- 미국 국립표준기술연구소(NIST) 클라우드 보안 프레임워크(CSF)
- HIPAA(미국 건강 보험 양도 및 책임에 관한 법)
- Payment Card Industry(PCI) 데이터 보안 표준(DSS)

이를 위해 전체 규정 준수 AWS Config 규칙 세트를 계정에 배포합니다. 섹션을 참조하세요AMS Config 규칙 라이브러리. AWS Config 규칙은 리소스에 대해 원하는 구성을 나타내며 AWS 리소스 설정의 구성 변경에 대해 평가됩니다. 모든 구성 변경은 규정 준수를 테스트하기 위해 많은 수의 규칙을 트리거합니다. 예를 들어, Amazon S3 버킷을 생성하고 NIST 표준을 위반하여 공개적으로 읽을 수 있도록 구성한다고 가정해 보겠습니다. ams-nist-cis-s3-bucket-public-read-prohibited 규칙은 위반을 감지하고 구성 보고서에서 S3 버킷에 규정 미준수 레이블을 지정합니다. 이 규칙은 자동 인시던트 문제 해결 범주에 속하므로 즉시 인시던트 보고서를 생성하여 문제를 알립니다. 더 심각한 다른 규칙 위반으로 인해 AMS가 문제를 자동으로 해결할 수 있습니다. Accelerate의 위반에 대한 대응을(를) 참조하세요.

> **Important**
>
> 예를 들어 AMS가 문제 해결 범주에 관계없이 위반 사항을 해결하도록 하려면 AMS에 규정 미준수 리소스를 해결하도록 요청하는 서비스 요청을 제출합니다. 서비스 요청에 "AMS 구성 규칙 수정의 일부로 불만이 아닌 리소스 *RESOURCE_ARNS_OR_IDs*, 계정의 구성 규칙 *CONFIG_RULE_NAME*을 수정하십시오"와 같은 설명을 포함하고 위반을 수정하는 데 필요한 입력을 추가합니다.
>
> 예를 들어 설계상 퍼블릭 액세스가 필요한 특정 S3 버킷에 대해 조치를 취하지 않으려면 예외를 생성할 수 있습니다. 단원을 참조하십시오Accelerate에서 규칙 예외 생성.

AMS Config 규칙 라이브러리

Accelerate는 계정을 보호하기 위해 AMS 구성 규칙 라이브러리를 배포합니다. 이러한 구성 규칙은 로 시작합니다ams-. AWS Config 콘솔, AWS CLI 또는 AWS Config API에서 계정 내 규칙과 해당 규정 준수 상태를 볼 수 있습니다. 사용에 대한 일반적인 내용은 ViewingConfiguration Compliance를 AWS Config참조하세요.

> **Note**
>
> 옵트인 AWS 리전및 Gov 클라우드 리전의 경우 리전 제한으로 인해 구성 규칙의 하위 집합만 배포합니다. AMS Accelerate 구성 규칙 테이블에서 식별자와 연결된 링크를 확인하여 리전의 규칙 가용성을 확인합니다.
> 배포된 AMS Config 규칙은 제거할 수 없습니다.

규칙 테이블

ams_config_rules.zip으로 다운로드합니다.

AMS 구성 규칙

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-guardduty-enabled-centralized	GuardDuty	주기적	문제 해결	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 2.2,3.4,8.2.1,
ams-nist-cis-vpc-flow-logs-enabled	VPC	주기적	문제 해결	CIS: CIS.6, NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-5,PR.PT-1, HIPAA: 164.308(a)(3)(ii)(A),164.312(b), PCI: 2.2,10.1, 10.3.2,10.3.3,10.3.4,10.3.5,10.3.6;
ams-eks-secrets-encrypted	EKS	주기적	인시던트	CIS: NA, NIST-CSF: NA, HIPAA: NA, PCI: NA,
ams-eks-endpoint-no-public-access	EKS	주기적	인시던트	CIS: NA, NIST-CSF: NA, HIPAA: NA, PCI: NA,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-vpc-default-security-group-closed	VPC	구성 변경 사항	인시던트	CIS: CIS.11,CIS.12,CIS.9, NIST-CSF: DE.AE-1,PR.AC-3,PR.AC-5,PR.PT-4, HIPAA: 164.312(e)(1), PCI: 1.2,1.3,2.1,2.2,1.2.1,1.3.1,1.3.2,2.2.2
ams-nist-cis-iam-password-policy	IAM	주기적	인시던트	CIS: NA, NIST-CSF: PR.AC-1,PR.AC-4, HIPAA: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.308(a)(3)(ii)(B),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(C),164.312(a)(1), PCI: 7.1.2,7.1.3,7.2.2;
ams-nist-cis-iam-root-access-key-check	IAM	주기적	인시던트	CIS: CIS.16,CIS.4; NIST-CSF: PR.AC-1,PR.AC-4,PR.PT-3; HIPAA: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.308(a)(3)(ii)(B),164.308(a)(4)(4)(ii)(A),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(C),164.312(a)(1), PCI: 2,7.1.2,7.1.1.3.1.7.

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-iam-user-mfa-enabled	IAM	주기적	인시던트	CIS: CIS.16, NIST-CSF: PR.AC-1,PR.AC-4, HIPAA: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.308(a)(3)(ii)(B),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(C),164.312(a)(1); PCI: 2.2,7.1.2,7.1.3.7.2.2.1
ams-nist-cis-restricted-ssh	보안 그룹	구성 변경 사항	인시던트	CIS: CIS.16; NIST-CSF: PR.AC-1,PR.AC-4; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(C),164.312(a)(1); PCI: 2.2,7.2.1,8.1.4;
ams-nist-cis-restricted-common-ports	보안 그룹	구성 변경 사항	인시던트	CIS: CIS.11,CIS.12,CIS.9; NIST-CSF: DE.AE-1,PR.AC-3,PR.AC-5,PR.PT-4; HIPAA: 164.308(a)(3)(i),164.308(a)(3)(ii)(B),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1); PCI:2,1.3,1.2.

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-s3-account-level-public-access-blocks	S3	구성 변경 사항	인시던트	CIS: CIS.9,CIS.12,CIS.14, NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4, HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1), PCI: 1.2,1.2.1,1.3,1.3.1,1.3.2,1.3.4,1.3.3.6,2.2.2;
ams-nist-cis-s3-bucket-public-read-prohibited	S3	구성 변경 사항	인시던트	CIS: CIS.12,CIS.14,CIS.9, NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4, HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1), PCI: 1.2,1.3,2.2,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2;
ams-nist-cis-s3-bucket-public-write-prohibited	S3	구성 변경 사항	인시던트	CIS: CIS.12,CIS.14,CIS.9, NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4, HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1), PCI: 1.2,1.3,2.2,1.2.1,1.3.1,1.3.2,1.3.3.4,1.3.6,2.2.2;

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-s3-bucket-server-side-encryption-enabled	S3	구성 변경 사항	인시던트	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv),164.312(c)(2),164.312(e)(2)(ii), PCI: 2.2,3.4,10.5,8.2.1,
ams-nist-cis-securityhub-enabled	Security Hub	주기적	인시던트	CIS: CIS.3,CIS.4,CIS.6, CIS.12,CIS.16,CIS.19, NIST-CSF: PR.DS-5,PR.PT-1, HIPAA: 164.312(b), PCI: NA,
ams-nist-cis-ec2-instance-managed-by-systems-manager	EC2	구성 변경 사항	Report	CIS: CIS.2,CIS.5, NIST-CSF: ID.AM-2,PR.IP-1, HIPAA: 164.308(a)(5)(ii)(B), PCI: 2.4,
ams-nist-cis-cloudtrail-enabled	CloudTrail	주기적	Report	CIS: CIS.16,CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-5,PR.MA-2,PR.PT-1; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(b); PCI: 10.1,10.2.1,10.2.2,10.2.3,10.2.410.2.5,10.2.7,10.2.6,10.3.1,10.3.2,10.3.3,,10.3.4,,10.3.5, 10.3.6;
ams-nist-cis-access-keys-rotated	IAM	주기적	Report	CIS: CIS.16, NIST-CSF: PR.AC-1, HIPAA: 164.308(a)(4)(ii)(B), PCI: 2.2,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-acm-certificate-expiration-check	Certificate Manager	구성 변경 사항	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.AC-5,PR.PT-4, HIPAA: NA, PCI: 4.1,
ams-nist-cis-alb-http-to-https-redirection-check	ALB	주기적	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-2, HIPAA: 164.312(a)(2)(iv), 164.312(e)(1),164.312(e)(2)(i),164.312(e)(2)(ii), PCI: 2.3,4.1,8.2.1
ams-nist-cis-api-gw-cache-enabled-and-encrypted	API Gateway	구성 변경 사항	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 3.4,
ams-nist-cis-api-gw-execution-logging-enabled	API Gateway	구성 변경 사항	Report	CIS: CIS.6, NIST-CSF: DE.AE-1,DE.AE-3,PR.PT-1, HIPAA: 164.312(b), PCI: 10.1,10.3.1,10.3.2,10.3.3,10.3.4,10.3.5,10.3.610.5.4
ams-nist-autoscaling-group-elb-healthcheck-required	ELB	구성 변경 사항	Report	CIS: NA, NIST-CSF: PR.PT-1,PR.PT-5, HIPAA: 164.312(b), PCI: 2.2,
ams-nist-cis-cloud-trail-encryption-enabled	CloudTrail	주기적	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 2.2,3.4,10.5,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-cloud-trail-log-file-validation-enabled	CloudTrail	주기적	Report	CIS: CIS.6; NIST-CSF: PR.DS-6; HIPAA: 164.312(c)(1),164.312(c)(2); PCI: 2.2,10.5, 11.5,10.5.2,10.5.5;
ams-nist-cis-cloudtrail-s3-dataevents-enabled	CloudTrail	주기적	Report	CIS: CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-5,PR.PT-1; HIPAA: 164.308(a)(3)(ii)(A),164.312(b); PCI: 2.2,10.1, 10.2.1,10.2.2,10.2.3,10.2.5 10.3.1,10.3.210.3.3,10.3.4, 10.3.5,,10.3.6;
ams-nist-cis-cloudwatch-alarm-action-check	CloudWatch	구성 변경 사항	Report	CIS: CIS.13,CIS.14, NIST-CSF: NA, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 3.4,
ams-nist-cis-cloudwatch-log-group-encrypted	CloudWatch	주기적	Report	CIS: CIS.13,CIS.14, NIST-CSF: NA, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 3.4,
ams-nist-cis-codebuild-project-envvar-awscred-check	CodeBuild	구성 변경 사항	Report	CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1); PCI: 8.2.1;

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-codebuild-project-source-repo-url-check	CodeBuild	구성 변경 사항	Report	CIS: CIS.18; NIST-CSF: PR.DS-5; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1); PCI: 8.2.1;
ams-nist-cis-db-instance-backup-enabled	RDS	구성 변경 사항	Report	CIS: CIS.10, NIST-CSF: ID.BE-5,PR.DS-4,PR.IP-4,PR.PT-5,RC.RP-1, HIPAA: 164.308(a)(7)(i),164.308(a)(7)(ii)(A),164.308(a)(7)(ii)(B), PCI: NA
ams-nist-cis-dms-replication-not-public	DMS	주기적	Report	CIS: CIS.12,CIS.14,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.3.4,1.3.6.2.2;
ams-nist-dynamodb-autoscaling-enabled	DynamoDB	주기적	Report	CIS: NA, NIST-CSF: ID.BE-5,PR.DS-4,PR.PT-5,RC.RP-1, HIPAA: 164.308(a)(7)(i),164.308(a)(7)(ii)(C), PCI: NA

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-dynamodb-pitr-enabled	DynamoDB	주기적	Report	CIS: CIS.10, NIST-CSF: ID.BE-5,PR.DS-4,PR .IP-4,PR.PT-5,RC.RP-1, HIPAA: 164.308(a)(7)(i),1 64.308(a)(7)(ii)(A),164.308 (a)(7)(ii)(B), PCI: NA
ams-nist-dynamodb-throughput-limit-check	DynamoDB	주기적	Report	CIS: NA, NIST-CSF: NA, HIPAA: 164.312(b), PCI: NA
ams-nist-ebs-optimized-instance	EBS	구성 변경 사항	Report	CIS: NA, NIST-CSF: NA, HIPAA: 164.308(a)(7)(i), PCI: NA
ams-nist-cis-ebs-snapshot-public-restorable-check	EBS	주기적	Report	CIS: CIS.12,CIS.14,CIS. 9; NIST-CSF: PR.AC-3,P R.AC-4,PR.AC-5,PR. DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i),1 64.308(a)(4)(ii)(A),164.308 (a)(4)(ii)(C),164.312(a) (1),164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1 .3.3.4,1.3.6,2.2;
ams-nist-ec2-instance-detailed-monitoring-enabled	EC2	구성 변경 사항	Report	CIS: NA, NIST-CSF: DE.AE-1,PR.PT-1, HIPAA: 164.312(b), PCI: NA,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-ec2-instance-no-public-ip	EC2	구성 변경 사항	Report	CIS: CIS.12,CIS.14,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.2,1.3.4,1.3.6,2.2;
ams-nist-cis-ec2-managedinstance-association-compliance-status-check	EC2	구성 변경 사항	Report	CIS: CIS.12,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.2,1.3.4,1.3.6,2.2;
ams-nist-cis-ec2-managedinstance-patch-compliance-status-check	EC2	구성 변경 사항	Report	CIS: CIS.2,CIS.5, NIST-CSF: ID.AM-2,PR.IP-1, HIPAA: 164.308(a)(5)(ii)(B), PCI: 6.2,
ams-nist-cis-ec2-stopped-instance	EC2	주기적	Report	CIS: CIS.2, NIST-CSF: ID.AM-2,PR.IP-1, HIPAA: NA, PCI: NA,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-ec2-volume-inuse-check	EC2	구성 변경 사항	Report	CIS: CIS.2, NIST-CSF: PR.IP-1, HIPAA: NA, PCI: NA,
ams-nist-cis-efs-encrypted-check	EFS	주기적	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 3.4,8.2.1,
ams-nist-cis-eip-attached	EC2	구성 변경 사항	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 3.4,8.2.1,
ams-nist-cis-elasticache-redis-cluster-automatic-backup-check	ElastiCache	주기적	Report	CIS: CIS.10, NIST-CSF: ID.BE-5,PR.DS-4,PR .IP-4,PR.PT-5,RC.RP-1, HIPAA: 164.308(a)(7)(i),164.308(a)(7)(ii)(A),164.308(a)(7)(ii)(B), PCI: NA
ams-nist-cis-opensearch-encrypted-at-rest	OpenSearch	주기적	Report	CIS: CIS.14,CIS.13, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 3.4,8.2.1,
ams-nist-cis-opensearch-in-vpc-only	OpenSearch	주기적	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 3.4,8.2.1,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-elb-acm-certificate-required	Certificate Manager	구성 변경 사항	Report	CIS: CIS.12,CIS.9, NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4, HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1), PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2;
ams-nist-elb-deletion-protection-enabled	ELB	구성 변경 사항	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-2, HIPAA: 164.312(a)(2)(iv), 164.312(e)(1),164.312(e)(2)(i),164.312(e)(2)(ii), PCI: 4.1,8.2.1
ams-nist-cis-elb-logging-enabled	ELB	구성 변경 사항	Report	CIS: CIS.6, NIST-CSF: DE.AE-1,DE.AE-3,PR.PT-1, HIPAA: 164.312(b), PCI: 10.1,10.3.1,10.3.2,10.3.3,10.3.4,10.3.5,10.3.610.5.4
ams-nist-cis-emr-kerberos-enabled	EMR	주기적	Report	CIS: CIS.6, NIST-CSF: DE.AE-1,DE.AE-3,PR.PT-1, HIPAA: 164.312(b), PCI: 10.1,10.3.1,10.3.2,10.3.3,10.3.4,10.3.5,10.3.610.5.4

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-emr-master-no-public-ip	EMR	주기적	Report	CIS: CIS.14,CIS.16; NIST-CSF: PR.AC-1,PR.AC-4,PR.AC-6; HIPAA: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.308(a)(3)(ii)(B),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(C),164.312(a)(1); PCI: 7.2.1;
ams-nist-cis-encrypted-volumes	EBS	구성 변경 사항	Report	CIS: CIS.12,CIS.9, NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.PT-3,PR.PT-4, HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1), PCI: 1.2,1.3,1.2.1,1.3.2,1.3.4,1.3.6,2.2;
ams-nist-cis-guardduty-non-archived-findings	GuardDuty	주기적	Report	CIS: CIS.12,CIS.13,CIS.16,CIS.19,CIS.3,CIS.4,CIS.6,CIS.8; NIST-CSF: DE.AE-2,DE.AE-3,DE.CM-4,DE.DP-5,ID.RA-1,ID.RA-3,PR.DS-5,PR.PT-1; HIPAA: 164.308(a)(5)(ii)(C),164.308(a)(6)(ii),164.312(b); PCI: 6.1,11.4,5.1.2;

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-iam-group-has-users-check	IAM	구성 변경 사항	Report	CIS: NA, NIST-CSF: PR.AC-4,PR.AC-1, HIPAA: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.308(a)(3)(ii)(B),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(C),164.312(a)(1), PCI: 7.1.2,7.1.3,7.2.2;
ams-nist-cis-iam-policy-no-statements-with-admin-access	IAM	구성 변경 사항	Report	CIS: CIS.16, NIST-CSF: PR.AC-6,PR.AC-7, HIPAA: 164.308(a)(4)(ii)(B),164.308(a)(5)(ii)(D),164.312(d), PCI: 8.2.3,8.2.4,8.2.5
ams-nist-cis-iam-user-group-membership-check	IAM	구성 변경 사항	Report	CIS: CIS.16,CIS.4, NIST-CSF: PR.AC-1,PR.AC-4,PR.PT-3, HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(a)(2)(i), PCI: 2.2,7.1.2,7.2.1,8.1.1
ams-nist-cis-iam-user-no-policies-check	IAM	구성 변경 사항	Report	CIS: CIS.16, NIST-CSF: PR.AC-1,PR.AC-7, HIPAA: 164.308(a)(4)(ii)(B),164.312(d), PCI: 8.3,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-iam-user-unused-credentials-check	IAM	주기적	Report	CIS: CIS.16, NIST-CSF: PR.AC-1,PR.AC-4,PR.PT-3, HIPAA: 164.308(a)(3)(i),164.308(a)(3)(ii)(A),164.308(a)(3)(ii)(B),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(C),164.312(a)(1), PCI: 2.7.1.2,7.1.7.2.7.
vpc의 ams-nist-cis-ec2-instances instances-in-vpc	EC2	구성 변경 사항	Report	CIS: CIS.11,CIS.12,CIS.9, NIST-CSF: DE.AE-1,PR.AC-3,PR.AC-5,PR.PT-4, HIPAA: 164.308(a)(3)(i),164.308(a)(3)(ii)(B),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(B),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1); PCI:2,1.3,1.2.
ams-nist-cis-internet-gateway-authorized-vpc-only	인터넷 게이트웨이	주기적	Report	CIS: CIS.9,CIS.12, NIST-CSF: NA, HIPAA: NA, PCI: NA,
ams-nist-cis-kms-cmk-not-scheduled-for-deletion	KMS	주기적	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: NA, PCI: 3.5,3.6,
ams-nist-lambda-concurrency-check	Lambda	구성 변경 사항	Report	CIS: NA, NIST-CSF: NA, HIPAA: 164.312(b), PCI: NA

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-lambda-dlq-check	Lambda	구성 변경 사항	Report	CIS: NA, NIST-CSF: NA, HIPAA: 164.312(b), PCI: NA
ams-nist-cis-lambda-function-public-access-prohibited	Lambda	구성 변경 사항	Report	CIS: CIS.12,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.2,1.3.4,2.2;
ams-nist-cis-lambda-inside-vpc	Lambda	구성 변경 사항	Report	CIS: CIS.12,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.2,1.3.4,2.2;
ams-nist-cis-mfa-enabled-for-iam-console-access	IAM	주기적	Report	CIS: CIS.16, NIST-CSF: PR.AC-7, HIPAA: 164.312(d), PCI: 2.2,8.3,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-multi-region-cloudtrail-enabled	CloudTrail	주기적	Report	CIS: CIS.6, NIST-CSF: DE.AE-1,DE.AE-3,PR .DS-5,PR.MA-2,PR.PT-1, HIPAA: 164.308(a)(3) (ii)(A),164.312(b), PCI: 2.2,10.1,10.2.1,10.2.2,10.2 .3,10.2.410.2.5,10.2.6,10.2 .7,10.3.1,,10.3.2,10.3.3,10 .3.4,10.3.5;10.3.6
ams-nist-rds-enhanced-monitoring-enabled	RDS	구성 변경 사항	Report	CIS: NA, NIST-CSF: PR.PT-1, HIPAA: 164.312(b), PCI: NA,
ams-nist-cis-rds-instance-public-access-check	RDS	구성 변경 사항	Report	CIS: CIS.12,CIS.14,CIS. 9; NIST-CSF: PR.AC-3,P R.AC-4,PR.AC-5,PR. DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i),1 64.308(a)(4)(ii)(A),164.308 (a)(4)(ii)(C),164.312(a) (1),164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1 .3.3.4,1.3.6,2.2;
ams-nist-rds-multi-az-support	RDS	구성 변경 사항	Report	CIS: NA, NIST-CSF: ID.BE-5,PR.DS-4,PR .PT-5,RC.RP-1, HIPAA: 164.308(a)(7)(i),1 64.308(a)(7)(ii)(C), PCI: NA,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-rds-snapshots-public-prohibited	RDS	구성 변경 사항	Report	CIS: CIS.12,CIS.14,CIS.9, NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4, HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1), PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.3.4,1.3.6,2.2;
ams-nist-cis-rds-storage-encrypted	RDS	구성 변경 사항	Report	CIS: CIS.13,CIS.5,CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-1,PR.PT-1; HIPAA: 164.312(a)(2)(iv), 164.312(b), 164.312(e)(2)(ii); PCI: 3.4,10.1,10.2.1,10.2.2,10.2.3,10.2.410.2.5,10.3.1,10.3.2,10.3.3,10.3.4,10.3.5,,,,,10.3.6,,,,8.2.1;
ams-nist-cis-redshift-cluster-configuration-check	RedShift	구성 변경 사항	Report	CIS: CIS.6,CIS.13,CIS.5, NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-1,PR.PT-1, HIPAA: 164.312(a)(2)(iv), 164.312(b), 164.312(e)(2)(ii), PCI: 3.4,8.2.1,10.1,10.2.1,10.2.2,10.2.310.2.4,10.2.5,10.3.1,,10.3.2,10.3.3,,,10.3.4,,,,10.3.5,,,10.3.6;

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-redshift-cluster-public-access-check	RedShift	구성 변경 사항	Report	CIS: CIS.12,CIS.14,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.3.4,1.3.6,2.2;
ams-nist-cis-redshift-require-tls-ssl	RedShift	주기적	Report	CIS: CIS.13,CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312(a)(2)(iv),164.312(e)(1),164.312(e)(2)(i),164.312(e)(2)(ii); PCI: 2.3,4.1;
ams-nist-cis-root-account-hardware-mfa-enabled	IAM	주기적	Report	CIS: CIS.16,CIS.4, NIST-CSF: PR.AC-7, HIPAA: 164.312(d), PCI: 2.2,8.3,
ams-nist-cis-root-account-mfa-enabled	IAM	주기적	Report	CIS: CIS.16,CIS.4, NIST-CSF: PR.AC-7, HIPAA: 164.312(d), PCI: 2.2,8.3,
ams-nist-cis-s3-bucket-default-lock-enabled	S3	구성 변경 사항	Report	CIS: CIS.14,CIS.13, NIST-CSF: ID.BE-5,PR.PT-5,RC.RP-1, HIPAA: NA, PCI: NA,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-s3-bucket-logging-enabled	S3	구성 변경 사항	Report	CIS: CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-5,PR.PT-1; HIPAA: 164.308(a)(3)(ii)(A), 164.312(b); PCI: 2.2,10.1, 10.2.1,,10.2.2,10.2.310.2.4,10.2.510.2.7,10.3.110.3.2, 10.3.3,10.3.4,,,10.3.5,10.3.6;
ams-nist-cis-s3-bucket-replication-enabled	S3	구성 변경 사항	Report	CIS: CIS.10, NIST-CSF: ID.BE-5,PR.DS-4,PR.IP-4,PR.PT-5,RC.RP-1, HIPAA: 164.308(a)(7)(i),164.308(a)(7)(ii)(A),164.308(a)(7)(ii)(B), PCI: 2.2,10.5.3
ams-nist-cis-s3-bucket-ssl-requests-only	S3	구성 변경 사항	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-2, HIPAA: 164.312(a)(2)(iv),164.312(c)(2),164.312(e)(1),164.312(e)(2)(i),164.312(e)(2)(ii), PCI: 2.2,4.1,8.2.1;
ams-nist-cis-s3-bucket-versioning-enabled	S3	주기적	Report	CIS: CIS.10, NIST-CSF: ID.BE-5,PR.DS-4,PR.DS-6,PR.IP-4,PR.PT-5,RC.RP-1, HIPAA: 164.308(a)(7)(i),164.308(a)(7)(ii)(A),164.308(a)(7)(ii)(B),164.312(c)(1),164.312(c)(2), PCI: 10.5.3

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-sagemaker-endpoint-configuration-kms-key-configured	SageMaker	주기적	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 3.4,8.2.1,
ams-nist-cis-sagemaker-notebook-instance-kms-key-configured	SageMaker	주기적	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 3.4,8.2.1,
ams-nist-cis-sagemaker-notebook-no-direct-internet-access	SageMaker	주기적	Report	CIS: CIS.12,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A),164.308(a)(4)(ii)(C),164.312(a)(1),164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.2,1.3.4,1.3.6,2.2;
ams-nist-cis-secretsmanager-rotation-enabled-check	Secrets Manager	구성 변경 사항	Report	CIS: CIS.16, NIST-CSF: PR.AC-1, HIPAA: 164.308(a)(4)(ii)(B), PCI: NA,
ams-nist-cis-secretsmanager-scheduled-rotation-success-check	Secrets Manager	구성 변경 사항	Report	CIS: CIS.16, NIST-CSF: PR.AC-1, HIPAA: 164.308(a)(4)(ii)(B), PCI: NA,

규칙 이름	서비스:	트리거	작업	프레임워크
ams-nist-cis-sns-encrypted-kms	SNS	구성 변경 사항	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 8.2.1,
ams-nist-cis-vpc-sg-open-only-to-authorized-ports	VPC	구성 변경 사항	Report	CIS: CIS.11,CIS.12,CIS.9, NIST-CSF: DE.AE-1,PR.AC-3,PR.AC-5,PR.PT-4, HIPAA: 164.312(e)(1), PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,2.2.2
ams-nist-vpc-vpn-2-터널-up	VPC	구성 변경 사항	Report	CIS: NA, NIST-CSF: ID.BE-5,PR.DS-4,PR.PT-5,RC.RP-1, HIPAA: 164.308(a)(7)(i), PCI: NA,
ams-cis-ec2-ebs-encryption-by-default	EC2	주기적	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 2.2,3.4,8.2.1,
ams-cis-rds-snapshot-encrypted	RDS	구성 변경 사항	Report	CIS: CIS.13,CIS.14, NIST-CSF: PR.DS-1, HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii), PCI: 3.4,8.2.1,
ams-cis-redshift-cluster-maintenance settings-check	RedShift	구성 변경 사항	Report	CIS: CIS.5; NIST-CSF: PR.DS-4,PR.IP-1,PR.IP-4; HIPAA: 164.308(a)(5)(ii)(A),164.308(a)(7)(ii)(A); PCI: 6.2;

Accelerate의 위반에 대한 대응

모든 Config 규칙 위반은 구성 보고서에 표시됩니다. 이는 범용 응답입니다. 규칙의 수정 범주(심각도)에 따라 AMS는 다음 표에 요약된 추가 작업을 수행할 수 있습니다. 특정 규칙에 대해 작업 코드를 사용자 지정하는 방법에 대한 자세한 내용은 섹션을 참조하세요사용자 지정 조사 결과 응답.

문제 해결 작업

작업 코드	AMS 작업
Report	1. Config 보고서에 추가
Incident	1. Config 보고서에 추가 2. Accelerate의 자동 인시던트 보고서
Remediate	1. Config 보고서에 추가 2. Accelerate의 자동 인시던트 보고서 3. Accelerate의 자동 문제 해결

추가 도움말 요청

> **Note**
>
> AMS는 문제 해결 범주에 관계없이 모든 위반을 해결할 수 있습니다. 도움을 요청하려면 서비스 요청을 제출하고 "AMS 구성 규칙 수정의 일부로 불만이 아닌 리소스 *RESOURCE_ARNS_OR_IDs* 리소스 ARNs/IDs>, 계정의 구성 규칙 *CONFIG_RULE_NAME*"과 같은 설명으로 AMS가 수정할 리소스를 표시하고 위반을 수정하는 데 필요한 입력을 추가합니다.

AMS Accelerate에는 규정 미준수 리소스를 해결하는 데 도움이 되는 AWS Systems Manager 자동화 문서 및 실행서 라이브러리가 있습니다.

Config 보고서에 추가

AMS는 계정에 있는 모든 규칙 및 리소스의 규정 준수 상태를 추적하는 Config 보고서를 생성합니다. CSDM에서 보고서를 요청할 수 있습니다. Config 콘솔, AWS CLI 또는 AWS AWS Config API에서 규정 준수 상태를 검토할 수도 있습니다. Config 보고서에는 다음이 포함됩니다.

- 잠재적 위협 및 잘못된 구성을 발견하기 위한 환경의 상위 규정 미준수 리소스
- 시간 경과에 따른 리소스 및 구성 규칙 준수
- 규정 미준수 리소스를 수정하기 위한 구성 규칙 설명, 규칙의 심각도 및 권장 문제 해결 단계

리소스가 규정 미준수 상태가 되면 Config 보고서에서 리소스 상태(및 규칙 상태)가 규정 미준수가 됩니다. 규칙이 Config 보고서 전용 문제 해결 범주에 속하는 경우 기본적으로 AMS는 추가 작업을 수행하지 않습니다. 언제든지 서비스 요청을 생성하여 AMS에 추가 도움말 또는 수정을 요청할 수 있습니다.

자세한 내용은 AWS Config Reporting을 참조하세요.

Accelerate의 자동 인시던트 보고서

중간 정도 심각한 규칙 위반의 경우 AMS는 자동으로 인시던트 보고서를 생성하여 리소스가 규정 미준수 상태가 되었음을 알리고 어떤 작업을 수행할지 묻습니다. 인시던트에 대응할 때 다음과 같은 옵션이 있습니다.

- AMS가 인시던트에 나열된 규정 미준수 리소스를 수정하도록 요청합니다. 그런 다음 규정 미준수 리소스를 수정하려고 시도하고 기본 인시던트가 해결되면 사용자에게 알립니다.
- 콘솔에서 또는 자동 배포 시스템(예: CI/CD 파이프라인 템플릿 업데이트)을 통해 규정 미준수 항목을 수동으로 해결한 다음 인시던트를 해결할 수 있습니다. 규정 미준수 리소스는 규칙 일정에 따라 재평가되며, 리소스가 규정 미준수로 평가되면 새 인시던트 보고서가 생성됩니다.
- 규정 미준수 리소스를 해결하지 않고 인시던트만 해결하도록 선택할 수 있습니다. 나중에 리소스 구성을 업데이트하면 AWS Config가 재평가를 트리거하고 해당 리소스의 규정 미준수를 평가하라는 알림을 다시 받게 됩니다.

Accelerate의 자동 문제 해결

가장 중요한 규칙은 자동 문제 해결 범주에 속합니다. 이러한 규칙을 준수하지 않으면 계정의 보안 및 가용성에 큰 영향을 미칠 수 있습니다. 리소스가 다음 규칙 중 하나를 위반하는 경우:

1. AMS는 인시던트 보고서를 자동으로 알려줍니다.
2. AMS는 자동화된 SSM 문서를 사용하여 자동 문제 해결을 시작합니다.
3. AMS는 자동 문제 해결의 성공 또는 실패로 인시던트 보고서를 업데이트합니다.
4. 자동 수정에 실패하면 AMS 엔지니어가 문제를 조사합니다.

Accelerate에서 규칙 예외 생성

AWS Config 규칙 리소스 예외 기능을 사용하면 특정 규칙에 대한 특정 규정 미준수 리소스의 보고를 억제할 수 있습니다.

> **Note**
>
> 제외된 리소스는 AWS 여전히 Config Service 콘솔에 규정 미준수로 표시됩니다. 제외된 리소스는 Config Reports(resource_exception:True)에 특수 플래그와 함께 표시됩니다. CSDMs 보고서를 생성할 때 해당 열에 따라 해당 리소스를 필터링할 수 있습니다.

규정을 준수하지 않는 것으로 알려진 리소스가 있는 경우 해당 Config 보고서에서 특정 구성 규칙에 대한 특정 리소스를 제거할 수 있습니다. 방법:

보고서에서 제외할 구성 규칙 및 리소스 목록과 함께 계정에 대해 Accelerate에 서비스 요청을 제출합니다. 명시적인 비즈니스 정당화를 제공해야 합니다(예: *resource_name_1* 및 *resource_name_2*가 백업되지 않도록 보고할 필요 없음). Accelerate 서비스 요청 제출에 대한 도움말은 섹션을 참조하세요Accelerate에서 서비스 요청 생성.

요청에 다음 입력을 붙여 넣은 다음(모든 리소스에 대해 그림과 같이 모든 필수 필드가 포함된 별도의 블록 추가) 제출합니다.

```
[
    {
        "resource_name": "resource_name_1",
        "config_rule_name": "config_rule_name_1",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    },
    {
        "resource_name": "resource_name_2",
        "config_rule_name": "config_rule_name_2",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    }
]
```

Accelerate에서 AWS Config 비용 절감

옵션을 사용하여 `AWS::EC2::Instance` 리소스 유형을 주기적으로 기록하여 AWS Config 비용을 줄일 수 있습니다. 주기적 레코딩은 24시간마다 한 번씩 리소스의 최신 구성 변경 사항을 캡처하여 전달되는 변경 횟수를 줄입니다. 활성화된 경우는 24시간이 끝날 때 리소스의 최신 구성 AWS Config 만 기록합니다. 이를 통해 지속적인 모니터링이 필요하지 않은 특정 운영 계획, 규정 준수 및 감사 사용 사례에 맞게 구성 데이터를 조정할 수 있습니다. 이 변경은 임시 아키텍처에 의존하는 애플리케이션이 있는 경우에만 권장됩니다. 즉, 인스턴스 수를 지속적으로 늘리거나 줄입니다.

`AWS::EC2::Instance` 리소스 유형에 대한 정기 기록을 옵트인하려면 AMS 전송 팀에 문의하세요.

사용자 지정 조사 결과 응답

AMS Accelerate가 일부 조사 결과(준수되지 않은 Config 규칙)에 응답하는 방법을 선택할 수 있습니다. 조사 결과를 수정하거나, 수정 승인을 요청하거나, 다음 월간 비즈니스 검토(MBR)에 보고하여 조사 결과에 응답하도록 AMS를 구성할 수 있습니다. AMS Accelerate Config 규칙에 대한 기본 응답을 변경할 수 있습니다. 규칙을 보려면 구성 규정 준수 > 규칙 테이블로 이동하거나 규칙 테이블을 ZIP 파일 ams_config_rules.zip으로 다운로드합니다.

기본 응답을 변경하면 더 많은 조사 결과를 수정하여 계정의 보안 및 규정 준수 상태를 높일 수 있습니다. 더 많은 조사 결과를 수정하면 수동 검토 및 승인을 기다려야 하는 사례가 줄어듭니다. AMS 문제 해결 런북의 광범위한 라이브러리는 규정 미준수 리소스를 지속적으로 수정하며 필요한 경우에만 연락을 받습니다.

사용자 지정 응답은 새 리소스 또는 새 이벤트가 있는 기존 리소스에만 사용됩니다. 예를 들어 변경 후 규정 미준수가 된 리소스입니다. 이는 이전 리소스는 수정 전에 심층 검사가 필요한 경향이 있으며 생성되거나 변경될 때 리소스 수정을 적용하는 것이 더 쉽기 때문입니다. 언제든지 리소스에 대한 결과 수정을 요청하려면 서비스 요청을 제출합니다.

기본 응답의 변경 요청

클라우드 아키텍트(CAs 온보딩 중에 사용자와 협력하여 기본 설정을 수집합니다. 그런 다음 CAs 내부 AMS 시스템에서 초기 구성을 설정합니다. 온보딩 후 서비스 요청을 생성하여 구성에 대한 업데이트를 요청합니다. 필요한 만큼 구성 업데이트를 요청할 수 있습니다. 작업은 서비스 요청이 생성된 계정에 대한 구성만 업데이트합니다. 여러 계정을 동시에 업데이트해야 하는 경우 Cloud Architect에 문의하세요. CA는 감사 목적으로 기본 설정으로 서비스 요청을 삭제하도록 요청합니다.

조사 결과 및 계정에 대한 기본 응답 변경

항상 각 계정 및 결과에 대한 응답 기본 설정이 필요합니다. AMS는 기본 응답을 제공하므로(구성 규정 준수 참조)이 구성은 선택 사항입니다. 각 결과에 대한 기본 응답을 다음 옵션으로 변경할 수 있습니다.

- 해결 방법: AMS가 결과를 수동 또는 자동으로 해결합니다. AMS는 문제 해결을 검토하고 실패 시 알려줍니다.
- 승인 요청: AMS는 아웃바운드 사례를 생성하여 조사 결과에 대해 알려줍니다. 수정을 승인하거나 제외하기 전에 결과를 검토하려는 경우이 옵션을 사용합니다. 그러면 AMS가 원하는 작업을 실행합니다.
- 작업 없음(보고서만 해당): AMS는 결과를 수정하거나 에스컬레이션하는 작업을 수행하지 않습니다. 결과는 콘솔과 MBRs.

> **Note**
>
> AMS에서 수정해야 하는 규칙의 구성은 변경할 수 없습니다. 예를 들어 Amazon GuardDuty 및 VPC 흐름 로그를 활성화합니다.

리소스별 기본 응답 변경

태그를 사용하여 특정 리소스에 대한 응답을 추가로 구성할 수 있습니다. Resource Tagger를 사용하여 기존 태그 또는 태그 리소스를 사용할 수 있습니다. 자세한 내용은 단원을 참조하십시오리소스 태거 가속화). 태그가 있는 리소스의 구성은 결과에 대한 기본 작업보다 우선합니다. 리소스에 서로 다른 관련 구성의 태그가 여러 개 있는 경우 AMS는 사용자 지정 수정을 실행할 수 없습니다. 대신 AMS는 아웃바운드 서비스 요청을 보내 상황을 알립니다. 예를 들어 s3-bucket-server-side-encryption-enabled 조사 결과의 경우 다음을 수행할 수 있습니다.

- 태그 키 값 페어가 "Regulated: True"인 'remediate' 비암호화 S3 버킷으로 응답을 변경합니다.
- 암호화되지 않은 S3 버킷에 'Regulated: False' 태그가 있는 경우 응답을 'no action'으로 변경합니다.
- 암호화되지 않은 S3 버킷의 기본 응답을 '승인 요청'으로 변경합니다. 이는 "Regulated: True" 또는 "Regulated: False" 태그가 없는 모든 S3 버킷에 적용됩니다.

사용자 지정 결과 응답을 실행하는 데 필요한 입력을 추가할 수도 있습니다. 예를 들어 암호화 키가 필요한 문제 해결의 경우 AMS에 키 IDs 제공할 수 있습니다. 문제 해결 런북의 입력 파라미터를 변경할

수 있지만 AMS는 사용자 지정 런북과의 통합을 지원하지 않습니다. Config 보고서의 AMS 문제 해결 런북에 대한 설명은 섹션을 참조하세요AWS Config 제어 규정 준수 보고서.

Accelerate의 인시던트 대응

알림을 받으면 AMS 팀은 자동 및 수동 수정을 사용하여 리소스를 정상 상태로 되돌립니다. 문제 해결에 실패하면 AMS는 인시던트 관리 프로세스를 시작하여 팀과 협업합니다. 구성 파일에서 기본 구성을 업데이트하여 기준을 변경할 수 있습니다.

AMS Accelerate의 인시던트 대응 및 온보딩

온보딩 중에 AMS Accelerate는 기존 규정 미준수 리소스에 대한 자동 인시던트 생성을 억제합니다. 대신 Cloud Service Deliver Manager(CSDM)는 검토를 위한 모든 규정 미준수 규칙과 리소스가 포함된 보고서를 제공합니다. AMS가 수정할 규칙을 식별한 후 지원 센터 콘솔에서 해당 규칙과 리소스를 나타내는 서비스 요청을 생성합니다. 다음 서비스 요청 템플릿은 규정 미준수 리소스를 수동으로 수정하기 위한 AMS에 대한 고객 요청의 예입니다. AMS에 추가 질문이 있는 경우 서비스 요청에서 사용자와 협력하여 필요한 정보를 수집합니다.

```
Hello,
Please remediate the following resources for the Config Rule "ENCRYPTED_VOLUMES".
Resource List:
    "Vol-12345678"
    "Vol-87654312"
Thank you
```

온보딩 프로세스가 완료되면 AMS Accelerate는 자동 인시던트로 표시된 규칙에 대해 각 규정 미준수 리소스에 대한 인시던트를 자동으로 생성합니다.

Accelerate의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 지연 시간이 짧고 처리량이 많으며 중복성이 높은 네트워킹과 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공합니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 조치를 수행하는 애플리케이션과 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성 및 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AMS Accelerate 연속성 관리에 대한 자세한 내용은 섹션을 참조하세요AMS Accelerate의 연속성 관리.

end-of-support 운영 체제에 대한 보안 제어

운영 체제 제조업체의 '지원 end-of-support' 또는 EOS의 일반 지원 기간을 벗어나고 보안 업데이트를 받지 않는 운영 체제는 보안 위험이 증가합니다.

AWS 는 운영 체제 end-of-support를 처리하는 데 도움이 되는 몇 가지 서비스를 제공합니다. Windows end-of-support 대한 자세한 내용은 Windows ServerEnd-of-Support 마이그레이션 프로그램을 참조하세요.

> **Note**
>
> 이 주제에 대한 추가 정보는 AWS Artifact 보고서에 액세스하여 확인할 수 있습니다. 자세한 내용은 AWS Artifact의 보고서 다운로드 섹션을 참조하세요. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 AWS 아티팩트 시작하기를 참조하세요. 이 정보에는 민감한 보안 콘텐츠가 포함되어 있으므로이 사용 설명서에 포함되지 않습니다.

Accelerate의 보안 모범 사례

AMS Accelerate는 적합성 팩을 사용합니다. 적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 이러한 적합성 팩을 가장 잘 구성하는 방법에 대한 자세한 내용은 AWS Config의 NIST CSF 운영 모범 사례 및 CIS 운영 모범 사례 상위 20개를 참조하세요.

변경 요청 보안 검토

AWS Managed Services 변경 요청 검토 프로세스를 통해 AMS는 요청된 변경 사항이 계정에서 사용자를 대신하여 구현될 때 보안 검토를 수행할 수 있습니다.

AMS Accelerate 기술 표준 최소 보안 기준, 구성 및 프로세스를 정의하여 계정의 기본 보안을 설정합니다. AMS가 요청된 변경 사항을 구현하면 이러한 표준을 따릅니다.

AMS는 AMS 기술 표준을 기준으로 모든 변경 요청을 평가합니다. 기술 표준을 벗어나 계정의 보안 태세를 저하시킬 수 있는 모든 변경 사항은 보안 검토 프로세스를 거칩니다. 이 프로세스 중에 AMS가 관

련 위험을 강조 표시하고 승인된 위험 승인자가 검토 및 승인하여 보안 및 비즈니스 요구 사항의 균형을 유지합니다.

고객 보안 위험 관리 프로세스

AMS Accelerate Customer Security Risk Management(CSRM) 프로세스는 위험을 명확하게 식별하고 적절한 소유자에게 알리는 데 도움이 됩니다. 이 프로세스는 환경의 보안 위험을 최소화하고 식별된 위험에 대한 지속적인 운영 오버헤드를 줄입니다.

기본적으로 조직의 누군가가 AMS가 관리형 환경에 대한 변경을 구현하도록 요청하면 AMS는 변경 사항을 검토하여 요청이 기술 표준을 벗어나 계정의 보안 태세를 변경할 수 있는지 확인합니다. 보안 위험이 높거나 매우 높으면 승인된 보안 담당자가 변경 검토를 수락하거나 거부합니다. 요청된 변경 사항도 AMS의 계정 운영 능력에 부정적인 영향을 미치는지 평가됩니다. 검토에서 가능한 부정적인 영향이 발견되면 AMS 내에서 추가 검토 및 승인이 필요합니다.

위험 수락 유효성 및 검토

위험 수락은 승인 날짜로부터 1년 동안 유효합니다. 이전에 수락된 위험 시나리오가 1년 후에 다시 발생하는 경우 위험 수락을 검토하고 재승인해야 적용할 수 있습니다. 이 연간 검토는 위험 결정이 현재 기술 표준, 규제 요구 사항 및 조직의 진화하는 위험 프로필과 일치하도록 합니다.

수신 거부

위험이 높거나 매우 높은 경우 CSRM 프로세스의 승인 기반 워크플로에서 옵트아웃할 수 있습니다. 특정 계정의 CSRM 옵션을 표준 CSRM에서 알림 전용으로 변경하려면 Cloud Service Delivery Manager와 협력하여 일회성 위험 수락을 생성합니다. 알림 전용 옵션을 진행하도록 선택하면 AMS는 위험 범주에 관계없이 요청된 변경 사항을 구현합니다. AMS는 변경 구현 전에 승인을 구하는 대신 승인된 위험 승인자에게 위험 알림을 보냅니다.

AMS CSRM 프로세스, 새 AMS 계정을 온보딩할 때 기본 CSRM 옵션을 변경하는 방법 또는 기존 계정을 업데이트하는 방법에 대한 자세한 내용은 Cloud Architects 또는 Cloud Service Delivery Manager에게 문의하세요.

> **Note**
>
> AMS는 모든 계정에서 표준 CSRM의 기본 옵션을 사용할 것을 강력히 권장합니다.

AMS Accelerate 기술 표준

다음은 Accelerate 기술 표준 범주입니다.

ID	범주
AMS-STD-X002	AWS Identity and Access Management
AMS-STD-X003	네트워크 보안
AMS-STD-X004	침투 테스트
AMS-STD-X005	Amazon GuardDuty
AMS-STD-X007	로깅

AMS Accelerate의 표준 제어

다음은 AMS의 표준 컨트롤입니다.

AMS-STD-X002 - AWS Identity and Access Management (IAM)

ID	기술 표준
1.0	제한 시간 지속 시간
1.1	페더레이션 사용자 기본 제한 시간 세션은 1시간이며 최대 4시간까지 늘릴 수 있습니다.
1.2	Microsoft Windows Server의 RDP 세션 제한 시간은 15분으로 설정되며 사용 사례에 따라 연장할 수 있습니다.
2.0	AWS 루트 계정 사용
2.1	어떤 이유로든 루트 계정 사용량이 있는 경우 관련 조사 결과를 생성하도록 Amazon GuardDuty를 구성해야 합니다.

ID	기술 표준
2.2	루트 계정의 액세스 키는 생성해서는 안 됩니다.
3.0	사용자 생성 및 수정
3.1	프로그래밍 방식 액세스 권한과 읽기 전용 권한이 있는 IAM 사용자/역할은 시간 제한 정책 없이 생성할 수 있습니다. 그러나 권한 o는 계정의 모든 Amazon Simple Storage Service 버킷에서 객체(예: S3:GetObject) 읽기를 허용하지 않습니다.
3.1.1	콘솔 액세스 및 읽기 전용 권한을 가진 IAM 인간 사용자는 시간 제한 정책(최대 180일)을 사용하여 생성할 수 있지만 시간 제한 정책을 removal/renewal/extension하면 위험 알림이 발생합니다. 그러나 계정의 모든 S3 버킷에서 객체(예: S3:GetObject)를 읽을 수 있는 권한은 허용되지 않습니다.
3.2	고객 계정의 인프라 변경 권한(쓰기 및 권한 관리)을 사용한 콘솔 및 프로그래밍 방식 액세스에 대한 IAM 사용자 및 역할은 위험 수락 없이 생성해서는 안 됩니다. 특정 버킷이 AMS와 관련이 없는 태그의 범위 및 태그 지정 작업에 있는 한 위험 수락 없이 허용되는 S3 객체 수준 쓰기 권한에는 예외가 있습니다.
3.3	Microsoft Windows Servers에서는 Microsoft 그룹 관리형 서비스 계정(gMSA)만 생성해야 합니다.
4.0	정책, 작업 및 APIs

ID	기술 표준
4.4	정책은 위험 수락 없이 "Effect": "Allow" with "Action": "*" over "Resource": "*"에 해당하는 문과 함께 관리자 액세스 권한을 제공해서는 안 됩니다.
4.6	고객 IAM 정책의 AMS 인프라 키에 대한 KMS 키 정책에 대한 API 호출은 허용되지 않아야 합니다.
4.8	Amazon Route 53에서 AMS 인프라 DNS 레코드를 변경하는 작업은 허용되지 않아야 합니다.
4.9	적절한 프로세스를 따른 후 콘솔 액세스 권한이 생성된 IAM 인간 사용자는 신뢰 정책, 역할 수임 및 시간 제한 정책을 제외하고 직접 연결된 정책이 없어야 합니다.
4.10	동일한 계정 AWS Secrets Manager 내의 특정 보안 암호 또는 네임스페이스에 대한 읽기 액세스 권한이 있는 Amazon EC2 인스턴스 프로파일을 생성할 수 있습니다.
4.12	IAM 정책에는 AMS Amazon CloudWatch 로그 그룹에서 로그:DeleteLogGroup 및 로그:DeleteLogStream 허용 작업이 포함된 작업이 포함되어서는 안 됩니다.
4.13	다중 리전 키를 생성할 수 있는 권한은 허용되지 않아야 합니다.
4.14	서비스별 S3 조건 키 s3:ResourceAccount를 사용하여 계정 번호를 지정하여 버킷에 대한 액세스를 고객 계정으로 제한하여 고객 계정에 아직 생성되지 않은 S3 버킷 ARN에 대한 액세스를 제공할 수 있습니다.

ID	기술 표준
4.15.1	S3 스토리지 렌즈 사용자 지정 대시보드에 대한 보기, 생성, 나열 및 삭제 액세스 권한을 가질 수 있습니다.
4.16	Amazon Redshift 데이터베이스에서 작업할 수 있도록 역할/사용자에게 SQL Workbench 관련 전체 권한을 부여할 수 있습니다.
4.17	CLI의 대안으로 고객 역할에 모든 AWS CloudShell 권한을 부여할 수 있습니다.
4.18	AWS 서비스가 신뢰할 수 있는 보안 주체인 IAM 역할도 IAM 기술 표준을 준수해야 합니다.
4.19	서비스 연결 역할(SLRs)은 IAM 서비스 팀에서 구축 및 유지 관리하므로 AMS IAM 기술 표준의 적용을 받지 않습니다.
4.20	IAM 정책은 계정의 모든 S3 버킷에서 객체(예: S3:GetObject) 읽기를 허용하지 않아야 합니다.
4.21	리소스 유형 “저장 계획”에 대한 모든 IAM 권한을 고객에게 부여할 수 있습니다.
4.22	AMS 엔지니어는 Amazon S3, Amazon S3 객체, 데이터베이스 등)를 수동으로 복사하거나 이동할 수 없습니다. Amazon Relational Database Service DynamoDB
6.0	교차 계정 정책
6.1	IAM 역할은 고객 레코드에 따라 동일한 고객에게 속한 AMS 계정 간에 정책을 신뢰합니다.

ID	기술 표준
6.2	IAM 역할은 동일한 AMS 고객이 비 AMS 계정을 소유한 경우에만(동일한 계정인지 확인하거나 이메일 도메인을 고객의 회사 이름과 일치시켜) AMS 계정과 비 AMS AWS Organizations 계정 간의 신뢰 정책을 구성해야 합니다.
6.3	IAM 역할은 위험 수락 없이 AMS 계정과 타사 계정 간의 정책을 신뢰합니다.
6.4	동일한 고객의 AMS 계정 간에 고객 관리형 CMKs에 액세스하는 교차 계정 정책을 구성할 수 있습니다.
6.5	AMS 계정을 통해 비 AMS 계정 내의 모든 KMS 키에 액세스하기 위한 교차 계정 정책을 구성할 수 있습니다.
6.6	타사 계정에서 AMS 계정 내의 KMS 키에 액세스하기 위한 교차 계정 정책은 위험 수락 없이 허용되지 않아야 합니다.
6.6.1	비 AMS 계정이 AMS 계정 내의 모든 KMS 키에 액세스하기 위한 교차 계정 정책은 동일한 AMS 고객이 비 AMS 계정을 소유한 경우에만 구성할 수 있습니다.
6.7	동일한 고객의 AMS 계정 간에 데이터를 저장할 수 있는 모든 S3 버킷 데이터 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 교차 계정 정책을 구성할 수 있습니다.

ID	기술 표준
6.8	읽기 전용 액세스 권한이 있는 AMS 계정의 비 AMS 계정에 데이터를 저장할 수 있는 모든 S3 버킷 데이터 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 교차 계정 정책을 구성할 수 있습니다.
6.9	AMS를 비AMS 계정(또는 비AMS에서 AMS 계정)에 쓰기 권한으로 데이터를 저장할 수 있는 S3 버킷 데이터 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 교차 계정 정책은 AMS 계정이 동일한 AMS 고객이 소유한 경우에만(동일 AWS Organizations 한 계정인지 확인하거나 이메일 도메인을 고객의 회사 이름과 일치시켜) 구성해야 합니다.
6.10	읽기 전용 액세스 권한이 있는 AMS 계정의 타사 계정에 데이터를 저장할 수 있는 모든 S3 버킷 데이터 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 교차 계정 정책을 구성할 수 있습니다.
6.11	쓰기 액세스 권한이 있는 AMS 계정의 타사 계정에 데이터를 저장할 수 있는 S3 버킷 데이터 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 교차 계정 정책은 위험 수락 없이 구성해서는 안 됩니다.
6.12	데이터를 저장할 수 있는 AMS 고객 S3 버킷 또는 리소스(asAmazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 타사 계정의 교차 계정 정책은 위험 수락 없이 구성해서는 안 됩니다.

ID	기술 표준
7.0	사용자 그룹
7.1	읽기 전용 및 비변동 권한이 있는 IAM 그룹은 허용됩니다.
8.0	리소스 기반 정책
8.4	AMS 인프라 리소스는 리소스 기반 정책을 연결하여 승인되지 않은 자격 증명으로 관리로부터 보호해야 합니다.
8.2	고객이 다른 정책을 명시적으로 지정하지 않는 한 고객 리소스는 최소 권한 리소스 기반 정책으로 구성해야 합니다.

AMS-STD-X003 - 네트워크 보안

다음은 X003 - 네트워크 보안에 대한 표준 제어입니다.

ID	기술 표준
	네트워킹
1.0	향후 제어를 위해 예약됨
2.0	EC2 인스턴스에서 탄력적 IP 허용
3.0	데이터 영역 TLS 1.2 이상에서 AMS 컨트롤 플레인 및 확장별를 사용해야 합니다.
5.0	9.0에 따라 로드 밸런서에 연결되지 않은 경우 보안 그룹에 인바운드 규칙에서 소스가 0.0.0.0/0이 아니어야 합니다.
6.0	위험 수락 없이 S3 버킷 또는 객체를 공개해서는 안 됩니다.

ID	기술 표준
7.0	포트 SSH/22 또는 SSH/2222(SFTP/2222 아님), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 또는 1604, LDAP/389 또는 636 및 RPC/135에서 서버 관리 액세스는 보안 그룹을 통해 VPC 외부에서 허용되지 않아야 합니다.
8.0	포트(MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433) 또는 사용자 지정 포트의 데이터베이스 관리 액세스는 보안 그룹을 통해 DX, VPC 피어 또는 VPN을 통해 VPC로 라우팅되지 않은 퍼블릭 IPs에서 허용되지 않아야 합니다.
8.1	고객 데이터를 저장할 수 있는 리소스는 퍼블릭 인터넷에 직접 노출되어서는 안 됩니다.
9.0	인터넷에서 포트 HTTP/80, HTTPS/8443 및 HTTPS/443을 통한 직접 애플리케이션 액세스는 로드 밸런서에만 허용되며 EC2 인스턴스, ECS/EKS/Fargate 컨테이너 등과 같은 직접 컴퓨팅 리소스에는 허용되지 않습니다.
10.0	고객 프라이빗 IP 범위에서 포트 HTTP/80 및 HTTPS/443을 통한 애플리케이션 액세스를 허용할 수 있습니다.
11.0	AMS 인프라에 대한 액세스를 제어하는 보안 그룹에 대한 모든 변경은 위험 수락 없이 허용되지 않아야 합니다.
12.0	AMS Security는 보안 그룹이 인스턴스에 연결되도록 요청될 때마다 표준을 참조합니다.

ID	기술 표준
14.0	프라이빗 호스팅 영역을 AMS에서 비 AMS 계정(또는 비 AMS에서 AMS 계정)으로 VPCs와 교차 계정 연결은 내부 도구를 사용하여 동일한 AMS 고객이 비 AMS 계정을 소유한 경우에만(동일한 AWS 조직 계정인지 확인하거나 이메일 도메인을 고객의 회사 이름과 일치시켜) 구성해야 합니다.
15.0	동일한 고객에게 속한 계정 간의 VPC 피어링 연결을 허용할 수 있습니다.
16.0	AMS 기본 AMIs는 내부 도구를 사용하여 동일한 고객이 두 계정을 소유하는 한(동일한 계정인지 확인하거나 이메일 도메인을 고객의 회사 이름과 일치시켜) 비 AMS AWS Organizations 계정과 공유할 수 있습니다.
17.0	FTP 포트 21은 위험 수락 없이 보안 그룹에 구성해서는 안 됩니다.
18.0	고객이 모든 계정을 소유하는 한 전송 게이트웨이를 통한 교차 계정 네트워크 연결이 허용됩니다.
19.0	프라이빗 서브넷을 퍼블릭으로 설정하는 것은 허용되지 않습니다.
20.0	타사 계정(고객이 소유하지 않음)과의 VPC 피어링 연결은 허용되지 않습니다.
21.0	타사 계정(고객이 소유하지 않음)과의 Transit Gateway 연결은 허용되지 않습니다.
22.0	AMS가 고객에게 서비스를 제공하는 데 필요한 네트워크 트래픽은 고객 네트워크 송신 지점에서 차단되어서는 안 됩니다.

ID	기술 표준
23.0	고객 인프라에서 Amazon EC2에 대한 인바운드 ICMP 요청에는 위험 알림이 필요합니다.
24.0	보안 그룹을 통해 DX, VPC-peer 또는 VPN을 통해 Amazon VPC로 라우팅된 퍼블릭 IPs의 인바운드 요청은 허용됩니다.
25.0	DX, VPC-peer 또는 VPN을 통해 Amazon VPC로 라우팅되지 않은 퍼블릭 IPs의 인바운드 요청은 위험 승인을 받아야 합니다.
26.0	Amazon EC2에서 모든 대상으로의 아웃바운드 ICMP 요청이 허용됩니다.
27.0	보안 그룹 공유
27.1	보안 그룹이이 보안 표준을 충족하는 경우 동일한 계정VPCs와 동일한 조직의 계정 간에 공유할 수 있습니다.
27.2	보안 그룹이이 표준을 충족하지 못하고 이전에이 보안 그룹에 대해 위험 수락이 필요한 경우, 동일한 계정의 VPCs 간 또는 동일한 조직의 계정 간 보안 그룹 공유 기능의 사용은 해당 새 VPC 또는 계정에 대한 위험 수락 없이 허용되지 않습니다.

AMS-STD-X004 - 침투 테스트

다음은 X004 - 침투 테스트를 위한 표준 컨트롤입니다.

1. AMS는 pentest 인프라를 지원하지 않습니다. 이는 고객의 책임입니다. 예를 들어 Kali는 Linux의 AMS 지원 배포판이 아닙니다.
2. 고객은 침투 테스트를 준수해야 합니다.
3. 고객이 계정 내에서 인프라 침투 테스트를 수행하려는 경우 24시간 전에 AMS에 미리 알립니다.

4. AMS는 고객의 변경 요청 또는 서비스 요청에 명시적으로 명시된 고객 요구 사항에 따라 고객 테스트 인프라를 프로비저닝합니다.
5. 인프라를 테스트하는 고객의 자격 증명 관리는 고객의 책임입니다.

AMS-STD-X005 - GuardDuty

다음은 X005 - GuardDuty에 대한 표준 컨트롤입니다.

1. GuardDuty는 모든 고객 계정에서 항상 활성화되어야 합니다.
2. GuardDuty 알림은 동일한 계정 또는 동일한 조직의 다른 관리형 계정에 저장되어야 합니다.
3. GuardDuty의 신뢰할 수 있는 IP 목록 기능은 사용해서는 안 됩니다. 대신 자동 아카이브를 대안으로 사용할 수 있으며, 이는 감사 목적에 유용합니다.

AMS-STD-X007 - 로깅

다음은 X007 - 로깅에 대한 표준 컨트롤입니다.

ID	기술 표준
1.0	로그 유형
1.1	OS 로그: 모든 호스트는 최소 호스트 인증 이벤트, 승격된 권한의 모든 사용에 대한 액세스 이벤트, 성공 및 실패를 포함한 액세스 및 권한 구성에 대한 모든 변경 사항에 대한 액세스 이벤트를 로깅해야 합니다.
1.2	AWS CloudTrail: 로그를 S3 버킷에 전달하도록 CloudTrail 관리 이벤트 로깅을 활성화하고 구성해야 합니다.
1.3	VPC 흐름 로그: 모든 네트워크 트래픽 로그는 VPC 흐름 로그를 통해 로깅되어야 합니다.
1.4	Amazon S3 서버 액세스 로깅: 로그를 저장하는 AMS 필수 S3 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다.

ID	기술 표준
1.5	AWS Config 스냅샷: AWS Config 모든 리전에서 지원되는 모든 리소스에 대한 구성 변경을 기록하고 구성 스냅샷 파일을 하루에 한 번 이상 S3 버킷에 전달해야 합니다.
1.7	애플리케이션 로그: 고객은 애플리케이션에서 로깅을 활성화하고 CloudWatch Logs 로그 그룹 또는 S3 버킷에 저장할 수 있습니다.
1.8	S3 객체 수준 로깅: 고객은 S3 버킷에서 객체 수준 로깅을 활성화할 수 있습니다.
1.9	서비스 로깅: 고객은 모든 핵심 서비스와 같은 SSPS 서비스에 대한 로그를 활성화하고 전달할 수 있습니다.
1.10	Elastic Load Balancing(Classic/Application Load Balancer/Network Load Balancer) 로그: 액세스 및 오류 로그 항목은 AMS 2.0 관리형 S3 버킷에 저장되어야 합니다.
2.0	액세스 제어
2.3	로그를 저장하는 AMS 필수 S3 버킷은 타사 계정 사용자를 버킷 정책의 원칙으로 허용해서는 안 됩니다.
2.4	CloudWatch Logs 로그 그룹의 로그는 고객이 승인한 보안 담당자의 명시적 승인 없이 삭제해서는 안 됩니다.
3.0	로그 보존
3.1	AMS 필수 CloudWatch Logs 로그 그룹의 로그 보존 기간은 최소 90일이어야 합니다.

ID	기술 표준
3.2	로그를 저장하는 AMS 필수 S3 버킷의 최소 보존 기간은 로그에서 18개월이어야 합니다.
3.3	AWS Backup 스냅샷은 지원되는 리소스에서 최소 31일 동안 보존할 수 있어야 합니다.
4.0	암호화(Encryption)
4.1	로그를 저장하는 AMS Teams에 필요한 모든 S3 버킷에서 암호화를 활성화해야 합니다.
4.2	고객 계정에서 다른 계정으로 로그를 전달하는 것은 암호화되어야 합니다.
5.0	무결성
5.1	로그 파일 무결성 메커니즘을 활성화해야 합니다. 즉, AMS 팀에 필요한 AWS CloudTrail 추적에서 “로그 파일 검증”을 구성합니다.
6.0	로그 전달
6.1	모든 로그는 한 AMS 계정에서 동일한 고객의 다른 AMS 계정으로 전달할 수 있습니다.
6.2	내부 도구를 사용하여 동일한 AMS 고객이 비 AMS 계정을 소유한 경우에만(동일한 계정인지 확인하거나 이메일 도메인을 고객의 회사 이름 및 PAYER 연결 계정과 일치 AWS Organizations 시켜) 모든 로그를 AMS에서 비 AMS 계정으로 전달할 수 있습니다.

환경에서 보안 위험이 높거나 매우 높은 변경 사항

다음과 같은 변경 사항으로 인해 환경에서 보안 위험이 높거나 매우 높습니다.

AWS Identity and Access Management

- High_Risk-IAM-001: 루트 계정에 대한 액세스 키 생성
- High_Risk-IAM-002: 추가 액세스를 허용하는 SCP 정책 수정
- High_Risk-IAM-003: AMS 인프라를 손상시킬 수 있는 SCP 정책 수정
- High_Risk-IAM-004: 고객 계정에서 인프라 변경 권한(쓰기, 권한 관리 또는 태그 지정)이 있는 역할/사용자 생성
- High_Risk-IAM-005: IAM 역할은 AMS 계정과 타사 계정(고객이 소유하지 않음) 간의 정책을 신뢰합니다.
- High_Risk-IAM-006: 타사 계정을 통해 AMS 계정에서 모든 KMS 키에 액세스하기 위한 교차 계정 정책)
- High_Risk-IAM-007: 데이터를 저장할 수 있는 AMS 고객 S3 버킷 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 타사 계정의 교차 계정 정책
- High_Risk-IAM-008: 고객 계정의 인프라 변경 권한을 사용하여 IAM 권한 할당
- High_Risk-IAM-009: 계정의 모든 S3 버킷에 대한 나열 및 읽기 허용

네트워크 보안

- High_Risk-NET-001: 인터넷에서 OS 관리 포트 SSH/22 또는 SSH/2222(SFTP/2222 아님), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 또는 1604, LDAP/389 또는 636 및 NETBIOS/137-139를 엽니다.
- High_Risk-NET-002: 데이터베이스 관리 포트 MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 또는 인터넷의 모든 관리 고객 포트 열기
- High_Risk-NET-003: 모든 컴퓨팅 리소스에서 직접 애플리케이션 포트 HTTP/80, HTTPS/8443 및 HTTPS/443을 엽니다. 예: 인터넷에서 EC2 인스턴스, ECS/EKS/Fargate 컨테이너 등
- High_Risk-NET-004: AMS 인프라에 대한 액세스를 제어하는 보안 그룹에 대한 모든 변경 사항
- High_Risk-NET-006: 타사 계정과의 VPC 피어링(고객이 소유하지 않음)
- High_Risk-NET-007: 고객 방화벽을 모든 AMS 트래픽의 송신 지점으로 추가
- High_Risk-NET-008: 타사 계정과의 Transit Gateway 연결이 허용되지 않음
- High_Risk-S3-001: S3 버킷에서 퍼블릭 액세스 프로비저닝 또는 활성화

로깅

- High_Risk-LOG-001: CloudTrail을 비활성화합니다.
- High_Risk-LOG-002: VPC 흐름 로그를 비활성화합니다.

- High_Risk-LOG-003: AMS 관리형 계정에서 타사 계정(고객이 소유하지 않음)으로 모든 메서드(S3 이벤트 알림, SIEM 에이전트 풀, SIEM 에이전트 푸시 등)를 통한 로그 전달
- High_Risk-LOG-004: CloudTrail에 비 AMS 추적 사용

기타사항

- High_Risk-ENC-001: 활성화된 경우 모든 리소스에서 암호화 비활성화

보안 FAQ

AMS는 글로벌 운영 센터를 통해 연중무휴 follow-the-sun 제공합니다. 전용 AMS 운영 엔지니어는 대시보드와 인시던트 대기열을 적극적으로 모니터링합니다. 일반적으로 AMS는 자동화를 통해 계정을 관리합니다. 드문 경우지만 특정 문제 해결 또는 배포 전문 지식이 필요한 경우 AMS 운영 엔지니어가 AWS 계정에 액세스할 수 있습니다.

다음은 AMS 운영 엔지니어 또는 자동화가 계정에 액세스할 때 AMS Accelerate가 사용하는 보안 모범 사례, 제어, 액세스 모델 및 감사 메커니즘에 대한 일반적인 질문입니다.

AMS 운영 엔지니어는 언제 내 환경에 액세스하나요?

AMS 운영 엔지니어는 계정 또는 인스턴스에 지속적으로 액세스할 수 없습니다. 고객 계정에 대한 액세스 권한은 알림, 인시던트, 변경 요청 등과 같은 정당한 비즈니스 사용 사례에 대해서만 AMS 운영자에게 부여됩니다. 액세스는 AWS CloudTrail 로그에 문서화됩니다.

액세스 정당화, 트리거 및 트리거 이니시에이터는 섹션을 참조하세요AMS 고객 계정 액세스 트리거.

AMS 운영 엔지니어는 내 계정에 액세스할 때 어떤 역할을 맡습니까?

드물지만(~5%) 환경에서 사람의 개입이 필요한 경우 AMS 운영 엔지니어는 기본 읽기 전용 액세스 역할로 계정에 로그인합니다. 기본 역할은 Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift, Amazon ElastiCache와 같은 데이터 스토어에 일반적으로 저장되는 콘텐츠에 액세스할 수 없습니다.

AMS 운영 엔지니어 및 시스템이 계정에서 서비스를 제공하는 데 필요한 역할 목록은 섹션을 참조하세요AMS 고객 계정 액세스 IAM 역할.

AMS 작업 엔지니어는 내 계정에 어떻게 액세스하나요?

고객 계정에 액세스하기 위해 AMS 운영 엔지니어는 AWS 내부 AMS 액세스 서비스를 사용합니다. 이 내부 서비스는 계정에 대한 액세스가 안전하고 감사되도록 안전한 프라이빗 채널을 통해서만 사용할 수 있습니다.

1. AMS 작업 엔지니어는 내부 AMS 액세스 서비스 인증을 2단계 인증과 함께 사용합니다. 또한 운영 엔지니어는 AWS 계정에 액세스해야 하는 필요성을 설명하는 비즈니스 근거(인시던트 티켓 또는 서비스 요청 ID)를 제공해야 합니다.
2. 운영 엔지니어의 권한 부여에 따라 AMS 액세스 서비스는 엔지니어에게 적절한 역할(읽기 only/Operator/Admin)과 AWS 콘솔에 대한 로그인 URL을 제공합니다. 계정에 대한 액세스는 수명이 짧고 시간 제한이 있습니다.
3. Amazon EC2 인스턴스에 액세스하기 위해 AMS 작업 엔지니어는 브로커와 동일한 내부 AMS 액세스 서비스를 사용합니다. 액세스 권한이 부여되면 AMS 운영 엔지니어는 AWS Systems Manager Session Manager 를 사용하여 수명이 짧은 세션 자격 증명으로 인스턴스에 액세스합니다.

   Windows 인스턴스에 대한 RDP 액세스를 제공하기 위해 운영 엔지니어는 Amazon EC2 Systems Manager를 사용하여 인스턴스에 로컬 사용자를 생성하고 인스턴스로 포트 전달을 설정합니다. 작업 엔지니어는 인스턴스에 대한 RDP 액세스에 로컬 사용자 자격 증명을 사용합니다. 로컬 사용자 자격 증명은 세션이 끝날 때 제거됩니다.

다음 다이어그램은 AMS 운영 엔지니어가 계정에 액세스하는 데 사용하는 프로세스를 간략하게 설명합니다.

AMS 관리형 AWS 계정에서 AMS의 변경 사항을 추적하려면 어떻게 해야 합니까?

계정 액세스

자동화 또는 AMS Accelerate 운영 팀의 변경 사항을 추적하는 데 도움이 되도록 AMS는 Amazon Athena 콘솔 및 AMS Accelerate 로그에 변경 레코드 SQL 인터페이스를 제공합니다. 이러한 리소스는 다음 정보를 제공합니다.

- 계정에 액세스한 사람.
- 계정에 액세스한 시간입니다.

- 계정에 액세스하는 데 사용된 권한입니다.
- 계정에서 AMS Accelerate가 변경한 사항입니다.
- 계정에서 변경한 이유입니다.

리소스 구성

CloudTrail 로그를 보고 지난 90일 동안 AWS 리소스의 구성을 추적합니다. 구성이 90일보다 오래된 경우 Amazon S3의 로그에 액세스합니다.

인스턴스 로그

Amazon CloudWatch 에이전트는 운영 체제 로그를 수집합니다. CloudWatch 로그를 보고 운영 체제에서 지원하는 로그인 및 기타 작업 로그를 확인합니다.

자세한 내용은 AMS Accelerate 계정의 변경 사항 추적 단원을 참조하십시오.

내 계정에 대한 AMS 운영 엔지니어 액세스에 대한 프로세스 제어는 무엇입니까?

AMS에 가입하기 전에 운영 엔지니어는 범죄 신원 조회를 거칩니다. AMS 엔지니어는 고객 인프라를 관리하기 때문에 필수 연간 신원 조회도 수행합니다. 엔지니어가 신원 조회에 실패하면 액세스가 취소됩니다.

모든 AMS 운영 엔지니어는 리소스에 대한 액세스 권한을 부여받기 전에 인프라 보안, 데이터 보안 및 인시던트 대응과 같은 필수 보안 교육을 완료해야 합니다.

권한 있는 액세스는 어떻게 관리되나요?

일부 사용자는 추가 교육을 완료하고 승격된 액세스를 위한 권한 있는 액세스 권한을 유지해야 합니다. 액세스 및 사용량을 검사하고 감사합니다. AMS는 권한이 있는 액세스를 예외적인 상황이나 최소 권한 액세스가 요청을 충족할 수 없는 상황으로 제한합니다. 권한 있는 액세스도 시간 제한입니다.

AMS 운영 엔지니어가 MFA를 사용하나요?

예. 모든 사용자는 MFA 및 존재 증명을 사용하여 서비스를 제공해야 합니다.

AMS 직원이 조직을 떠나거나 직무 역할을 변경하면 액세스는 어떻게 되나요?

고객 계정 및 리소스에 대한 액세스는 내부 그룹 멤버십을 통해 프로비저닝됩니다. 멤버십은 AMS의 특정 직무 역할, 보고 관리자 및 고용 상태를 포함한 엄격한 기준을 기반으로 합니다. 운영 엔지니어의 직군이 변경되거나 사용자 ID가 비활성화되면 액세스가 취소됩니다.

내 계정에 대한 AMS 운영 엔지니어 액세스를 제어하는 액세스 제어는 무엇입니까?

환경에 액세스하기 위한 “알아야 할 필요” 및 “최소 권한” 원칙을 적용하는 여러 계층의 기술 제어가 있습니다. 다음은 액세스 제어 목록입니다.

- 고객 계정 및 리소스에 액세스하려면 모든 운영 엔지니어가 특정 내부 AWS 그룹에 속해야 합니다. 그룹 멤버십은 반드시 알아야 할 필요성을 기반으로 하며 사전 정의된 기준으로 자동화됩니다.
- AMS는 환경에 대한 '지속성 없음' 액세스를 연습합니다. 즉, AMS 작업을 통한 AWS 계정 액세스는 수명이 짧은 보안 인증 정보로 "just-in-time"됩니다. 계정에 대한 액세스는 내부 비즈니스 사례 정당화(서비스 요청, 인시던트, 변경 관리 요청 등)가 제출되고 검토된 후에만 제공됩니다.
- AMS는 최소 권한 원칙을 따릅니다. 따라서 권한 있는 운영 엔지니어는 기본적으로 읽기 전용 액세스를 수임합니다. 쓰기 액세스는 인시던트 또는 변경 요청으로 인해 환경을 변경해야 하는 경우에만 엔지니어가 사용합니다.
- AMS는 쉽게 식별할 수 있는 표준 AWS Identity and Access Management 역할을 사용하여 “ams” 접두사를 사용하여 계정을 모니터링하고 관리합니다. 감사를 AWS CloudTrail 위해 모든 액세스가 로그인됩니다.
- AMS는 자동 백엔드 도구를 사용하여 변경 실행의 고객 정보 검증 단계에서 계정에 대한 무단 변경을 감지합니다.

AMS는 루트 사용자 액세스를 어떻게 모니터링하나요?

루트 액세스는 항상 인시던트 대응 프로세스를 트리거합니다. AMS는 Amazon GuardDuty 탐지를 사용하여 루트 사용자 활동을 모니터링합니다. GuardDuty가 알림을 생성하면 AMS는 추가 조사를 위한 이벤트를 생성합니다. AMS는 예기치 않은 루트 계정 활동이 감지되면 이를 알리고 AMS 보안 팀이 조사를 시작합니다.

AMS는 보안 인시던트에 어떻게 대응하나요?

AMS는 Amazon GuardDuty, Amazon Macie와 같은 탐지 서비스 및 고객이 보고한 보안 문제에서 생성된 보안 이벤트를 조사합니다. AMS는 보안 대응 팀과 협력하여 보안 인시던트 대응(SIR) 프로세스를 실행합니다. AMS SIR 프로세스는 NIST SP 800-61 개정 2, 컴퓨터 보안 인시던트 처리 가이드 프레임워크를 기반으로 하며 연중무휴 follow-the-sun 제공합니다. AMS는 사용자와 협력하여 보안 인시던트를 신속하게 분석하고 억제합니다.

AMS는 어떤 업계 표준 인증 및 프레임워크를 준수하나요?

다른 AWS 서비스와 마찬가지로 AWS Managed Services는 OSPAR, HIPAA, HITRUST, GDPR, SOC*, ISO*, FedRAMP(중간/높음), IRAP 및 PCI 인증을 받았습니다. 와 AWS 일치하는 고객 규정 준수 인증, 규정 및 프레임워크에 대한 자세한 내용은 AWS 규정 준수를 참조하세요.

보안 가드레일

AWS Managed Services는 여러 제어를 사용하여 정보 자산을 보호하고 AWS 인프라를 안전하게 유지할 수 있도록 지원합니다. AMS Accelerate는 AWS Config 규칙 및 수정 작업 라이브러리를 유지 관리하여 계정이 보안 및 운영 무결성에 대한 업계 표준을 준수하도록 합니다. AWS Config 규칙은 기록된 리소스의 구성 변경을 지속적으로 추적합니다. 변경 사항이 규칙의 조건을 위반하는 경우 AMS는 해당 결과를 사용자에게 보고합니다. 위반의 심각도에 따라 위반을 자동으로 또는 요청으로 해결할 수 있습니다.

AMS는 규칙을 사용하여 다음 표준의 요구 사항을 충족 AWS Config 합니다.

- 인터넷 보안 센터(CIS)
- 미국 국립표준기술연구소(NIST) 클라우드 보안 프레임워크(CSF)
- HIPAA(미국 건강 보험 양도 및 책임에 관한 법)
- Payment Card Industry(PCI) 데이터 보안 표준(DSS)

자세한 내용은 AMS Accelerate의 보안 관리 섹션을 참조하세요.

보안 인증, 프레임워크 및 규정 준수에 대한 최신 보고서에 액세스하려면 어떻게 해야 하나요 AWS?

다음 방법을 사용하여 AWS 서비스에 대한 현재 보안 및 규정 준수 보고서를 찾을 수 있습니다.

- AWS Artifact를 사용하여 AWS 서비스의 보안, 가용성 및 기밀성에 대한 최신 보고서를 다운로드할 수 있습니다.

- 글로벌 규정 준수 프레임워크를 준수하는 AWS Managed Services를 포함한 대부분의 AWS 서비스 목록은 섹션을 참조하세요https://aws.amazon.com/compliance/services-in-scope/. 예를 들어 PCI를 선택하고 AWS Managed Services를 검색합니다.

  "AMS"를 검색하여 AMS 관리형 AWS 계정에서 AMS별 보안 아티팩트를 찾을 수 있습니다. AWS Managed Services는 SOC 3의 범위 내에 있습니다.
- AWS SOC 2(시스템 및 조직 제어) 보고서가 AWS Artifact 리포지토리에 게시됩니다. 이 보고서는 미국 공인회계사협회(AICPA) TSP 섹션 100, 신뢰 서비스 기준의 보안, 가용성 및 기밀성 기준을 충족하는 AWS 제어를 평가합니다.

AMS는 AMS 기능의 다양한 측면에 대한 참조 아키텍처 다이어그램을 공유하나요?

AMS 참조 아키텍처를 보려면 AWS Managed Services for Proactive Monitoring PDF를 다운로드합니다.

AMS는 내 계정에 액세스하는 사용자와 액세스를 위한 비즈니스 요구 사항을 어떻게 추적하나요?

서비스 연속성과 계정 보안을 지원하기 위해 AMS는 선제적 상태 또는 유지 관리, 상태 또는 보안 이벤트, 계획된 활동 또는 고객 요청에 대한 응답으로만 계정 또는 인스턴스에 액세스합니다. 계정에 대한 액세스는 AMS Accelerate의 액세스 모델에 설명된 대로 AMS 프로세스를 통해 승인됩니다. 이러한 권한 부여 흐름에는 우발적이거나 부적절한 액세스를 방지하기 위한 가드레일이 포함되어 있습니다. 액세스 흐름의 일환으로 AMS는 비즈니스 요구 사항을 권한 부여 시스템에 제공합니다. 이러한 비즈니스 요구 사항은 AMS로 연 사례와 같이 계정과 연결된 작업 항목일 수 있습니다. 또는 패치 솔루션과 같은 승인된 워크플로가 비즈니스 요구 사항일 수 있습니다. 모든 액세스에는 액세스 요청을 비즈니스 요구 사항에 맞게 조정하기 위해 비즈니스 규칙에 따라 내부 AMS 시스템에서 실시간으로 검증, 확인 및 승인하는 근거가 필요합니다.

AMS 운영 엔지니어에게는 유효한 비즈니스 요구 없이 계정에 액세스할 수 있는 경로가 제공되지 않습니다. 모든 계정 액세스 및 관련 비즈니스 요구 사항은 AWS 계정 내의 AWS CloudTrail 항목으로 내보내집니다. 이를 통해 완전한 투명성과 자체 감사 및 검사를 수행할 수 있는 기회가 제공됩니다. 검사 외에도 AMS는 자동 검사를 수행하고 필요에 따라 액세스 요청에 대한 수동 검사를 수행하며 비정상적인 액세스를 검토하기 위해 도구 및 인적 액세스에 대한 감사를 수행합니다.

AMS 엔지니어는 Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift와 같은 AWS 데이터 스토리지 서비스에 저장된 데이터에 액세스할 수 있나요?

AMS 엔지니어는 데이터 스토리지에 일반적으로 사용되는 AWS 서비스에 저장된 고객 콘텐츠에 액세스할 수 없습니다. 이러한 서비스에서 데이터를 읽거나 쓰거나 수정하거나 삭제하는 데 사용되는 AWS APIs에 대한 액세스는 AMS 엔지니어 액세스에 사용되는 IAM 역할과 관련된 명시적 IAM 거부 정책에 의해 제한됩니다. 또한 내부 AMS 가드레일 및 자동화는 AMS 운영 엔지니어가 거부 조건을 제거하거나 수정하는 것을 방지합니다.

AMS 엔지니어는 Amazon EBS, Amazon EFS 및 Amazon FSx에 저장된 고객 데이터에 액세스할 수 있나요?

AMS 엔지니어는 Amazon EC2 인스턴스에 관리자로 로그인할 수 있습니다. 운영 체제(OS) 문제 및 패치 실패를 포함하되 이에 국한되지 않는 특정 시나리오에서 문제를 해결하려면 관리자 액세스가 필요합니다. AMS 엔지니어는 일반적으로 시스템 볼륨에 액세스하여 감지된 문제를 해결합니다. 그러나 AMS 엔지니어에 대한 액세스는 시스템 볼륨으로 제한되거나 제한되지 않습니다.

내 환경에 대한 권한이 높은 자동화 역할에 대한 액세스는 어떻게 제한되거나 제어되나요?

`ams-access-admin` 역할은 AMS 자동화에서만 사용됩니다. 이러한 자동화는 AMS가 원격 측정, 상태 및 보안 데이터 수집을 위해 환경에 배포하는 데 사용하는 필수 리소스를 배포, 관리 및 유지 관리하여 운영 기능을 수행합니다. AMS 엔지니어는 자동화 역할을 수임할 수 없으며 내부 시스템의 역할 매핑에 의해 제한됩니다. 런타임 시 AMS는 범위가 축소된 최소 권한 세션 정책을 모든 자동화에 동적으로 적용합니다. 이 세션 정책은 자동화의 기능과 권한을 제한합니다.

AMS는 자동화 역할에 대한 AWS Well-Architected Framework에서 권장하는 최소 권한 원칙을 어떻게 구현하나요?

런타임 시 AMS는 범위가 축소된 최소 권한 세션 정책을 모든 자동화에 적용합니다. 이렇게 범위가 축소된 세션 정책은 자동화의 기능과 권한을 제한합니다. IAM 리소스를 생성할 권한이 있는 세션 정책에도 권한 경계를 연결해야 합니다. 이 권한 경계는 권한 에스컬레이션 위험을 줄입니다. 모든 팀은 해당 팀에서만 사용하는 세션 정책을 온보딩합니다.

자동화 역할과 관련된 무단 액세스 시도 또는 의심스러운 활동을 탐지하는 데 사용되는 로깅 및 모니터링 시스템은 무엇입니까?

AWS 는 AWS 서비스 팀이 내부적으로 사용할 수 있는 핵심 로그 아카이브 기능을 제공하는 중앙 집중식 리포지토리를 유지 관리합니다. 이러한 로그는 높은 확장성, 내구성 및 가용성을 위해 Amazon S3 에 저장됩니다. 그러면 AWS 서비스 팀은 중앙 로그 서비스에서 서비스 로그를 수집, 보관 및 볼 수 있습니다.

의 프로덕션 호스트 AWS 는 마스터 기준 이미지를 사용하여 배포됩니다. 기준 이미지에는 보안을 위한 로깅 및 모니터링을 포함하는 표준 구성 및 함수 세트가 탑재되어 있습니다. 이러한 로그는 AWS 보안 인시던트가 의심되는 경우 근본 원인 분석을 위해 보안 팀이 저장하고 액세스할 수 있습니다.

지정된 호스트에 대한 로그는 해당 호스트를 소유한 팀에서 사용할 수 있습니다. 팀은 운영 및 보안 분석을 위해 로그를 검색할 수 있습니다.

자동화 인프라와 관련된 보안 인시던트 또는 침해는 어떻게 처리되며 신속한 대응 및 완화에 도움이 되는 프로토콜은 무엇입니까?

AWS 비상 계획 및 인시던트 대응 플레이북은 보안 인시던트를 탐지, 완화, 조사 및 평가하기 위한 도구와 프로세스를 정의하고 테스트했습니다. 이러한 계획 및 플레이북에는 계약 및 규제 요구 사항에 따라 잠재적 데이터 침해에 대응하기 위한 지침이 포함되어 있습니다.

자동화 인프라에서 정기적인 보안 평가, 취약성 스캔 및 침투 테스트를 수행합니까?

AWS 보안은 다양한 도구를 사용하여 AWS 환경의 호스트 운영 체제, 웹 애플리케이션 및 데이터베이스에 대한 정기적인 취약성 검사를 수행합니다. AWS 보안 팀은 또한 해당 공급업체 결함에 대한 뉴스 피드를 구독하고 공급업체의 웹 사이트 및 기타 관련 아웃렛에서 새 패치를 사전에 모니터링합니다.

자동화 인프라에 대한 액세스는 권한 있는 직원으로만 어떻게 제한되나요?

AWS 시스템에 대한 액세스는 최소 권한을 기반으로 할당되며 승인된 개인이 승인합니다. 역할 및 책임 영역(예: 액세스 요청 및 승인, 변경 관리 요청 및 승인, 변경 개발, 테스트 및 배포 등)은 AWS 시스템의 무단 또는 의도하지 않은 수정 또는 오용을 줄이기 위해 서로 다른 개인으로 분리됩니다. 그룹 또는 공유 계정은 시스템 경계 내에서 허용되지 않습니다.

자동화 파이프라인에서 보안 표준을 유지하고 무단 액세스 또는 데이터 침해를 방지하기 위해 구현되는 조치는 무엇입니까?

서비스, 호스트, 네트워크 디바이스, Windows 및 UNIX 그룹을 포함한 리소스에 대한 액세스는 적절한 소유자 또는 관리자가 AWS 독점 권한 관리 시스템에서 승인합니다. 권한 관리 도구 로그는 액세스 변경 요청을 캡처합니다. 직무 변경은 리소스에 대한 직원의 액세스를 자동으로 취소합니다. 해당 직원에 대한 지속적인 액세스를 요청하고 승인해야 합니다.

AWS 는 원격 위치에서 내부 AWS 네트워크에 인증하기 위해 승인된 암호화 채널을 통한 2단계 인증을 요구합니다. 방화벽 디바이스는 컴퓨팅 환경에 대한 액세스를 제한하고, 컴퓨팅 클러스터의 경계를 적용하고, 프로덕션 네트워크에 대한 액세스를 제한합니다.

감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호하기 위한 프로세스가 구현됩니다. 감사 레코드에는 필요한 분석 요구 사항을 지원하기 위한 데이터 요소 세트가 포함되어 있습니다. 또한 온디맨드 검사 또는 분석을 위해, 그리고 보안 관련 또는 비즈니스에 영향을 미치는 이벤트에 대응하여 승인된 사용자가 감사 레코드를 사용할 수 있습니다.

AWS 시스템(예: 네트워크, 애플리케이션, 도구 등)에 대한 사용자 액세스 권한은 종료 또는 비활성화 후 24시간 이내에 취소됩니다. 비활성 사용자 계정은 최소 90일마다 비활성화 및/또는 제거됩니다.

권한 에스컬레이션 또는 액세스 오용을 감지하여 AMS 팀에 사전에 알리기 위해 액세스 또는 감사 로깅에 대한 이상 탐지 또는 모니터링이 켜져 있습니까?

의 프로덕션 호스트 AWS 에는 보안을 위한 로깅이 탑재되어 있습니다. 이 서비스는 로그온, 실패한 로그인 시도 및 로그오프를 포함하여 호스트에서 인적 작업을 로깅합니다. 이러한 로그는 AWS 보안 인시던트가 의심되는 경우 근본 원인 분석을 위해 보안 팀이 저장하고 액세스할 수 있습니다. 지정된 호스트에 대한 로그는 해당 호스트를 소유한 팀에서도 사용할 수 있습니다. 서비스 팀은 프런트엔드 로그 분석 도구를 사용하여 로그에서 운영 및 보안 분석을 검색할 수 있습니다. 프로세스는 로그 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호하는 데 도움이 되도록 구현됩니다. AWS 보안 팀은 로그 분석을 수행하여 정의된 위험 관리 파라미터를 기반으로 이벤트를 식별합니다.

AMS 관리형 계정에서 추출되는 고객 데이터 유형은 무엇이며 이를 어떻게 활용하고 저장하나요?

AMS는 어떤 목적으로도 콘텐츠에 액세스하거나 사용하지 않습니다. AMS는 고객 콘텐츠를 고객 계정과 AWS 서비스 관련하여 고객 또는 최종 사용자가에서 처리, 저장 또는 호스팅하기 AWS 위해 전송하

는 소프트웨어(기계 이미지 포함), 데이터, 텍스트, 오디오, 비디오 또는 이미지와 고객 또는 최종 사용자가 사용을 통해 위에서 도출한 모든 계산 결과로 정의합니다 AWS 서비스.

AMS Accelerate의 모니터링 및 이벤트 관리

AMS Accelerate 모니터링 시스템은 AWS 리소스에 장애, 성능 저하 및 보안 문제가 있는지 모니터링합니다.

관리형 계정인 AMS Accelerate는 해당 AWS 리소스에 대한 경보를 구성 및 배포하고, 이러한 리소스를 모니터링하고, 필요한 경우 문제 해결을 수행합니다.

AMS Accelerate 모니터링 시스템은 Resource Tagger 및 Alarm Manager와 같은 내부 도구를 사용하며, AWS 서비스AWS AppConfig, Amazon CloudWatch(CloudWatch), Amazon EventBridge(이전 명칭: CloudWatch), Amazon GuardDuty, Amazon Macie, 등의 기능을 활용합니다 AWS Health.

AMS Accelerate는 운영 우수성을 달성하는 데 도움이 되는 다양한 운영 서비스를 제공합니다 AWS. 연중무휴 24시간 헬프데스크, 사전 모니터링, 보안, 패치 적용, 로깅 및 백업을 포함한 몇 가지 주요 운영 기능을 AWS 클라우드 통해 AMS가에서 전반적인 운영 우수성을 달성하는 데 어떻게 도움이 되는지 빠르게 이해하려면 AMS 참조 아키텍처 다이어그램을 참조하세요.

주제

- 모니터링이란 무엇입니까?
- 모니터링 작동 방식
- AMS의 기준 모니터링 알림
- AMS의 애플리케이션 인식 인시던트 알림
- 경보 관리자 가속화
- 알림의 AMS 자동 문제 해결
- AMS에서 Amazon EventBridge 관리형 규칙 사용
- AMS의 신뢰할 수 있는 수정자

Amazon EKS 모니터링에 대한 자세한 내용은 섹션을 참조하세요. AMS Accelerate에서 Amazon EKS 모니터링 및 인시던트 관리

모니터링이란 무엇입니까?

AMS Accelerate 모니터링은 다음과 같은 이점을 제공합니다.

- 선택한 모든 또는 지원되는 AWS 리소스에 대해 관리형 계정 전체에서 정책을 생성, 관리 및 배포하는 기본 구성입니다.

- 관리형 계정에 대한 다른 모니터링을 구성하지 않더라도 기본 보호 수준을 갖도록 하는 모니터링 기준입니다. 자세한 내용은 AMS의 기준 모니터링 알림 단원을 참조하십시오.
- 요구 사항에 맞게 기준 리소스 경보를 사용자 지정하는 기능입니다.
- 가능한 경우 애플리케이션에 미치는 영향을 방지하거나 줄이기 위해 AMS Operations에서 알림을 자동으로 수정합니다. 예를 들어 독립 실행형 Amazon EC2 인스턴스를 사용 중이고 시스템 상태 확인에 실패한 경우 AMS는 인스턴스를 중지했다가 다시 시작하여 인스턴스 복구를 시도합니다. 자세한 정보는 알림의 AMS 자동 문제 해결을 참조하십시오.
- OpsCenter를 사용하여 활성 및 이전에 해결된 알림에 대한 가시성. 예를 들어 Amazon EC2 인스턴스에서 CPU 사용률이 예기치 않게 높은 경우 AWS Systems Manager 콘솔에 대한 액세스(OpsCenter 콘솔에 대한 액세스 포함)를 요청하고 OpsCenter 콘솔에서 직접 OpsItem을 볼 수 있습니다. OpsCenter
- 알림을 조사하여 적절한 조치를 결정합니다. 자세한 내용은 AMS Accelerate의 인시던트 관리 단원을 참조하십시오.
- 계정 및 지원되는 AWS 서비스의 구성을 기반으로 생성된 알림입니다. 계정의 모니터링 구성은 알림을 생성하는 계정의 모든 리소스 파라미터를 나타냅니다. 계정의 모니터링 구성에는 CloudWatch 경보 정의와 알림(경보 또는 이벤트)을 생성하는 EventBridge(이전에는 CloudWatch Events라고 함)가 포함됩니다. 리소스 파라미터에 대한 자세한 내용은 섹션을 참조하세요AMS의 기준 모니터링 알림.
- 임박, 진행 중, 취소 또는 잠재적 장애, 성능 저하 또는 계정에 구성된 기준 모니터링에서 생성된 보안 문제에 대한 알림(알림이라고 함). 알림의 예로는 CloudWatch 경보, 이벤트 또는 GuardDuty 또는 같은 서비스의 결과가 AWS 있습니다 AWS Health.

모니터링 작동 방식

AWS Managed Services(AMS)의 모니터링 아키텍처에 대한 다음 그래픽을 참조하세요.

다음 다이어그램은 AMS Accelerate 모니터링 아키텍처를 보여줍니다.

리소스 태거를 사용하여 정의된 정책에 따라 리소스에 태그가 지정되고 경보 정의가 배포되면 다음 목록에서 AMS 모니터링 프로세스를 설명합니다.

- 생성: 계정 온보딩 시 AMS는 관리형 계정에서 생성된 모든 리소스에 대한 기준 모니터링(CloudWatch(CW) 경보 및 CW 이벤트 규칙의 조합)을 구성합니다. 기준 모니터링 구성은 CW 경보가 트리거되거나 CW 이벤트가 생성될 때 알림을 생성합니다.
- 집계: 리소스에서 생성된 모든 알림은 계정의 SNS 주제로 전달하여 AMS 모니터링 시스템으로 전송됩니다. AMS가 Amazon EC2 알림을 그룹화하는 방법을 구성할 수도 있습니다. AMS는 동일한 EC2

인스턴스와 관련된 모든 알림을 단일 인시던트로 그룹화하거나 기본 설정에 따라 알림당 하나의 인시던트를 생성합니다. Cloud Service Delivery Manager 또는 Cloud Architect와 협력하여 언제든지 이 구성을 변경할 수 있습니다.

- 처리: AMS는 알림을 분석하고 영향 가능성을 기반으로 처리합니다. 알림은 다음에 설명된 대로 처리됩니다.
  - 알려진 고객 영향이 있는 알림: 이로 인해 새 인시던트 보고서가 생성되고 AMS는 인시던트 관리 프로세스를 따릅니다.

    알림 예: Amazon EC2 인스턴스가 시스템 상태 확인에 실패하고 AMS는 인스턴스를 중지했다가 다시 시작하여 인스턴스 복구를 시도합니다.
  - 고객 영향이 불확실한 알림: 이러한 유형의 알림의 경우 AMS는 인시던트 보고서를 보내며, 대부분의 경우 AMS가 조치를 취하기 전에 영향을 확인하도록 요청합니다. 그러나 인프라 관련 검사를 통과하면 AMS는 인시던트 보고서를 보내지 않습니다.

    예: Amazon EC2 인스턴스에서 10분 이상 >85% CPU 사용률에 대한 알림은 사용량에 따라이 동작이 예상될 수 있으므로 인시던트로 즉시 분류할 수 없습니다. 이 예제에서 AMS Automation은 리소스에 대한 인프라 관련 검사를 수행합니다. 이러한 검사가 통과하면 CPU 사용량이 99%를 초과하더라도 AMS는 알림 알림을 보내지 않습니다. 자동화가 리소스에서 인프라 관련 검사가 실패하고 있음을 감지하면 AMS는 알림 알림을 보내고 완화가 필요한지 확인합니다. 알림은이 단원에서 자세히 설명합니다. AMS는 알림에서 완화 옵션을 제공합니다. 알림이 인시던트임을 확인하는 알림에 회신하면 AMS가 새 인시던트 보고서를 생성하고 AMS 인시던트 관리 프로세스가 시작됩니다. "고객 영향 없음" 또는 3일 동안 전혀 응답하지 않음 응답을 수신하는 서비스 알림은 해결됨으로 표시되고 해당 알림은 해결됨으로 표시됩니다.
  - 고객 영향이 없는 알림: 평가 후 AMS가 알림에 고객에게 영향이 없다고 판단하면 알림이 종료됩니다.

    예를 들어,는 교체가 필요하지만 이후 해당 인스턴스가 종료되었음을 EC2 인스턴스에 AWS Health 알립니다.

EC2 인스턴스 그룹화된 알림

동일한 EC2 인스턴스의 알림을 단일 인시던트로 그룹화하도록 AMS 모니터링을 구성할 수 있습니다. Cloud Service Delivery Manager 또는 Cloud Architect가 이를 구성할 수 있습니다. 각 AMS 관리형 계정에 대해 구성할 수 있는 파라미터는 4개입니다.

1. 범위: 계정 전체 또는 태그 기반 중 하나를 선택합니다.
   - 해당 계정의 모든 EC2 인스턴스에 적용되는 구성을 지정하려면 범위 = 계정 전체를 선택합니다.

- 특정 태그가 있는 계정의 EC2 인스턴스에만 적용되는 구성을 지정하려면 범위 = 태그 기반을 선택합니다.

2. 그룹화 규칙: 클래식 또는 인스턴스를 선택합니다.
   - 계정의 모든 리소스에 대해 인스턴스 수준 그룹화를 구성하려면 범위 = 계정 전체 및 그룹화 규칙 = 인스턴스를 선택합니다.
   - 인스턴스 수준 그룹화를 사용하도록 계정의 특정 리소스를 구성하려면 해당 인스턴스에 태그를 지정한 다음 범위 = 태그 기반 및 그룹화 규칙 = 인스턴스 수준을 선택합니다.
   - 계정의 알림에 인스턴스 그룹화를 사용하지 않으려면 그룹화 규칙 = 클래식을 선택합니다.
3. 참여 옵션: 없음, 보고서만 또는 기본값을 선택합니다.
   - 구성이 활성화되어 있는 동안 AMS가 인시던트를 생성하거나 해당 리소스의 경보에 대한 자동화를 실행하지 않도록 하려면 없음을 선택합니다.
   - 구성이 활성화되어 있는 동안 AMS가 인시던트를 생성하거나 해당 리소스에서 경보에 대한 자동화를 실행하지 않고 자동 복구 Systems Manager 문서를 실행하지 않고 보고에 이러한 이벤트의 레코드를 포함하려면 보고서만 선택합니다. 이는 상호 작용하는 인시던트 지원 사례의 양을 줄이고 일부 리소스의 일부 인시던트가 비프로덕션 계정의 인시던트와 같이 즉각적인 주의가 필요하지 않은 경우에 유용할 수 있습니다.
   - AMS가 알림을 처리하고, 자동화를 실행하고, 필요한 경우 인시던트 사례를 생성하려면 기본값을 선택합니다.
4. 해결 시간: 24시간, 48시간 또는 72시간을 선택합니다. 마지막으로 인시던트 사례가 자동으로 종료되는 시기를 구성합니다. 마지막 사례 대응의 시간이 구성된 이후 해결 값에 도달하면 인시던트가 종료됩니다.

경고 알림

알림 처리의 일환으로 영향 분석을 기반으로 AWS Managed Services(AMS)는 인시던트를 생성하고 영향을 확인할 수 있는 문제 해결을 위한 인시던트 관리 프로세스를 시작합니다. 영향을 확인할 수 없는 경우 AMS는 서비스 알림을 통해 계정과 연결된 이메일 주소로 알림 알림을 보냅니다. 일부 시나리오에서는이 알림이 전송되지 않습니다. 예를 들어 인프라 관련 검사가 높은 CPU 사용률 알림을 통과하면 알림이 전송되지 않습니다. 자세한 내용은의 알림 처리 프로세스를 위한 AMS 모니터링 아키텍처 다이어그램을 참조하세요모니터링 작동 방식.

태그 기반 알림

태그를 사용하여 리소스에 대한 알림 알림을 다른 이메일 주소로 보냅니다. 여러 개발자 팀이 동일한 계정을 사용할 때 단일 이메일 주소로 전송된 알림으로 인해 혼동이 발생할 수 있으므로 태그 기반 알

림은 사용하는 것이 가장 좋습니다. 태그 기반 알림은 선택한 EC2 인스턴스 그룹화된 알림 설정의 영향을 받지 않습니다.

태그 기반 알림으로 다음을 수행할 수 있습니다.

- 특정 이메일 주소로 알림 전송: `key = OwnerTeamEmail`,를 사용하여 특정 이메일 주소로 전송해야 하는 알림이 있는 리소스에 태그를 지정합니다`value = EMAIL_ADDRESS`.
- 여러 이메일 주소로 알림 전송: 여러 이메일 주소를 사용하려면 쉼표로 구분된 값 목록을 지정합니다. 예, `key = OwnerTeamEmail`, `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`. 값 필드의 총 문자 수는 260자를 초과할 수 없습니다.
- 사용자 지정 태그 키 사용: 사용자 지정 태그 키를 사용하려면 태그 기반 통신에 대한 자동 알림을 활성화하는 데 명시적으로 동의하는 이메일에 사용자 지정 태그 키 이름을 CSDM에 제공합니다. 모든 인스턴스와 리소스에서 고객 응대 태그에 동일한 태그 지정 전략을 사용하는 것이 가장 좋습니다.

> **Note**
>
> 키 값 `OwnerTeamEmail`은 카멜 형식일 필요는 없습니다. 그러나 태그는 대/소문자를 구분하므로 권장 형식을 사용하는 것이 좋습니다.
> 이메일 주소는 도메인에서 로컬 부분을 분리하려면 "at sign"(@)을 사용하여 완전히 지정해야 합니다. 잘못된 이메일 주소의 예: `Team.AppATabc.xyz` 또는 `john.doe`. 태그 지정 전략에 대한 일반적인 지침은 AWS 리소스 태그 지정을 참조하세요. 태그에 개인 식별 정보(PII)를 추가하지 마세요. 가능하면 배포 목록 또는 별칭을 사용합니다.
> 태그 기반 알림은 EC2, Elastic Block Store(EBS), Elastic Load Balancing(ELB), Application Load Balancer(ALB), Network Load Balancer, Relational Database Service(RDS), OpenSearch, Elastic File System(EFS), FSx 및 Site-to-Site VPN과 같은 Amazon 서비스의 리소스에 대해 지원됩니다.

AMS의 기준 모니터링 알림

AMS Accelerate 모니터링 기본값에 대해 알아봅니다. 자세한 내용은 AMS Accelerate의 모니터링 및 이벤트 관리 단원을 참조하십시오.

다음 표에는 모니터링되는 항목과 기본 알림 임계값이 나와 있습니다. 사용자 지정 구성 문서를 사용하여 알림 임계값을 변경하거나 서비스 요청을 제출할 수 있습니다. 사용자 지정 경보 구성을 변경하는 방법에 대한 지침은 섹션을 참조하세요Accelerate 경보 구성 변경. 경보가 임계값을 초과할 때 알림을

받으려면 AMS의 표준 알림 프로세스 외에도 경보 구성을 덮어쓸 수 있습니다. 지침은 경보 관리자 가속화 섹션을 참조하세요.

Amazon CloudWatch는 지표의 보존 기간을 연장합니다. 자세한 내용은 CloudWatch 제한을 참조하세요.

> **Note**
>
> AMS Accelerate는 정기적으로 기준 모니터링을 보정합니다. 새 계정은 항상 최신 기준 모니터링으로 온보딩되며 표에는 새로 온보딩된 계정에 대한 기준 모니터링이 설명되어 있습니다. AMS Accelerate는 기존 계정의 기준 모니터링을 정기적으로 업데이트하며 업데이트가 적용되기 전에 지연이 발생할 수 있습니다.

기준 모니터링의 알림

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
별표가 지정된(*) 알림의 경우 AMS는 가능한 경우 영향을 사전에 평가하고 수정합니다. 수정이 불가능한 경우 AMS는 인시던트를 생성합니다. 자동화가 문제를 해결하지 못하는 경우 AMS는 인시던트 사례를 알리고 AMS 엔지니어가 참여합니다. 또한 Direct-Customer-Alerts SNS 주제를 옵트인하면 이러한 알림이 이메일로 직접 전송됩니다.		
Application Load Balancer 인스턴스	ApplicationLoadBalancerErrorCount (HTTPCode_ELB_5XX_Count/RequestCount)*100 1분, 연속 5회 동안 합계 > 15%.	Application LoadBalancer HTTP 5XX 오류 수 Loadbalancer에서 생성된 초과 HTTP 5XX 응답 코드 수에 대한 CloudWatch 경보입니다.
Application Load Balancer 인스턴스	RejectedConnectionCount 1분, 연속 5회 동안 합계 > 0%.	Application LoadBalancer 거부된 연결 수 로드 밸런서가 최대값에 도달하여 거부된 연결 수에 대한 CloudWatch 경보

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Application Load Balancer 대상	TargetConnectionErrorCount (HTTPCode_Target_5XX_Count/RequestCount)*100 1분, 연속 5회 동안 합계 > 15%.	${ElasticLoadBalancingV2::TargetGroup::FullName} - Application LoadBalancer 대상 연결 오류 수 - ${ElasticLoadBalancingV2::TargetGroup::UUID} 대상에서 생성된 초과 HTTP 5XX 응답 코드 수에 대한 CloudWatch 경보입니다.
Application Load Balancer 대상	ApplicationLoadBalancerTargetGroupErrorCount 1분, 연속 5회 동안 합계 > 0%.	${ElasticLoadBalancingV2::TargetGroup::FullName} - Application LoadBalancer 대상 HTTP 5XX 오류 수 - ${ElasticLoadBalancingV2::TargetGroup::UUID} 로드 밸런서와 등록된 인스턴스 간에 연결 수가 설정되지 않은 경우 CloudWatch 경보가 발생합니다.
Amazon EC2 인스턴스 - 모든 OSs	CPUUtilization* 인스턴스가 폴링 Systems Manager 명령에 응답하지 않는 경우 5분 동안 > 95%, 연속 6회.	${EC2::InstanceId}: CPU가 너무 높음 CloudWatch 경보. CPU 사용률이 높다는 것은 교착 상태, 무한 루프, 악성 공격 및 기타 이상과 같은 애플리케이션 상태의 변화를 나타내는 지표입니다. 다음은 Direct-Customer-Alerts 경보입니다.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Amazon EC2 인스턴스 - 모든 OSs	StatusCheckFailed 5분 동안 > 0%, 연속 3회.	${EC2::InstanceId}: 상태 확인 실패 CloudWatch 경보. 상태 확인 실패는 지정된 ID의 Amazon EC2 인스턴스가 하나 이상의 자동 상태 확인에 실패했음을 나타냅니다. 즉, 인스턴스가 올바르게 작동하거나 연결할 수 없는 문제가 발생했습니다.
Amazon EC2 인스턴스 - Linux	최소 mem_used_percent 5분, 연속 6회 동안 >= 95%.	${EC2::InstanceId}: 메모리 없음 CloudWatch 경보. Memory Free는 지정된 Amazon EC2 인스턴스에서 사용 가능한 메모리(RAM)가 정의된 임계값 미만으로 떨어졌음을 나타냅니다. 이로 인해 메모리 문제, 시스템 충돌이 발생할 수 있으며 인스턴스에 더 많은 RAM이 필요할 수 있음을 나타냅니다. 다음은 Direct-Customer-Alerts 경보입니다.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Amazon EC2 인스턴스 - Linux	평균 스왑_사용_백분율 5분, 연속 6회 동안 >= 95%.	${EC2::InstanceId}: 스왑 프리 CloudWatch 경보. Amazon EC2 인스턴스의 평균 swap_used_percent는 현재 사용 중인 할당된 스왑 공간의 평균 백분율이 사전 정의된 임계값을 초과했음을 나타냅니다. 이로 인해 성능 저하, 병목 현상 및 메모리 문제가 발생할 수 있습니다. 다음은 Direct-Customer-Alerts 경보입니다.
Amazon EC2 인스턴스 - Linux	최대 disk_used_percent 5분, 연속 6회 동안 >= 95%.	${EC2::InstanceId}: 디스크 사용량이 너무 높음 - ${EC2::Disk::UUID} CloudWatch 경보. 디스크 사용량이 너무 높음은 특정 Amazon EC2 또는 식별된 디스크의 디스크 사용률이 용량에 근접하고 있음을 나타냅니다. 이로 인해 성능 저하, 애플리케이션 오류 및 시스템 불안정이 발생할 수 있습니다. 다음은 Direct-Customer-Alerts 경보입니다.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Amazon EC2 인스턴스 - Windows	사용 중인 최소 메모리 % 커밋된 바이트 5분, 연속 6회 동안 >= 95%.	${EC2::InstanceId}: 메모리 없음 CloudWatch 경보. Memory Free는 지정된 Amazon EC2 인스턴스에서 사용 가능한 메모리(RAM)가 정의된 임계값 미만으로 떨어졌음을 나타냅니다. 이로 인해 메모리 문제, 시스템 충돌이 발생할 수 있으며 인스턴스에 더 많은 RAM이 필요할 수 있음을 나타냅니다. 다음은 Direct-Customer-Alerts 경보입니다.
Amazon EC2 인스턴스 - Windows	최대 LogicalDisk % 여유 공간 5분 동안 <= 5%, 연속 6회.	${EC2::InstanceId}: 디스크 사용량이 너무 높음 - ${EC2::Disk::UUID} CloudWatch 경보. Amazon EC2 Windows 인스턴스 내 논리적 디스크(파일 시스템 파티션)의 여유 공간이 사전 정의된 임계값을 초과했음을 나타냅니다. 디스크 공간 부족으로 인해 디스크 공간 부족이 발생할 수 있습니다. 다음은 Direct-Customer-Alerts 경보입니다.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Amazon EFS	AMSEFSBurstCreditBalanceExhausted. BurstCreditBalance가 15분 동안 1000 미만입니다.	${EFS::FileSystemId}: EFS: 버스트 크레딧 밸런스 Amazon EFS 파일 시스템의 BurstCreditBalance에 대한 CloudWatch 경보입니다.
Amazon EFS	AMSEFSClientConnectionsLimit. ClientConnections > 15분 동안 24,000.	${EFS::FileSystemId}: EFS: 클라이언트 연결 제한 Amazon EFS 파일 시스템의 ClientConnections에 대한 CloudWatch 경보입니다.
Amazon EFS	AMSEFSThroughputUtilizationLimit. 1시간 동안 EFS 처리량 사용률 > 80%.	${EFS::FileSystemId}: EFS: 처리량 사용률 제한 Amazon EFS 파일 시스템의 처리량 사용률에 대한 CloudWatch 경보입니다.
Amazon EFS	AMSEFSPercentIOLimit. PercentIOLimit > 95, 75분.	${EFS::FileSystemId}: EFS: PercentIOLimit Amazon EFS 파일 시스템의 PercentIOLimit에 대한 CloudWatch 경보입니다.
Amazon EKS	Amazon EKS 섹션을 참조하세요AMS Accelerate에서 Amazon EKS 모니터링 및 인시던트 관리의 기준 알림.	

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Elastic Load Balancing 인스턴스	SpilloverCountBackendConnectionErrors 1분 동안 > 1, 연속 횟수 15회.	Classic LoadBalancer 스필오버 수 경보 서지 대기열이 가득 차서 거부된 요청 수가 초과되면 CloudWatch 경보가 발생합니다.
Elastic Load Balancing 인스턴스	HTTPCode_ELB_5XX_Count 5분 동안 합계 > 0, 연속 횟수 3회.	로드 밸런서에서 시작된 초과 HTTP 5XX 응답 코드 수에 대한 CloudWatch 경보입니다.
Elastic Load Balancing 인스턴스	SurgeQueueLength 1분 동안 > 100, 연속 15회.	Classic LoadBalancer 서지 대기열 길이 경보입니다. 초과 요청 수가 라우팅 보류 중인 경우 CloudWatch 경보가 발생합니다.
FSx for ONTAP	AMSFSXONTAPIOPSUtilization. 2시간 동안 FSX:ONTAP IOPS 사용률 > 80%.	${FSx::FileSystemId}: FSX:ONTAP IOPS 사용률 FSx for ONTAP 인스턴스의 IOPS 사용률 제한에 대한 CloudWatch 경보입니다.
FSx for ONTAP	AMSFSXONTAPThroughputUtilization. 2시간 동안 FSX:ONTAP 처리량 사용률 > 80%.	${FSx::FileSystemId}: FSX:ONTAP 처리량 사용률 FSx for ONTAP 볼륨의 처리량 제한에 대한 CloudWatch 경보입니다.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
FSx for ONTAP	AMSFSXONTAPVolumeInodeUtilization. 2시간 동안 FSX:ONTAP Inode 사용률 > 80%.	${FSx::FileSystemId}: ${FSx::ONTAP::VolumeId} FSX:ONTAP Inode 사용률 FSx for ONTAP 볼륨의 파일 용량 사용률 제한에 대한 CloudWatch 경보입니다.
FSx for ONTAP	AMSFSXONTAPVolumeCapacityUtilization. 2시간 동안 FSX:ONTAP 볼륨 용량 사용률 > 80%.	${FSx::FileSystemId}:${FSx::ONTAP::VolumeId} FSx for ONTAP 볼륨의 볼륨 용량 사용률 제한에 대한 CloudWatch 경보입니다.
FSx for Windows File Server	AMSFSXWindowsThroughputUtilization. 2시간 동안 FSX:Windows 처리량 사용률 > 80%.	${FSx::FileSystemId}: FSX:Windows 처리량 사용률 FSx for Windows File Server 인스턴스의 처리량 제한에 대한 CloudWatch 경보입니다.
FSx for Windows File Server	AMSFSXWindowsIOPSUtilization. 2시간 동안 FSX:Windows IOPS 사용률 > 80%.	${FSx::FileSystemId}: FSX:Windows IOPS 사용률 FSx for Windows File Server 인스턴스의 IOPS 사용률 제한에 대한 CloudWatch 경보입니다.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
GuardDuty 서비스	해당 사항 없음. 모든 결과(위협 목적)가 모니터링됩니다. 각 결과는 알림에 해당합니다. GuardDuty 조사 결과의 변경 사항입니다. 이러한 변경은 새롭게 생성된 결과 또는 기존 결과의 후속 발생을 포함합니다.	지원되는 GuardDuty 결과 유형 목록은 GuardDuty 활성 결과 유형을 참조하세요.
Health	AWS Health Dashboard	AMS에서 모니터링하는 서비스와 관련하여 AMS 작업의 조치가 필요한 AWS Health Dashboard (AWS Health) 이벤트의 상태가 변경되면 알림이 전송됩니다. 자세한 내용은 지원되는 서비스를 참조하세요.
IAM	Amazon EC2 IAM 인스턴스 프로파일이 존재하지 않습니다. IAM 인스턴스 프로파일이 누락되었습니다.	Amazon EC2 IAM 인스턴스 프로파일 교체에 대한 지침은 IAM 역할 교체의 IAM 설명서를 참조하세요.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
IAM	Amazon EC2 IAM 인스턴스 프로파일에 정책이 너무 많습니다. IAM 인스턴스 프로파일에는 10개의 정책이 있으며 추가 정책을 추가할 수 없습니다.	• IAM의 AWS Service Quota를 수정하여 역할당 관리형 정책 수를 20개로 늘립니다. 서비스 할당량에 대한 자세한 내용은 서비스 할당량 보기를 참조하세요. • 이러한 인스턴스와 연결된 IAM 역할에 대한 불필요한 관리형 정책을 제거하여 관리형 정책 수를 현재 IAM 할당량 미만으로 줄입니다. AMS 필수 정책을 유지해야 합니다. • 이러한 인스턴스와 연결된 IAM 역할에 대한 정책을 통합하여 관리형 정책 수를 현재 IAM 할당량 미만으로 줄입니다. AMS 필수 정책을 유지해야 합니다. AMS 필수 정책은 AMS Accelerate 사용 설명서: 섹션을 참조하세요IAM 권한 변경 세부 정보.
Macie	새로 생성된 알림 및 기존 알림에 대한 업데이트. Macie는 조사 결과에서 변경 사항을 찾습니다. 이러한 변경은 새롭게 생성된 결과 또는 기존 결과의 후속 발생을 포함합니다.	Amazon Macie 알림. 지원되는 Amazon Macie 알림 유형 목록은 Amazon Macie 조사 결과 분석을 참조하세요. Macie는 모든 계정에 대해 활성화되어 있지 않습니다.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
NATGateways	PacketsDropCount: 15분 동안 packetsdropcount가 > 0인 경우 경보	NatGateway PacketsDropCount 0보다 큰 값은 NAT 게이트웨이에 일시적 문제가 있음을 나타낼 수 있습니다.
NATGateways	ErrorPortAllocation: NAT 게이트웨이가 15분 이상의 평가 기간 동안 포트를 할당할 수 없는 경우 경보	NatGateway ErrorPortAllocation NAT 게이트웨이가 소스 포트 할당에 실패한 횟수. 값이 0보다 크면 동시 연결이 너무 많음을 나타냅니다.
OpenSearch 클러스터	클러스터상태 빨간색 최대값은 1분, 연속 1회 동안 >= 1입니다.	ClusterStatus 빨간색 CloudWatch 경보. 도메인의 저장 데이터를 암호화하는 데 사용되는 암호화 AWS KMS 키는 비활성화됩니다. 정상 작동으로 복원하려면 다시 활성화해야 합니다. 자세한 내용은 빨간색 클러스터 상태를 참조하세요.
OpenSearch 도메인	KMSKeyError >= 1분, 연속 1회.	KMS 키 오류 CloudWatch 경보. 하나 이상의 기본 샤드와 복제본이 노드에 할당되지 않았습니다. 자세한 내용은 Amazon OpenSearch Service의 저장 데이터 암호화를 참조하세요.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
OpenSearch 도메인	KMSKeyInaccessible >= 1분, 연속 1회.	KMS 키 액세스할 수 없음 오류 CloudWatch 경보. 하나 이상의 기본 샤드와 복제본이 노드에 할당되지 않았습니다. 자세한 내용은 Amazon OpenSearch Service의 저장 데이터 암호화를 참조하세요.
OpenSearch 도메인	클러스터상태 노란색 최대값은 1분, 연속 1회 동안 >= 1입니다.	ClusterStatus 노란색 하나 이상의 복제 샤드가 노드에 할당되지 않았습니다. 자세한 내용은 노란색 클러스터 상태를 참조하세요.
OpenSearch 도메인	FreeStorageSpace 최소값은 1분, 연속 1회 동안 <= 20480입니다.	사용 가능한 스토리지 공간 부족 클러스터 속 노드의 여유 스토리지 공간이 20GiB까지 떨어졌습니다. 자세한 내용은 사용 가능한 스토리지 공간 부족을 참조하세요.
OpenSearch 도메인	ClusterIndexWritesBlocked 5분 동안 >= 1, 연속 1회.	클러스터 인덱스 쓰기 차단됨 클러스터가 쓰기 요청을 차단하고 있습니다. 자세한 내용은 ClusterBlockException을 참조하세요.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
OpenSearch 도메인	Nodes(노드) 최소 1일 동안 < x, 연속 1회.	노드 다운 x는 클러스터의 노드 수입니다. 이 경보는 클러스터에서 하나 이상의 노드가 하루 동안 연결되지 않았음을 나타냅니다. 자세한 내용은 실패한 클러스터 노드를 참조하세요.
OpenSearch 도메인	CPUUtilization 15분 동안 평균 >= 80%, 연속 3회.	데이터 노드의 높은 CPU 사용량 100% CPU 사용률은 드물지 않지만 평균값이 높게 지속되는 것은 문제가 있습니다. 기존 인스턴스 유형의 크기를 올바르게 조정하거나 인스턴스를 추가하는 것이 좋습니다.
OpenSearch 도메인	JVMMemoryPressure 최대 >= 80%, 5분, 연속 3회.	데이터 노드의 높은 메모리 사용량 사용량이 늘어나면 클러스터에서 메모리 부족 오류가 발생할 수 있습니다. 수직 확장을 고려하세요. OpenSearch는 Java 힙에 인스턴스 RAM의 절반을 사용하고 힙 크기는 최대 32GiB입니다. 인스턴스를 최대 64GiB의 RAM까지 수직 확장할 수 있으며 인스턴스를 추가하면 수평 확장도 가능합니다.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
OpenSearch 도메인	MasterCPUUtilization 15분 동안 평균 >= 50%, 연속 3회.	마스터 노드 높은 CPU 사용량 전용 마스터 노드에 더 큰 인스턴스 유형을 사용하는 것이 좋습니다. 클러스터 안정성 및 블루/그린(Blue/Green) 배포의 역할로 인해 전용 마스터 노드는 데이터 노드보다 평균 CPU 사용량이 낮아야 합니다.
OpenSearch 도메인	MasterJVMMemoryPressure 최대 >= 15분, 연속 1회 동안 80%.	마스터 노드 높은 JVM 메모리 압력 전용 마스터 노드에 더 큰 인스턴스 유형을 사용하는 것이 좋습니다. 클러스터 안정성 및 블루/그린(Blue/Green) 배포의 역할로 인해 전용 마스터 노드는 데이터 노드보다 평균 CPU 사용량이 낮아야 합니다.
OpenSearch 인스턴스	AutomatedSnapshotFailure 최대값은 1분, 연속 1회 동안 >= 1입니다.	자동 스냅샷 실패 CloudWatch 경보. 자동 스냅샷에 오류가 발생했습니다. 이런 오류는 red 클러스터 상태로 인해 자주 발생했습니다. 자세한 내용은 빨간색 클러스터 상태를 참조하세요.
Amazon RDS	평균 CPU 사용률 15분 동안 > 90%, 연속 2회.	${RDS::DBInstanceIdentifier}: CPUUtilization CloudWatch 경보.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Amazon RDS	DiskQueueDepth의 합계 1분 동안 > 75%, 연속 15회.	${RDS::DBInstanceIdentifier}: DiskQueue CloudWatch 경보.
Amazon RDS	평균 FreeStorageSpace 5분, 연속 2회 동안 < 1,073,741,824바이트.	${RDS::DBInstanceIdentifier}: FreeStorageSpace CloudWatch 경보.
Amazon RDS	스토리지 부족 알림 DB 인스턴스에 할당된 스토리지가 소진되면 트리거됩니다.	RDS-EVENT-0007, Amazon RDS 이벤트 알림 사용의 세부 정보를 참조하세요.
Amazon RDS	DB 인스턴스 실패 호환되지 않는 구성 또는 기본 스토리지 문제로 인해 DB 인스턴스에 장애가 발생했습니다. DB 인스턴스에 대해 특정 시점으로 복구를 시작합니다.	RDS-EVENT-0031, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	RDS -0034 장애 조치가 시도되지 않았습니다. 최근에 DB 인스턴스에 장애 조치가 발생하였기 때문에 Amazon RDS가 요청한 장애 조치를 실행하지 않습니다.	RDS-EVENT-0034, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Amazon RDS	RDS - 0035 DB 인스턴스 잘못된 파라미터 예를 들어 메모리 관련 파라미터가이 인스턴스 클래스에 대해 너무 높게 설정되어 있기 때문에 MySQL을 시작할 수 없습니다. 따라서 작업은 메모리 파라미터를 수정하고 DB 인스턴스를 재부팅하는 것입니다.	RDS-EVENT-0035, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	잘못된 서브넷 IDs 인스턴스 DB 인스턴스가 호환되지 않는 네트워크에 있습니다. 특정 서브넷 ID 중 일부가 잘못되었거나 존재하지 않습니다.	서비스 이벤트. RDS-EVENT-0036, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	RDS-0045 DB 인스턴스 읽기 전용 복제본 오류 읽기 전용 복제 프로세스에서 오류가 발생하였습니다. 자세한 내용은 이벤트 메시지 섹션을 참조하세요. 읽기 전용 복제본 오류 문제 해결에 대한 자세한 내용은 MySQL 읽기 전용 복제본 문제 해결을 참조하세요.	RDS-EVENT-0045, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	RDS-0057 statspack 사용자 계정 생성 오류 읽기 전용 복제본에 대한 복제가 종료되었습니다.	서비스 이벤트. RDS-EVENT-0057, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Amazon RDS	RDS-0058 DB 인스턴스 읽기 복제 종료 Statspack 사용자 계정인 PERFSTAT 생성 중 오류가 발생하였습니다. Statspack 옵션을 추가하기 전에 계정을 삭제합니다.	서비스 이벤트. RDS-EVENT-0058, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	DB 인스턴스 복구 시작 SQL Server DB 인스턴스가 미러를 재구성 중입니다. 이때 미러가 재구성될 때까지 성능이 저하됩니다. 복구 모델이 FULL이 아닌 데이터베이스가 발견되었습니다. 복구 모델이 FULL로 다시 변경되었고 미러링 복구가 시작되었습니다. (<dbname>: <recovery model found>[,...])	서비스 이벤트. RDS-EVENT-0066은 Amazon RDS 이벤트 범주 및 이벤트 메시지에서 세부 정보를 참조하세요.
Amazon RDS	DB 클러스터에 대한 장애 조치가 실패했습니다.	RDS-EVENT-0069, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	잘못된 권한 복구 S3 버킷 SQL Server 기본 백업 및 복원을 위해 Amazon S3 버킷에 액세스하는 데 사용하는 IAM 역할이 잘못 구성되었습니다. 자세한 내용은 기본 백업 및 복원 설정을 참조하세요.	서비스 이벤트. RDS-EVENT-0081은 Amazon RDS 이벤트 범주 및 이벤트 메시지에서 세부 정보를 참조하세요.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Amazon RDS	Aurora가 Amazon S3 버킷에서 백업 데이터를 복사할 수 없습니다.	RDS-EVENT-0082, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	DB 인스턴스가 할당된 스토리지의 90% 이상을 소비한 경우 스토리지 부족 알림.	서비스 이벤트. RDS-EVENT-0089는 Amazon RDS 이벤트 범주 및 이벤트 메시지에서 세부 정보를 참조하세요.
Amazon RDS	Aurora Serverless DB 클러스터에 대한 조정 실패 시 알림 서비스입니다.	서비스 이벤트. RDS-EVENT-0143은 Amazon RDS 이벤트 카테고리 및 이벤트 메시지에서 세부 정보를 참조하세요.
Amazon RDS	DB 인스턴스가 잘못된 상태입니다. 아무 조치도 필요하지 않습니다. 자동 확장은 나중에 다시 시도합니다.	RDS-EVENT-0219, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	DB 인스턴스가 스토리지 전체 임계값에 도달했으며 데이터베이스가 종료되었습니다.	RDS-EVENT-0221, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	이 이벤트는 Amazon RDS 인스턴스 스토리지 Autoscaling을 조정할 수 없으며 Autoscaling이 실패한 여러 이유가 있을 수 있음을 나타냅니다.	RDS-EVENT-0223, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	스토리지 자동 확장은 최대 스토리지 임계값에 도달하는 보류 중인 확장 스토리지 작업을 트리거했습니다.	RDS-EVENT-0224, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Amazon RDS	DB 인스턴스에는 현재 가용 영역에서 사용할 수 없는 스토리지 유형이 있습니다. 자동 확장은 나중에 다시 시도합니다.	RDS-EVENT-0237, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	서브넷에 사용 가능한 IP 주소가 충분하지 않아 Amazon RDS가 프록시 용량을 프로비저닝할 수 없습니다.	RDS-EVENT-0243, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon RDS	의 스토리지가 허용된 스토리지 할당량을 초과 AWS 계정 했습니다.	RDS-EVENT-0254, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
Amazon Redshift 클러스터	유지 관리 모드가 아닌 경우 클러스터의 상태 5분 동안 < 1	RedshiftClusterHealthStatus 자세한 내용은 CloudWatch 지표를 사용하여 Amazon Redshift 모니터링을 참조하세요.
Site-to-Site VPN	VPNTunnelDown TunnelState <= 0, 1분, 연속 횟수 20회.	${AWS::EC2::VpnConnectionId} - VPNTunnelDown TunnelState는 두 터널이 모두 다운되면 0, 한 터널이 가동되면 05, 두 터널이 모두 가동되면 1.0입니다.

서비스/리소스 유형	알림 소스 및 트리거 조건	알림 이름 및 참고 사항
Systems Manager Agent	Systems Manager에서 관리하지 않는 EC2 인스턴스 SSM 에이전트가 설치되지 않았습니다. SSM 에이전트가 인스턴스에 설치되었지만 에이전트 서비스가 실행되고 있지 않습니다. SSM 에이전트에는 AWS Systems Manager 서비스에 대한 네트워크 경로가 없습니다.	Systems Manager Agent를 중단시키는 추가 조건이 있습니다. 자세한 내용은 관리형 노드 가용성 문제 해결을 참조하세요.

문제 해결 노력에 대한 자세한 내용은 섹션을 참조하세요알림의 AMS 자동 문제 해결.

Andrew의 동영상을 보고 자세히 알아보기(7:03)

AMS의 애플리케이션 인식 인시던트 알림

애플리케이션 인식 자동 인시던트 알림을 사용하여 AMS가 사용자를 대신하여 생성하는 지원 사례에 맞게 통신 환경을 사용자 지정할 수 있습니다. 이 기능을 사용하면 AMS는 AWS Service Catalog AppRegistry에서 사용자 지정 워크로드 기본 설정을 검색하여 애플리케이션에 대한 메타데이터로 AMS 인시던트 통신을 보강하고 사용자를 대신하여 AMS에서 생성한 지원 사례의 심각도를 사용자 지정합니다. 이 기능을 사용하려면 먼저 AWS Service Catalog AppRegistry에 온보딩해야 합니다.

AMS Accelerate 모니터링 기본값에 대한 자세한 내용은 섹션을 참조하세요AMS Accelerate의 모니터링 및 이벤트 관리.

AppRegistry에 온보딩 및 애플리케이션 생성

AppRegistry에 온보딩하려면 AppRegistry 관리자 안내서AWS Service Catalog 의 AppRegistry 시작하기를 참조하세요. 온보딩 후 다음 방법 중 하나를 사용하여 애플리케이션을 생성합니다.

1. AWS 콘솔: 콘솔을 통해 AppRegistry에서 애플리케이션을 생성하는 방법에 대한 자세한 내용은 AppRegistry 관리자 안내서의 애플리케이션 생성을 AWS 참조하세요. AWS Service Catalog AppRegistry

2. CloudFormation: 다른 리소스를 정의하는 것처럼 AppRegistry 애플리케이션을 정의할 수 있습니다. 자세한 내용은 CloudFormation 사용 설명서의 AWS Service Catalog AppRegistry 리소스 유형 참조를 참조하세요.
3. AMS 자동화: 애플리케이션 등록 프로세스를 간소화하기 위해 AMS는 SSM 자동화 문서를 제공합니다`AWSManagedServices-CreateAppRegistryApplication`. 이 방법을 사용하려면 다음 예제에 설명된 AWS CLI 대로 https://console.aws.amazon.com/systems-manager/ 또는를 사용하여 AWS Systems Manager 콘솔에서 문서를 호출합니다.

```
# The following registers a new application with customized severity
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["normal"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# The following registers a new application with no customizations
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# You can also register applications using CloudFormation stacks
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["STACKS"],"AppTagValue":
[""],"CFNStackNames":["arn:aws:cloudformation:us-east-1:123456789012:stack/
stack-2343eddq/1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
```

태그를 생성하여 사례 보강 활성화

AMS가 애플리케이션 메타데이터에 액세스하려면 먼저 애플리케이션에 태그를 지정해야 합니다. 다음 표에는 필요한 태그가 나열되어 있습니다.

접두사가 있는 태그`ams:rt:`는 Resource Tagger를 통해 적용됩니다.

태그 키	태그 값
ams 관리형	true
ams:rt:ams-managed	true

애플리케이션에 대한 AMS 지원 사례 심각도 사용자 지정

애플리케이션이 조직에 얼마나 중요한지 지정하여 AMS에서 생성한 지원 사례의 심각도를 사용자 지정할 수 있습니다. 이 설정은 AppRegistry의 애플리케이션과 연결된 속성 그룹에 의해 제어됩니다. 속성 그룹 이름의 이름은 다음 패턴과 일치해야 합니다.

```
AMS.<ApplicationName>.CommunicationOptions
```

위의 패턴에서는 애플리케이션을 생성할 때 AppRegistry에 사용된 이름과 일치해야 `ApplicationName` 합니다.

예제 콘텐츠:

```
{
"SchemaVersion": "1.0",
"Criticality": "low"
}
```

SchemaVersion

이를 통해 사용 중인 스키마 버전과 사용할 수 있는 기능의 하위 집합이 결정됩니다.

스키마 버전	Feature
1.0	중요도 값에 따른 사용자 지정 지원 사례 심각도

중요도

이 애플리케이션의 중요도에 따라 AMS 자동 시스템에서 생성된 지원 사례의 심각도가 결정됩니다.

유효한 값:

```
low|normal|high|urgent|critical
```

심각도 수준에 대한 자세한 내용은 API 참조의 SeverityLevel을 참조하세요. AWS Support

필수 여부: 예

필요한 권한 검토

이 기능을 사용하려면 AMS가 다음 AWS Identity and Access Management 권한에 액세스해야 합니다.

- iam:ListRoleTags
- iam:ListUserTags
- resourcegroupstaggingapi:GetResources
- servicecatalog-appregistry:GetApplication
- servicecatalog-appregistry:ListAssociatedAttributeGroups
- servicecatalog-appregistry:GetAttributeGroup

> **Important**
> 이전 작업을 거부하는 IAM 정책 또는 서비스 제어 정책(SCP)이 없는지 확인합니다.

API 호출은 `ams-access-admin` 역할에 의해 이루어집니다. 다음은 볼 수 있는 내용의 예입니다.

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

경보 관리자 가속화

AMS Accelerate는 태그 기반 경보 관리자를 사용하여 AWS 리소스에 경보를 적용하여 기준 모니터링 전략을 구현하고 모든 AWS 리소스가 모니터링 및 보호되도록 합니다. 태그 기반 경보 관리자와 통합하여 유형, 플랫폼 및 기타 태그를 기반으로 리소스 구성을 사용자 지정하여 리소스가 모니터링되도록 할 수 있습니다 AWS . 온보딩 중에 Alarm Manager가 Accelerate 계정에 배포됩니다.

경보 관리자의 작동 방식

계정이 AMS Accelerate에 온보딩되면 구성 프로필이라고 하는 두 개의 JSON 문서가 AWS AppConfig의 계정에 배포됩니다. 두 프로필 문서는 모두 경보 관리자 애플리케이션과 AMS Accelerate 인프라 환경에 있습니다.

두 구성 프로필의 이름은 AMSManagedAlarms(기본 구성 프로필)와 CustomerManagedAlarms(사용자 지정 구성 프로필)입니다.

- 기본 구성 프로필:
  - 이 프로파일에 있는 구성에는 AMS Accelerate가 모든 고객 계정에 배포하는 기본 구성이 포함되어 있습니다. 이 구성에는 기본 AMS Accelerate 모니터링 정책이 포함되어 있습니다.

    > **Important**
    >
    > AMS Accelerate는 언제든지이 프로필을 업데이트할 수 있으므로이 프로필을 수정하지 마십시오. 변경한 내용은 모두 지워집니다.

  - 이러한 정의를 수정하거나 비활성화하려면 Accelerate 경보 기본 구성 수정 및 섹션을 참조하세요기본 Accelerate 경보 구성 비활성화.
- 사용자 지정 구성 프로필:
  - 이 프로필의 모든 구성은 전적으로 사용자가 관리합니다. 사용자가 명시적으로 요청하지 않는 한 AMS Accelerate는이 프로필을 덮어쓰지 않습니다.
  - 이 프로파일에서 원하는 사용자 지정 경보 정의를 지정할 수 있으며 AMS Accelerate 관리형 기본 구성에 대한 수정을 지정할 수도 있습니다. 자세한 내용은 Accelerate 경보 기본 구성 수정 및 기본 Accelerate 경보 구성 비활성화 섹션을 참조하세요.
  - 이 프로필을 업데이트하면 경보 관리자는 AWS 계정의 모든 관련 리소스에 변경 사항을 자동으로 적용합니다.
  - AWS Management Console 또는 AWS CLI/SDK 도구를 사용하여이 프로파일을 업데이트할 수 있습니다. 구성 업데이트에 대한 지침은 AWS AppConfig 사용 설명서를 참조하세요.
  - 사용자 지정 프로필은 처음에는 비어 있지만 프로필 문서에 배치된 모든 경보 정의는 기본 구성 외에도 적용됩니다.

Alarm Manager에서 생성한 모든 CloudWatch 경보에는 태그 키 ams:alarm-manager:managed 및 태그 값이 true로 포함됩니다. 이는 경보 관리자가 생성한 경보만 관리하고 자체 경보를 방해하지 않도록

하기 위한 것입니다. Amazon CloudWatch ListTagsForResource API를 사용하여 이러한 태그를 볼 수 있습니다.

> **Important**
>
> 사용자 지정 경보 정의와 기본 경보 정의가 동일한 ConfigurationID로 지정된 경우(참조구성 프로파일 가속화: 모니터링), 사용자 지정 정의가 기본 규칙보다 우선합니다.

Accelerate Alarm Manager 시작하기

기본적으로 AMS Accelerate로 온보딩하면 구성이에 배포되어 리소스에 대한 경보 기준이 AWS AppConfig정의됩니다. 경보 정의는 ams:rt:* 태그가 있는 리소스에만 적용됩니다. 이러한 태그는를 사용하여 적용하는 것이 좋습니다리소스 태거 가속화. AMS Accelerate에 관리하려는 리소스를 알리기 위해 기본 리소스 태거 구성을 설정합니다.

Resource Tagger를 사용하여 AMS Accelerate가 모니터링할 리소스에 태그 키 ams:rt:ams-managedwith tag value true를 적용합니다.

다음은 모든 Amazon EC2 인스턴스에 대한 모니터링을 옵트인하는 데 사용할 수 있는 Resource Tagger 사용자 지정 프로파일의 예입니다. 일반 정보는 단원을 참조하십시오리소스 태거 가속화.

```
{
    "AWS::EC2::Instance": {
        "AMSManageAllEC2Instances": {
            "Enabled": true,
            "Filter": {
                "InstanceId": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

이 Resource Tagger 구성을 적용하는 방법에 대한 자세한 내용은 섹션을 참조하세요Resource Tagger 구성 보기 또는 변경.

경보 관리자 태그 가속화

기본적으로 AMS Accelerate로 온보딩하면 구성이에 배포되어 리소스에 대한 경보 기준이 AWS AppConfig정의됩니다. 경보 정의는 ams:rt:* 태그가 있는 리소스에만 적용됩니다. 이러한 태그는를 사용하여 적용하는 것이 좋습니다리소스 태거 가속화. AMS Accelerate에 관리하려는 리소스를 알리기 위해 기본 리소스 태거 구성을 설정합니다.

Resource Tagger를 사용하여 AMS Accelerate가 모니터링할 리소스에 태그 키 ams:rt:ams-managedwith tag value true를 적용합니다.

주제

- Resource Tagger를 사용하여 태그 가속화
- Resource Tagger 없이 태그 가속화
- 를 사용하여 태그 가속화 CloudFormation
- Terraform을 사용하여 태그 가속화

Resource Tagger를 사용하여 태그 가속화

태그 기반 경보 관리자는 리소스당 CloudWatch 경보의 수명 주기를 관리하지만 관리형 리소스에는 AMS Accelerate에서 정의한 특정 태그가 있어야 합니다. Resource Tagger를 사용하여 Linux 및 Windows 기반 인스턴스 모두에 기본 AMS 관리형 경보 세트를 적용하려면 다음 단계를 따르세요.

1. 계정 내에서 AppConfig 콘솔로 이동합니다.
2. ResourceTagger 애플리케이션을 선택합니다.
3. 구성 프로필 탭을 선택한 다음 CustomerManagedTags 선택합니다.
4. 생성을 클릭하여 새 프로필을 생성합니다.
5. JSON을 선택하고 구성을 정의합니다. 필터 및 플랫폼 정의에 대한 자세한 예는 섹션을 참조하세요리소스 태거 가속화.

```
{
"AWS::EC2::Instance": {
   "MonitorAllInstances": {
       "Enabled": true,
       "Filter": {
           "Platform": "*"
       },
       "Tags": [
```

```
            {
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }
        ]
    }
}
}
```

6. 호스팅 구성 버전 생성을 클릭합니다.
7. 배포 시작을 클릭합니다.
8. 다음 배포 세부 정보를 정의합니다.

```
Environment: AMSInfrastructure Hosted configuration version: <Select the version
 that you have just created>
               Deployment Strategy: AMSNoBakeDeployment
```

9. 배포 시작을 클릭합니다.

인스턴스에 태그`"ams:rt:ams-managed": "true"`가 지정되어 추가 `"ams:rt:ams-monitoring-policy": "ams-monitored"` 및 `"ams:rt:ams-monitoring-policy-platform": "ams-monitored-linux"`가 인스턴스에 적용되도록 합니다. 그러면 이러한 태그로 인해 인스턴스에 적절한 경보가 생성됩니다. 이 프로세스에 대한 자세한 내용은 Accelerate의 모니터링 단원을 참조하십시오.

Himanshu의 비디오를 보고 자세히 알아보기(11:04)

Resource Tagger 없이 태그 가속화

태그 기반 경보 관리자는 리소스당 CloudWatch 경보의 수명 주기를 관리하지만 관리형 리소스에는 AMS Accelerate에서 정의한 특정 태그가 있어야 합니다. AMS Accelerate는 Resource Tagger에서 태그가 적용되었다고 가정하는 기본 구성 프로파일을 제공합니다.

Resource Tagger가 아닌 또는 Terraform과 같은 CloudFormation 리소스에 태그를 적용하는 대체 방법을 사용하려면 리소스에 태그를 적용하지 않고 선택한 태그 지정 방법과 경쟁하도록 Resource Tagger를 비활성화해야 합니다. 사용자 지정 Resource Tagger 구성 프로필을 변경하여 읽기 전용 모드를 활성화하는 방법에 대한 지침은 섹션을 참조하세요Resource Tagger의 리소스 수정 방지.

Resource Tagger를 읽기 전용 모드로 설정하고 구성 프로파일을 배포한 후 선택한 태그 지정 방법을 사용하여 다음 지침에 따라 리소스에 태그를 적용합니다.

리소스 유형	태그 키	태그 값
지원되는 모든 리소스(이 표에 설명됨)	ams:rt:ams-monitoring-policy	ams-monitored
EC2 인스턴스(Linux)	ams:rt:ams-monitoring-policy-platform	ams-monitored-linux
EC2 인스턴스(Windows)	ams:rt:ams-monitoring-policy-platform	ams-monitored-windows
KMS를 사용하는 OpenSearch 도메인	ams:rt:ams-monitoring-with-kms	ams-monitored-with-kms
전용 마스터 노드가 있는 OpenSearch 도메인	ams:rt:ams-monitoring-with-master	ams-monitored-with-master

이러한 태그 키와 값이 있는 리소스는 AMS Accelerate Alarm Manager에서 관리합니다.

를 사용하여 태그 가속화 CloudFormation

> **Note**
>
> 를 사용하여 태그를 적용하기 전에 먼저 Resource Tagger를 읽기 전용 모드로 설정했는지 확인합니다. CloudFormation그렇지 않으면 Resource Tagger가 구성 프로파일을 기반으로 태그를 수정할 수 있습니다. Resource Tagger를 읽기 전용 모드로 설정하는 방법과 자체 태그 제공에 대한 지침은 섹션을 참조하세요Resource Tagger 없이 태그 가속화.

를 사용하여 태그를 적용하려면 스택 수준(CloudFormation 리소스 태그 참조) 또는 개별 리소스 수준(예: EC2 인스턴스 태그 생성 참조)에서 태그를 적용할 CloudFormation수 있습니다. EC2

다음은에서 관리하는 Amazon EC2 인스턴스에 AMS Accelerate 경보 관리 태그를 적용하는 방법의 예입니다 CloudFormation.

```
Type: AWS::EC2::Instance
Properties:
 InstanceType: "t3.micro"
```

```
 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

다음은 AMS Accelerate 경보 관리 태그를에서 관리하는 Auto Scaling 그룹에 적용하는 방법의 예입니다 CloudFormation. Auto Scaling 그룹은 자체적으로 생성된 Amazon EC2 인스턴스에 태그를 전파합니다.

```
Type: AWS::AutoScaling::AutoScalingGroup
Properties:
 AutoScalingGroupName: "TestASG"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Terraform을 사용하여 태그 가속화

> **Note**
>
> 를 사용하여 태그를 적용하기 전에 먼저 Resource Tagger를 읽기 전용 모드로 설정해야 합니다. CloudFormation그렇지 않으면 Resource Tagger가 구성 프로파일을 기반으로 태그를 수정할 수 있습니다. Resource Tagger를 읽기 전용 모드로 설정하는 방법과 자체 태그 제공에 대한 지침은 섹션을 참조하세요Resource Tagger 없이 태그 가속화.

Terraform을 사용하여 리소스 태그를 관리하는 방법에 대한 설명은 Terraform 설명서 Resource Tagging을 참조하세요.

다음은 Terraform에서 관리하는 Amazon EC2 인스턴스에 AMS Accelerate 경보 관리 태그를 적용하는 방법의 예입니다.

```
resource "aws_instance" "test_linux_instance" {
```

```
    # ...ami and other properties...

    instance_type = "t3.micro"

    tags = {
      "aws:rt:ams-monitoring-policy" = "ams-monitored"
      "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
    }
  }
```

다음은 Terraform에서 관리하는 Auto Scaling 그룹에 AMS 경보 관리 태그를 적용하는 방법의 예입니다. Auto Scaling 그룹은 태그를 자신이 생성한 EC2 인스턴스로 전파합니다.

```
resource "aws_autoscaling_group" "test_asg" {
name = "terraform-test"
# ...other properties...

tags = {
  "aws:rt:ams-monitoring-policy" = "ams-monitored"
  "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
}
}
```

경보 관리자 구성 프로파일 가속화

계정이 AMS Accelerate에 온보딩되면 구성 프로필이라고 하는 두 개의 JSON 문서가 AWS AppConfig를 사용하여 계정에 배포됩니다(What is AWS AppConfig 참조). 두 프로필 문서는 모두 경보 관리자 애플리케이션과 AMS Accelerate 인프라 환경에 있습니다.

주제

- 구성 프로파일 가속화: 모니터링
- 구성 프로파일 가속화: 가상 파라미터 대체
- 경보 구성 가속화 예제
- Accelerate Alarm Manager 구성 보기
- Accelerate 경보 구성 변경
- Accelerate 경보 기본 구성 수정
- Accelerate 경보 구성 변경 사항 배포

- Accelerate 경보 변경 사항 롤백
- Accelerate 경보 유지
- 기본 Accelerate 경보 구성 비활성화

구성 프로파일 가속화: 모니터링

기본 구성 프로필 문서와 사용자 지정 구성 프로필 문서 모두 동일한 구조를 따릅니다.

```
  {
    "<ResourceType>": {
        "<ConfigurationID>": {
            "Enabled": true,

            "Tag": {
                "Key": "...",
                "Value": "..."
            },
            "AlarmDefinition": {
                ...
            }
        },
        "<ConfigurationID>": {
            ...
        }
    },
    "<ResourceType>": {
        ...
    }
}
```

- ResourceType:이 키는 지원되는 다음 문자열 중 하나여야 합니다. 이 JSON 객체 내의 구성은 지정된 AWS 리소스 유형과만 관련이 있습니다. 지원되는 리소스 유형:

```
AWS::EC2::Instance
AWS::EC2::Instance::Disk
AWS::RDS::DBInstance
AWS::Elasticsearch::Domain
AWS::OpenSearch::Domain
AWS::Redshift::Cluster
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup
```

```
AWS::ElasticLoadBalancing::LoadBalancer
AWS::FSx::FileSystem::ONTAP
AWS::FSx::FileSystem::ONTAP::Volume
AWS::FSx::FileSystem::Windows
AWS::EFS::FileSystem
AWS::EC2::NatGateway
AWS::EC2::VPNConnection
```

- ConfigurationID:이 키는 프로파일에서 고유해야 하며 다음 구성 블록의 이름을 고유하게 지정해야 합니다. 기본 프로필에 지정된 것과 동일한 ConfigurationID를 사용자 지정 프로필에 지정하면 사용자 지정 프로필에 정의된 구성 블록이 적용됩니다.
  - 활성화됨: (선택 사항, default=true) 구성 블록을 적용할지 여부를 지정합니다. 구성 블록을 비활성화하려면 false로 설정합니다. 비활성화된 구성 블록은 프로파일에 없는 것처럼 동작합니다.
  - 태그:이 경보 정의가 적용되는 태그를 지정합니다. 이 태그 키와 값이 있는 모든 리소스(적절한 리소스 유형)에는 지정된 정의로 생성된 CloudWatch 경보가 있습니다. 이 필드는 다음 필드가 있는 JSON 객체입니다.
    - 키: 일치시킬 태그의 키입니다. Resource Tagger를 사용하여 리소스에 태그를 적용하는 경우 태그의 키는 항상 ams:rt:로 시작합니다.
    - 값: 일치시킬 태그의 값입니다.
  - AlarmDefinition: 생성할 경보를 정의합니다. 필드가 CloudWatch `PutMetricAlarm` API 호출에 있는 그대로 전달되는 JSON 객체입니다(의사파라미터 제외, 자세한 내용은 참조구성 프로파일 가속화: 가상 파라미터 대체). 필요한 필드에 대한 자세한 내용은 PutMetricAlarm 설명서를 참조하세요.

    또는

    CompositeAlarmDefinition: 생성할 복합 경보를 정의합니다. 복합 경보를 생성할 때 생성한 다른 경보의 경보 상태를 고려하는 경보에 대한 규칙 표현식을 지정합니다. 필드가 있는 그대로에 전달되는 JSON 객체입니다`CloudWatchPutCompositeAlarm`. 복합 경보는 규칙의 모든 조건이 충족되는 경우에만 ALARM 상태로 전환됩니다. 복합 경보의 규칙 표현식에 지정된 경보에는 지표 경보 및 기타 복합 경보가 포함될 수 있습니다. 필요한 필드에 대한 자세한 내용은 PutCompositeAlarm 설명서를 참조하세요.

    두 옵션 모두 다음 필드를 제공합니다.

    - AlarmName: 리소스에 대해 생성하려는 경보의 이름을 지정합니다. 이 필드에는 PutMetricAlarm 설명서에 지정된 것과 동일한 규칙이 모두 있습니다. 하지만 경보 이름은 리전에서 고유해야 하므로 경보 관리자에는 한 가지 추가 요구 사항이 있습니다. 경보 이름에 고유 식별자 의사파라미터를 지정해야 합니다(그렇지 않으면 경보 관리자가 경보 이름 앞에 리

소스의 고유 식별자를 추가함). 예를 들어 AWS::EC2::Instance 리소스 유형의 경우 경보 이름${EC2::InstanceId}에를 지정해야 합니다. 그렇지 않으면 경보 이름 시작 부분에 암시적으로 추가됩니다. 식별자 목록은 섹션을 참조하세요구성 프로파일 가속화: 가상 파라미터 대체.

다른 모든 필드는 PutMetricAlarm 또는 PutCompositeAlarm 설명서에 지정된 것과 같습니다.

- AlarmRule:이 복합 경보의 상태를 확인하기 위해 평가할 다른 경보를 지정합니다. 참조하는 각 경보에 대해 CloudWatch에 존재하거나 계정의 경보 관리자 구성 프로필에 지정되어야 합니다.

> **Important**
>
> Alarm Manager 구성 문서에서 AlarmDefinition 또는 CompositeAlarmDefinition을 지정할 수 있지만 둘 다 동시에 사용할 수는 없습니다.

다음 예제에서 시스템은 두 개의 지정된 지표 경보가 임계값을 초과할 때 경보를 생성합니다.

```
{
  "AWS::EC2::Instance": {
    "LinuxResourceAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:mylinuxinstance",
        "Value": "true"
      },
      "CompositeAlarmDefinition": {
        "AlarmName": "${EC2::InstanceId} Resource Usage High",
        "AlarmDescription": "Alarm when a linux EC2 instance is using too much CPU and
 too much Disk",
        "AlarmRule": "ALARM(\"${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}\") AND ALARM(\"${EC2::InstanceId}: CPU Too High\")"
      }
    }
  }
}
```

> **Important**
>
> 경보 관리자가 구성 중단으로 인해 경보를 생성하거나 삭제할 수 없는 경우 Direct-Customer-Alerts SNS 주제로 알림을 보냅니다. 이 경보를 AlarmDependencyError라고 합니다.

이 SNS 주제에 대한 구독을 확인하는 것이 좋습니다. 주제에 게시된 메시지를 수신하려면 엔드포인트에서 주제를 구독해야 합니다. 자세한 내용은 1단계: 주제 생성을 참조하세요.

> **Note**
>
> 이상 탐지 경보가 생성되면 경보 관리자는 지정된 지표에 필요한 이상 탐지 모델을 자동으로 생성합니다. 이상 탐지 경보가 삭제되면 경보 관리자는 연결된 이상 탐지 모델을 삭제하지 않습니다.
> Amazon CloudWatch는 특정 리전에서 보유할 수 있는 이상 탐지 모델의 수를 제한합니다. AWS 모델 할당량을 초과하면 경보 관리자는 새 이상 탐지 경보를 생성하지 않습니다. 사용하지 않는 모델을 삭제하거나 AMS 파트너와 협력하여 한도 증가를 요청해야 합니다.
> AMS Accelerate에서 제공하는 많은 기준 경보 정의에는 SNS 주제인 MMS-Topic이 대상으로 나열됩니다. 이는 AMS Accelerate 모니터링 서비스에서 사용하기 위한 것이며 경보 알림이 AMS Accelerate에 도달하기 위한 전송 메커니즘입니다. 서비스는 알 수 없는 경보를 무시하므로 MMS-Topic을 기준에 제공된 경보(및 동일한 경보의 재정의) 이외의 경보의 대상으로 지정하지 마십시오. 이로 인해 AMS Accelerate가 사용자 지정 경보에 대해 작동하지 않습니다.

구성 프로파일 가속화: 가상 파라미터 대체

구성 프로필 중 하나에서 다음과 같이 대체되는 가상파라미터를 지정할 수 있습니다.

- 글로벌 - 프로필의 모든 위치:
  - ${AWS::AccountId}: AWS 계정 ID로 대체됨
  - ${AWS::Partition}: 리소스의 파티션이에 있는 것으로 대체되었습니다(대부분 AWS 리전 의 경우 'aws'). AWS 리전자세한 내용은 ARN 참조의 파티션 항목을 참조 하세요.
  - ${AWS::Region}: 리소스가 배포된 리전의 리전 이름으로 대체됨(예: us-east-1)
- AWS::EC2::Instance 리소스 유형 블록에서:
  - ${EC2::InstanceId}: (식별자)가 Amazon EC2 인스턴스의 인스턴스 ID로 대체되었습니다.
  - ${EC2::InstanceName}: Amazon EC2 인스턴스의 이름으로 대체됩니다. 인스턴스 이름이 정의되지 않은 경우 Amazon EC2 인스턴스의 인스턴스 ID로 대체합니다.
- AWS::EC2::Instance::Disk 리소스 유형 블록에서:
  - ${EC2::InstanceId}: (identifier) Amazon EC2 인스턴스의 인스턴스 ID로 대체됩니다.
  - ${EC2::InstanceName}: Amazon EC2 인스턴스의 이름으로 대체됩니다. 인스턴스 이름이 정의되지 않은 경우 Amazon EC2 인스턴스의 인스턴스 ID로 대체합니다.

  - ${EC2::Disk::Device}: 디스크 이름으로 대체됩니다. (Linux만 해당, CloudWatch 에이전트에서 관리하는 인스턴스의 경우).
  - ${EC2::Disk::FSType}: 디스크의 파일 시스템 유형으로 대체됩니다. (Linux만 해당, CloudWatchAgent에서 관리하는 인스턴스의 경우).
  - ${EC2::Disk::Path}: 디스크 경로로 대체됩니다. (Windows만 해당, CloudWatch Agent에서 관리하는 인스턴스에서만 드라이브 레이블(예: c:/)입니다.)
  - ${EC2::Disk::UUID}: (identifier) 디스크를 고유하게 식별하는 생성된 UUID로 대체되며, AWS::EC2::Instance::Disk 리소스 유형에 따라 경보가 볼륨당 하나의 경보를 생성하므로 경보 이름에 지정해야 합니다. ${EC2::Disk::UUID}를 지정하면 경보 이름의 고유성이 유지됩니다.
- AWS::OpenSearch::Domain 리소스 유형 블록에서:
  - ${OpenSearch::DomainName}: (식별자)가 OpenSearch 도메인의 이름으로 대체되었습니다.
- AWS::Elasticsearch::Domain 리소스 유형 블록에서:
  - ${Elasticsearch::DomainName}: (식별자)가 Elasticsearch 도메인의 이름으로 대체되었습니다.
- AWS::ElasticLoadBalancing::LoadBalancer 리소스 유형 블록에서:
  - ${ElasticLoadBalancing::LoadBalancer::Name}: (식별자)가 V1 Load Balancer의 이름으로 대체되었습니다.
- AWS::ElasticLoadBalancingV2::LoadBalancer 리소스 유형 블록에서:
  - ${ElasticLoadBalancingV2::LoadBalancer::Arn}: V2 Load Balancer의 ARN으로 대체됩니다.
  - ${ElasticLoadBalancingV2::LoadBalancer}: V2 Load Balancer의 ARN으로 대체됩니다.
  - ${ElasticLoadBalancingV2::LoadBalancer::Name}: (식별자)가 V2 Load Balancer의 이름으로 대체되었습니다.
  - ${ElasticLoadBalancingV2::LoadBalancer::FullName}: V2 Load Balancer의 전체 이름으로 대체됩니다.
- AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup 리소스 유형 블록에서:
  - ${ElasticLoadBalancingV2::TargetGroup::FullName}: (식별자)가 V2 Load Balancer의 대상 그룹 이름으로 대체되었습니다.
  - ${ElasticLoadBalancingV2::TargetGroup::UUID}: (식별자)가 V2 Load Balancer 대해 생성된 UUID로 대체되었습니다.
  - ${ElasticLoadBalancingV2::LoadBalancer::FullName}: V2 Load Balancer의 전체 이름으로 대체됩니다.
- AWS::EC2::NatGateway 리소스 유형 블록에서:
  - ${NatGateway::NatGatewayId}: (식별자)가 NAT 게이트웨이 ID로 대체되었습니다.

- AWS::RDS::DBInstance 리소스 유형 블록에서:
  - ${RDS::DBInstanceIdentifier}: (식별자)가 RDS DB 인스턴스 식별자로 대체되었습니다.
- AWS::Redshift::Cluster 리소스 유형 블록에서:
  - ${Redshift::ClusterIdentifier}: (identifier)가 Redshift 클러스터 식별자로 대체되었습니다.
- AWS::EC2::VPNConnection 리소스 유형 블록에서:
  - ${AWS::EC2::VpnConnectionId}: (식별자)가 VPN ID로 대체되었습니다.
- AWS::EFS::FileSystem 리소스 유형 블록에서:
  - ${EFS::FileSystemId}: (식별자) EFS 파일 시스템의 파일 시스템 ID로 대체됩니다.
- AWS::FSx::FileSystem::ONTAP 리소스 유형 블록에서:
  - ${FSx::FileSystemId}: (식별자) FSX 파일 시스템의 파일 시스템 ID로 대체됩니다.
  - ${FSx::FileSystem::Throughput}: FSX 파일 시스템의 처리량으로 대체됩니다.
  - ${FSx::FileSystem::Iops}: FSX 파일 시스템의 IOPS로 대체됩니다.
- AWS::FSx::FileSystem::ONTAP::Volume 리소스 유형 블록에서:
  - ${FSx::FileSystemId}: (식별자) FSX 파일 시스템의 파일 시스템 ID로 대체됩니다.
  - ${FSx::ONTAP::VolumeId}: (식별자) 볼륨 ID로 대체됩니다.
- AWS::FSx::FileSystem::Windows 리소스 유형 블록에서:
  - ${FSx::FileSystemId}: (식별자) FSX 파일 시스템의 파일 시스템 ID로 대체됩니다.
  - ${FSx::FileSystem::Throughput}: FSX 파일 시스템의 처리량으로 대체됩니다.

> **Note**
>
> 식별자로 표시된 모든 파라미터는 경보 이름에 해당 식별자를 지정하지 않는 한 생성된 경보 이름의 접두사로 사용됩니다.

경보 구성 가속화 예제

다음 예제에서 시스템은 일치하는 Linux 인스턴스에 연결된 각 디스크에 대해 경보를 생성합니다.

```
{
    "AWS::EC2::Instance::Disk": {
        "LinuxDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mylinuxinstance",
```

```
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "disk_used_percent",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "device",
                        "Value": "${EC2::Disk::Device}"
                    },
                    {
                        "Name": "fstype",
                        "Value": "${EC2::Disk::FSType}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

다음 예제에서 시스템은 일치하는 Windows 인스턴스에 연결된 각 디스크에 대해 경보를 생성합니다.

```
{
     "AWS::EC2::Instance::Disk": {
        "WindowsDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mywindowsinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "LogicalDisk % Free Space",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
```

```
                    },
                    {
                        "Name": "objectname",
                        "Value": "LogicalDisk"
                    },
                    {
                        "Name": "instance",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

Accelerate Alarm Manager 구성 보기

AMSManagedAlarms와 CustomerManagedAlarms는 AppConfig GetConfiguration에서 검토할 수 있습니다.

다음은 `GetConfiguration` 호출의 예입니다.

```
aws appconfig get-configuration --application AMSAlarmManager --environment
 AMSInfrastructure --configuration AMSManagedAlarms --client-id
      any-string outfile.json
```

- 애플리케이션: 기능을 제공하는 AppConfig의 논리적 단위입니다. 경보 관리자의 경우이 단위는 입니다. `AMSAlarmManager`
- 환경: AMSInfrastructure 환경입니다.
- 구성: AMS Accelerate 기준 경보를 보려면 값은 이고, 고객 경보 정의를 `AMSManagedAlarms`보려면 구성은 입니다. `CustomerManagedAlarms`
- 클라이언트 ID: 모든 문자열이 될 수 있는 고유한 애플리케이션 인스턴스 식별자입니다.
- 경보 정의는 지정된 출력 파일에서 볼 수 있으며,이 경우 다음과 같습니다. `outfile.json`

AMSInfrastructureenvironment에서 과거 배포를 확인하여 계정에 배포된 구성 버전을 확인할 수 있습니다.

Accelerate 경보 구성 변경

새 경보 정의를 추가하거나 업데이트하려면 구성 문서를 배포CloudFormation 를 사용하여 구성 변경 가속화 배포하거나 CreateHostedConfigurationVersion API를 호출할 수 있습니다.

이는 AppConfig CLI 명령이 기대하는 base64에서 파라미터 값을 생성하는 Linux 명령줄 명령입니다. 자세한 내용은 AWS CLI 설명서 Binary/Blob(Binary Large Object)을 참조하세요.

예를 들면 다음과 같습니다.

```
aws appconfig create-hosted-configuration-version --application-id application-id --
configuration-profile-id configuration-profile-id --content base64-string
      --content-type application/json
```

- 애플리케이션 ID: 애플리케이션 AMS AlarmManager의 ID입니다. ListApplications API 직접 호출을 통해 이를 확인할 수 있습니다.
- 구성 프로필 ID: CustomerManagedAlarms 구성의 ID입니다. ListConfigurationProfiles API 직접 호출을 통해 확인할 수 있습니다.
- 콘텐츠: 문서를 생성하고 baseBase64로 인코딩하여 생성할 콘텐츠의 Base64 문자열: cat alarms-v2.json | base64(Binary/Blob(Binary Large Object) 참조).

  콘텐츠 유형: 경보 정의는 JSON으로 작성`application/json`되므로 MIME 유형입니다.

> **Important**
>
> 대상에 새 구성을 배포하는 경우의 책임과 결과를 이해하는 신뢰할 수 있는 사용자로 Start Deployment 및 StopDeployment API 작업에 대한 액세스를 제한합니다.

AWS AppConfig 기능을 사용하여 구성을 생성하고 배포하는 방법에 대한 자세한 내용은 AWS AppConfig 작업을 참조하세요.

Accelerate 경보 기본 구성 수정

기본 구성 프로필은 수정할 수 없지만 기본 구성 블록과 동일한 ConfigurationID를 사용하여 사용자 지정 프로필에 구성 블록을 지정하여 기본값에 대한 재정의를 제공할 수 있습니다. 이렇게 하면 전체 구성 블록이 태그 지정 구성을 적용할 기본 구성 블록을 덮어씁니다.

예를 들어 다음과 같은 기본 구성 프로파일을 고려합니다.

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 5,
                ...
            }
        }
    }
}
```

이 경보의 임계값을 10으로 변경하려면 변경하려는 부분뿐만 아니라 전체 경보 정의를 제공해야 합니다. 예를 들어 다음과 같은 사용자 지정 프로필을 제공할 수 있습니다.

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
```

```
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 10,
                ...
            }
        }
    }
}
```

> **Important**
>
> 구성 변경 사항을 적용한 후에는 배포해야 합니다. SSM AppConfig에서는 구성을 생성한 후 새 버전의 구성을 배포해야 합니다.

Accelerate 경보 구성 변경 사항 배포

사용자 지정을 완료한 후에는 AppConfig 또는를 사용하여 배포해야 합니다 CloudFormation.

주제

- AppConfig를 사용하여 경보 구성 변경 가속화 배포
- CloudFormation 를 사용하여 구성 변경 가속화 배포

AppConfig를 사용하여 경보 구성 변경 가속화 배포

사용자 지정이 완료되면 AppConfig를 사용하여 StartDeployment로 변경 사항을 배포합니다.

```
  aws appconfig start-deployment --application-id application_id
   --environment-id environment_id Vdeployment-strategy-id
   deployment_strategy_id --configuration-profile-id configuration_profile_id --
configuration-version 1
```

- 애플리케이션 ID: 애플리케이션의 IDAMSAlarmManager로 ListApplications API 직접 호출을 통해 찾을 수 있습니다.
- 환경 ID: ListEnvironments API 직접 호출을 통해 찾을 수 있습니다.
- 배포 전략 ID: ListDeploymentStrategies API 직접 호출을 통해 이를 찾을 수 있습니다.

- 구성 프로필 ID:의 IDCustomerManagedAlarms입니다. ListConfigurationProfiles API 직접 호출을 통해 이를 찾을 수 있습니다.
- 구성 버전: 배포할 구성 프로필의 버전입니다.

> **Important**
>
> Alarm Manager는 구성 프로필에 지정된 대로 경보 정의를 적용합니다. 또는 CloudWatch CLI/SDK를 AWS Management Console 사용하여 CloudWatch 경보를 수동으로 수정하면 자동으로 되돌려지므로 경보 관리자를 통해 변경 사항을 정의해야 합니다. 경보 관리자가 생성하는 경보를 이해하려면 값이 인 `ams:alarm-manager:managed` 태그를 찾을 수 있습니다`true`. 새 구성을 대상에 배포할 때의 책임과 결과를 이해하는 신뢰할 수 있는 사용자로 StartDeployment 및 StopDeployment API 작업에 대한 액세스를 제한합니다.

AWS AppConfig 기능을 사용하여 구성을 생성하고 배포하는 방법에 대한 자세한 내용은 AWS AppConfig 설명서를 참조하세요.

CloudFormation 를 사용하여 구성 변경 가속화 배포

를 사용하여 `CustomerManagedAlarms` 구성 프로필을 배포하려는 경우 다음 CloudFormation 템플릿을 사용할 CloudFormation수 있습니다. `AMSAlarmManagerConfigurationVersion.Content` 필드에 원하는 JSON 구성을 입력합니다.

스택 또는 CloudFormation 스택 세트에 템플릿을 배포하면 구성에 필요한 JSON 형식을 따르지 않으면 `AMSResourceTaggerDeployment` 리소스 배포가 실패합니다. 예상 형식에 대한 구성 프로파일 가속화: 모니터링 자세한 내용은 섹션을 참조하세요.

이러한 템플릿을 CloudFormation 스택 또는 스택 세트로 배포하는 방법에 대한 도움말은 아래 관련 AWS CloudFormation 설명서를 참조하세요.

- AWS CloudFormation 콘솔에서 스택 생성
- AWS CLI를 사용하여 스택 생성
- 스택 세트 생성

> **Note**
>
> 이러한 템플릿 중 하나를 사용하여 구성 버전을 배포한 다음 CloudFormation 스택/스택 세트를 삭제하면 템플릿 구성 버전이 현재 배포된 버전으로 유지되고 추가 배포가 이루어지지 않습니

다. 기본 구성으로 되돌리려면 스택을 삭제하는 대신 수동으로 빈 구성(예: {})을 배포하거나 스택을 빈 구성으로 업데이트해야 합니다.

JSON

```
{
  "Description": "Custom configuration for the AMS Alarm Manager.",
  "Resources": {
    "AMSAlarmManagerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "Content": "{}",
        "ContentType": "application/json"
      }
    },
    "AMSAlarmManagerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSAlarmManagerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-EnvironmentId"
        }
      }
```

```
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Alarm Manager.
Resources:
  AMSAlarmManagerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      Content: |
        {

        }
      ContentType: application/json
  AMSAlarmManagerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      ConfigurationVersion:
        !Ref AMSAlarmManagerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-Alarm-Manager-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-Alarm-Manager-Configuration-EnvironmentId
```

Accelerate 경보 변경 사항 롤백

이전 구성 프로필 버전을 지정하고 StartDeployment를 실행하여 동일한 배포 메커니즘을 통해 경보 정의를 롤백할 수 있습니다.

Accelerate 경보 유지

AMS에서 모니터링하는 리소스가 삭제되면 해당 리소스에 대해 Alarm Manager에서 생성한 모든 경보가 Alarm Manager에서 자동으로 삭제됩니다. 감사, 규정 준수 또는 기록 목적으로 특정 경보를 유지해야 하는 경우 경보 관리자 보존 태그 지정 기능을 사용합니다.

모니터링되는 리소스가 삭제된 후에도 경보를 유지하려면 다음 예제와 같이 경보의 사용자 지정 구성에 `"ams:alarm-manager:retain"` 태그를 추가합니다.

```
{
  "AWS::EC2::Instance": {
    "AMSCpuAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:ams-monitoring-policy",
        "Value": "ams-monitored"
      },
      "AlarmDefinition": {
        "AlarmName": "${EC2::InstanceId}: CPU Too High",
        "AlarmDescription": "AMS Baseline Alarm for EC2 CPUUtilization",
        [...]
        "Tags": [
          {
            "Key": "ams:alarm-manager:retain",
            "Value": "true"
          }
        ]
      }
    }
  }
}
```

`"ams:alarm-manager:retain"` 태그로 구성된 경보는 모니터링되는 리소스가 종료될 때 경보 관리자에 의해 자동으로 삭제되지 않습니다. 보관된 경보는 CloudWatch를 사용하여 수동으로 제거할 때까지 CloudWatch에서 무기한 유지됩니다.

기본 Accelerate 경보 구성 비활성화

AMS Accelerate는 기준 경보를 기반으로 계정에 기본 구성 프로파일을 제공합니다. 그러나이 기본 구성은 경보 정의를 재정의하여 비활성화할 수 있습니다. 사용자 지정 구성 프로필에서 규칙의 ConfigurationID를 재정의하고 활성화된 필드를 false 값으로 지정하여 기본 구성 규칙을 비활성화할 수 있습니다.

예를 들어 기본 구성 프로필에 다음 구성이 있는 경우:

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                ...
            }
        }
    }
```

사용자 지정 구성 프로필에 다음을 포함하여이 태그 지정 규칙을 비활성화할 수 있습니다.

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": false
        }
    }
}
```

이러한 변경을 수행하려면 CreateHostedConfigurationVersion API를 JSON 프로파일 문서와 함께 호출하고(참조Accelerate 경보 구성 변경) 이후에 배포해야 합니다(참조Accelerate 경보 구성 변경 사항 배포). 새 구성 버전을 생성할 때 이전에 생성한 사용자 지정 경보도 JSON 프로파일 문서에 포함해야 합니다.

> **Important**
>
> AMS Accelerate가 기본 구성 프로파일을 업데이트하면 구성된 사용자 지정 경보에 대해 보정되지 않으므로 사용자 지정 구성 프로파일에서 기본 경보를 재정의할 때 기본 경보에 대한 변경 사항을 검토합니다.

Accelerate에 대한 추가 CloudWatch 경보 생성

Amazon EC2 인스턴스에 대한 사용자 지정 CloudWatch 지표 및 경보를 사용하여 AMS Accelerate에 대한 추가 CloudWatch 경보를 생성할 수 있습니다.

애플리케이션 모니터링 스크립트와 사용자 지정 지표를 생성합니다. 예제 스크립트에 대한 자세한 내용과 액세스는 Amazon EC2 Linux 인스턴스의 메모리 및 디스크 지표 모니터링을 참조하세요.

Linux Amazon EC2 인스턴스에 대한 CloudWatch 모니터링 스크립트는 사용자 지정 CloudWatch 지표를 생성하고 사용하는 방법을 보여줍니다. 이 예제는 Linux 인스턴스에 대한 메모리, 스왑 및 디스크 공간 사용률 측정치를 보고하는 완벽하게 작동하는 예로 구성된 Perl 스크립트입니다.

> **Important**
>
> AMS Accelerate는 사용자가 생성한 CloudWatch 경보를 모니터링하지 않습니다.

알림의 AMS 자동 문제 해결

확인 후 AWS Managed Services(AMS)는이 섹션에 설명된 특정 조건 및 프로세스에 따라 특정 알림을 자동으로 해결합니다.

알림 이름	설명	Thresholds	작업
상태 확인 실패	가능한 하드웨어 장애 또는 인스턴스의 장애 상태입니다.	시스템에서 지난 15분 이내에 한 번 이상 실패 상태를 감지했습니다.	AMS 자동 수정은 먼저 인스턴스에 액세스할 수 있는지 확인합니다. 인스턴스에 액세스할 수 없는 경우 인스턴스가 중지되고 다시 시작됩니다. 중지 및 시작을 사용하면 인스턴스가 새 기본 하드웨어로 마이그레이션할 수 있습니다. 자세한 내용은 “EC2 상태 확인 실패 수정 자동화” 섹션을 참조하세요.

알림 이름	설명	Thresholds	작업
AMSLinuxDiskUsage	EC2 인스턴스에서 1개의 탑재 지점(볼륨에 지정된 공간)의 디스크 사용량이 가득 차면 트리거됩니다.	임계값이 지난 30분 동안 정의된 값을 6회 초과합니다.	AMS 자동 수정은 먼저 임시 파일을 삭제합니다. 이렇게 해도 충분한 디스크 공간이 확보되지 않으면 볼륨이 가득 차면 가동 중지를 방지하기 위해 볼륨이 확장됩니다.
AMSWindowsDiskUsage	EC2 인스턴스에서 1개의 탑재 지점(볼륨에 지정된 공간)의 디스크 사용량이 채워지는 경우.	임계값이 지난 30분 동안 정의된 값을 6회 초과합니다.	AMS 자동 수정은 먼저 임시 파일을 삭제합니다. 이렇게 해도 충분한 디스크 공간이 확보되지 않으면 볼륨이 가득 차면 가동 중지를 방지하기 위해 볼륨이 확장됩니다.

알림 이름	설명	Thresholds	작업
RDS-EVENT-0089	DB 인스턴스가 할당된 스토리지의 90% 이상을 사용하였습니다.	스토리지가 90% 이상 할당되었습니다.	AMS 자동 수정은 먼저 DB가 수정 가능하고 사용 가능하거나 스토리지가 가득 찬 상태인지 확인합니다. 그런 다음 CloudFormation 변경 세트를 통해 할당된 스토리지, IOPS 및 스토리지 처리량을 늘리려고 시도합니다. 스택 드리프트가 이미 감지된 경우 가동 중지 시간을 방지하기 위해 RDS API로 돌아갑니다. RDS DB 인스턴스에 다음 태그를 추가하여이 기능을 옵트아웃할 수 있습니다. `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

알림 이름	설명	Thresholds	작업
RDS-EVENT-0007	DB 인스턴스에 할당된 스토리지가 소진되었습니다. 해결하려면 추가 스토리지를 할당합니다.	스토리지는 100% 할당됩니다.	AMS 자동 수정은 먼저 DB가 수정 가능하고 사용 가능하거나 스토리지가 가득 찬 상태인지 확인합니다. 그런 다음 CloudFormation 변경 세트를 통해 할당된 스토리지, IOPS 및 스토리지 처리량을 늘리려고 시도합니다. 스택 드리프트가 이미 감지된 경우 가동 중지 시간을 방지하기 위해 RDS API로 돌아갑니다. RDS DB 인스턴스에 다음 태그를 추가하여이 기능을 옵트아웃할 수 있습니다. `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

알림 이름	설명	Thresholds	작업
RDS-EVENT-0224	요청된 할당된 스토리지가 구성된 최대 스토리지 임계값에 도달하거나 초과합니다.	DB 인스턴스의 최대 스토리지 임계값이 소진되었거나 요청된 할당된 스토리지보다 크거나 같습니다.	AMS 자동 수정은 먼저 요청된 양의 RDS 스토리지가 최대 스토리지 임계값을 위반하는지 확인합니다. 확인되면 AMS는 CloudFormation 변경 세트를 사용하여 최대 스토리지 임계값을 30% 늘리거나 CloudFormation을 통해 리소스가 프로비저닝되지 않은 경우 RDS API를 직접 늘리려고 시도합니다. RDS DB 인스턴스에 다음 태그를 추가하여이 기능을 옵트아웃할 수 있습니다. `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

알림 이름	설명	Thresholds	작업
RDS-Storage-Capacity	DB 인스턴스에 할당된 스토리지에 1GB 미만이 남아 있습니다.	스토리지는 99% 할당됩니다.	AMS 자동 수정은 먼저 DB가 수정 가능하고 사용 가능하거나 스토리지가 가득 찬 상태인지 확인합니다. 그런 다음 CloudFormation 변경 세트를 통해 할당된 스토리지, IOPS 및 스토리지 처리량을 늘리려고 시도합니다. 스택 드리프트가 이미 감지된 경우 가동 중지 시간을 방지하기 위해 RDS API로 돌아갑니다. RDS DB 인스턴스에 다음 태그를 추가하여이 기능을 옵트아웃할 수 있습니다. `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

알림 이름	설명	Thresholds	작업
AMSFSXONTAPVolumeCapacityUtilization	Amazon FSx for NetApp ONTAP 볼륨이 기본 할당 스토리지(80%)보다 많이 소비되었습니다.	FSx for ONTAP 볼륨 용량 사용률은 2시간 동안 80%를 초과합니다(기본값).	AMS 자동 수정은 먼저 볼륨 수명 주기 상태가 수정 가능한 상태인지 확인한 다음 파일 시스템 최대 용량을 확인하면서 볼륨 크기를 10% 확장합니다. 파일 시스템에 볼륨 확장을 위한 충분한 스토리지 용량이 없는 경우 볼륨과 파일 시스템이 함께 확장됩니다. 이 확장은 7일 기간 내에 최대 3회로 제한됩니다. AMS Automation이 확장하는 최대 스토리지 제한은 5120GiB입니다. **Note** 볼륨 위에 iSCSI LUN이 구성된 경우 운영 체제 수준에서 iSCSI LUN을 확장합니다. 자세한 내용은 FSx for ONTAP LUN이 읽기 전용 모드인 이유를 참조하세요.

EC2 상태 확인 실패: 수정 자동화 참고 사항

AMS 자동 수정이 EC2 상태 확인 실패 문제와 함께 작동하는 방식:

- Amazon EC2 인스턴스에 연결할 수 없는 경우 인스턴스를 중지했다가 다시 시작해야 새 하드웨어로 마이그레이션하고 복구할 수 있습니다.
- 문제의 루트가 OS 내에 있는 경우(fstab에서 디바이스 누락, 커널 손상 등) 자동화가 인스턴스를 복구할 수 없습니다.
- 인스턴스가 Auto Scaling 그룹에 속하는 경우 자동화는 아무 작업도 수행하지 않습니다. AutoScalingGroup 조정 작업은 인스턴스를 대체합니다.
- 인스턴스에 EC2 Auto Recovery가 활성화된 경우 문제 해결은 조치를 취하지 않습니다.

EC2 볼륨 사용량 수정 자동화

AWS Managed Services(AMS) 자동 수정이 EC2 볼륨 사용 문제와 함께 작동하는 방식:

- 자동화는 먼저 볼륨 확장이 필요한지 여부와 볼륨 확장을 수행할 수 있는지 확인합니다. 확장이 적절한 것으로 간주되는 경우 자동화를 통해 볼륨 용량을 늘릴 수 있습니다. 이 자동화된 프로세스는 성장의 필요성과 제어되고 제한된 확장의 균형을 맞춥니다.
- 볼륨을 확장하기 전에 자동화는 인스턴스에서 정리 작업(Windows: Disk Cleaner, Linux: Logrotate + Simple Service Manager 에이전트 로그 제거)을 수행하여 공간을 확보하려고 시도합니다.

> **Note**
>
> 정리 작업은 지속적인 기능을 위해 CPU 크레딧에 의존하기 때문에 EC2 "T" 패밀리 인스턴스에서 실행되지 않습니다.

- Linux에서는 자동화가 EXT2, EXT3, EXT4 및 XFS 유형의 파일 시스템 확장만 지원합니다.
- Windows에서는 자동화가 NTFS(New Technology File System) 및 ReFS(Resilient File System)만 지원합니다.
- 자동화는 논리적 볼륨 관리자(LVM) 또는 RAID 배열의 일부인 볼륨을 확장하지 않습니다.
- 자동화는 인스턴스 스토어 볼륨을 확장하지 않습니다.
- 영향을 받는 볼륨이 이미 2TiB보다 큰 경우 자동화는 조치를 취하지 않습니다.
- 자동화를 통한 확장은 시스템 수명 주기 동안 일주일에 최대 3회, 총 5회로 제한됩니다.
- 이전 확장이 지난 6시간 이내에 발생한 경우 자동화는 볼륨을 확장하지 않습니다.

이러한 규칙으로 인해 자동화가 조치를 취할 수 없는 경우 AMS는 아웃바운드 서비스 요청을 통해 사용자에게 연락하여 수행할 다음 조치를 결정합니다.

Amazon RDS 스토리지 부족 이벤트 수정 자동화

AWS Managed Services(AMS) 자동 수정이 Amazon RDS 스토리지 부족 이벤트 문제와 작동하는 방식:

- Amazon RDS 인스턴스 스토리지를 확장하기 전에 자동화는 여러 검사를 수행하여 Amazon RDS 인스턴스가 수정 가능하고 사용 가능한 상태인지 또는 스토리지 가득 참 상태인지 확인합니다.
- CloudFormation 스택 드리프트가 감지되면 Amazon RDS API를 통해 수정이 이루어집니다.
- 트리거 이벤트에 따라 문제 해결은 속성 , `MaxAllocatedStorage`, `Iops`또는 `AllocatedStorage`를 수정합니다`StorageThroughput`. 다른 Amazon RDS 인스턴스 속성은 수정되지 않습니다. 자세한 내용은 DB 인스턴스 설정을 참조하세요.
- 다음 시나리오에서는 문제 해결 작업이 실행되지 않습니다.
  - Amazon RDS 인스턴스 상태가 "사용 가능" 또는 "스토리지 가득 참"이 아닙니다.
  - Amazon RDS 인스턴스 스토리지는 현재 수정할 수 없습니다(예: 지난 6시간 동안 스토리지가 수정된 경우).
  - Amazon RDS 인스턴스에 오토 스케일링 스토리지가 활성화되어 있습니다.
- 문제 해결은 6시간마다 1회 확장으로 제한되며 14일 동안 최대 3회 확장으로 제한됩니다.
- 이러한 시나리오가 발생하면 AMS는 아웃바운드 인시던트를 통해 사용자에게 연락하여 다음 조치를 결정합니다.

ONTAP 볼륨 용량 수정 자동화

AWS Managed Services(AMS) 자동 수정이 ONTAP 볼륨 용량 문제와 작동하는 방식:

- 볼륨을 확장하기 전에 자동화는 볼륨 수명 주기 상태가 수정 가능한 상태인지 확인합니다.
- 자동화는 파일 시스템 최대 용량을 확인하면서 볼륨 크기를 10% 확장합니다.
- 파일 시스템에 볼륨 확장을 수용하기에 충분한 스토리지 용량이 없는 경우 볼륨 및 파일 시스템 용량이 모두 확장됩니다.
- 수정은 7일 기간 내에 3개 이하의 업데이트로 제한됩니다.
- AMS Automation이 확장하는 최대 스토리지 제한은 5120GiB입니다.
- 볼륨 위에 iSCSI LUN이 구성된 경우 자동 수정이 완료된 후 OS 수준에서 iSCSI LUN을 수동으로 확장해야 합니다. 자세한 내용은 FSx for ONTAP LUN이 읽기 전용 모드인 이유를 참조하세요.

AMS에서 Amazon EventBridge 관리형 규칙 사용

AMS Accelerate는 Amazon EventBridge 관리형 규칙을 사용합니다. 관리형 규칙은 AMS에 직접 연결된 고유한 유형의 규칙입니다. 이러한 규칙은 수신 이벤트를 일치시키고 처리를 위해 대상으로 전송합니다. 관리형 규칙은 AMS에서 사전 정의하며 서비스에서 고객 계정을 관리하는 데 필요한 이벤트 패턴을 포함합니다. 달리 정의되지 않은 한 소유 서비스만 이러한 관리형 규칙을 활용할 수 있습니다.

AMS Accelerate 관리형 규칙은 `events.managedservices.amazonaws.com` 서비스 보안 주체에 연결됩니다. 이러한 관리형 규칙은 AWSServiceRoleForManagedServices_Events 서비스 연결 역할을 통해 관리됩니다. 이러한 규칙을 삭제하려면 고객의 특별 확인이 필요합니다. 자세한 내용은 AMS에 대한 관리형 규칙 삭제를 참조하세요.

규칙에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 규칙을 참조하세요.

AMS에서 배포한 Amazon EventBridge 관리형 규칙

Amazon EventBridge 관리형 규칙

규칙 이름	설명	정의

AmsAccessRolesRule	이 규칙은 특정 AMS Accelerate 역할 및 정책의 수정 사항을 수신합니다.	<pre>{
		"source": ["aws.iam"],
		"detail-type": ["AWS API Call via CloudTrail"],
		"detail": {
		"eventName": [
		"DeleteRole",
		"DeletePolicy",
		"CreatePolicyVersion",
		"AttachRolePolicy",
		"DetachRolePolicy"
		],
		"requestParameters": {
		"$or": [
		{
		"roleName": [
		"ams-access-admin",
		"ams-access-admin-operations",
		"ams-access-operations",
		"ams-access-read-only",
		"ams-access-security-analyst",</pre>

규칙 이름	설명	정의

```
                    "ams-access-security-analyst-
read-only"
                ]
            },
            {
                "policyArn": [
                    "arn:*:iam::*:policy/ams-ac
cess-allow-pass-role",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-cloudshell-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-operations-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-update-iam-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-ssr-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-read-only-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-extended-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-operations-policy"
                ]
            },
          ]
        },
   },
}
```

규칙 이름	설명	정의

AMSCoreRule	이 규칙은 AWS Config 및 Amazon CloudWatch 이벤트를 AMS Config 문제 해결 및 AMS 모니터링 서비스에 정중하게 전달합니다. AWS Config 이벤트는 AWS Systems Manager OpsItems. Amazon CloudWatch 이벤트는 CloudWatch 경보를 모니터링합니다.	<pre>{
		    {
		        "source": ["aws.config", "aws.cloudwatch"],
		        "detail-type": ["Config Rules Compliance Change", "CloudWatch Alarm State Change"],
		    }
		}</pre>

AMS에 대한 관리형 규칙 생성

Amazon EventBridge 관리형 규칙을 수동으로 생성할 필요가 없습니다. AWS 관리 콘솔 AWS CLI, 또는 AWS API에서 AMS에 온보딩하면 AMS가 사용자를 대신하여 AMS를 생성합니다.

AMS에 대한 관리형 규칙 편집

AMS에서는 관리형 규칙을 편집할 수 없습니다. 각 관리형 규칙의 이름 및 이벤트 패턴은 AMS에서 사전 정의됩니다.

AMS에 대한 관리형 규칙 삭제

관리형 규칙을 수동으로 삭제할 필요가 없습니다. AWS 관리 콘솔, AWS CLI또는 AWS API의 AMS에서 오프보드하면 AMS가 리소스를 정리하고 AMS가 소유한 모든 관리형 규칙을 삭제합니다.

AMS가 오프보딩 중에 관리형 규칙을 제거하지 못하는 경우 Amazon EventBridge 콘솔, AWS CLI 또는 AWS API를 사용하여 관리형 규칙을 수동으로 삭제할 수도 있습니다. 이렇게 하려면 먼저 AMS에서 오프보드하고 관리형 규칙을 강제로 삭제해야 합니다.

AMS의 신뢰할 수 있는 수정자

Trusted Remediator는 AWS Trusted Advisor, AWS Security Hub CSPM및 AWS Compute Optimizer 권장 사항의 문제 해결을 자동화하는 AWS Managed Services 솔루션입니다. Trusted Remediator는 Security Hub CSPM 및 Compute Optimizer가 비용을 절감하거나 Trusted Advisor, 시스템 가용성을 개선하거나, 성능을 최적화하거나,의 보안 격차를 좁힐 수 있는 기회를 나타낼 때 권장 사항을 생성합니다 AWS 계정. Trusted Remediator를 사용하면 확립된 모범 사례를 사용하는 안전하고 표준화된 방식으로 이러한 보안, 성능, 비용 최적화, 내결함성 및 서비스 제한 권장 사항을 해결할 수 있습니다. Trusted Remediator를 사용하면 문제 해결 솔루션을 구성할 수 있으며 생성한 일정에 따라 자동으로 실행되므로 문제 해결 프로세스가 간소화됩니다. 이 간소화된 접근 방식은 수동 개입 없이 일관되고 효율적으로 문제를 해결합니다.

신뢰할 수 있는 교정기 주요 이점

다음은 Trusted Remediator의 주요 이점입니다.

- 보안, 성능 및 비용 최적화 개선: 신뢰할 수 있는 해결 방법을 사용하면 계정의 전반적인 보안 태세를 강화하고, 리소스 사용률을 최적화하고, 운영 비용을 절감할 수 있습니다.
- 셀프 서비스 설정 및 구성: 요구 사항 및 기본 설정에 맞게 신뢰할 수 있는 수정자를 구성할 수 있습니다.
- 자동 Trusted Advisor 검사, Security Hub CSPM 제어 및 AWS Compute Optimizer 권장 사항 수정: 구성 후 신뢰할 수 있는 수정자는 선택한 검사에 대한 수정 작업을 자동으로 실행합니다. 이 자동화를 사용하면 수동 개입이 필요하지 않습니다.
- 모범 사례 구현: 해결 작업은 확립된 모범 사례를 기반으로 하므로 표준화되고 효과적인 방식으로 문제를 해결합니다.
- 예약된 실행: day-to-day 운영 워크플로에 맞는 수정 일정을 선택할 수 있습니다.

Trusted Remediator를 사용하면 AWS 환경에서 식별된 문제를 사전에 해결할 수 있으므로 모범 사례를 준수하고 안전하고 성능이 뛰어나며 비용 효율적인 클라우드 인프라를 유지할 수 있습니다.

신뢰할 수 있는 수정자 작동 방식

다음은 신뢰할 수 있는 수정자 워크플로의 그림입니다.

Trusted Remediator는 Trusted Advisor에 대한 Security Hub CSPM 및 Compute Optimizer 권장 사항을 평가하고 OpsCenter AWS Systems Manager OpsItems를 AWS 계정 생성합니다. 그런 다음 Trusted Remediator 자동화 문서를 사용하여 OpsItems를 자동으로 또는 수동으로 수정할 수 있습니다. 다음은 각 문제 해결 유형에 대한 세부 정보입니다.

- 자동 수정: 신뢰할 수 있는 수정자가 자동화 문서를 실행하고 실행을 모니터링합니다. 자동화 문서가 완료되면 Trusted Remediator가 Opsitem을 해결합니다.
- 수동 수정: 신뢰할 수 있는 수정자는 검토할 수 있도록 OpsItem을 생성합니다. 검토 후 자동화 문서를 시작합니다.

수정 로그는 Amazon S3 버킷에 저장됩니다. S3 버킷의 데이터를 사용하여 보고를 위한 사용자 지정 빠른 대시보드를 구축할 수 있습니다. 또한 AMS는 신뢰할 수 있는 수정자에 대한 요청 시 보고서를 제공합니다. 이러한 보고서를 받으려면 CSDM에 문의하십시오. 자세한 내용은 신뢰할 수 있는 수정자 보고서 단원을 참조하십시오.

신뢰할 수 있는 문제 해결사의 주요 용어

다음은 AMS에서 신뢰할 수 있는 교정기를 사용할 때 알아야 할 유용한 용어입니다.

- AWS Trusted Advisor, AWS Security Hub and AWS Compute Optimizer:에서 제공하는 클라우드 최적화 서비스 AWS. Trusted Advisor, Security Hub CSPM 및 Compute Optimizer는 환경을 검사 AWS 하고 다음 6가지 범주의 모범 사례를 기반으로 권장 사항을 제공합니다.
  - 비용 최적화
  - 성능
  - 보안
  - 내결함성
  - 운영 우수성
  - 서비스 한도

자세한 내용은 , 및 AWS Trusted Advisor AWS Security Hub 단원을 참조하십시오AWS Compute Optimizer.

- 신뢰할 수 있는 해결사: Trusted Advisor 검사, AWS Security Hub CSPM 권장 사항 및 AWS Compute Optimizer 권장 사항을 위한 AMS 문제 해결 솔루션입니다. Trusted Remediator를 사용하면 보안, 성능을 개선하고 비용을 절감하기 위해 알려진 모범 사례를 사용하여 Trusted Advisor 검사, Security Hub CSPM 제어 및 Compute Optimizer 권장 사항을 안전하게 해결할 수 있습니다. Trusted Remediator는 설정 및 구성이 쉽습니다. 를 한 번 구성하면 Trusted Remediator가 원하는 일정(매일 또는 매주)에 따라 문제 해결을 실행합니다.
- AWS Systems Manager SSM 문서:가 AWS 리소스에서 AWS Systems Manager 수행하는 작업을 정의하는 JSON 또는 YAML 파일입니다. SSM 문서는 여러 AWS 리소스 및 인스턴스에서 운영 작업을 자동화하는 선언적 사양 역할을 합니다.
- AWS Systems Manager OpsCenter OpsItem: 환경의 운영 문제를 추적하고 해결하는 데 도움이 되는 클라우드 운영 문제 관리 리소스입니다 AWS . OpsItems는 AWS 서비스 및 리소스 전반의 운영 데이터 및 문제에 대한 중앙 집중식 보기 및 관리 시스템을 제공합니다. 각 OpsItem은 잠재적 보안 위험, 성능 문제 또는 운영 인시던트와 같은 운영 문제를 나타냅니다.
- 구성: 구성은의 AWS AppConfig기능인에 저장된 속성 집합입니다 AWS Systems Manager. 의 Trusted Remediator 애플리케이션은 계정 수준에서 문제 해결을 구성하는 데 AWS AppConfig 도움이 됩니다. AWS AppConfig 콘솔 또는 API를 사용하여 구성을 편집할 수 있습니다.
- 실행 모드: 실행 모드는 Compute Optimizer 및 Security Hub CSPM의 각 Trusted Advisor 검사 결과 및 권장 사항에 대한 문제 해결을 실행하는 방법을 결정하는 구성 속성입니다. 자동, 수동, 조건부, 비활성의 네 가지 실행 모드가 지원됩니다.
- 리소스 재정의:이 기능은 리소스 태그를 사용하여 특정 리소스에 대한 구성을 재정의합니다.
- 수정 항목 로그: 신뢰할 수 있는 수정자 수정 S3 로그 버킷의 로그 파일입니다. 문제 해결 항목 로그는 문제 해결 OpsItems 생성될 때 생성됩니다. 이 로그 파일에는 수동 실행 수정 OpsItems 및 자동 실행 수정 OpsItems. 이 로그 파일을 사용하여 모든 문제 해결 항목을 추적합니다.
- 자동 문제 해결 실행 로그: 신뢰할 수 있는 문제 해결자 문제 해결 S3 로그 버킷의 로그 파일입니다. SSM 문서 자동 실행이 완료되면 자동 문제 해결 실행 로그가 생성됩니다. 이 로그에는 자동 실행 문제 해결 OpsItems. 이 로그 파일을 사용하여 자동 문제 해결을 추적합니다.

AMS에서 신뢰할 수 있는 문제 해결사 시작하기

신뢰할 수 있는 수정자는 추가 비용 없이 AMS에서 사용할 수 있습니다. Trusted Remediator는 단일 계정 및 다중 계정 구성을 지원합니다.

신뢰할 수 있는 해결사에 온보딩

AMS 계정을 Trusted Remediator에 온보딩하려면 Cloud Architects 또는 Cloud Service Delivery Manager(CSDMs에 이메일을 보내십시오. 이메일 본문에 다음 정보를 포함합니다.

- AWS 계정: 12자리 계정 식별 번호입니다. 신뢰할 수 있는 해결자에게 온보딩하려는 모든 계정은 동일한 Accelerate 고객에게 속해야 합니다.
  - 위임된 관리자 계정: 단일 또는 여러 계정에 대한 Trusted Advisor Compute Optimizer 및 Security Hub CSPM 검사 구성에 사용되는 계정입니다.
  - 멤버 계정: 위임된 관리자 계정에 연결된 계정입니다. 이러한 계정은 위임된 관리자 계정에서 구성을 상속합니다. 하나의 멤버 계정 또는 여러 개의 멤버 계정을 가질 수 있습니다.

    > **Note**
    >
    > 멤버 계정은 위임된 관리자 계정에서 구성을 상속합니다. 특정 계정에 대해 다른 구성이 필요한 경우 원하는 구성으로 여러 위임된 관리자 계정을 온보딩합니다. 온보딩하기 전에 Cloud Architects와 함께 계정 구조와 구성을 계획합니다.

- AWS 리전: 리소스가 AWS 리전 있는 입니다. 목록은 AWS 서비스 리전별 단원을 AWS 리전참조하십시오.
- 해결 일정 및 시간: 선호하는 해결 일정(일별 또는 주별). Trusted Remediator는 Trusted Advisor 검사를 수집하고 예약된 시간에 문제 해결을 시작합니다. 예를 들어 매주 일요일 오전 1시에 대한 수정 일정을 호주 동부 표준시로 설정할 수 있습니다.
- 알림 이메일: Trusted Remediator는 알림 이메일을 사용하여 문제 해결 시 매일 알려줍니다. 알림 이메일 제목은 "신뢰할 수 있는 해결 방법 수정 요약"이며 콘텐츠는 지난 24시간 동안 실행된 신뢰할 수 있는 해결 방법에 대한 정보를 제공합니다.

> **Note**
>
> 예약된 모든 문제 해결 후 애플리케이션과 리소스를 검토합니다. 추가 지원이 필요한 경우 AMS에 문의하십시오.

필수 세부 정보가 포함된 온보딩 요청을 CA 또는 CSDM에 제출하면 AMS가 신뢰할 수 있는 해결자에게 계정을 온보딩합니다. Trusted Remediator는의 기능 AWS AppConfig인 AWS Systems Manager를 사용하여 Trusted Advisor 검사에 대한 구성을 정의합니다. 이러한 구성은에 저장된 속성 집합입니다 AWS AppConfig. 리소스에 대한 무단 요금을 방지하기 위해 계정이 신뢰할 수 있는 해결자에게 온보딩

되면 지원되는 모든 Trusted Advisor 검사가 비활성으로 설정됩니다. 온보딩 후 AWS AppConfig 콘솔 또는 API를 사용하여 구성을 관리할 수 있습니다. 이러한 구성을 통해 특정 Trusted Advisor 검사를 자동으로 수정하거나 나머지 검사를 평가하고 수동으로 수정할 수 있습니다. 구성은 사용자 지정이 가능하므로 각 Trusted Advisor 검사에 구성을 적용할 수 있습니다. 자세한 내용은 신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성 단원을 참조하십시오.

수정할 검사 및 권장 사항 선택

기본적으로 수정 실행 모드는 구성의 모든 Trusted Advisor 검사, Compute Optimizer 권장 사항 및 Security Hub CSPM 권장 사항에 대해 비활성입니다. 이렇게 하면 무단 수정을 방지하고 리소스를 보호할 수 있습니다. AMS는 Trusted Advisor 검사 문제 해결을 위해 선별된 SSM 자동화 문서를 제공합니다.

신뢰할 수 있는 수정자를 사용하여 수정하려는 검사를 선택하려면 다음 단계를 완료하세요.

1. 지원되는 Trusted Advisor, Compute Optimizer 권장 사항, Security Hub CSPM 권장 사항 및 관련 SSM 자동화 문서의 이름을 검토하여 신뢰할 수 있는 수정자로 수정하려는 점검 및 권장 사항을 결정합니다.
2. 구성을 업데이트하여 선택한 Trusted Advisor 검사, Compute Optimizer 권장 사항 및 Security Hub CSPM 권장 사항에 대한 문제 해결을 활성화합니다. 검사를 선택하는 방법에 대한 지침은 섹션을 참조하세요신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성.

신뢰할 수 있는 수정자에서 수정 사항 추적

계정 수준 구성을 업데이트한 후 신뢰할 수 있는 수정자는 각 수정에 대해 OpsItems 생성합니다. Trusted Remediator는 문제 해결 일정에 따라 OpsItems의 자동 문제 해결을 위해 SSM 문서를 실행합니다. Systems Manager OpsItems 보는 방법에 대한 지침은 섹션을 참조하세요신뢰할 수 있는 수정자에서 문제 해결 추적. OpsCenter

신뢰할 수 있는 수정자에서 수동 수정 실행

Compute Optimizer 및 Security Hub CSPM의 Trusted Advisor 검사 및 권장 사항을 수동으로 수정할 수 있습니다. 수동 수정을 시작하면 신뢰할 수 있는 수정자가 수동 실행 OpsItem을 생성합니다. OpsItems을 수정하려면 SSM 자동화 문서를 검토하고 시작해야 합니다. 자세한 내용은 신뢰할 수 있는 수정자에서 수동 수정 실행 단원을 참조하십시오.

Trusted Remediator에서 지원하는 Compute Optimizer 권장 사항

다음 표에는 지원되는 Compute Optimizer 권장 사항, SSM 자동화 문서, 사전 구성된 파라미터 및 자동화 문서의 예상 결과가 나열되어 있습니다. 검사 문제 해결을 위해 SSM 자동화 문서를 활성화하기 전에 비즈니스 요구 사항에 따라 가능한 위험을 이해하는 데 도움이 되는 예상 결과를 검토하세요.

문제 해결을 활성화하려는 지원되는 검사에 대해 각 Compute Optimizer 검사에 해당하는 구성 규칙이 있는지 확인합니다. 자세한 내용은 Trusted Advisor 검사 옵트인을 참조 AWS Compute Optimizer 하세요.

최적화 옵션	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
규모 조정		
Amazon EC2 인스턴스 권장 사항	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation Compute Optimizer 권장 사항에 따라 Amazon EC2 인스턴스 유형이 업데이트되었습니다. 옵션이 있는 경우 동일한 플랫폼 파라미터(아키텍처, 하이퍼바이저, 네트워크 인터페이스, 가상화 유형 등)를 유지하면서 가장 최적의 옵션을 선택합니다.	• MinimumDaysSinceLastChange: 마지막 인스턴스 유형 변경 이후 최소 일수를 지정하는 파라미터입니다. 기본값은 7일입니다. 제약 조건 없음 • CreateAMIBeforeResize: 크기를 조정하기 전에 인스턴스 AMI를 백업으로 생성하려면를 'true'로 설정합니다. 백업을 생성하지 않으려면를 'false'로 설정합니다. 기본값은 'true'입니다. 제약 조건 없음
Amazon EBS 볼륨 권장 사항	AWSManagedServices-ModifyEBSVolume Amazon EBS 볼륨은 Compute Optimizer 권장 사항에 따라 수정됩니다. 수정에는 볼륨 유형, 크기, IOPS, 볼륨 생성(gp2, gp3 등)이 포함될 수 있습니다.	• CreateSnapshot: 볼륨을 수정하기 전에 스냅샷을 생성하려면를 'true'로 설정합니다. 스냅샷을 생성하지 않으려면를 'false'로 설정합니다. 기본값은 'true'입니다. 제약 조건 없음

최적화 옵션	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		• VolumeType: 원하는 볼륨 유형입니다. 유형을 지정하지 않으면 기존 유형이 유지됩니다. 제약 조건 없음 • VolumeSize: 원하는 볼륨 크기로, GiB 단위입니다. 대상 볼륨 크기는 볼륨의 기존 크기보다 크거나 같아야 합니다. 크기를 지정하지 않으면 기존 크기가 유지됩니다. 제약 조건 없음 • Iops: 요청된 초당 I/O 작업 수(IOPS). 이 파라미터는 io1, io2 및 gp3 볼륨에만 유효합니다. 제약 조건 없음 • 처리량: 볼륨에 프로비저닝할 처리량으로, 최대 1,000MiB/s입니다. 이 파라미터는 gp3 볼륨에만 유효합니다. 제약 조건 없음 • RemediateStackDrift: 드리프트 수정을 시작하려면 볼륨 수정으로 인해 드리프트가 발생하는 경우 'true'로 설정합니다. 드리프트 수정을 시도하지 않으려면를 'false'로 설정합니다. 기본값은 'true'입니다. 제약 조건 없음

최적화 옵션	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Lambda 함수 권장 사항	AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory AWS Lambda Compute Optimizer 권장 사항에 따라 함수 메모리 최적화.	RecommendedMemorySize: 권장 옵션과 다른 경우 사용자 지정 메모리 크기입니다. 제약 조건 없음
유휴 리소스		
유휴 Amazon EBS 볼륨	AWSManagedServices-DeleteUnusedEBSVolume 연결되지 않은 Amazon EBS 볼륨이 삭제됩니다.	• CreateSnapshot: 볼륨을 삭제하기 전에 스냅샷을 생성하려면를 'true'로 설정합니다. 스냅샷을 생성하지 않으려면를 'false'로 설정합니다. 기본값은 'true'입니다. 제약 조건 없음 • MinimumUnattachedDays: 삭제할 Amazon EBS 볼륨의 연결되지 않은 최소 일수, 최대 62일. 기본값은 7입니다. 제약 조건 없음
유휴 Amazon EC2 인스턴스	AWSManagedServices-StopEC2Instance 유휴 Amazon EC2 인스턴스가 중지됩니다.	ForceStopWithInstanceStore: 인스턴스 스토어를 사용하는 인스턴스를 강제로 중지하려면를 'true'로 설정합니다. 강제 중지하지 않으려면를 'false'로 설정합니다. 기본값 'false'는 인스턴스 중지를 방지합니다. 제약 조건 없음

최적화 옵션	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
유휴 Amazon RDS 인스턴스	AWSManagedServices-StopIdleRDSInstance 유휴 Amazon RDS 인스턴스를 중지합니다. 지원되는 엔진은 MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL입니다. 이 문서는 Aurora MySQL 및 Aurora PostgreSQL에는 적용되지 않습니다. 인스턴스는 최대 7일까지 중지되고 자동으로 다시 시작됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

Trusted Advisor Trusted Remediator에서 지원하는 검사

다음 표에는 지원되는 Trusted Advisor 검사, SSM 자동화 문서, 사전 구성된 파라미터 및 자동화 문서의 예상 결과가 나열되어 있습니다. 검사 문제 해결을 위해 SSM 자동화 문서를 활성화하기 전에 비즈니스 요구 사항에 따라 가능한 위험을 이해하는 데 도움이 되는 예상 결과를 검토하세요.

문제 해결을 활성화하려는 지원되는 Trusted Advisor 검사에 대해 각 검사에 해당하는 구성 규칙이 있는지 확인합니다. 자세한 내용은 기반 AWS Trusted Advisor 검사 보기를 참조하세요 AWS Config. 검사에 해당 AWS Security Hub CSPM 제어가 있는 경우 Security Hub CSPM 제어가 활성화되어 있는지 확인합니다. 자세한 내용은 Security Hub CSPM에서 제어 활성화를 참조하세요. 미리 구성된 파라미터 관리에 대한 자세한 내용은 Trusted Remediator의 Configure Trusted Advisor check remediation를 참조하세요.

Trusted Advisor Trusted Remediator에서 지원하는 비용 최적화 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Z4AUBRNSmz 연결되지 않은 탄력적 IP 주소	AWSManagedServices-TrustedRemediatorReleaseElasticIP	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
	리소스와 연결되지 않은 탄력적 IP 주소를 해제합니다.	
c18d2gz150 - Amazon EC2 인스턴스 중지됨	AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - 일 수 동안 중지된 Amazon EC2 인스턴스가 종료됩니다.	• CreateAMIBeforeTermination: Amazon EC2 인스턴스를 종료하기 전에 인스턴스 AMI를 백업으로 생성하려면를 선택합니다`true`. 종료하기 전에 백업을 생성하지 않으려면를 선택합니다`false`. 기본값은 `true`입니다. • AllowedDays: 인스턴스가 종료되기 전에 중지된 상태의 일수입니다. 기본값은 30입니다. 제약 조건 없음
c18d2gz128 수명 주기 정책이 구성되지 않은 Amazon ECR 리포지토리	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy 수명 주기 정책이 아직 없는 경우 지정된 리포지토리에 대한 수명 주기 정책을 생성합니다.	ImageAgeLimit: Amazon ECR 리포지토리의 'any' 이미지에 대한 일(1~365) 단위의 최대 수명 제한입니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
DAvU99Dc4C 사용률이 낮은 Amazon EBS 볼륨	AWSManagedServices-DeleteUnusedEBSVolume 지난 7일 동안 볼륨이 연결되지 않은 경우 사용률이 낮은 Amazon EBS 볼륨을 삭제합니다. Amazon EBS 스냅샷은 기본적으로 생성됩니다.	• CreateSnapshot: 로 설정하면 `true`자동화가 삭제되기 전에 Amazon EBS 볼륨의 스냅샷을 생성합니다. 기본 설정은 `true`입니다. 유효한 값은 `true` 및 `false` (대소문자 구분)입니다. • MinimumUnattachedDays: 삭제할 EBS 볼륨의 연결되지 않은 최소 일수, 최대 62일. 로 설정하면 `0`SSM 문서는 연결되지 않은 기간을 확인하지 않고 볼륨이 현재 연결되지 않은 경우 볼륨을 삭제합니다. 기본값은 입니다7. 제약 조건 없음
hjLMh88uM8 유휴 로드 밸런서	AWSManagedServices-DeleteIdleClassicLoadBalancer 사용되지 않고 등록된 인스턴스가 없는 경우 유휴 Classic Load Balancer를 삭제합니다.	IdleLoadBalancerDays: Classic Load Balancer가 유휴 상태로 간주하기 전에 연결을 요청한 일수입니다. 기본값은 7일입니다. 자동 실행이 활성화된 경우 활성 백엔드 인스턴스가 없는 경우 자동화는 유휴 Classic Load Balancer를 삭제합니다. 활성 백엔드 인스턴스가 있지만 정상 백엔드 인스턴스가 없는 모든 유휴 Classic Load Balancer의 경우 자동 문제 해결이 사용되지 않으며 수동 문제 해결을 위한 OpsItems이 생성됩니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Ti39halfu8 Amazon RDS 유휴 DB 인스턴스	AWSManagedServices-StopIdleRDSInstance 지난 7일 동안 유휴 상태였던 Amazon RDS DB 인스턴스가 중지됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
COr6dfpM05 AWS Lambda 메모리 크기에 대한 과다 프로비저닝된 함수	AWSManagedServices-ResizeLambdaMemory AWS Lambda 함수의 메모리 크기가 에서 제공하는 권장 메모리 크기로 조정됩니다 Trusted Advisor.	RecommendedMemorySize: Lambda 함수에 대한 권장 메모리 할당입니다. 값 범위는 128~10240입니다. 자동화가 실행되기 전에 Lambda 함수 크기가 수정된 경우이 자동화에서 권장 값으로 설정을 덮어쓸 수 있습니다 Trusted Advisor.
Qch7DwouX1 낮은 사용률의 Amazon EC2 인스턴스	AWSManagedServices-StopEC2Instance(자동 및 수동 실행 모드 모두에 대한 기본 SSM 문서) 사용률이 낮은 Amazon EC2 인스턴스는 중지됩니다.	ForceStopWithInstanceStore: 인스턴스 스토어를 사용하여 인스턴스를 강제 중지`true`하려면 로 설정합니다. 그렇지 않으면 `false`(으)로 설정합니다. 의 기본값은 인스턴스 중지를 `false` 방지합니다. 유효한 값은 true 또는 false(대소문자 구분)입니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Qch7DwouX1 낮은 사용률의 Amazon EC2 인스턴스	AWSManagedServices-ResizeInstanceByOneLevel Amazon EC2 인스턴스는 동일한 인스턴스 패밀리 유형에서 한 인스턴스 유형 아래로 크기가 조정됩니다. 크기 조정 작업 중에 인스턴스가 중지 및 시작되고 SSM 문서 실행이 완료된 후 초기 상태로 돌아갑니다. 이 자동화는 Auto Scaling 그룹에 있는 인스턴스의 크기 조정을 지원하지 않습니다.	• MinimumDaysSinceLastChange: 마지막 인스턴스 유형 변경 이후 최소 일수입니다. 인스턴스 유형이 지정된 시간 내에 수정된 경우 인스턴스 유형은 변경되지 않습니다. `0`를 사용하여이 검증을 건너뜁니다. 기본값은 7입니다. • CreateAMIBeforeResize: 크기를 조정하기 전에 인스턴스 AMI를 백업으로 생성하려면를 선택합니다`true`. 백업을 생성하지 않으려면를 선택합니다`false`. 기본값은 `false`입니다. 유효한 값은 `true` 및 `false` (대/소문자 구분)입니다. • ResizeIfStopped: 인스턴스가 중지된 상태인 경우에도 인스턴스 크기 변경을 진행하려면를 선택합니다`true`. 중지된 상태인 경우 인스턴스의 크기를 자동으로 조정하지 않으려면를 선택합니다`false`. 유효한 값은 `true` 및 `false` (대소문자 구분)입니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Qch7DwouX1 낮은 사용률의 Amazon EC2 인스턴스	AWSManagedServices-TerminateInstance Auto Scaling 그룹의 일부가 아니고 종료 방지 기능이 활성화되지 않은 경우 활용률이 낮은 Amazon EC2 인스턴스가 종료됩니다. AMI는 기본적으로 생성됩니다.	CreateAMIBeforeTermination: EC2 인스턴스를 종료하기 전에 인스턴스 AMI를 백업으로 생성`false`하려면 이 옵션을 `true` 또는 로 설정합니다. 기본값은 `true`입니다. 유효한 값은 `true` 및 `false` (대/소문자 구분)입니다. 제약 조건 없음
G31sQ1E9U Underutilized Amazon Redshift Clusters	AWSManagedServices-PauseRedshiftCluster Amazon Redshift 클러스터가 일시 중지되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1cj39rr6v Amazon S3 불완전 멀티파트 업로드 중단 구성	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Amazon S3 버킷은 특정 일 후에도 불완전하게 유지되는 멀티파트 업로드를 중단하도록 수명 주기 규칙으로 구성됩니다.	DaysAfterInitiation:Amazon S3가 불완전한 멀티파트 업로드를 중지한 이후의 일수입니다. 기본값은 7일로 설정됩니다. 제약 조건 없음
c1z7kmr00n Amazon EC2 인스턴스 비용 최적화 권장 사항	에서 Amazon EC2 인스턴스 권장 사항 및 유휴 Amazon EC2 인스턴스를 사용합니다Trusted Remediator에서 지원하는 Compute Optimizer 권장 사항.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1z7kmr02n Amazon EBS 볼륨 비용 최적화 권장 사항	의 Amazon EBS 볼륨 권장 사항 및 유휴 Amazon EBS 볼륨을 사용합니다Trusted Remediator에서 지원하는 Compute Optimizer 권장 사항.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c1z7kmr03n DB 인스턴스를 위한 Amazon RDS 비용 최적화 권장 사항	의 유휴 Amazon RDS 인스턴스를 사용합니다Trusted Remediator에서 지원하는 Compute Optimizer 권장 사항.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1z7kmr05n AWS Lambda 함수에 대한 비용 최적화 권장 사항	의 Lambda 함수 권장 사항을 사용합니다Trusted Remediator에서 지원하는 Compute Optimizer 권장 사항.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

Trusted Advisor Trusted Remediator에서 지원하는 보안 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
12Fnkpl8Y5 노출된 액세스 키	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey 노출된 IAM 액세스 키가 비활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 노출된 IAM 액세스 키로 구성된 애플리케이션은 인증할 수 없습니다.
Hs4Ma3G127 - API Gateway REST 및 WebSocket API 실행 로깅을 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: APIGateway.1	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging 실행 로깅은 API 단계에서 활성화됩니다.	LogLevel: 실행 로깅을 활성화하는 로깅 수준 ERROR - 로깅은 오류에 대해서만 활성화됩니다. INFO - 모든 이벤트에 대해 로깅이 활성화됩니다. 실행 로그를 활성화하려면 API Gateway에 계정의 CloudWatch에 로그를 읽고 쓸 수 있는 권한을 부여해야 합니다. 자세한 내용은 API Gateway

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		에서 REST APIs에 대한 CloudWatch 로깅 설정을 참조하세요.
Hs4Ma3G129 - API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: APIGateway.3	AWSManagedServices-EnableApiGateWayXRayTracing X-Ray 추적은 API 단계에서 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G202 - API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다. 해당 AWS Security Hub CSPM 검사: APIGateway.5	AWSManagedServices-EnableAPIGatewayCacheEncryption API Gateway REST API 단계에 캐시가 활성화된 경우 API Gateway REST API 캐시 데이터에 대해 유휴 시 암호화를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G177 - 해당 AWS Security Hub CSPM 검사 - 로드 밸런서와 연결된 Auto Scaling 그룹은 로드 밸런서 상태 확인 AutoScaling.1	AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck Auto Scaling 그룹에 대해 Elastic Load Balancing 상태 확인이 활성화됩니다.	HealthCheckGracePeriod: Auto Scaling이 서비스되는 Amazon Elastic Compute Cloud 인스턴스의 상태를 확인하기 전에 대기하는 초 단위 시간입니다. Auto Scaling 그룹에 연결된 Elastic Load Balancing 로드 밸런서 중 하나라도 비정상으로 보고하면 Elastic Load Balancing 상태 확인을 켜면 실행 중인 인스턴스가 교체될 수 있습니다. 자세한 내용은 Auto Scaling 그룹에 Elastic Load Balancing 로드 밸런서 연결을 참조하세요.
Hs4Ma3G245 - CloudFormation 스택은 Amazon Simple Notification Service와 통합되어야 합니다. 해당 AWS Security Hub CSPM 검사: CloudFormation.1	AWSManagedServices-EnableCFNStackNotification 알림을 위해 CloudFormation 스택을 Amazon SNS 주제와 연결합니다.	NotificationARNs 선택한 CloudFormation 스택과 연결할 Amazon SNS 주제의 ARNs입니다. 자동 수정을 활성화하려면 `NotificationARNs` 사전 구성된 파라미터를 제공해야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G210 - CloudFront 배포에는 로깅이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: CloudFront.2	AWSManagedServices-EnableCloudFrontDistributionLogging Amazon CloudFront 배포에 대해 로깅이 활성화됩니다.	• BucketName: 액세스 로그를 저장할 Amazon S3 버킷의 이름입니다. • S3KeyPrefix: theAmazon CloudFront 배포 로그의 S3 버킷에 있는 위치의 접두사입니다. • IncludeCookies: 액세스 로그에 쿠키를 포함할지 여부를 나타냅니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. • BucketName • S3KeyPrefix • IncludeCookies 이 문제 해결 제약 조건은 CloudFront 배포에 대한 로깅을 켜려면 어떻게 해야 하나요?를 참조하세요.
Hs4Ma3G109 - CloudTrail 로그 파일 검증을 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: CloudTrail.4	AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation CloudTrail 추적 로그 검증을 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G108 - CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다. 해당 AWS Security Hub CSPM 검사: CloudTrail.5	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail 는 CloudWatch Logs와 통합됩니다.	• CloudWatchLogsLogGroupName: CloudTrail 로그가 전달되는 CloudWatch Logs 로그 그룹의 이름입니다. 계정에 있는 로그 그룹을 사용해야 합니다. • CloudWatchLogsRoleName: 사용자의 로그 그룹에 쓰기 위해 맡을 CloudWatch Logs 엔드포인트의 IAM 역할 이름입니다. 계정에 있는 역할을 사용해야 합니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. • CloudWatchLogsLogGroupName • CloudWatchLogsRoleName
Hs4Ma3G217 - CodeBuild 프로젝트 환경에는 로깅 AWS 구성이 있어야 합니다. 해당 AWS Security Hub CSPM 검사: CodeBuild.4	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig CodeBuild 프로젝트에 대한 로깅을 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G306 - Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: DocumentDB.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot Amazon DocumentDB 수동 클러스터 스냅샷에서 퍼블릭 액세스를 제거합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G308 - Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: DocumentDB.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection Amazon DocumentDB 클러스터에 대한 삭제 보호를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G323 - DynamoDB 테이블에 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: DynamoDB.6	AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection 비 AMS DynamoDB 테이블에 대한 삭제 방지를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
ePs02jT06w - Amazon EBS 퍼블릭 스냅샷	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot Amazon EBS 스냅샷에 대한 퍼블릭 액세스가 비활성화되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G118 - VPC 기본 보안 그룹은 인바운드 또는 아웃바운드 트래픽을 허용하지 않아야 합니다. 해당 AWS Security Hub CSPM 검사: EC2.2	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG 기본 보안 그룹의 모든 수신 및 송신 규칙이 제거됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G117 - 연결된 EBS 볼륨은 유휴 시 암호화되어야 합니다. 해당 AWS Security Hub CSPM 검사: EC2.3	AWSManagedServices-EncryptInstanceVolume 인스턴스에 연결된 Amazon EBS 볼륨이 암호화됩니다.	• 볼륨을 암호화하기 위한 KMSKeyId: AWS KMS key ID 또는 ARN입니다. • DeleteStaleNonEncryptedSnapshotBackups: 암호화되지 않은 이전 볼륨의 스냅샷 백업을 삭제할지 여부를 결정하는 플래그입니다. 가 복원에 `false` 도움이 되도록 로 설정된 경우 문제 해결 및 롤백의 일부로 인스턴스`DeleteStaleNonEncryptedSnapshotBackups` 가 재부팅될 수 있습니다.
Hs4Ma3G120 - 중지된 EC2 인스턴스는 지정된 기간 후에 제거해야 합니다. 해당 AWS Security Hub CSPM 검사: EC2.4	AWSManagedServices-TerminateInstance(자동 및 수동 실행 모드 모두에 대한 기본 SSM 문서) 30일 동안 중지된 Amazon EC2 인스턴스는 종료됩니다.	CreateAMIBeforeTermination:. EC2 인스턴스를 종료하기 전에 인스턴스 AMI를 백업으로 생성하려면를 선택합니다`true`. 종료하기 전에 백업을 생성하지 않으려면를 선택합니다`false`. 기본값은 `true`입니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G120 - 중지된 EC2 인스턴스는 지정된 기간 후에 제거해야 합니다. 해당 AWS Security Hub CSPM 검사: EC2.4	AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - Security Hub에 정의된 일수 동안 중지된 Amazon EC2 인스턴스(기본값은 30)가 종료됩니다.	CreateAMIBeforeTermination: EC2 인스턴스를 종료하기 전에 인스턴스 AMI를 백업으로 생성하려면를 선택합니다`true`. 종료하기 전에 백업을 생성하지 않으려면를 선택합니다`false`. 기본값은 `true`입니다. 제약 조건 없음
Hs4Ma3G121 - EBS 기본 암호화를 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: EC2.7	AWSManagedServices-EncryptEBSByDefault Amazon EBS 암호화는 기본적으로 특정에 대해 활성화됩니다. AWS 리전	사전 구성된 파라미터는 허용되지 않습니다. 암호화 기본 제공은 리전별 설정입니다. 리전에 대해 활성화하면 해당 리전의 개별 볼륨 또는 스냅샷에 대해 비활성화할 수 없습니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G124 - Amazon EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다. 해당 AWS Security Hub CSPM 검사: EC2.8	AWSManagedServices-TrustedRemediatorEnableEC2InstanceIMDSv2 Amazon EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용합니다.	• IMDSv1MetricCheckPeriod: CloudWatch에서 IMDSv1 사용량 지표를 분석할 일수(42-455)입니다. Amazon EC2 인스턴스가 지정된 기간 내에 생성된 경우 분석은 인스턴스 생성 날짜부터 시작됩니다. • HttpPutResponseHopLimit: 인스턴스 메타데이터 토큰에 허용되는 최대 네트워크 홉 수입니다. 이 값은 1 및 2 홉 간에 구성할 수 있습니다. 홉 제한은 인스턴스에서 직접 실행되는 프로세스에 대한 토큰 액세스를 1 제한하는 반면, 홉 제한은 인스턴스에서 실행되는 컨테이너에서의 액세스를 2 허용합니다. 제약 조건 없음
Hs4Ma3G207 - EC2 서브넷이 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다. 해당 AWS Security Hub CSPM 검사: EC2.15	AWSManagedServices-UpdateAutoAssignPublicIpv4Addresses VPC 서브넷은 퍼블릭 IP 주소를 자동으로 할당하지 않도록 구성됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G209 - 미사용 네트워크 액세스 제어 목록이 제거됨 해당 AWS Security Hub CSPM 검사: EC2.16	AWSManagedServices-DeleteUnusedNACL 미사용 네트워크 ACL 삭제	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G215 - 미사용 Amazon EC2 보안 그룹은 제거해야 합니다. 해당 AWS Security Hub CSPM 검사: EC2.22	AWSManagedServices-DeleteSecurityGroups 사용하지 않는 보안 그룹을 삭제합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G247 - Amazon EC2 Transit Gateway가 VPC 연결 요청을 자동으로 수락해서는 안 됩니다. 해당 AWS Security Hub CSPM 검사: EC2.23	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach - 지정된 비 AMS Amazon EC2 Transit Gateway에 대한 VPC 연결 요청의 자동 수락을 비활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G235 - ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: ECR.2	AWSManagedServices-TrustedRemediatorSetImageTagImmutability 지정된 리포지토리에 대한 이미지 태그 변경 가능성 설정을 IMMUTABLE로 설정합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G216 - ECR 리포지토리에는 하나 이상의 수명 주기 정책이 구성되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy ECR 리포지토리에는 수명 주기 정책이 구성되어 있습니다.	LifecyclePolicyText: 리포지토리에 적용할 JSON 리포지토리 정책 텍스트입니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. LifecyclePolicyText
Hs4Ma3G325 - EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog EKS 클러스터에 대해 감사 로그가 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G183 - HTTP 헤더를 삭제하도록 애플리케이션 로드 밸런서를 구성해야 합니다. 해당 AWS Security Hub CSPM 검사: ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer가 잘못된 헤더 필드로 구성되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G184 - Application Load Balancer 및 Classic Load Balancer 로깅을 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: ELB.5	AWSManagedServices-EnableELBLogging(자동 및 수동 실행 모드 모두에 대한 기본 SSM 문서) Application Load Balancer 및 Classic Load Balancer 로깅이 활성화되어 있습니다.	• BucketName: 버킷 이름(ARN 아님). 버킷 정책이 로깅을 위해 올바르게 구성되어 있는지 확인합니다. • S3KeyPrefix: Elastic Load Balancing 로그에 대한 Amazon S3 버킷 위치의 접두사입니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. • BucketName • S3KeyPrefix Amazon S3 버킷에는 버킷에 액세스 로그를 쓸 수 있는 권한을 Elastic Load Balancing에 부여하는 버킷 정책이 있어야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G184 - Application Load Balancer 및 Classic Load Balancer 로깅을 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: ELB.5	AWSManagedServices-EnableELBLoggingV2 Application Load Balancer 및 Classic Load Balancer 로깅이 활성화되어 있습니다.	• TargetBucketTagKey: 대상 Amazon S3 버킷을 식별하는 데 사용되는 태그 이름(대소문자 구분)입니다. 와 함께 사용하여 액세스 로깅을 위한 대상 버킷 역할을 할 버킷에 `TargetBucketTagValue` 태그를 지정합니다. • TargetBucketTagValue: 대상 Amazon S3 버킷을 식별하는 데 사용되는 태그 값(대소문자 구분)입니다. 와 함께 사용하여 액세스 로깅을 위한 대상 버킷 역할을 할 버킷에 `TargetBucketTagKey` 태그를 지정합니다. • S3BucketPrefix: Amazon S3 버킷의 접두사(논리적 계층 구조)입니다. 지정하는 접두사에는 문자열 `AWSLogs`가 포함되지 않아야 합니다. 자세한 내용은 접두사를 사용한 객체 구성을 참조하세요. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix Amazon S3 버킷에는 버킷에 액세스 로그를 쓸 수 있는 권한을 Elastic Load Balancing에 부여하는 버킷 정책이 있어야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G326 - Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: EMR.2	AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess 계정에 대해 Amazon EMR 퍼블릭 액세스 차단 설정이 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G135 - AWS KMS 키를 실수로 삭제해서는 안 됩니다. 해당 AWS Security Hub CSPM 검사: KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS 키 삭제가 취소되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G299 - Amazon DocumentDB 수동 클러스터 스냅샷은 퍼블릭이어서는 안 됩니다. 해당 AWS Security Hub CSPM 검사: Neptune.4	AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection Amazon Neptune 클러스터에 대한 삭제 보호를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G319 - Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: NetworkFirewall.9	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection - AWS Network Firewall에 대한 삭제 보호를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G223 - OpenSearch 도메인은 노드 간에 전송된 데이터를 암호화해야 합니다. 해당 AWS Security Hub CSPM 검사: OpenSearch.3	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption 도메인에 대해 노드 간 암호화가 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. node-to-node 암호화가 활성화된 후에는 설정을 비활성화할 수 없습니다. 대신 암호화된 도메인의 수동 스냅샷을 만들고, 다른 도메인을 생성하고, 데이터를 마이그레이션한 다음 이전 도메인을 삭제합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G222 - CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅을 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: Opensearch.4	AWSManagedServices-EnableOpenSearchLogging OpenSearch 도메인에 대해 오류 로깅이 활성화되어 있습니다.	CloudWatchLogGroupArn: anAmazon CloudWatch Logs 로그 그룹의 ARN입니다. 자동 문제 해결을 활성화하려면 미리 구성된 파라미터인 CloudWatchLogGroupArn을 제공해야 합니다. Amazon CloudWatch 리소스 정책은 권한으로 구성해야 합니다. 자세한 내용은 Amazon OpenSearch Service 사용 설명서의 감사 로그 활성화를 참조하세요.
Hs4Ma3G221 - OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: Opensearch.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch 도메인은 감사 로깅이 활성화된 상태로 구성됩니다.	CloudWatchLogGroupArn: 로그를 게시할 CloudWatch Logs 그룹의 ARN입니다. 자동 문제 해결을 활성화하려면 미리 구성된 파라미터를 제공해야 합니다. CloudWatchLogGroupArn Amazon CloudWatch 리소스 정책은 권한으로 구성해야 합니다. 자세한 내용은 Amazon OpenSearch Service 사용 설명서의 감사 로그 활성화를 참조하세요.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G220 - OpenSearch 도메인에 대한 연결은 TLS 1.2를 사용하여 암호화해야 합니다. 해당 AWS Security Hub CSPM 검사: Opensearch.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 TLS 정책은 `Policy-Min-TLS-1-2-2019-07`로 설정되며 HTTPS(TLS)를 통한 암호화된 연결만 허용됩니다.	사전 구성된 파라미터는 허용되지 않습니다. TLS 1.2를 사용하려면 OpenSearch 도메인에 연결해야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로파일과 TLS의 영향을 이해합니다.
Hs4Ma3G194 - Amazon RDS 스냅샷은 프라이빗이어야 합니다. 해당 AWS Security Hub CSPM 검사: RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Amazon RDS 스냅샷에 대한 퍼블릭 액세스가 비활성화되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G192 - RDS DB 인스턴스는 PubliclyAccessible AWS 구성에 따라 퍼블릭 액세스를 금지해야 합니다. 해당 AWS Security Hub CSPM 검사: RDS.2	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance RDS DB 인스턴스에서 퍼블릭 액세스를 비활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G189 - Amazon RDS DB 인스턴스에 대해 향상된 모니터링이 구성됨 해당 AWS Security Hub CSPM 검사: RDS.6	AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring Amazon RDS DB 인스턴스에 대한 향상된 모니터링 활성화	• MonitoringInterval: DB 인스턴스에 대해 Enhanced Monitoring 지표가 수집되는 시점 사이의 초 단위 간격입니다. 유효한 간격은 0, 1, 5, 10, 15, 30 및 60입니다. 확장 모니터링 지표의 수집을 비활성화하려면 0을 지정합니다. • MonitoringRoleName: Amazon RDS가 향상된 모니터링 지표를 Amazon CloudWatch Logs로 전송하도록 허용하는 IAM 역할의 이름입니다. 역할을 지정하지 않으면 기본 역할`rds-monitoring-role` 이 사용되거나 존재하지 않는 경우 기본 역할이 생성됩니다. 자동화 실행 전에 향상된 모니터링이 활성화된 경우이 자동화에서 사전 구성된 파라미터에 구성된 MonitoringInterval 및 MonitoringRoleName 값을 사용하여 설정을 덮어쓸 수 있습니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G190 - Amazon RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: RDS.7	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection Amazon RDS 클러스터에 대해 삭제 방지가 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G198 - Amazon RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: RDS.8	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection Amazon RDS 인스턴스에 대해 삭제 방지가 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G199 - RDS DB 인스턴스는 CloudWatch Logs에 로그를 게시해야 합니다. 해당 AWS Security Hub CSPM 검사: RDS.9	AWSManagedServices-TrustedRemediatorEnableRDSLogExports RDS DB 인스턴스 또는 RDS DB 클러스터에 대해 RDS 로그 내보내기가 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 서비스 연결 역할 AWSServiceRoleForRDS가 필요합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G160 - RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다. 해당 AWS Security Hub CSPM 검사: RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management RDS 인스턴스에 대해 인증이 활성화됩니다.	ApplyImmediately:이 요청의 수정 사항과 보류 중인 수정 사항이 최대한 빨리 비동기식으로 적용되는지 여부를 나타냅니다. 변경 사항을 즉시 적용하려면를 선택합니다`true`. 다음 유지 관리 기간에 대한 변경을 예약하려면를 선택합니다`false`. 제약 조건 없음
Hs4Ma3G161 - RDS 클러스터에 대해 IAM 인증을 구성해야 합니다. 해당 AWS Security Hub CSPM 검사: RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication RDS 클러스터에 대해 IAM 인증이 활성화됩니다.	ApplyImmediately:이 요청의 수정 사항과 보류 중인 수정 사항이 최대한 빨리 비동기식으로 적용되는지 여부를 나타냅니다. 변경 사항을 즉시 적용하려면를 선택합니다`true`. 다음 유지 관리 기간에 대한 변경을 예약하려면를 선택합니다`false`. 제약 조건 없음
Hs4Ma3G162 - RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade Amazon RDS에 대한 마이너 버전 자동 업그레이드 구성이 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 문제 해결이 수행되려면 Amazon RDS 인스턴스가 `available` 상태여야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G163 - 스냅샷에 태그를 복사하도록 RDS DB 클러스터를 구성해야 합니다. 해당 AWS Security Hub CSPM 검사: RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagtosnapshot` Amazon RDS 클러스터에 대한 설정이 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 문제 해결을 수행하려면 Amazon RDS 인스턴스가 사용 가능한 상태여야 합니다.
Hs4Ma3G164 - 스냅샷에 태그를 복사하도록 RDS DB 인스턴스를 구성해야 합니다. 해당 AWS Security Hub CSPM 검사: RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagsToSnapshot` Amazon RDS에 대한 설정이 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 문제 해결을 수행하려면 Amazon RDS 인스턴스가 사용 가능한 상태여야 합니다.
rSs93HQwa1 Amazon RDS 퍼블릭 스냅샷	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Amazon RDS 스냅샷에 대한 퍼블릭 액세스가 비활성화되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G103 - Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다. 해당 AWS Security Hub CSPM 검사: Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster Amazon Redshift 클러스터의 퍼블릭 액세스가 비활성화되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 퍼블릭 액세스를 비활성화하면 인터넷에서 들어오는 모든 클라이언트가 차단됩니다. 그리고 Amazon Redshift 클러스터는 몇 분 동안 수정 중 상태인 반면 수정은 클러스터에 대한 퍼블릭 액세스를 비활성화합니다.
Hs4Ma3G106 - Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: Redshift.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging 유지 관리 기간 동안 Amazon Redshift 클러스터에 대한 감사 로깅이 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. BucketName: 버킷이 동일해야 합니다 AWS 리전. 클러스터에는 읽기 버킷이 있어야 하며 객체 권한을 부여해야 합니다. 자동화 실행 전에 Redshift 클러스터 로깅이 활성화된 경우이 자동화에서 사전 구성된 파라미터에 구성된 `BucketName` 및 `S3KeyPrefix` 값으로 로깅 설정을 덮어쓸 수 있습니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G105 - Amazon Redshift는 메이저 버전으로 자동 업그레이드가 활성화되어 있어야 합니다. 해당 AWS Security Hub CSPM 검사: Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade - 메이저 버전 업그레이드는 유지 관리 기간 동안 클러스터에 자동으로 적용됩니다. Amazon Redshift 클러스터에는 즉각적인 가동 중지가 없지만 메이저 버전으로 업그레이드하는 경우 유지 관리 기간 동안 Amazon Redshift 클러스터에 가동 중지가 발생할 수 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G104 - Amazon Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다. 해당 AWS Security Hub CSPM 검사: Redshift.7	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting Amazon Redshift 클러스터에 대해 향상된 VPC 라우팅이 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G173 - 버킷 수준에서 S3 퍼블릭 액세스 차단 설정을 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: S3.8	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess 버킷 수준 퍼블릭 액세스 블록은 Amazon S3 버킷에 적용됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 수정 사항은 S3 객체 가용성에 영향을 미칠 수 있습니다. Amazon S3가 액세스를 평가하는 방법에 대한 자세한 내용은 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단을 참조하세요.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G230 - S3 버킷 서버 액세스 로깅을 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: S3.9	AWSManagedServices-EnableBucketAccessLogging(자동 및 수동 실행 모드 모두에 대한 기본 SSM 문서) Amazon S3 서버 액세스 로깅이 활성화되었습니다.	• TargetBucket: 서버 액세스 로그를 저장할 S3 버킷의 이름입니다. • TargetObjectKeyFormat: 로그 객체의 Amazon S3 키 형식(값은 대/소문자를 구분함). 로그 객체에 대한 S3 키의 단순 형식을 사용하려면를 선택합니다`SimplePrefix` . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 EventTime을 사용하려면를 선택합니다`PartitionedPrefixEventTime` . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 DeliveryTime을 사용하려면를 선택합니다`PartitionedPrefixDeliveryTime` . 유효 값은 `SimplePrefix` , `PartitionedPrefixEventTime` 및 `PartitionedPrefixDeliveryTime` 입니다. 자동 문제 해결을 활성화하려면 사전 구성된 파라미터인 TargetBucket을 제공해야 합니다. 대상 버킷은 로그 전송에 대한 올바른 권한을 가진 원본 버킷과 동일한 AWS 리전 및 AWS 계정 에 있어야 합니다. 자세한 내용은 Amazon S3 서버 액세스 로깅 활성화를 참조하세요.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G230 – S3 버킷 서버 액세스 로깅을 활성화해야 합니다. 해당 AWS Security Hub CSPM 검사: S3.9	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 - Amazon S3 버킷 로깅이 활성화되어 있습니다.	• TargetBucketTagKey: 대상 버킷을 식별하기 위한 태그 이름(대소문자 구분)입니다. 이 및 TargetBucketTagValue를 사용하여 액세스 로깅의 대상 버킷으로 사용할 버킷에 태그를 지정합니다. • TargetBucketTagValue: 대상 버킷을 식별하기 위한 태그 값(대소문자 구분)으로,이 및 TargetBucketTagKey를 사용하여 액세스 로깅의 대상 버킷으로 사용할 버킷에 태그를 지정합니다. • TargetObjectKeyFormat: 로그 객체의 Amazon S3 키 형식(값은 대소문자를 구분함): 로그 객체의 S3 키에 단순 형식을 사용하려면 SimplePrefix를 선택합니다. 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 EventTime을 사용하려면 PartitionedPrefixEventTime을 선택합니다. 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 DeliveryTime을 사용하려면 PartitionedPrefixDeliveryTime을 선택합니다. 기본값은 PartitionedPrefixEventTime입니다. 자동 문제 해결을 활성화하려면 TargetBucketTagKey 및 TargetBucketTagValue 파라미터를 제공해야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		대상 버킷은 로그 전송에 대한 올바른 권한을 가진 원본 버킷과 동일한 AWS 리전 및 AWS 계정 에 있어야 합니다. 자세한 내용은 Amazon S3 서버 액세스 로깅 활성화를 참조하세요.
Pfx0RwqBli Amazon S3 버킷 권한	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess 퍼블릭 액세스 차단	사전 구성된 파라미터는 허용되지 않습니다. 이 검사는 여러 알림 기준으로 구성됩니다. 이 자동화는 퍼블릭 액세스 문제를 해결합니다. 에서 플래그가 지정된 Trusted Advisor 다른 구성 문제에 대한 수정은 지원되지 않습니다. 이 문제 해결은 AWS 서비스 생성된 S3 버킷(예: cf-templates-000000000000) 문제 해결을 지원합니다.
Hs4Ma3G272 - 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다. 해당 AWS Security Hub CSPM 검사: SageMaker.3	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess SageMaker 노트북 인스턴스에서는 사용자의 루트 액세스가 비활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 문제를 해결하면 SageMaker 노트북 인스턴스가 InService 상태인 경우 중단이 발생합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G179 - SNS 주제는를 사용하여 저장 시 암호화되어야 합니다. AWS KMS 해당 AWS Security Hub CSPM 검사: SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest SNS 주제는 서버 측 암호화로 구성됩니다.	KmsKeyId: 서버 측 암호화(SSE)에 사용할 Amazon SNS용 AWS 관리형 고객 마스터 키(CMK) 또는 사용자 지정 CMK의 ID입니다. 기본값은 로 설정됩니다`alias/aws/sns` . 사용자 지정 AWS KMS 키를 사용하는 경우 올바른 권한으로 구성해야 합니다. 자세한 내용은 Amazon SNS 주제에 대한 서버 측 암호화(SSE) 활성화를 참조하세요.
Hs4Ma3G158 - SSM 문서는 공개되어서는 안 됩니다. 해당 AWS Security Hub CSPM 검사: SSM.4	AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing - SSM 문서의 퍼블릭 공유를 비활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G136 - Amazon SQS 대기열은 저장 시 암호화되어야 합니다. 해당 AWS Security Hub CSPM 검사: SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest Amazon SQS의 메시지는 암호화됩니다.	• SqsManagedSseEnabled: Amazon SQS 소유 암호화 키를 사용하여 서버 측 대기열 암호화를 활성화`true`하려면 로 설정하고 키를 사용하여 서버 측 대기열 암호화를 활성화`false`하려면 로 설정합니다 AWS KMS . • KMSKeyId: 대기열의 서버 측 암호화에 사용할 Amazon SQS용 AWS 관리형 고객 마스터 키(CMK) 또는 사용자 지정 CMK의 ID 또는 별칭입니다. Amazon SQS 제공되지 않으면 alias/aws/sqs 사용됩니다. • KmsDataKeyReusePeriodSeconds: AWS KMS 다시 호출하기 전에 Amazon SQS가 데이터 키를 재사용하여 메시지를 암호화하거나 해독할 수 있는 초 단위의 시간 길이입니다. 초 단위의 정수로, 60초(1분)에서 86,400초(24시간) 사이입니다. 이 로 설정된 경우이 설정은 무시`SqsManagedSseEnabled` 됩니다`true`. 암호화된 대기열에 대한 익명 SendMessage 및 ReceiveMessage 요청은 거부됩니다. SSE를 사용할 수 있는 대기열에 대한 모든 요청에서는 HTTPS 및 서명 버전 4를 사용해야 합니다.

Trusted Advisor Trusted Remediator에서 지원하는 내결함성 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c18d2gz138 Amazon DynamoDB의 지점 실시간 복구	AWSManagedServices-TrustedRemediatorEnableDDBPITR DynamoDB 테이블에 대한 point-in-time으로 복구를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
R365s2Qddf Amazon S3 Bucket Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning Amazon S3 버킷 버전 관리가 활성화되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 문제 해결은 AWS 서비스 생성된 S3 버킷(예: cf-templates-00000000000)의 문제 해결을 지원하지 않습니다.
BueAdJ7NrP Amazon S3 버킷 로깅	AWSManagedServices-EnableBucketAccessLogging Amazon S3 버킷 로깅이 활성화되었습니다.	• TargetBucket: 서버 액세스 로그를 저장할 S3 버킷의 이름입니다. • TargetObjectKeyFormat: 로그 객체에 대한 Amazon S3 키의 간단한 형식을 사용하려면 로그 객체에 대한 Amazon S3 키 형식을 선택합니다SimplePrefix . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 EventTime을 사용하려면를 선택합니다PartitionedPrefixEventTime . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 DeliveryTime을 사용하려면를 선택합니다PartitionedPrefixDeliveryTime . 기본값은 PartitionedPrefixEventTime 입니다. 유효한 값은 SimplePre

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		`fix` , `PartitionedPrefixEventTime` 및 `PartitionedPrefixDeliveryTime` (대소문자 구분)입니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. • TargetBucket 대상 버킷은 로그 전송에 대한 올바른 권한을 가진 원본 버킷과 동일한 AWS 리전 및 AWS 계정 에 있어야 합니다. 자세한 내용은 Amazon S3 서버 액세스 로깅 활성화를 참조하세요.
f2iK5R6Dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ 다중 가용 영역 배포가 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 변경 중에 성능 저하가 발생할 수 있습니다.
H7IgTzjTYb Amazon EBS 스냅샷	AWSManagedServices-TrustedRemediatorCreateEBSSnapshot Amazon EBSsnapshots가 생성됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
opQPADkZvH RDS 백업	AWSManagedServices-EnableRDSBackupRetention DB에 대해 Amazon RDS 백업 보존이 활성화됩니다.	• BackupRetentionPeriod: 자동 백업을 보존할 일수(1~35일)입니다. • ApplyImmediately: RDS 백업 보존 변경 및 보류 중인 수정 사항이 가능한 한 빨리 비동기적으로 적용되는지 여부를 나타냅니다. 변경 사항을 즉시 `true` 적용하거나 다음 유지 관리 기간에 대한 변경 사항을 예약`false`하도록 선택합니다. `ApplyImmediately` 파라미터가 로 설정된 경우 db에서 `true`보류 중인 변경 사항이 RDSBackup 보존 설정과 함께 적용됩니다.
c1qf5bt013 Amazon RDS DB 인스턴스의 스토리지 자동 조정이 꺼져 있음	AWSManagedServices-TrustedRemediatorEnableRDSInstanceStorageAutoScaling - Amazon RDS DB 인스턴스에 대해 스토리지 자동 크기 조정이 활성화되어 있습니다.	• MaxAllocatedStorageIncrease Percentage: AllocatedStorage를 설정하기 위한 현재 AllocatedStorage의 증가 비율입니다. MaxAllocatedStorage 기본값은 로 설정됩니다26. 최대 스토리지 임계값을 현재 할당된 스토리지보다 10% 이상 높게 설정해야 합니다. 최대 스토리지 임계값을 26% 이상으로 설정하는 것이 가장 좋습니다. 자세한 내용은 Amazon Relational Database Service 스토리지 자동 크기 조정을 사용하여 용량 자동 관리를 참조하세요. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
7qGXsKIUw Classic Load Balancer 연결 드레이닝	AWSManagedServices-TrustedRemediatorEnableCLBConnectionDraining Classic Load Balancer에 대해 연결 드레이닝이 활성화되어 있습니다.	ConnectionDrainingTimeout: 인스턴스 등록을 취소하기 전에 기존 연결을 열어 두는 최대 시간입니다. 기본값은 300 초로 설정됩니다. 제약 조건 없음
c18d2gz106 Amazon EBS가 AWS Backup 플랜에 포함되지 않음	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS는 AWS Backup 플랜에 포함되어 있습니다.	문제 해결은 다음 태그 페어를 사용하여 Amazon EBS 볼륨에 태그를 지정합니다. 태그 페어는 태그 기반 리소스 선택 기준과 일치해야 합니다 AWS Backup. • TagKey • TagValue 제약 조건 없음
c18d2gz107 AWS Backup 계획에 포함되지 않은 Amazon DynamoDB 테이블	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlanAddDynamoDBToBackupPlan Amazon DynamoDB 테이블은 AWS Backup 플랜에 포함되어 있습니다.	문제 해결은 다음 태그 페어를 사용하여 Amazon DynamoDB에 태그를 지정합니다. 태그 페어는 태그 기반 리소스 선택 기준과 일치해야 합니다 AWS Backup. • TagKey • TagValue 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c18d2gz117 Amazon EFS는 AWS Backup 플랜에 포함되지 않음	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS는 AWS Backup 플랜에 포함되어 있습니다.	문제 해결은 다음 태그 페어를 사용하여 Amazon EFS에 태그를 지정합니다. 태그 페어는 태그 기반 리소스 선택 기준과 일치해야 합니다 AWS Backup. • TagKey • TagValue 제약 조건 없음
c18d2gz105 Network Load Balancer 교차 로드 밸런싱	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing Network Load Balancer에서 교차 영역 로드 밸런싱이 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt026 Amazon RDS `synchronous_commit` 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS에 대해 파라미터`synchronous_commit` 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt030 Amazon RDS `innodb_flush_log_at_trx_commit` 파라미터가 가 아님 `1`	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS의 경우 파라미터`innodb_flush_log_at_trx_commit` 가 로 설정되어 `1` 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c1qf5bt031 Amazon RDS `sync_binlog` 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS에 대해 파라미터`sync_binlog` 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt036 Amazon RDS `innodb_default_row_format` 파라미터 설정이 안전하지 않음	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS의 경우 파라미터`innodb_default_row_format` 가 로 설정되어 `DYNAMIC` 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c18d2gz144 Amazon EC2 세부 모니터링이 활성화되지 않음	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring Amazon EC2에 대해 세부 모니터링이 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

Trusted Advisor Trusted Remediator에서 지원하는 성능 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
COr6dfpM06 AWS Lambda 메모리 크기에 대한 과소 프로비저닝된 함수	AWSManagedServices-ResizeLambdaMemory Lambda 함수 메모리 크기는에서 제공하는 권장 메모리 크기로 조정됩니다 Trusted Advisor.	RecommendedMemorySize: Lambda 함수에 대한 권장 메모리 할당입니다. 값 범위는 128~10240입니다. 자동화 실행 전에 Lambda 함수 크기가 수정된 경우이 자동화는에서 권장

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		하는 값으로 설정을 덮어쓸 수 있습니다 Trusted Advisor.
ZRxQlPsb6c 높은 사용률의 Amazon EC2 인스턴스	AWSManagedServices-ResizeInstanceByOneLevel Amazon EC2 인스턴스는 동일한 인스턴스 패밀리 유형에서 하나의 인스턴스 유형으로 크기가 조정됩니다. 인스턴스는 크기 조정 작업 중에 중지 및 시작되고 실행이 완료된 후 초기 상태로 돌아갑니다. 이 자동화는 Auto Scaling 그룹에 있는 인스턴스의 크기 조정을 지원하지 않습니다.	• MinimumDaysSinceLastChange: 마지막 인스턴스 유형이 변경된 이후 최소 일수입니다. 인스턴스 유형이 지정된 시간 내에 수정된 경우 인스턴스 유형은 변경되지 않습니다. `0`를 사용하여이 검증을 건너뜁니다. 기본값은 7입니다. • CreateAMIBeforeResize: 크기를 조정하기 전에 인스턴스 AMI를 백업으로 생성하려면를 선택합니다`true`. 백업을 생성하지 않으려면를 선택합니다`false`. 기본값은 `false`입니다. 유효한 값은 `true` 및 `false` (대소문자 구분)입니다. • ResizeIfStopped: 인스턴스가 중지된 상태인 경우에도 인스턴스 크기 변경을 진행하려면를 선택합니다`true`. 중지된 상태인 경우 인스턴스의 크기를 자동으로 조정하지 않으려면를 선택합니다`false`. 유효한 값은 `true` 및 `false` (대/소문자 구분)입니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c1qf5bt021 최적 값보다 작은 값을 사용하는 Amazon RDS innodb_change_buffering 파라미터	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS의 NONE 경우 innodb_change_buffering 파라미터 값이 로 설정됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt025 Amazon RDS autovacuum 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS에 대해 파라미터autovacuum 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt028 Amazon RDS enable_indexonlyscan 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS에 대해 파라미터enable_indexonlyscan 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt029 Amazon RDS enable_indexscan 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS에 대해 파라미터enable_indexscan 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c1qf5bt032 Amazon RDS `innodb_stats_persistent` 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS에 대해 파라미터`innodb_stats_persistent` 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt037 Amazon RDS `general_logging` 파라미터가 켜져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS에 대해 파라미터`general_logging` 가 꺼져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

Trusted Advisor Trusted Remediator에서 지원하는 서비스 제한 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
lN7RR0l7J9 EC2-VPC 탄력적 IP 주소	AWSManagedServices-UpdateVpcElasticIPQuota EC2-VPC 탄력적 IP 주소에 대한 새로운 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 0K 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.
kM7QQ0l7J9 VPC 인터넷 게이트웨이	AWSManagedServices-IncreaseServiceQuota - VPC 인터넷 게이트웨이에 대한 새로운 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 0K 상태로 업데이트되기 전에이 자동화가 여러 번

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.
jL7PP0l7J9 VPC	AWSManagedServices-IncreaseServiceQuota VPC에 대한 새 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.
fW7HH0l7J9 Auto Scaling 그룹	AWSManagedServices-IncreaseServiceQuota Auto Scaling 그룹에 대한 새 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.
3Njm0DJQO9 RDS 옵션 그룹	AWSManagedServices-IncreaseServiceQuota Amazon RDS 옵션 그룹에 대한 새로운 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.
EM8b3yLRTr ELB Application Load Balancers	AWSManagedServices-IncreaseServiceQuota ELB Application Load Balancer에 대한 새 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
8wlqYSt25K ELB 네트워크 로드 밸런서	AWSManagedServices-IncreaseServiceQuota ELB Network Load Balancer에 대한 새로운 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.

Trusted Advisor Trusted Remediator에서 지원하는 운영 우수성 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c18d2gz125 Amazon API Gateway에서 실행 로그를 기록하지 않음	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging 실행 로깅은 API 단계에서 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 실행 로그를 활성화하려면 API Gateway에 계정의 CloudWatch에 로그를 읽고 쓸 수 있는 권한을 부여해야 합니다. 자세한 내용은 API Gateway에서 REST APIs에 대한 CloudWatch 로깅 설정을 참조하세요.
c18d2gz168 로드 밸런서에 Elastic Load Balancing 삭제 보호 기능이 활성화되지 않음	AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection - Elastic Load Balancer에 대해 삭제 방지가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt012 Amazon RDS Performance	AWSManagedServices-TrustedRemediatorEnableRDSPerformanceInsights	• PerformanceInsightsRetentionPeriod: 성능 개선 도우미 데이터를 보존할 일수입니다. 유효한 값: 7

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Insights가 꺼져 있음	Amazon RDS에 대해 성능 개선 도우미가 켜져 있습니다.	또는 월 * 31. 여기서 월은 1~23개월의 개월 수입니다. 예: 93 (3개월 * 31), 341 (11개월 * 31), 589 (19개월 * 31) 또는 731. • PerformanceInsightsKMSKeyId: 성능 개선 도우미 데이터의 암호화를 위한 AWS KMS 키 ID입니다. PerformanceInsightsKMSKeyId 값을 지정하지 않으면 Amazon RDS가 기본 AWS KMS 키를 사용합니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c1fd6b96l4 Amazon S3 액세스 로그 활성화됨	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 Amazon S3 버킷 액세스 로깅이 활성화되었습니다.	• TargetBucketTagValue: 태그 값(대소문자 구분)을 사용하여 대상 버킷을 식별하고,이 및 TargetBucketTagKey를 사용하여 액세스 로깅의 대상 버킷으로 사용할 버킷에 태그를 지정합니다. • TargetObjectKeyFormat: 로그 객체의 Amazon S3 키 형식(값은 대/소문자를 구분함). 로그 객체에 대한 S3 키의 단순 형식을 사용하려면를 선택합니다`SimplePrefix` . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 EventTime을 사용하려면를 선택합니다`PartitionedPrefixEventTime` . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 DeliveryTime을 사용하려면를 선택합니다`PartitionedPrefixDeliveryTime` . 유효 값은 `SimplePrefix` , `PartitionedPrefixEventTime` 및 `PartitionedPrefixDeliveryTime` 입니다. 자동 문제 해결을 활성화하려면 사전 구성된 파라미터인 TargetBucketTagKey 및 TargetBucketTagValue를 제공해야 합니다. 대상 버킷은 로그 전송에 대한 올바른 권한을 가진 원본 버킷과 동일한 AWS 리전 및 AWS 계정 에 있어야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		자세한 내용은 Amazon S3 서버 액세스 로깅 활성화를 참조하세요.

Trusted Remediator에서 지원하는 Security Hub CSPM 권장 사항

다음 표에는 지원되는 Security Hub CSPM 권장 사항, SSM 자동화 문서, 사전 구성된 파라미터 및 자동화 문서의 예상 결과가 나열되어 있습니다. 검사 문제 해결을 위해 SSM 자동화 문서를 활성화하기 전에 예상 결과를 검토하여 비즈니스 요구 사항에 따라 가능한 위험을 이해하는 데 도움이 됩니다.

계정에 대해 Security Hub CSPM을 활성화해야 합니다. 자세한 내용은 Security Hub CSPM 활성화를 참조하세요.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
security-hub-IAM-22 IAM.22: 45일 동안 사용하지 않은 IAM 사용자 자격 증명을 제거해야 합니다.	AWSManagedServices-TrustedRemediatorDeactivateIamUserUnusedCredentials	DeleteAccessKeys: 사용하지 않는 액세스 키를 영구적으로 삭제하려면 true로 설정하고 비활성화하려면 false로 설정합니다(비활성화되지만 복구 가능). 제약 조건 없음
security-hub-IAM-3 IAM.3: IAM 사용자의 액세스 키는 90일 이하마다 교체해야 합니다.	AWSManagedServices-TrustedRemediatorRotateIamAccessKeysOlderThan90Days	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
security-hub-IAM-8	AWSManagedServices-TrustedRemediatorDeactivateIamUserUnusedCredentials	DeleteAccessKeys: 사용하지 않는 액세스 키를 영구적으로 삭제하려면 true로 설정하고 비활성화하려면 false

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
IAM.8: 미사용 IAM 사용자 자격 증명을 제거해야 합니다.		로 설정합니다(비활성화되지만 복구 가능). 제약 조건 없음
security-hub-networkfirewall-10 NetworkFirewall.10: Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다.	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallSubnetChangeProtection	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
security-hub-networkfirewall-2 NetworkFirewall.2: Network Firewall 로깅을 활성화해야 합니다.	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallCloudWatchLog	LogGroupName: 로그를 전송할 CloudWatch 로그 그룹의 이름입니다. LogTypes: 활성화할 로그 유형입니다. 유효한 값은 `FLOW`, `ALERT`, `TLS`입니다. 제약 조건 없음
security-hub-stepfunctions-1 StepFunctions.1: Step Functions 상태 시스템에는 로깅이 켜져 있어야 합니다.	AWSManagedServices-TrustedRemediatorEnableStepFunctionsLogging	LogGroupName: Step Functions 로깅을 위한 CloudWatch 로그 그룹의 이름입니다. LoggingLevel: Step Functions의 로깅 수준입니다. 유효한 값은 `ALL`, `ERROR`, `FATAL`입니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
security-hub-lambda-7 Lambda.7: Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.	AWSManagedServices-TrustedRemediatorEnableLambdaXrayActiveTracing	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성

구성은 Trusted Remediator 애플리케이션의 AWS AppConfig 일부로에 저장됩니다. 각 Trusted Advisor 검사 범주에는 별도의 구성 프로필이 있습니다. Trusted Advisor 범주에 대한 자세한 내용은 검사 범주 보기를 참조하세요.

리소스별 또는 Trusted Advisor 검사별로 문제 해결을 구성할 수 있습니다. 리소스 태그를 사용하여 예외를 적용할 수 있습니다.

> **Note**
>
> 조사 Trusted Advisor 결과 수정은 현재를 사용하여 구성되며 AWS AppConfig,이 기능은 현재 완전히 지원됩니다. AMS는 향후 변경될 것으로 예상합니다. 이 방법은 변경될 수 AWS AppConfig있으므로에 의존하는 자동화를 빌드하지 않는 것이 가장 좋습니다. 호환성을 위해 향후 현재 AWS AppConfig 구현을 기반으로 구축된 자동화를 업데이트하거나 수정해야 할 수 있습니다.
> Compute Optimizer -> EC2 인스턴스 기능 플래그에는 추가 파라미터가 있습니다.
>
> - allow-upscale 과소 프로비저닝된 최적화되지 않은 EC2 인스턴스를 확장할 수 있습니다. 기본값은 "false"입니다.
> - min-savings-opportunity-percentage 자동 문제 해결을 위한 최소 절감률 기회입니다. 기본값은 10%입니다.

기본 문제 해결 구성

개별 Trusted Advisor 검사에 대한 구성은 AWS AppConfig 플래그로 저장됩니다. 플래그 이름은 검사 이름과 일치합니다. 각 검사 구성에는 다음 속성이 포함됩니다.

- execution-mode: 신뢰할 수 있는 수정자가 기본 수정을 수행하는 방법을 결정합니다.
  - 자동: 신뢰할 수 있는 수정자는 OpsItem을 생성하고, SSM 문서를 실행한 다음, 실행 성공 후 OpsItem을 해결하여 리소스를 자동으로 수정합니다.
  - 수동: OpsItem이 생성되지만 SSM 문서가 자동으로 실행되지 않습니다. AWS Systems Manager OpsCenter 콘솔의 OpsItem에서 SSM 문서를 검토하고 수동으로 실행합니다.
  - 조건부: 수정은 기본적으로 비활성화되어 있습니다. 태그를 사용하여 특정 리소스에 대해 활성화할 수 있습니다. 자세한 내용은 다음 섹션 리소스 태그를 사용하여 문제 해결 사용자 지정 및 단원을 참조하십시오리소스 재정의 태그를 사용하여 문제 해결 사용자 지정.
  - 비활성: 수정이 발생하지 않고 OpsItem이 생성되지 않습니다. 비활성으로 설정된 Trusted Advisor 검사의 실행 모드는 재정의할 수 없습니다.
- pre configured-parameters: 자동 문제 해결에 필요한 SSM 문서 파라미터 값을 쉼표(,)로 구분하여 `Parameter=Value` 형식으로 입력합니다. 각 검사에 대해 연결된 SSM 문서에 대해 Trusted Advisor Trusted Remediator에서 지원하는 검사 지원되는 사전 구성된 파라미터는 섹션을 참조하세요.
- alternative-automation-document:이 속성은 지원되는 다른 문서(특정 검사에 사용할 수 있는 경우)로 기존 자동화 문서를 재정의하는 데 도움이 됩니다. 기본적으로이 속성은 선택되지 않습니다.

> **Note**
>
> `alternative-automation-document` 속성은 사용자 지정 자동화 문서를 지원하지 않습니다. 에 나열된 기존의 지원되는 Trusted Remediator 자동화 문서를 사용할 수 있습니다Trusted Advisor Trusted Remediator에서 지원하는 검사.
> 예를 들어 검사 에는 AWSManagedServices-StopEC2InstanceQch7DwouX1, AWSManagedServices-ResizeInstanceByOneLevel 및 AWSManagedServices-TerminateInstance의 세 가지 관련 SSM 문서가 있습니다. AWSManagedServices-StopEC2Instance 의 값은 AWSManagedServices-ResizeInstanceByOneLevel 또는 AWSManagedServices-TerminateInstance일 `alternative-automation-document` 수 있습니다(AWSManagedServices-StopEC2Instance는를 해결하기 위한 기본 SSM 문서임Qch7DwouX1).

각 속성의 값은 해당 속성의 제약 조건과 일치해야 합니다.

> **Tip**
>
> Trusted Advisor 검사에 기본 구성을 적용하기 전에 다음 섹션에 설명된 리소스 태그 지정 및 리소스 재정의 기능을 사용하는 것이 좋습니다. 기본 구성은 계정 내 모든 리소스에 적용되며, 모든 경우에 바람직하지 않을 수 있습니다.

다음은 실행 모드가 수동으로 설정되고 속성이 제약 조건과 일치하는 예제 콘솔 스크린샷입니다.

리소스 태그를 사용하여 문제 해결 사용자 지정

검사 구성의 automated-for-tagged-only 및 manual-for-tagged-only 속성을 사용하면 개별 검사를 수정하는 방법에 대한 리소스 태그를 지정할 수 있습니다. 동일한 태그 또는 태그를 공유하는 리소스 그룹에 일관된 문제 해결 동작을 적용해야 하는 경우이 방법을 사용하는 것이 가장 좋습니다. 다음은 이러한 태그에 대한 설명입니다.

- automated-for-tagged-only: 기본 실행 모드에 관계없이 자동으로 수정할 검사에 대한 리소스 태그(하나 이상의 태그 페어, 쉼표로 구분)를 지정합니다.
- manual-for-tagged-only: 기본 실행 모드에 관계없이 수동으로 실행해야 하는 문제 해결에 대한 리소스 태그(하나 이상의 태그 페어, 쉼표로 구분)를 지정합니다.

예를 들어 모든 비프로덕션 리소스에 대해 자동 문제 해결을 활성화하고 프로덕션 리소스에 대해 수동 문제 해결을 적용하려면 다음과 같이 구성을 설정할 수 있습니다.

```
"execution-mode": "Conditional",
"automated-for-tagged-only": "Environment=Non-Production",
"manual-for-tagged-only": "Environment=Production",
```

리소스에 이전 구성이 설정된 경우 문제 해결 동작이 다음과 같은지 확인합니다.

- 'Environment=Non-Production'으로 태그가 지정된 리소스는 자동으로 수정됩니다.
- 'Environment=Production'으로 태그가 지정된 리소스는 수정을 위해 수동 개입이 필요합니다.

- '환경' 태그가 없는 리소스는 기본 실행 모드(이 경우 '조건부')를 따릅니다. 따라서 나머지 리소스에 대해서는 아무런 조치도 취하지 않습니다.)

구성에 대한 추가 지원은 Cloud Architect에 문의하십시오.

리소스 재정의 태그를 사용하여 문제 해결 사용자 지정

리소스 재정의 태그를 사용하면 태그에 관계없이 개별 리소스의 문제 해결 동작을 사용자 지정할 수 있습니다. 리소스에 특정 태그를 추가하면 해당 리소스의 기본 실행 모드와 Trusted Advisor 검사를 재정의할 수 있습니다. 리소스 재정의 태그는 기본 구성 및 리소스 태그 지정 설정보다 우선합니다. 따라서 리소스 재정의 태그를 사용하여 리소스에 대해 기본 실행 모드를 자동, 수동 또는 조건부로 설정하면 기본 실행 모드와 리소스 태그 지정 구성을 재정의합니다.

리소스의 실행 모드를 재정의하려면 다음 단계를 완료합니다.

1. 문제 해결 구성을 재정의할 리소스를 식별합니다.
2. 재정의하려는 Trusted Advisor 검사의 검사 ID를 확인합니다. 에서 지원되는 검사에 대한 Trusted Advisor 검사 IDs 찾을 수 있습니다Trusted Advisor Trusted Remediator에서 지원하는 검사.
3. 다음 키와 값을 사용하여 리소스에 태그를 추가합니다.

   - 태그 키: `TR-`*`Trusted Advisor check ID`*`-Execution-Mode` (대/소문자 구분)

     앞의 태그 키 예제에서를 재정의하려는 Trusted Advisor 검사의 고유 식별로 `Trusted Advisor check ID` 바꿉니다.
   - 태그 값: 태그 값에 다음 값 중 하나를 사용합니다.
     - 자동: 신뢰할 수 있는 수정자는이 Trusted Advisor 검사에 대한 리소스를 자동으로 수정합니다.
     - 수동: 리소스에 대한 OpsItem이 생성되지만 수정이 자동으로 수행되지 않습니다. OpsItem에서 수동으로 문제 해결을 검토하고 실행합니다.
     - 비활성:이 리소스 및 지정된 Trusted Advisor 검사에 대해 수정 및 OpsItem 생성이 수행되지 않습니다.

예를 들어 Trusted Advisor 검사 ID가 인 Amazon EBS 볼륨을 자동으로 해결하려면 EBS 볼륨에 태그를 `DAvU99Dc4C` 추가합니다. 태그 키는 `TR-DAvU99Dc4C-Execution-Mode`이고 태그 값은 입니다`Automated`.

다음은 태그 섹션을 보여주는 콘솔의 예입니다.

실행 모드 결정 워크플로

리소스 및 각 Trusted Advisor 검사에 대한 실행 모드를 구성하는 데는 여러 수준이 있습니다. 다음 다이어그램은 Trusted Remediator가 구성에 따라 사용할 실행 모드를 결정하는 방법을 보여줍니다.

문제 해결 자습서 구성

다음 자습서에서는 신뢰할 수 있는 문제 해결자에서 일반적인 문제 해결을 생성하는 예를 제공합니다.

수동으로 모든 리소스 문제 해결

이 예제에서는 Trusted Advisor 검사 ID가 DAvU99Dc4C(사용되지 않은 Amazon EBS 볼륨)인 모든 Amazon EBS 볼륨에 대한 수동 문제 해결을 구성합니다.

검사 ID DAvU99Dc4C를 사용하여 Amazon EBS 볼륨에 대한 수동 문제 해결 구성

1. https://console.aws.amazon.com/systems-manager/appconfig AWS AppConfig 콘솔을 엽니다.

   위임된 관리자 계정으로 로그인해야 합니다.
2. 애플리케이션 목록에서 신뢰할 수 있는 수정자를 선택합니다.
3. Cost Optimization 구성 프로파일을 선택합니다.
4. 사용률이 낮은 Amazon EBS 볼륨 플래그를 선택합니다.
5. 실행 모드에서 수동을 선택합니다.
6. automated-for-tagged-only 속성과 manual-for-tagged-only 속성이 비어 있는지 확인합니다. 이러한 속성은 일치하는 태그가 있는 리소스의 기본 실행 모드를 재정의하는 데 사용됩니다.

   다음은 태그automated-for-tagged-only manual-for-tagged-only 수동 값이 있는 속성 섹션의 예입니다.

7. 저장을 선택하여 값을 업데이트한 다음 새 버전 저장을 선택하여 변경 사항을 적용합니다. 신뢰할 수 있는 수정자가 변경 사항을 인식하려면 새 버전 저장을 선택해야 합니다.
8. Amazon EBS 볼륨에 키가 있는 태그가 없는지 확인합니다`TR-DAvU99Dc4C-Execution-Mode`. 이 태그 키는 해당 EBS 볼륨의 기본 실행 모드를 재정의합니다.

선택한 리소스를 제외한 모든 리소스 자동 수정

이 예제에서는 Trusted Advisor 검사 ID가 DAvU99Dc4C(사용되지 않는 Amazon EBS 볼륨)인 모든 Amazon EBS 볼륨에 대해 자동 문제 해결을 구성합니다. 단, 수정되지 않는 지정된 볼륨(비활성으로 지정됨.

선택한 비활성 리소스를 제외하고 검사 ID가 DAvU99Dc4C인 Amazon EBS 볼륨에 대한 자동 문제 해결 구성

1. https://console.aws.amazon.com/systems-manager/appconfig AWS AppConfig 콘솔을 엽니다.

   위임된 관리자 계정으로 로그인해야 합니다.
2. 애플리케이션 목록에서 신뢰할 수 있는 수정자를 선택합니다.
3. Cost Optimization 구성 프로파일을 선택합니다.
4. 사용률이 낮은 Amazon EBS 볼륨 플래그를 선택합니다.
5. 실행 모드에서 자동을 선택합니다.
6. automated-for-tagged-only 속성과 manual-for-tagged-only 속성이 비어 있는지 확인합니다. 이러한 속성은 일치하는 태그가 있는 리소스의 기본 실행 모드를 재정의하는 데 사용됩니다.

   다음은 태그automated-for-tagged-only manual-for-tagged-only의 빈 값과 실행 모드의 자동 값이 있는 속성 섹션의 예입니다.

7. 저장을 선택하여 값을 업데이트한 다음 새 버전 저장을 선택하여 변경 사항을 적용합니다. 신뢰할 수 있는 수정자가 변경 사항을 인식하려면 새 버전 저장을 선택해야 합니다.

   이 시점에서 모든 Amazon EBS 볼륨은 자동 문제 해결을 위해 설정됩니다.
8. 선택한 Amazon EBS 볼륨에 대한 자동 문제 해결 재정의:

   a. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.

   b. Elastic Block Store, 볼륨을 선택합니다.

   c. [Tags]를 선택합니다.

   d. 태그 관리를 선택합니다.

   e. 다음 태그를 추가합니다.

   - 키: TR-DAvU99Dc4C-Execution-Mode
   - 값: 비활성

다음은 키 및 값 필드를 보여주는 태그 섹션의 예입니다.

f. 문제 해결에서 제외하려는 모든 Amazon EBS 볼륨에 대해 2~5단계를 반복합니다.

태그가 지정된 리소스 자동 수정

이 예제에서는 Trusted Advisor 검사 ID가 DAvU99Dc4C(사용되지 않은 Amazon EBS 볼륨)인 태그`Stage=NonProd`가 있는 모든 Amazon EBS 볼륨에 대해 자동 문제 해결을 구성합니다. 이 태그가 없는 다른 모든 리소스는 수정되지 않습니다.

검사 ID DAvU99Dc4C의 태그를 사용하여 Amazon EBS 볼륨에 **`Stage=NonProd`** 대한 자동 문제 해결 구성

1. https://console.aws.amazon.com/systems-manager/appconfig AWS AppConfig 콘솔을 엽니다.

   위임된 관리자 계정으로 로그인해야 합니다.
2. 애플리케이션 목록에서 신뢰할 수 있는 수정자를 선택합니다.
3. Cost Optimization 구성 프로파일을 선택합니다.
4. 사용률이 낮은 Amazon EBS 볼륨 플래그를 선택합니다.
5. 실행 모드에서 조건부를 선택합니다.
6. automated-for-tagged-only을 로 설정합니다`Stage=NonProd`. 이 속성은 일치하는 태그가 있는 리소스의 기본값을 재정`execution-mode`의합니다. manual-for-tagged-only 속성이 비어 있는지 확인합니다.

   다음은 automated-for-tagged-only이 Stage=NonProd로 설정되고 실행 모드에 조건부로 설정된 속성 섹션의 예입니다.

7. 선택적으로 사전 구성된 파라미터를 다음 중 하나로 설정합니다.

   - `CreateSnapshot=false` 삭제되기 전에 Amazon EBS 볼륨의 스냅샷을 생성하지 않으려면
   - `MinimumUnattachedDays=10` 삭제할 Amazon EBS 볼륨의 연결되지 않은 최소 일수를 10일로 설정하려면
   - `CreateSnapshot=false`, 위 두 가지 모두에 `MinimumUnattachedDays=10` 대해
8. 저장을 선택하여 값을 업데이트한 다음 새 버전 저장을 선택하여 변경 사항을 적용합니다. 신뢰할 수 있는 수정자가 변경 사항을 인식하려면 새 버전 저장을 선택해야 합니다.

9. Amazon EBS 볼륨에 키가 있는 태그가 없는지 확인합니다`TR-DAvU99Dc4C-Execution-Mode`. 이 태그 키는 해당 EBS 볼륨의 기본 실행 모드를 재정의합니다.

신뢰할 수 있는 해결 방법의 문제 해결 작업

신뢰할 수 있는 수정자에서 문제 해결 추적

OpsItems 문제 해결을 추적하려면 다음 단계를 완료하세요.

1. https://console.aws.amazon.com/systems-manager/ AWS Systems Manager 콘솔을 엽니다.
2. 작업 관리, OpsCenter를 선택합니다.
3. (선택 사항) 목록에 신뢰할 수 있는 수정자 OpsItem만 포함하도록 Source=Trusted OpsItems를 기준으로 목록을 필터링합니다.

   다음은 Source=Trusted Remediator로 필터링된 OpsCenter 화면의 예입니다.

> **Note**
>
> OpsItems 보는 것 외에도 AMS S3 버킷에서 문제 해결 로그를 볼 수 있습니다. OpsCenter 자세한 내용은 신뢰할 수 있는 수정자의 수정 로그 단원을 참조하십시오.

신뢰할 수 있는 수정자에서 수동 수정 실행

Trusted Remediator는 수동 문제 해결을 위해 구성된 검사에 대한 OpsItems 생성합니다. 이러한 검사를 검토하고 해결 프로세스를 수동으로 시작해야 합니다.

OpsItem을 수동으로 수정하려면 다음 단계를 완료하세요.

1. https://console.aws.amazon.com/systems-manager/ AWS Systems Manager 콘솔을 엽니다.
2. 작업 관리, OpsCenter를 선택합니다.
3. (선택 사항) 목록에 신뢰할 수 있는 수정자 OpsItem만 포함하도록 Source=Trusted OpsItems를 기준으로 목록을 필터링합니다.
4. 검토하려는 OpsItem을 선택합니다.
5. OpsItem의 운영 데이터를 검토합니다. 운영 데이터에는 다음 항목이 포함됩니다.

- trustedAdvisorCheckCategory: Trusted Advisor 검사 ID의 범주입니다. 예: 내결함성
- trustedAdvisorCheckId: 고유한 Trusted Advisor 검사 ID입니다.
- trustedAdvisorCheckMetadata: 리소스 ID를 포함한 리소스 메타데이터입니다.
- trustedAdvisorCheckName: Trusted Advisor 검사의 이름입니다.
- trustedAdvisorCheckStatus: 리소스에 대해 감지된 Trusted Advisor 검사의 상태입니다.

6. OpsItem을 수동으로 수정하려면 다음 단계를 완료하세요.

   a. 런북에서 연결된 런북(SSM 문서) 중 하나를 선택합니다.

   b. 실행을 선택합니다.

   c. AutomationAssumeRole에서 를 선택합니다 `arn:aws:iam::AWS ## ID:role/ams_ssm_automation_role`. AWS 계정 ID를 수정이 실행되는 계정 ID로 바꿉니다. 다른 파라미터 값은 작업 데이터를 참조하세요.

      리소스를 수동으로 해결하려면에 인증하는 데 사용되는 역할 또는 사용자에게 IAM 역할에 대한 `iam:PassRole` 권한이 AWS 계정 있어야 합니다`ams-ssm-automation-role`. 자세한 내용은 에 역할을 전달하거나 클라우드 아키텍트에 문의할 수 있는 사용자 권한 부여를 AWS 서비스 참조하세요.

   d. 실행을 선택합니다.

   e. 최신 상태 및 결과 열에서 SSM 문서 실행 진행 상황을 모니터링합니다.

   f. 문서가 완료되면 상태 설정, 해결됨을 선택하여 OpsItem을 수동으로 해결합니다. 문서가 실패하면 세부 정보를 검토하고 SSMdocument 다시 실행합니다. 추가 문제 해결 지원을 받으려면 서비스 요청을 생성합니다.

   문제 해결 없이 OpsItem을 해결하려면 상태를 해결됨으로 설정을 선택합니다.

7. 나머지 모든 수동 문제 해결 OpsItems 대해 3단계와 4단계를 반복합니다.

신뢰할 수 있는 해결 방법의 문제 해결

수동 문제 해결 및 문제 해결 실패에 대한 도움이 필요하면 AMS에 문의하십시오.

문제 해결 상태 및 결과를 보려면 다음 단계를 완료하세요.

1. https://console.aws.amazon.com/systems-manager/ AWS Systems Manager 콘솔을 엽니다.
2. 작업 관리, OpsCenter를 선택합니다.

3. (선택 사항) 목록에 신뢰할 수 있는 수정자 OpsItem만 포함하도록 Source=Trusted OpsItems를 기준으로 목록을 필터링합니다.
4. 검토하려는 OpsItem을 선택합니다.
5. 자동화 실행 섹션에서 문서 이름, 상태 및 결과를 검토합니다.
6. 다음과 같은 일반적인 자동화 실패를 검토합니다. 여기에 문제가 나열되지 않은 경우 CSDM에 문의하여 지원을 받으세요.

일반적인 문제 해결 오류

자동화 실행에 나열된 실행 없음

OpsItem과 연결된 실행이 없으면 잘못된 파라미터 값으로 인해 실행이 시작되지 않았음을 나타낼 수 있습니다.

문제 해결 단계

1. 운영 데이터에서 `trustedAdvisorCheckAutoRemediation` 속성 값을 검토합니다.
2. DocumentName 및 파라미터 값이 올바른지 확인합니다. 올바른 값을 보려면에서 SSM 파라미터를 구성하는 방법에 신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성 대한 세부 정보를 검토합니다. 지원되는 검사 파라미터를 검토하려면 섹션을 참조하세요. Trusted Advisor Trusted Remediator에서 지원하는 검사
3. SSM 문서의 값이 허용된 패턴과 일치하는지 확인합니다. 문서 콘텐츠에서 파라미터 세부 정보를 보려면 런북 섹션에서 문서 이름을 선택합니다.
4. 파라미터를 검토하고 수정한 후 SSM 문서를 수동으로 다시 실행합니다.
5. 이 오류가 다시 발생하지 않도록 하려면 구성에서 올바른 파라미터 값으로 문제 해결을 구성해야 합니다. 자세한 내용은 신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성 섹션을 참조하세요.

자동화 실행에서 실패한 실행

문제 해결 문서에는 API를 통해 다양한 작업을 AWS 서비스 수행하는 것과 상호 작용하는 여러 단계가 포함되어 있습니다. APIs 실패의 특정 원인을 식별하려면 다음 단계를 완료하세요.

문제 해결 단계

1. 개별 실행 단계를 보려면 자동화 실행 섹션에서 실행 ID, 링크를 선택합니다. 다음은 선택한 자동화의 실행 단계를 보여주는 Systems Manager 콘솔의 예입니다.

2. 실패 상태의 단계를 선택합니다. 다음은 오류 메시지의 예입니다.

   - `NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist`

     이 오류는 문제 해결 구성의 미리 구성된 파라미터에 잘못된 버킷 이름이 지정되었음을 나타냅니다.

     이 오류를 해결하려면 올바른 버킷 이름을 사용하여 자동화를 수동으로 실행합니다. 이 문제가 다시 발생하지 않도록 하려면 문제 해결 구성을 올바른 버킷 이름으로 업데이트합니다.
   - `DB instance my-db-instance-1 is not in available status for modification.`

     이 오류는 DB 인스턴스가 잘못된 상태이기 때문에 자동화가 예상대로 변경할 수 없음을 나타냅니다.

     이 오류를 해결하려면 자동화를 수동으로 실행합니다.

신뢰할 수 있는 수정자의 수정 로그

Trusted Remediator는 JSON 형식으로 로그를 생성하여 Amazon Simple Storage Service에 업로드합니다. 로그 파일은 AMS에서 생성하고 이름이 인 S3 버킷에 업로드됩니다`ams-trusted-remediator-{your-account-id}-logs`. AMS는 위임된 관리자 계정에 S3 버킷을 생성합니다. 로그 파일을 Quick으로 가져와 사용자 지정 문제 해결 보고서를 생성할 수 있습니다.

자세한 내용은 Quick과 신뢰할 수 있는 Remediator 통합 단원을 참조하십시오.

문제 해결 항목 로그

Trusted Remediator는 문제 해결 OpsItem이 생성될 `Remediation item log` 때를 생성합니다. 이 로그에는 수동 문제 해결 OpsItem 및 자동 문제 해결 OpsItem이 포함되어 있습니다. `Remediation item log`를 사용하여 모든 수정 사항의 개요를 추적할 수 있습니다.

Compute Optimizer 권장 사항에 대한 문제 해결 항목 로그 위치

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/compute_optimizer_remediation_items/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Compute Optimizer check ID`*`-`*`Resource ID`*`.json`

Trusted Advisor 검사를 위한 문제 해결 항목 로그 위치

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/remediation_items/*remediation creation time in yyyy-mm-dd format*/*10 digits epoch time or unix timestamp*-*Trusted Advisor check ID*- *Resource ID*.json

Security Hub CSPM 권장 사항에 대한 문제 해결 항목 로그 위치

s3://ams-trusted-remediator-*delegated-administrator-account*-id-logs/security_hub_remediation_items/*remediation creation time in yyyy-mm-dd format*/*10 digits epoch time or unix timestamp-Security Hub CSPM check ID-Resource ID*.json

문제 해결 항목 로그 샘플 파일 URL

s3:///ams-trusted-remediator-*111122223333*-logs/remediation_items/*2023-02-06*/*1675660464-DAvU99Dc4C-vol-00bd8965660b4c16d.json*

Compute Optimizer 문제 해결 항목 로그 형식

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor 문제 해결 항목 로그 형식

```
{
   "TrustedAdvisorCheckID": Trusted Advisor check ID,
   "TrustedAdvisorCheckName": Trusted Advisor check name,
   "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
   "ResourceID": Resource ID,
   "RemediationTime": Remediation creation time,
   "ExecutionMode": Automated or Manual,
   "OpsItemID": OpsItem ID
}
```

Security Hub CSPM 문제 해결 항목 로그 형식

```
{
 "AccountID": "Account_ID",
 "SecurityHubCheckID": "Security Hub check ID",
 "SecurityHubCheckName": "Security Hub check name",
 "ResourceID": "Resource ID",
 "RemediationTime": Remediation creation time,
 "ExecutionMode": "Automated or Manual",
 "OpsItemID": "OpsItem ID"
}
```

Compute Optimizer 문제 해결 항목 로그 형식 샘플 콘텐츠

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor 문제 해결 항목 로그 형식 샘플 콘텐츠

```
{
    "TrustedAdvisorCheckID": "DAvU99Dc4C",
    "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
    "TrustedAdvisorCheckResultTime": 1675614749,
    "ResourceID": "vol-00bd8965660b4c16d",
    "RemediationTime": 1675660464,
    "OpsItemID": "oi-cca5df7af718"
}
```

Security Hub CSPM 문제 해결 항목 로그 형식 샘플 콘텐츠

```
{
    "AccountID": "012345678901",
    "SecurityHubControlID": "security-hub-lambda-7",
    "SecurityHubControlName": "Lambda functions should have AWS X-Ray active tracing
 enabled",
```

```
    "SecurityHubControlResultTime": 1764580147,
    "ResourceID": "test-lambda-7-xray-disabled",
    "RemediationTime": 1764900171,
    "ExecutionMode": "Manual",
    "OpsItemID": "oi-ea12c3456d7f"
}
```

자동 문제 해결 실행 로그, Compute Optimizer, Security Hub CSPM 및 Trusted Advisor

Trusted Remediator는 자동 SSM 문서 실행이 완료되면 `Automated remediation execution log`를 생성합니다. 이 로그에는 자동 문제 해결 OpsItem에 대한 SSM 실행 세부 정보만 포함되어 있습니다. 이 로그 파일을 사용하여 자동 문제 해결을 추적할 수 있습니다.

Compute Optimizer 자동 문제 해결 로그 위치

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Compute Optimizer recommendation ID`*`.json`

Security Hub CSPM 자동 문제 해결 로그 위치

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Security Hub CSPM recommendation ID`*`.json`

Trusted Advisor 자동 문제 해결 로그 위치

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`-`*`Resource ID`*`.json`

Compute Optimizer 자동 문제 해결 로그 위치 예제

`s3://ams-trusted-remediator-`*`111122223333`*`-logs/remediation_executions/2025-06-26/1750908858-123456789012-compute-optimizer-ec2-i-1235173471d2cd789.json`

Security Hub CSPM 자동 문제 해결 로그 위치 예제

s3://ams-trusted-remediator-*111122223333*-logs/remediation_executions/2025-06-26/763247655-066028476520-security-hub-rds-8-miz-tr-sh-test-rds-instance-1.json

Trusted Advisor 자동 문제 해결 로그 위치 예제

s3://ams-trusted-remediator-*111122223333*-logs/remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-vol-00bd8965660b4c16d.json

자동 문제 해결 로그 형식 샘플 콘텐츠

```
{
    "OpsItemID": "oi-767c77e05301",
    "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",
    "SSMExecutionStatus": "Success"
}
```

멤버 계정 로그

신뢰할 수 있는 수정자는 계정이 온보딩되거나 오프보딩될 `Member accounts log` 때를 생성합니다. `Member accounts log`를 사용하여 각 멤버 계정의 계정 ID, 온보딩된 AWS 리전및 실행 시간을 찾을 수 있습니다.

멤버 계정 로그 위치

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/configuration_logs/member_accounts.json

멤버 계정 로그 샘플 파일 URL

s3://ams-trusted-remediator-*111122223333*-logs/configuration_logs/member_accounts.json

멤버 계정 로그 형식

```
{
    "delegated_administrator_account_id": Delegated Administrator account id,
    "appconfig_configuration_region": Trusted Remediator AppConfig Region,
    "member_accounts": [
        {
```

```
            "account_id": Member account id
            "account_partition": Member account partition (for example, aws),
            "regions": [
                {
                    "execution_time": Remediation execution time in cron schedule
 expression,
                    "execution_timezone": Timezone for the remediation execution time,
                    "region_name": AWS ## name
                }
                ...
            ]
        }
        ...
    ],
    "updated_at": Log update time,
}
```

멤버 계정 로그 형식 샘플 콘텐츠

```
{
    "delegated_administrator_account_id": "111122223333",
    "appconfig_configuration_region": "ap-southeast-2",
    "member_accounts": [
        {
            "account_id": "222233334444",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 9 * * 6",
                    "execution_timezone": "Australia/Sydney",
                    "region_name": "ap-southeast-2"
                },
                {
                    "execution_time": "0 5 * * 7",
                    "execution_timezone": "UTC",
                    "region_name": "us-east-1"
                }
            ]
        },
        {
            "account_id": "333344445555",
            "account_partition": "aws",
            "regions": [
```

```
                {
                    "execution_time": "0 1 * * 5",
                    "execution_timezone": "Asia/Seoul",
                    "region_name": "ap-northeast-2"
                }
            ]
        }
    ],
    "updated_at": "1730869607"
}
```

Quick과 신뢰할 수 있는 Remediator 통합

Amazon S3에 저장된 신뢰할 수 있는 수정자 로그를 Quick과 통합하여 사용자 지정 수정 보고서를 작성할 수 있습니다. 빠른 통합은 선택 사항입니다. 이 기능을 사용하면 로그를 사용하여 사용자 지정 보고 대시보드를 구축할 수 있습니다. 신뢰할 수 있는 수정자에 대한 요청 시 보고서를 얻으려면 CSDM에 문의하십시오. 사용 가능한 신뢰할 수 있는 수정자 보고서에 대한 자세한 내용은 섹션을 참조하세요신뢰할 수 있는 수정자 보고서.

빠른 데이터 시각화에 대한 자세한 내용은 빠른 데이터 시각화를 참조하세요.

문제 해결 항목 로그를 위해 빠른에 데이터 세트 추가

Quick for the Remediation 항목 로그에 데이터 세트를 추가하려면 다음 단계를 따르세요.

1. Quick 콘솔에 로그인합니다. Quick이 지원하는 모든에서 AWS 리전 Quick 보고서를 생성할 수 있습니다. 그러나 성능 향상과 비용 절감을 위해 신뢰할 수 있는 수정자 로깅 버킷이 있는 리전에서 보고서를 생성하는 것이 가장 좋습니다.
2. 데이터세트를 선택하세요.
3. S3를 선택합니다.
4. 새 S3 데이터 소스에 다음 값을 입력합니다.

   - 데이터 소스 이름: `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-items`.
   - 매니페스트 파일 업로드: 다음 콘텐츠가 포함된 JSON 파일을 생성하고 사용합니다. 파일을 생성할 때 URIPrefixes 키`logging_bucket_name`에서를 바꿉니다.

     ```
     {
         "fileLocations": [
     ```

```
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_items/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- 연결을 선택합니다.
- 데이터세트 생성 완료 창에서 시각화를 선택합니다.
- Quick은 새 분석 시트 페이지를 엽니다. 이제 문제 해결 항목 로그를 사용하여 새 분석을 생성할 준비가 되었습니다.

다음은 샘플 분석입니다.

자동 문제 해결 실행 로그를 위해 Quick에 데이터 세트 추가

1. Quick 콘솔에 로그인합니다. Quick이 지원하는 모든에서 AWS 리전 Quick 보고서를 생성할 수 있습니다. 그러나 성능 향상과 비용 절감을 위해 신뢰할 수 있는 수정자 로깅 버킷이 있는 리전에서 보고서를 생성하는 것이 가장 좋습니다.
2. 데이터세트를 선택하세요.
3. S3를 선택합니다.
4. 새 S3 데이터 소스에 다음 값을 입력합니다.

   - 데이터 소스 이름: `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-executions`.
   - 매니페스트 파일 업로드: 다음 콘텐츠가 포함된 JSON 파일을 생성한 다음이 파일을 사용합니다. 파일을 생성할 때 URIPrefixes 키logging_bucket_name에서를 바꿉니다.

```
{
    "fileLocations": [
```

```
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_executions/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- 연결을 선택합니다.
- 데이터세트 생성 완료 창에서 시각화를 선택합니다.
- Quick은 새 분석 시트 페이지를 엽니다. 이제 문제 해결 항목 로그를 사용하여 새 분석을 생성할 준비가 되었습니다.

다음은 샘플 분석입니다.

신뢰할 수 있는 해결 방법의 모범 사례

다음은 신뢰할 수 있는 해결 방법을 사용하는 데 도움이 되는 모범 사례입니다.

- 해결 결과에 대해 잘 모르는 경우 수동 실행 모드로 시작합니다. 때때로 처음부터 문제 해결을 위해 자동 실행을 적용하면 예상치 못한 결과가 발생할 수 있습니다.
- 문제 해결 및 OpsItems을 매주 검토하여 신뢰할 수 있는 문제 해결사 결과에 대한 인사이트를 얻습니다.
- 멤버 계정은 위임된 관리자 계정에서 구성을 상속합니다. 따라서 동일한 구성으로 여러 계정을 관리하는 데 도움이 되는 방식으로 계정을 구성하는 것이 중요합니다. 태그를 사용하여 기본 구성에서 리소스를 제외할 수 있습니다.

신뢰할 수 있는 해결사 FAQs

다음은 신뢰할 수 있는 수정자에 대해 자주 묻는 질문입니다.

Trusted Remediator란 무엇이며 어떤 이점이 있나요?

Compute Optimizer Trusted Advisor 또는 Security Hub CSPM에서 규정 미준수가 식별되거나 권장 사항이 발행되면 신뢰할 수 있는 해결사는 문제 해결을 적용하거나, 수동 문제 해결을 통해 승인을 구하거나, 예정된 월간 비즈니스 검토(MBR) 중에 문제 해결을 보고하여 지정된 기본 설정에 따라 응답합니다. 문제 해결은 원하는 문제 해결 시간 또는 일정에 이루어집니다. Trusted Remediator는 Trusted Advisor 검사를 개별적으로 또는 대량으로 구성하고 수정할 수 있는 유연성과 함께 검사를 셀프 서비스하고 조치를 취할 수 있는 기능을 제공합니다. 테스트된 문제 해결 문서 라이브러리를 통해 AMS는 안전 검사를 적용하고 AWS 모범 사례를 따라 계정을 지속적으로 높입니다. 구성에서 그렇게 하도록 지정한 경우에만 알림을 받습니다. AMS 사용자는 추가 비용 없이 신뢰할 수 있는 수정자를 선택할 수 있습니다.

Trusted Remediator는 다른와 어떤 관련이 있고 어떻게 작동하나요 AWS 서비스?

기존 엔터프라이즈 지원 계획의 일부로 Trusted Advisor 검사, Compute Optimizer 권장 사항 및 Security Hub CSPM 제어에 액세스할 수 있습니다. Trusted Remediator는 Trusted Advisor Compute Optimizer 및 Security Hub CSPM과 통합되어 기존 AMS 자동화 기능을 활용합니다. 특히 AMS는 자동 문제 해결을 위해 AWS Systems Manager 자동화 문서(런북)를 사용합니다. AWS AppConfig 는 문제 해결 워크플로를 구성하는 데 사용됩니다. Systems Manager OpsCenter를 통해 현재 및 과거 수정 사항을 모두 볼 수 있습니다. 문제 해결 로그는 Amazon S3 버킷에 저장됩니다. 로그를 사용하여 Quick에서 사용자 지정 보고 대시보드를 가져오고 빌드할 수 있습니다.

문제 해결은 누가 구성하나요?

계정의 구성을 소유합니다. 구성 관리는 사용자의 책임입니다. CA 또는 CDSM에 문의하여 구성 관리에 도움을 받을 수 있습니다. 구성 지원, 수동 문제 해결 및 문제 해결 실패에 대한 서비스 요청을 통해 AMS에 문의할 수도 있습니다.

SSM 자동화 문서는 어떻게 설치하나요?

SSM 자동화 문서는 온보딩된 AMS 계정에 자동으로 공유됩니다.

AMS 소유 리소스도 수정되나요?

AMS 소유 리소스는 신뢰할 수 있는 수정자에서 플래그를 지정하지 않습니다. Trusted Remediator는 리소스에만 중점을 둡니다.

에서 AWS 리전 신뢰할 수 있는 수정자는 무엇이며 누가 사용할 수 있습니까?

신뢰할 수 있는 수정자는 AMS Accelerate 고객에게 제공됩니다. 현재 지원 리전 목록은 AWS 서비스 리전별 섹션을 참조하세요.

신뢰할 수 있는 해결 방법으로 인해 리소스 드리프트가 발생하나요?

SSM 자동화 문서는 AWS API를 통해 리소스를 직접 업데이트하므로 리소스 드리프트가 발생할 수 있습니다. 태그를 사용하여 기존 CI/CD 패키지를 통해 생성된 리소스를 분리할 수 있습니다. 다른 리소스를 여전히 수정하면서 태그가 지정된 리소스를 무시하도록 신뢰할 수 있는 수정자를 구성할 수 있습니다.

신뢰할 수 있는 수정자를 일시 중지하거나 중지하려면 어떻게 해야 합니까?

AWS AppConfig 애플리케이션을 통해 신뢰할 수 있는 수정자를 끌 수 있습니다. 신뢰할 수 있는 수정자를 일시 중지하거나 중지하려면 다음 단계를 완료하세요.

1. https://console.aws.amazon.com/systems-manager/appconfig AWS AppConfig 콘솔을 엽니다.
2. 신뢰할 수 있는 수정자를 선택합니다.
3. 구성 프로필에서 설정을 선택합니다.
4. 신뢰할 수 있는 수정자 일시 중지 플래그를 선택합니다.
5. `suspended` 속성의 값을 로 설정합니다`true`.

> **Note**
>
> 이 절차를 사용하면 위임된 관리자 계정에 연결된 모든 계정에 대해 신뢰할 수 있는 수정자가 중지되므로 주의해야 합니다.

신뢰할 수 있는 해결자가 지원하지 않는 검사를 해결하려면 어떻게 해야 하나요?

지원되지 않는 검사에 대해서는 OOD(운영 온디맨드)를 통해 AMS에 계속 연락할 수 있습니다. AMS는 이러한 검사를 해결하는 데 도움이 됩니다. 자세한 내용은 온디맨드 작업을 참조하세요.

Trusted Remediator는 AWS Config 문제 해결과 어떻게 다릅니까?

AWS Config 문제 해결은 클라우드 리소스를 최적화하고 모범 사례를 준수하는 데 도움이 되는 또 다른 솔루션입니다. 다음은 두 솔루션 간의 몇 가지 운영 차이점입니다.

- Trusted Remediator는 Trusted Advisor Compute Optimizer 및 Security Hub CSPM을 감지 메커니즘으로 사용합니다. AWS Config 문제 해결은 AWS Config 규칙을 감지 메커니즘으로 사용합니다.
- 신뢰할 수 있는 수정자의 경우 미리 정의된 수정 일정에 따라 수정이 이루어집니다. 에서 AWS Config해결은 실시간으로 이루어집니다.

- Trusted Remediator의 각 수정에 대한 파라미터는 사용 사례에 따라 쉽게 사용자 지정할 수 있으며 리소스에 태그를 추가하여 수정을 자동화하거나 수동으로 수행할 수 있습니다.
- Trusted Remediator는 보고 기능을 제공합니다.
- Trusted Remediator는 문제 해결 목록 및 문제 해결 상태와 함께 이메일 알림을 보냅니다.

일부 Trusted Advisor 검사, Compute Optimizer 및 Security Hub CSPM 권장 사항에는 동일한 규칙이 있을 수 있습니다 AWS Config. 일치하는 AWS Config 규칙과 Trusted Advisor 확인이 있는 경우 하나의 수정만 활성화하는 것이 가장 좋습니다. 각 Trusted Advisor 검사의 AWS Config 규칙에 대한 자세한 내용은 섹션을 참조하세요Trusted Advisor Trusted Remediator에서 지원하는 검사.

Trusted Remediator는 계정에 어떤 리소스를 배포하나요?

Trusted Remediator는 Trusted Remediator 위임된 관리자 계정에 다음 리소스를 배포합니다.

- `ams-trusted-remediator-{your-account-id}-logs`이라는 Amazon S3 버킷. Trusted Remediator는 문제 해결 OpsItem이 생성될 때 `Remediation item log` JSON 형식으로를 생성하고 로그 파일을이 버킷에 업로드합니다.
- 지원되는 Trusted Advisor 검사, Compute Optimizer 및 Security Hub CSPM 권장 사항에 대한 문제 해결 구성을 보관하는 AWS AppConfig 애플리케이션입니다.

Trusted Remediator는 Trusted Remediator 멤버 계정에 리소스를 배포하지 않습니다.

AMS Accelerate에서 Amazon EKS 모니터링 및 인시던트 관리

Amazon EKS용 모니터링 및 인시던트 관리는 Amazon EKS 리소스에서 장애, 성능 저하 및 보안 문제를 모니터링합니다. AMS Accelerate는 Amazon Managed Service for Prometheus 알림 관리자 규칙을 구성 및 배포하고, 알림을 모니터링한 다음, 이러한 알림이 트리거될 때 인시던트 관리를 수행합니다. Amazon EKS의 모니터링 및 인시던트 관리는 AMS 경보 관리자를 사용하며 Amazon Managed Service for Prometheus, Amazon Managed Grafana, Amazon GuardDuty, 및 AWS Lambda와 같은 네이티브 AWS 서비스를 활용합니다AWS Config.

> **Important**
>
> Amazon EKS에 대한 모니터링 및 인시던트 관리는 아시아 태평양(말레이시아) 리전 AWS GovCloud (US), Windows 노드 또는 Windows 컨테이너를 지원하지 않습니다.

AMS Accelerate에서 Amazon EKS에 대한 모니터링 및 인시던트 관리란 무엇입니까?

Amazon EKS의 모니터링 및 인시던트 관리는 다음을 제공합니다.

- 선택한 Amazon EKS 클러스터의 관리형 계정에서 모니터 및 정책을 생성, 관리 및 배포하는 기본 구성입니다.
- Amazon EKS 클러스터에 대한 다른 모니터링을 구성하지 않더라도 Amazon EKS 워크로드의 가용성을 높일 수 있는 모니터링 기준입니다. 자세한 내용은 AMS Accelerate에서 Amazon EKS 모니터링 및 인시던트 관리의 기준 알림 단원을 참조하십시오.
- Amazon EKS 클러스터에 대해 구성된 기준 모니터링에 의해 생성되는 알림입니다. 이러한 알림을 알림이라고 합니다. 임박한 장애, 지속적인 장애, 후퇴 또는 잠재적 장애, 성능 저하 또는 보안 문제가 있는 경우 알림이 생성됩니다. 알림의 예로는 Prometheus 알림, 이벤트 또는 Amazon GuardDuty와 같은 AWS 서비스의 결과가 있습니다.
- 취할 수 있는 적절한 문제 해결 조치에 대한 지침이 포함된 알림 조사. 자세한 내용은 AMS Accelerate의 인시던트 보고서 및 서비스 요청을 참조하세요.
- 애플리케이션에 미치는 영향을 방지하거나 줄이기 위해 가능한 경우 승인에 따라 AMS 운영별로 알림 및 인시던트를 수정합니다. 자세한 내용은 AMS Accelerate의 인시던트 보고서 및 서비스 요청을 참조하세요.

- 리소스 사용률, 성능, CoreDNS 상태, 활성 알림 및 이전에 해결된 알림에 대한 가시성을 제공하는 사전 정의된 선택적 Amazon Managed Grafana 대시보드입니다. AMS 제공 템플릿을 사용하여 Amazon Managed Grafana를 구성하는 경우 Amazon Managed Grafana 콘솔을 열어 Amazon EKS 클러스터에 대한 지표 및 알림을 볼 수 있습니다.

AMS Accelerate에서 Amazon EKS에 대한 모니터링 및 인시던트 관리 작동 방식

생성: AMS는 EKS에 대한 온보딩 모니터링 및 인시던트 관리의 일환으로 관리형 계정에서 선택한 Amazon EKS 클러스터에 대한 기준 모니터링을 구성합니다. AMS는 Amazon Managed Service for Prometheus 알림 관리자 규칙과 Amazon CloudWatch 이벤트 규칙의 조합을 사용하여 기준 모니터링을 구성합니다. 클러스터의 AMS 구성 Prometheus 서버는 Prometheus 지표를 스크레이프하고 동일한 리전의 Amazon Managed Service for Prometheus 엔드포인트에 원격 작성합니다. 기본 모니터링 구성은 Prometheus 알림 관리자 규칙이 트리거되거나 CloudWatch 이벤트가 생성될 때 알림을 생성합니다.

집계: AMS는 리소스가 생성하는 모든 알림을 AMS에서 관리하는 Amazon Simple Notification Service 주제로 전달하여 AMS 모니터링 시스템에 전송합니다.

처리 및 영향 분석: AMS는 알림을 분석한 다음 영향 가능성을 기반으로 처리합니다. AMS는 다음과 같이 알림을 분류합니다.

- 알려진 고객 영향이 있는 알림: 이러한 알림의 경우 AMS는 인시던트 관리 프로세스를 사용하여 새 인시던트 보고서를 생성합니다.
- 고객에게 미치는 영향이 불확실한 알림: 이러한 알림의 경우 AMS는 인시던트 보고서를 전송합니다. 대부분의 경우 이러한 알림은 AMS가 조치를 취하기 전에 영향을 확인하도록 요청합니다. 이러한 알림의 경우 AMS는 세부 정보가 포함된 알림 알림을 보내고 알림에 완화 작업이 필요한지 확인합니다. AMS는 알림에서 작업을 완화하는 옵션을 제공합니다. 회신에서 알림이 인시던트임을 확인하면 AMS는 새 인시던트 보고서 생성을 트리거하고 인시던트 관리 프로세스를 시작합니다. "고객 영향 없음" 또는 3일 동안 전혀 응답하지 않음 응답을 수신하는 모든 서비스 알림은 해결된 것으로 표시됩니다. 또한 해당 알림은 해결됨으로 표시됩니다.
- 고객 영향이 없는 알림: 평가 후 AMS가 알림에 고객 영향이 없다고 판단하면 알림이 종료됩니다.

AMS 책임 매트릭스(RACI)

AMS 책임, 책임, 상담 및 정보 제공 또는 RACI 매트릭스는 다양한 활동에 대해 고객 또는 AMS에 기본 책임을 할당합니다. 다음 표에는 Amazon EKS용 모니터링 및 인시던트 관리를 사용하는 애플리케이션의 활동에 대한 고객 및 AMS의 책임에 대한 개요가 나와 있습니다.

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

활동	Customer	AMS
AMS 요구 사항 검색	정보	R
클러스터 액세스에 대한 AMS 권한(RBAC) 활성화	R	C
아직 없는 경우 작업자 노드에 Amazon EC2 Systems Manager Agent 설치	R	C
필요에 따라 AMS 네임스페이스에 Prometheus, Prometheus Node Exporter 및 kube-state-metrics와 같은 AMS 클러스터 내 구성 요소를 배포합니다.	C	R
AMS 컨트롤 플레인에서 Amazon Managed Service for Prometheus 프로비저닝	정보	R
AMS 컨트롤 플레인에서 Prometheus 알림 관리자 구성	정보	R

활동	Customer	AMS
Amazon Managed Grafana 템플릿 제공 및 구성 지원	C	R
GuardDuty EKS 감사 로그 모니터링 활성화	C	R
Amazon EKS 컨트롤 플레인 로깅 활성화	정보	R
Amazon EKS 컨트롤 플레인의 상태 및 성능 모니터링	정보	R
Amazon EKS 클러스터(클러스터, 노드, 워크로드, 포드, API Server 및 CoreDNS)의 상태 및 성능 모니터링	정보	R
Amazon EKS에 대한 알림 분류 및 인시던트 대응 제공	정보	R
인시던트 발생 시 진단 명령 실행	정보	R
인시던트 중 로그 분석(컨트롤 플레인 및 포드 로그)	정보	R
AWS 네트워크 문제에 대한 인시던트 대응	정보	R
GuardDuty EKS 감사 로그 모니터링 결과에 응답	정보	R
가능한 경우 인시던트를 해결하기 위한 조치에 대한 고객 지침을 제공합니다.	정보	R

AMS Accelerate에서 Amazon EKS 모니터링 및 인시던트 관리의 기준 알림

알림을 확인한 후 AMS는 Amazon EKS에 대해 다음 알림을 활성화한 다음 선택한 Amazon EKS 클러스터에 대한 모니터링 및 인시던트 관리에 참여합니다. 서비스 수준 계약(SLAs) 및 서비스 수준 목표(SLOs) 응답 시간은 선택한 계정 서비스 티어(Plus, Premium)에 따라 달라집니다. 자세한 내용은 AMS Accelerate의 인시던트 보고서 및 서비스 요청을 참조하세요.

알림 및 작업

다음 표에는 Amazon EKS 알림과 AMS가 수행하는 각 작업이 나열되어 있습니다.

Alert	임곗값	작업
컨테이너 OOM 종료됨	지난 10분 내의 총 컨테이너 재시작 수는 1개 이상이며 포드의 Kubernetes 컨테이너가 지난 10분 내에 “OOMKilled”라는 이유로 종료되었습니다.	AMS는 컨테이너 제한에 도달하거나 메모리 제한 초과 커밋으로 인해 OOM 종료가 발생하는지 조사한 다음 수정 조치를 조언합니다.
포드 작업 실패	Kubernetes 작업이 완료되지 않습니다. 실패는 하나 이상의 실패한 작업 상태가 있는 것으로 표시됩니다.	AMS는 Kubernetes 작업 또는 해당 cron 작업이 실패하는 이유를 조사한 다음 수정 조치를 조언합니다.
StatefulSet 다운	트래픽을 처리할 준비가 된 복제본 수가 최소 1분 동안 StatefulSet당 현재 기존 복제본 수와 일치하지 않습니다.	AMS는 포드 이벤트의 오류 메시지와 포드 로그의 오류 로그 조각을 검토하여 포드가 준비되지 않는 이유를 확인한 다음 수정 조치를 조언합니다.
HPA 조정 기능	상태 조건 “AbleToScale”이 최소 2분 동안 false이므로 Horizontal Pod Autoscaler(HPA)를 조정할 수 없습니다.	AMS는 배포 또는 StatefulSet와 같은 후속 워크로드 리소스에 대해 포드를 조정할 수 없는 Kubernetes Horizontal Pod Autoscaler(HPA)를 결정합니다.

Alert	임곗값	작업
HPA 지표 가용성	상태 조건 “ScalingActive”가 2분 이상 false이므로 Horizontal Pod Autoscaler(HPA)는 지표를 수집할 수 없습니다.	AMS는 HPA가 서버 구성 문제 또는 RBAC 권한 부여 문제와 관련된 지표와 같은 지표를 수집할 수 없는 이유를 결정합니다.
포드 준비되지 않음	Kubernetes 포드는 15분 이상 실행 중이 아닌 상태(예: 보류 중, 알 수 없음 또는 실패)로 유지됩니다.	AMS는 영향을 받는 포드(들)의 세부 정보를 조사하고 포드 로그에 관련 오류 및 이벤트가 있는지 검토한 다음 수정 조치를 조언합니다.
포드 충돌 루프	포드 컨테이너는 1시간 동안 15분마다 한 번 이상 다시 시작됩니다.	AMS는 리소스 부족, 다른 컨테이너에 의해 잠긴 파일, 다른 컨테이너에 의해 잠긴 데이터베이스, 서비스 종속성 실패, 외부 서비스에 대한 DNS 문제, 잘못된 구성 등 포드가 시작되지 않는 이유를 조사합니다.
데몬 세트가 잘못 예약됨	10분 동안 Kubernetes Daemonset 포드가 하나 이상 잘못 예약되어 있습니다.	AMS는 Daemonset이 실행되지 않아야 하는 노드에 예약된 이유를 결정합니다. 이는 잘못된 포드 nodeSelector/taints/affinities가 Daemonset 포드에 적용되었거나 노드(노드 풀)가 테인트되고 기존 포드가 제거되도록 예약되지 않은 경우에 발생할 수 있습니다.

Alert	임곗값	작업
Kubernetes API 오류	Kubernetes API 서버 오류율이 2분 동안 3%를 초과합니다.	AMS는 컨트롤 플레인 로그를 분석하여이 알림을 유발하는 오류의 볼륨과 유형을 확인하고 마스터 노드 또는 etcd Autoscaling 그룹에 대한 리소스 경합 문제를 식별합니다. API 서버가 복구되지 않으면 AMS는 Amazon EKS 서비스 팀을 참여시킵니다.
Kubernetes API 지연 시간	Kubernetes API 서버에 대한 요청의 99번째 백분위수 지연 시간이 2분 동안 1초를 초과합니다.	AMS는 컨트롤 플레인 로그를 분석하여 지연 시간을 유발하는 오류의 볼륨과 유형을 확인하고 마스터 노드 또는 etcd Auto Scaling 그룹에 대한 리소스 경합 문제를 식별합니다. API 서버가 복구되지 않으면 AMS는 Amazon EKS 서비스 팀을 참여시킵니다.
Kubernetes 클라이언트 인증서 만료	Kubernetes API 서버에 인증하는 데 사용되는 클라이언트 인증서가 24시간 이내에 만료됩니다.	AMS는 클러스터 인증서가 24시간 후에 만료됨을 알리기 위해이 알림을 보냅니다.
노드 준비되지 않음	노드 “준비” 조건 상태는 최소 10분 동안 false입니다.	AMS는 API 서버에 대한 kubelet 액세스를 방지하는 네트워크 문제와 같은 노드 조건 및 이벤트를 조사합니다.

Alert	임곗값	작업
노드 높은 CPU	CPU 부하가 5분 동안 80%를 초과합니다.	AMS는 하나 이상의 포드가 비정상적으로 많은 양의 CPU를 소비하는지 여부를 결정합니다. 그런 다음 AMS는 요청, 제한 및 포드 활동이 예상대로인지 확인합니다.
노드 OOM 종료 감지됨	4분 동안 노드에서 호스트 OOM 종료가 하나 이상 보고됩니다.	AMS는 컨테이너 제한에 도달하거나 노드 초과 커밋으로 인해 OOM 종료가 발생하는지 확인합니다. 애플리케이션 활동이 정상인 경우 AMS는 초과 커밋 및 포드 제한 수정에 대한 요청 및 제한에 대해 조언합니다.
노드 연결 트랙 제한	현재 연결 추적 항목 수와 최대 한도의 비율이 5분 동안 80%를 초과합니다.	AMS는 코어당 권장 conntrack 값을 알려줍니다. Kubernetes 노드는 노드의 총 메모리 용량에 비례하여 conntrack 최대값을 설정합니다. 로드가 많은 애플리케이션, 특히 더 작은 노드에서는 콘트랙 최대값을 쉽게 초과할 수 있으므로 연결이 재설정되고 제한 시간이 초과될 수 있습니다.
노드 클럭이 동기화되지 않음	2분 동안의 최소 동기화 상태는 0이고 초 단위의 최대 오류는 16 이상입니다.	AMS는 NTP(Network Time Protocol)가 설치되어 제대로 작동하는지 여부를 결정합니다.
포드 하이 CPU	컨테이너의 CPU 사용량이 최소 2분 동안 3분 동안 80%를 초과합니다.	AMS는 포드 로그를 조사하여 많은 양의 CPU를 소비하는 포드 작업을 결정합니다.

Alert	임곗값	작업
포드 고용량 메모리	컨테이너의 메모리 사용량이 2분 동안 지정된 메모리 제한의 80%를 초과합니다.	AMS는 포드 로그를 조사하여 많은 양의 메모리를 소비하는 포드 작업을 결정합니다.
CoreDNS 다운	CoreDNS가 15분 이상 Prometheus 대상 검색에서 사라졌습니다.	이는 내부 또는 외부 클러스터 서비스의 도메인 이름 확인이 중지되었음을 나타내는 중요한 알림입니다. AMS는 CoreDNS 포드의 상태를 확인하고, CoreDNS 구성을 확인하고, CoreDNS 포드를 가리키는 DNS 엔드포인트를 확인하고, CoreDNS 제한을 확인하고, 승인을 받아 CoreDNS 디버그 로깅을 활성화합니다.
CoreDNS 오류	CoreDNS는 10분 동안 DNS 요청의 3% 이상에 대해 SERVFAIL 오류를 반환합니다.	이 알림은 애플리케이션 문제 또는 잘못된 구성을 나타낼 수 있습니다. AMS는 CoreDNS 포드의 상태를 확인하고, CoreDNS 구성을 확인하고, CoreDNS 포드를 가리키는 DNS 엔드포인트를 확인하고, CoreDNS 제한을 확인하고, 승인을 받아 CoreDNS 디버그 로깅을 활성화합니다.

Alert	임곗값	작업
CoreDNS 지연 시간	DNS 요청 기간의 99번째 백분위수가 10분 동안 4초를 초과합니다.	이 알림 CoreDNS가 오버로드될 수 있음을 나타냅니다. AMS는 CoreDNS 포드의 상태를 확인하고, CoreDNS 구성을 확인하고, CoreDNS 포드를 가리키는 DNS 엔드포인트를 확인하고, CoreDNS 제한을 확인하고, 승인을 받아 CoreDNS 디버그 로깅을 활성화합니다.
CoreDNS 전달 지연 시간	CoreDNS가 요청을 kube-dns로 전달하는 응답 시간의 99번째 백분위수가 10분 동안 4초를 초과합니다.	CoreDNS가 신뢰할 수 있는 서버가 아니거나 domanin 이름에 대한 캐시 항목이 없는 경우 CoreDNS는 DNS 요청을 업스트림 DNS 서버로 전달합니다. 이 알림은 CoreDNS가 오버로드되거나 업스트림 DNS 서버에 문제가 있을 수 있음을 나타냅니다. AMS는 CoreDNS 포드의 상태를 확인하고, CoreDNS 구성을 확인하고, CoreDNS 포드를 가리키는 DNS 엔드포인트를 확인하고, CoreDNS 제한을 확인하고, 승인을 받아 CoreDNS 디버그 로깅을 활성화합니다.

Alert	임곗값	작업
CoreDNS 전달 오류	DNS 쿼리의 3% 이상이 5분 동안 실패합니다.	CoreDNS가 신뢰할 수 있는 서버가 아니거나 domanin 이름에 대한 캐시 항목이 없는 경우 CoreDNS는 DNS 요청을 업스트림 DNS 서버로 전달합니다. 이 알림은 업스트림 DNS 서버의 구성 오류 또는 문제를 나타냅니다. AMS는 CoreDNS 포드의 상태를 확인하고, CoreDNS 구성을 확인하고, CoreDNS 포드를 가리키는 DNS 엔드포인트를 확인하고, CoreDNS 제한을 확인하고, 승인을 받아 CoreDNS 디버그 로깅을 활성화합니다.

AMS Accelerate에서 Amazon EKS의 모니터링 및 인시던트 관리를 위한 요구 사항

Amazon EKS for AMS Accelerate의 모니터링 및 인시던트 관리에 지원되는 리소스 및/또는 필요한 리소스입니다.

- 지원되는 Kubernetes 버전: Amazon EKS 사용 설명서의 Amazon EKS Kubernetes 버전을 참조하세요.
- 노드 유형: Amazon EKS 관리형 노드가 지원됩니다. Windows 노드 및 컨테이너는 지원되지 않습니다.
- Kubernetes 클러스터 액세스: AMS에는 system:masters RBAC 클러스터 역할 및 클러스터 사용자가 필요합니다.
- Amazon EC2 노드의 SSM 에이전트: Bottle Rocket과 Amazon EKS AMIs 모두에 SSM 에이전트가 사전 설치되어 있습니다. 사용자 지정 AMIs 및 Amazon EC2 노드에 SSM 에이전트가 설치되어 있는지 확인합니다.

- Service Quotas 자세한 내용은 Amazon Managed Service for Prometheus 및 Amazon Managed Grafana의 서비스 할당량을 참조하세요. https://docs.aws.amazon.com/grafana/latest/userguide/AMG_quotas.html
- 지원되는 AWS 리전:

리전 이름	리전	지표 스토리지 리전
미국 동부(오하이오)	us-east-2	us-east-2
미국 동부(버지니아 북부)	us-east-1	us-east-1
미국 서부(오리건)	us-west-2	us-west-2
아시아 태평양(도쿄)	ap-northeast-1	ap-northeast-1
아시아 태평양(서울)	ap-northeast-2	ap-northeast-2
아시아 태평양(싱가포르)	ap-southeast-1	ap-southeast-1
아시아 태평양(시드니)	ap-southeast-2	ap-southeast-2
유럽(프랑크푸르트)	eu-central-1	eu-central-1
유럽(아일랜드)	eu-west-1	eu-west-1
유럽(런던)	eu-west-2	eu-west-2
Africa (Cape Town)	af-south-1	eu-west-1 eu-west-2
Asia Pacific (Hong Kong)	ap-east-1	ap-northeast-1 ap-northeast-2

Note

af-south-1, Africa(케이프타운) 및 ap-east-1, Asia Pacific(홍콩)의 Amazon EKS 클러스터에 대한 지표는 AWS 리전각각 동일한의 AMS 모니터링 서비스로 내보내집니다. 그런 다음 이에 대한 지표 AWS 리전 는 AMS 모니터링 서비스 내에서 처리 및 저장되는 여러 리전으로

전송됩니다. AMS 모니터링 서비스가 지표를 저장하는 데 사용하는 리전은 위의 표를 참조하세요.

AMS Accelerate에서 Amazon EKS에 대한 모니터링 및 인시던트 관리에 온보딩

Amazon EKS에 대한 모니터링 및 인시던트 관리에 온보딩하려면 다음 단계를 수행합니다.

1. Amazon EKS 비용 최적화 태그 활성화: Amazon EKS 사용 설명서의 결제를 위한 리소스 태그 지정을 참조하세요.
2. EKS에 대한 모니터링 및 인시던트 관리 온보딩 시작: 온보딩할 계정 IDs 및 클러스터 이름을 사용하여 Cloud Service Delivery Manager(CSDM)에 문의하세요.
3. 요구 사항 검증: 온보딩을 시작하기 전에 클라우드 아키텍트(CA)가 모든 요구 사항이 충족되었는지 확인합니다.
4. Kubernetes 역할 기반 액세스 제어(RBAC) 업데이트: AMS는 이러한 변경 사항을 구현하는 `eksctl` 명령을 공유합니다. 이러한 변경 사항을 검토한 다음 배포할 수 있습니다. AMS가 사용자를 대신하여 명령을 실행할 수 있는 권한을 갖도록 RBAC 업데이트를 배포해야 합니다. 이러한 업데이트에는 AMS IAM 역할을 Kubernetes 사용자에게 매핑하고, AMS에 대한 새 Kubernetes 클러스터 역할을 생성하고, AMS Kubernetes 클러스터 역할을 사용자에게 바인딩하는 작업이 포함됩니다.
5. 클러스터 구성 요소 배포: AMS는 클러스터의 AMS 관리형 네임스페이스에 다음 구성 요소를 배포합니다.
   - Prometheus 서버
   - Prometheus 노드 내보내기(에는 해당되지 않음 AWS Fargate)
   - kube-state-metrics
6. Prometheus 구성 업데이트 수행: AMS는 지표에 대한 원격 쓰기를 활성화하도록 Prometheus를 구성합니다.
7. (선택 사항) 대시보드 구성: CA를 사용하면 계정에서 Amazon Managed Grafana 대시보드를 구성할 수 있습니다.

> **Note**
>
> Amazon EKS 클러스터가 온보딩되면 AMS는 알림 신호를 분석하고 기준 평가를 수행하여 클러스터의 기존 문제를 식별합니다. 기준 평가가 완료되면 AMS는 Trusted Advisor와 클러스

터의 문제를 해결하는 데 사용할 수 있는 서비스 요청을 통해 조사 결과 및 수정 권장 사항을 공유합니다. 평가를 통해 AMS는 계정 수준 경보 임계값을 조정하여 EKS 클러스터와 관련된 Amazon EKS 모니터링 기준을 생성합니다. 이러한 결과에 대한 중복 AMS 응답을 제거하기 위해 이러한 알림 신호를 제외하도록 모니터링을 조정합니다. CSDM에서 기본 문제가 해결되었음을 알릴 때 신호를 포함하도록 모니터링을 재조정합니다.

AMS Accelerate의 Amazon EKS 모니터링 및 인시던트 관리에서 오프보딩

클라우드 서비스 전송 관리자(CSDM)에게 계정 IDs와 클러스터 이름을 알려 오프보딩 프로세스를 시작합니다. 오프보드하면 알림 처리, 지표 스토리지 및 지표 쿼리가 일시 중지되고 기본 Amazon Managed Service for Prometheus 데이터 보존 정책에 따라 지표가 삭제됩니다.

AMS는 다음 오프보딩 단계를 수행합니다.

1. AMS는 사용자 및 AMS 작업으로 전송되는 알림을 비활성화합니다.
2. AMS는 Amazon EKS 클러스터에서 Prometheus 인스턴스를 제거합니다.
3. AMS는 IAM 역할 및 AWS Config 규칙과 같이 계정에 설치된 다른 AWS 리소스를 제거합니다.

이러한 단계를 완료한 후에는 다음 오프보딩 단계를 완료해야 합니다.

1. `eksctl`를 사용하여 `aws-auth`에서 Kubernetes RBAC 권한을 제거합니다`ConfigMap`.
2. 이전에 설치한 경우 AMS에 연결하도록 구성한 Amazon Managed Grafana 인스턴스를 제거합니다.

AMS Accelerate의 연속성 관리

AMS는 AWS Backup 를 활용하여 AWS 서비스 전반의 데이터 백업을 중앙 집중화하고 자동화합니다. AMS 백업 계획은 다양한 사용 사례에 대한 모범 사례를 제공하지만 기존 백업 계획을 계속 사용할 수 있습니다. AMS 백업 관리에 온보딩한 후 AMS는 백업 보고서를 제공하고 AMS 전문가는 백업 작업을 지속적으로 모니터링하여 신뢰할 수 있는 백업 솔루션이 있는지 확인합니다.

자세한 내용은 AWS Backup: 작동 방식 및 지원되는 AWS 리소스와 타사 애플리케이션을 참조하세요.

AMS Accelerate는 운영 우수성을 달성하는 데 도움이 되는 다양한 운영 서비스를 제공합니다 AWS. 연중무휴 24시간 헬프데스크, 사전 모니터링, 보안, 패치 적용, 로깅 및 백업을 포함한 몇 가지 주요 운영 기능을 AWS 클라우드 통해 AMS가에서 전반적인 운영 우수성을 달성하는 데 어떻게 도움이 되는지 빠르게 이해하려면 AMS 참조 아키텍처 다이어그램을 참조하세요.

Carl의 비디오를 보고 자세히 알아보기(9:29)

주제

- AMS에서 연속성 관리 작동 방식
- AMS 백업 계획 선택
- 리소스에 태그를 지정하여 AMS 백업 계획 적용
- AMS 볼트에서 백업 보기
- AMS 백업 모니터링 및 보고

AMS에서 연속성 관리 작동 방식

AMS 백업 계획은 데이터가 백업되는 빈도와 백업에 대한 보존 정책을 정의합니다. AMS 백업 볼트는 백업 데이터를 정리된 상태로 유지합니다. 리소스가 백업 계획과 연결되면 호환되는 리소스가 점진적으로 백업됩니다. 첫 번째 백업은 전체 사본이며 후속 백업은 증분 변경 사항을 캡처합니다. 선택한 리소스 및 AMS 백업 계획에 따라 Point-in-time 복원(PITR)을 사용하면 복구 시간을 선택하여 리소스를 되감을 수 있습니다. AMS Backup Management를 시작하려면 AMS 백업 계획을 선택하고 리소스에 태그를 지정하면 됩니다.

> **Note**
>
> 시작하기 1: 서비스 옵트인 단계에 따라 각 계정 AWS 리전및 리소스 유형에 대해 AWS Backup 가 활성화되어 있는지 확인합니다.

시작하기 2: 온디맨드 백업에서 생성을 계속할 필요가 없습니다.

의 관련 주제 AWS Backup

- 백업 작업(생성, 편집, 복사, 복원, 삭제)
- 온디맨드 백업 생성
- 에서 백업 복사본 생성 AWS 리전
- AWS Backup 지원되는 서비스
- Point-in-time 복원
- AWS Backup Features

AMS 백업 계획 선택

AMS는 온보딩 중에 비용을 최소화하기 위해 네 번째 백업 계획과 함께 세 가지 백업 계획을 제공합니다. 지원되는 각 리소스에 대한 AMS 백업 계획을 선택하려면 리소스에 계획의 관련 태그를 지정합니다. Accelerate에 온보딩하면 AMS가 고객과 협력하여 요구 사항에 가장 적합한 백업 계획을 식별합니다.

Important

변경 사항이 손실될 수 있으므로 AMS 기본 백업 계획을 편집하지 마십시오. 대신 사용자 지정 구성에 대한 새 계획을 생성합니다. 자세한 내용은 백업 계획 생성을 참조하세요.

기본 AMS 백업 계획

AWS Backup 이 백업 계획에서는 연속 백업이 활성화되지 않습니다. 자세한 내용은 point-in-time 복원(PITR)을 사용하여 지정된 시간으로 복원을 참조하세요.

TAG 키: `ams:rt:backup-orchestrator`

TAG 값: `true`

기본 AMS 백업 계획	Start Time	Retention
hourly backup	N/A	N/A

기본 AMS 백업 계획	Start Time	Retention
daily backup	daily 4:00 UTC	7 days
weekly backup	Saturday, 2:00 UTC	4 weeks
monthly backup	1st of the month, 2:00 UTC	26 weeks
yearly backup	Jan 1st, 2:00 UTC	2 years

향상된 백업 계획

AWS Backup 연속 백업은 지원되는 리소스에서 최대 보존 기간(31일)으로 활성화됩니다. 자세한 내용은 point-in-time 복원(PITR)을 사용하여 지정된 시간으로 복원 및 point-in-time 복원(PITR)을 위해 지원되는 서비스 및 애플리케이션을 참조하세요.

TAG 키: `ams:rt:backup-orchestrator-enhanced`

TAG 값: `true`

향상된 백업 계획	Start Time	Retention
hourly backup	N/A	N/A
daily backup	daily 4:00 UTC	31일
weekly backup	Saturday, 2:00 UTC	6주
monthly backup	1st of the month, 2:00 UTC	26 weeks
yearly backup	Jan 1st, 2:00 UTC	2 years

데이터에 민감한 백업 계획

AWS Backup 연속 백업은 지원되는 리소스에서 최대 보존 기간(31일)으로 활성화됩니다. 자세한 내용은 point-in-time 복원(PITR)을 사용하여 지정된 시간으로 복원 및 시점 복원(PITR)을 위해 지원되는 서비스 및 애플리케이션을 point-in-time 참조하세요.

TAG 키: `ams:rt:backup-orchestrator-data-sensitive`

TAG 값: `true`

데이터에 민감한 백업 계획	Start Time	Retention
hourly backup	every hour	7일
daily backup	daily 4:00 UTC	31일
weekly backup	Saturday, 2:00 UTC	6주
monthly backup	1st of the month, 2:00 UTC	26 weeks
yearly backup	Jan 1st, 2:00 UTC	2 years

AMS Accelerate 온보딩 백업 계획

AWS Backup 이 백업 계획에서는 연속 백업이 활성화되지 않습니다. 자세한 내용은 point-in-time 복원(PITR)을 사용하여 지정된 시간으로 복원을 참조하세요.

TAG 키: `ams:rt:backup-orchestrator-onboarding`

TAG 값: `true`

AMS Accelerate 온보딩 백업 계획	Start Time	Retention
hourly backup	every hour	2주
daily backup	N/A	N/A
weekly backup	N/A	N/A
monthly backup	N/A	N/A
yearly backup	N/A	N/A

관련 AWS Backup 주제

- 백업 계획 생성

- Point-in-time 복원(PITR)을 사용하면 지원되는 리소스를 지속적으로 백업할 수 있으며 복구를 위한 특정 시간을 선택할 수 있습니다. 지원되는 리소스 목록은 리소스별 기능 가용성을 참조하세요.

리소스에 태그를 지정하여 AMS 백업 계획 적용

AMS 백업 계획에 리소스를 할당하려면 계획의 태그 키-값 페어로 리소스에 태그를 지정합니다. AMS Resource Tagger를 사용하여 AMS 백업 계획을 리소스의 하위 집합 또는 계정에서 지원되는 모든 리소스에 적용할 수 있습니다. 대체 방법을 사용하여 AWS CloudFormation 또는 Terraform과 같은 리소스에 태그를 적용하려면 선택한 태그 지정 방법과 경쟁하지 않도록 Resource Tagger를 끕니다. 자세한 내용은 Resource Tagger의 리소스 수정 방지 단원을 참조하십시오.

다음 예제에서는 Resource Tagger를 사용하여 계정의 Amazon Elastic Compute Cloud 인스턴스에 기본 AMS 백업 계획을 적용하는 방법을 보여줍니다. 이 백업 계획의 경우 태그 키`ams:rt:backup-orchestrator`와 값를 적용합니다`true`. 다른 백업 계획을 사용하려면 원하는 백업 계획의 태그 키와 일치하도록 키를 변경합니다. AMS Resource Tagger에 대해 알아보고 다음 참조된 프로파일을 Accelerate 계정의 현재(이미 구성됨) 프로파일과 통합하는 방법을 이해하려면 섹션을 참조하세요리소스 태거 가속화.

1. https://console.aws.amazon.com/systems-manager/appconfig AWS AppConfig 콘솔을 엽니다.
2. ResourceTagger 애플리케이션을 선택합니다.
3. 구성 프로필 탭을 선택한 다음 CustomerManagedTags를 선택합니다.
4. 생성을 선택하여 새 버전을 생성합니다.
5. JSON을 선택한 다음 다음 JSON 객체를 복사하여 붙여 넣습니다.

```
{
    "AWS::EC2::Instance": {
        "AccelerateBackupPlan": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "*"
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:backup-orchestrator",
                    "Value": "true"
```

```
                }
            ]
        }
    }
}
```

6. 호스팅 구성 버전 생성을 선택합니다.
7. Start deployment(배포 시작)를 선택합니다.
8. 다음 배포 세부 정보를 정의합니다.

```
Environment: AMSInfrastructure
Hosted configuration version: Select the version that you have just created.
Deployment Strategy: AMSNoBakeDeployment
```

9. Start deployment(배포 시작)를 선택합니다. Resource Tagger는 인스턴스에 태그를 지정`ams:rt:backup-orchestrator: true`하여 인스턴스가 기본 AMS 백업 계획에 따라 백업되도록 합니다.

AMS 볼트에서 백업 보기

태그를 사용하여 개별 볼트 수준에서 백업 볼트 알림을 제어할 수 있습니다. 태그를 추가`AMSNotificationOptOut`하고 특정 볼트에서 값을 로 설정하여 특정 볼트`True`에 대한 알림을 옵트아웃할 수 있습니다. 볼트에서 알림을 다시 받으려면 태그를 제거합니다.

AMS 백업 목록을 보려면 AWS Backup 콘솔을 엽니다. 탐색 창에서 백업 볼트를 선택하고 다음 표에서 AMS 백업 볼트 중 하나를 선택합니다. 백업 섹션에서 백업 볼트의 모든 백업 목록을 봅니다. 편집, 삭제 또는 복원할 백업을 선택합니다.

AMS 백업 계획을 위한 볼트

AMS 볼트 이름	AMS 백업 계획 태그 키
ams-automated-backups	ams:rt:backup-orchestrator
ams-automated-enhanced-backups	ams:rt:backup-orchestrator-enhanced
ams-automated-data-sensitive-backups	ams:rt:backup-orchestrator-data-sensitive
ams-onboarding-backups	ams:rt:backup-orchestrator-onboarding

기타 AMS 볼트

AMS 볼트 이름	설명
ams-manual-backups	This vault contains manually started backups created by the `AWSManagedServices-StartBackupJob` SSM Automation document and pre-patch backups created by AMS patch automations before patching.
ams-custom-backups	This is the recommended vault for backups created outside of AMS backup plans.

관련 AWS Backup 주제

- 리소스별 백업 보기
- 백업 작업

AMS 백업 모니터링 및 보고

> **Important**
>
> AMS 백업 모니터링 및 보고는 AMS 지원 리전에서만 사용할 수 있습니다. 미국 동부(버지니아), 미국 서부(캘리포니아 북부), 미국 서부(오레곤), 미국 동부(오하이오), 캐나다(중부), 남아메리카(상파울루), EU(아일랜드), EU(프랑크푸르트), EU(런던), EU(파리), 아시아 태평양(뭄바이), 아시아 태평양(서울), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 아시아 태평양(도쿄)입니다.

AMS는 일일 셀프 서비스 보고서와 리소스 적용 범위 및 백업 작업 상태에 대한 월별 보고서를 생성합니다. 월별 보고서는 월별 비즈니스 검토(MBRs. 일일 백업 보고서에 대한 자세한 내용은 일일 백업 보고서참조하십시오.

AMS 전문가는를 사용하여 구성된 모든 백업 작업을 모니터링합니다 AWS Backup. 백업 실패의 경우 AMS는 실패를 조사하고 가능한 경우 근본 원인 및 해결 옵션을 알려줍니다. 알림 노이즈를 방지하기 위해 계정에서 백업 실패 수가 많은 이벤트가 발생하는 경우 AMS는 각 개별 실패에 대해 알리는 대신 CSDM을 통해 집합적 권장 사항을 제공합니다.

AMS는 AWS 서비스의 독립 실행형 백업 기능을 사용하여 구성된 백업을 모니터링하지 않습니다.

AMS Accelerate의 패치 관리 이해

Important

패치 가속화 보고는 AWS Glue 리소스 기반 정책을 주기적으로 배포합니다. 패치 적용 시스템에 대한 AMS 업데이트는 기존 AWS Glue 리소스 기반 정책을 덮어씁니다.

Important

관리형 노드에 대한 대체 패치 리포지토리를 지정할 수 있습니다. AMS가 요청된 패치 구성을 구현하는 동안 선택한 리포지토리의 보안을 선택하고 검증할 책임은 사용자에게 있습니다. 또한 공급망 위험과 같이 이러한 리포지토리 사용으로 인한 위험도 허용해야 합니다.
다음은 패치 관리 프로세스의 보안을 위한 모범 사례입니다.

- 신뢰할 수 있고 검증된 리포지토리 소스만 사용
- 가능한 경우 표준 OS 공급업체 리포지토리 기본값
- 사용자 지정 리포지토리 구성을 정기적으로 감사

AMS Accelerate 패치 적용 시스템인 패치 추가 기능을 사용하여 보안 관련 업데이트 및 기타 유형의 업데이트로 인스턴스를 패치할 수 있습니다. Accelerate Patch 추가 기능은 AMS 인스턴스에 태그 기반 패치를 제공하는 기능입니다. (AWS Systems Manager SSM) 기능을 활용하므로 인스턴스에 태그를 지정하고 구성한 기준 및 창을 사용하여 해당 인스턴스에 패치를 적용할 수 있습니다. AMS Accelerate 패치 추가 기능은 온보딩 옵션입니다. Accelerate 계정을 온보딩하는 동안 획득하지 못한 경우 클라우드 서비스 제공 관리자(CSDM)에게 문의하여 획득하세요.

AMS Accelerate 패치 관리는 Systems Manager 패치 기준 기능을 사용하여 인스턴스에 적용되는 패치의 정의를 제어합니다. 패치 기준에는 모든 보안 패치와 같이 사전 승인된 패치 목록이 포함되어 있습니다. 인스턴스의 규정 준수는 인스턴스와 연결된 패치 기준과 비교하여 측정됩니다. AMS Accelerate는 기본적으로 인스턴스를 최신 상태로 유지하는 데 사용할 수 있는 모든 패치를 설치합니다.

Note

AMS Accelerate는 운영 체제(OS) 패치만 적용합니다. 예를 들어 Windows의 경우 Microsoft 업데이트가 아닌 Windows 업데이트만 적용됩니다.

보고서에 대한 자세한 내용은 단원을 참조하십시오AMS 호스트 관리 보고서.

AMS Accelerate는 운영 우수성을 달성하는 데 도움이 되는 다양한 운영 서비스를 제공합니다 AWS. 연중무휴 24시간 헬프데스크, 사전 모니터링, 보안, 패치 적용, 로깅 및 백업을 포함한 몇 가지 주요 운영 기능을 AWS 클라우드 통해 AMS가에서 전반적인 운영 우수성을 달성하는 데 어떻게 도움이 되는지 빠르게 이해하려면 AMS 참조 아키텍처 다이어그램을 참조하세요.

주제

- 패치 적용 권장 사항
- AMS에서 패치 유지 관리 기간 생성
- 후크가 있는 패치
- AMS Accelerate 패치 기준
- AMS Accelerate의 온디맨드 패치를 위한 IAM 역할 생성
- AMS Accelerate의 패치 알림 및 패치 실패 이해

패치 적용 권장 사항

애플리케이션 또는 인프라 운영에 종사하고 있다면 애플리케이션 팀의 다양한 요구 사항을 충족할 수 있을 만큼 유연하고 확장 가능한 운영 체제 (OS) 패치 솔루션의 중요성을 이해하고 있을 것입니다. 일반적인 조직에서는 변경할 수 없는 인스턴스가 포함된 아키텍처를 사용하는 애플리케이션 팀도 있고 변경 가능한 인스턴스에 애플리케이션을 배포하는 애플리케이션 팀도 있습니다.

패치 적용에 대한 AWS 권장 가이드에 대한 자세한 내용은 를 사용하는 하이브리드 클라우드의 변경 가능한 인스턴스에 대한 자동 패치 적용을 AWS Systems Manager 참조하세요.

> **Note**
>
> Accelerate Patch 추가 기능은 AMS 인스턴스에 태그 기반 패치를 제공하는 기능입니다. (AWS Systems Manager SSM) 기능을 활용하므로 인스턴스에 태그를 지정하고 구성한 기준 및 창을 사용하여 해당 인스턴스에 패치를 적용할 수 있습니다. AMS Accelerate 패치 추가 기능은 온보딩 옵션입니다. Accelerate 계정을 온보딩하는 동안 획득하지 못한 경우 클라우드 서비스 제공 관리자(CSDM)에게 문의하여 획득하세요.

패치 책임 권장 사항

영구 인스턴스의 패치 적용 프로세스에는 다음과 같은 팀과 작업이 포함되어야 합니다.

- 애플리케이션(DevOps) 팀은 애플리케이션 환경, OS 유형 또는 기타 기준에 따라 서버의 패치 그룹을 정의합니다. 또한 각 패치 그룹별 유지보수 윈도우도 정의합니다. 이 정보는 인스턴스에 연결된 태그에 저장되어야 합니다. 권장되는 태그 이름은 '패치 그룹' 및 '유지 관리 기간'입니다. 각 패치 주기 동안 애플리케이션 팀은 패치를 준비하고, 패치 적용 후 애플리케이션을 테스트하고, 패치 적용 중에 발생하는 애플리케이션 및 OS 관련 문제를 해결합니다.
- 보안 운영 팀은 애플리케이션 팀이 사용하는 다양한 OS 유형에 대한 패치 기준을 정의하고 Systems Manager Patch Manager를 통해 패치를 사용할 수 있도록 합니다.
- 자동 패치 솔루션은 정기적으로 실행되며 사용자 정의 패치 그룹 및 유지 관리 기간에 따라 패치 기준에 정의된 패치를 배포합니다.
- 거버넌스 및 규정 준수 팀은 패치 적용 지침과 예외 프로세스 및 메커니즘을 정의합니다.

자세한 내용은 변경 가능한 EC2 인스턴스에 대한 패치 솔루션 설계를 참조하세요.

애플리케이션 팀을 위한 지침

- 유지 관리 기간 생성 및 관리에 대해 검토하고 숙지하세요. 자세한 내용은 패치 적용에 대한 AWS Systems Manager 유지 관리 기간 및 SSM 유지 관리 기간 생성을 참조하세요. https://docs.aws.amazon.com/managedservices/latest/accelerate-guide/acc-patching.html#acc-p-maint-window 유지 관리 기간의 일반적인 구조와 사용을 이해하면 유지 관리 기간을 생성하는 사람이 아닌 경우 제공할 정보를 이해하는 데 도움이 됩니다.
- 고가용성(HA) 설정의 경우 가용 영역 및 환경(Dev/Test/Prod)당 하나의 유지 관리 기간을 갖도록 계획합니다. 이렇게 하면 패치 적용 중에도 가용성이 유지됩니다.
- 권장 유지 관리 기간은 4시간이며 1시간의 마감과 인스턴스 50개당 추가 1시간입니다.
- 프로덕션 패치 적용 전에 잠재적 문제를 식별할 수 있도록 각 버전 사이에 충분한 시간이 있는 패치 개발 및 테스트 버전.
- SSM 자동화를 통해 일반적인 사전 및 사후 패치 작업을 자동화하고 유지 관리 기간 작업으로 실행합니다. 패치 후 작업의 경우 마감에 도달하면 작업이 시작되지 않으므로 할당된 시간이 충분한지 확인해야 합니다.
- 특히 개발/테스트에 적용된 패치만 나중에 프로덕션에 적용되도록 하는 데 사용할 수 있는 패치 심각도 유형의 자동 승인 지연과 같은 패치 기준 및 기능에 익숙해지세요. 자세한 내용은 패치 기준 정보를 참조하세요.

보안 운영 팀을 위한 지침

- 패치 기준을 검토하고 숙지합니다. 패치 승인은 자동화된 방식으로 처리되며 다양한 규칙 옵션이 있습니다. 자세한 내용은 패치 기준 정보를 참조하세요.
- 애플리케이션 팀과 Dev/Test/Prod 패치 적용에 대한 요구 사항을 논의하고 이러한 요구 사항을 수용할 수 있도록 여러 기준을 개발합니다.

거버넌스 및 규정 준수 팀을 위한 지침

- 패치 적용은 "Opt Out" 함수여야 합니다. 패치가 해제되지 않도록 기본 유지 관리 기간과 자동 태그 지정이 있어야 합니다. AMS Resource Tagger는 이를 지원할 수 있습니다. 구현에 대한 지침은 클라우드 아키텍트(CA) 또는 클라우드 서비스 제공 관리자(CSDM)와이 옵션에 대해 논의하세요.
- 패치 적용 예외를 요청하려면 예외를 정당화하는 문서가 필요합니다. 최고 정보 보안 책임자(CISO) 또는 기타 승인 책임자가 요청을 승인하거나 거부해야 합니다.
- 패치 규정 준수는 패치 관리자 콘솔, Security Hub 또는 취약성 스캐너를 통해 정기적으로 검토해야 합니다.

고가용성 Windows 애플리케이션을 위한 예제 설계

개요:

- AZ당 유지 관리 기간 1개.
- 환경당 유지 관리 기간 세트 1개.
- 환경당 패치 기준 1개:
  - 개발: 0일 후 모든 심각도 및 분류를 승인합니다.
  - 테스트: 0일 후 중요 보안 업데이트 패치를 승인하고 7일 후 기타 모든 심각도 및 분류를 승인합니다.
  - 생산: 0일 후에 중요한 보안 업데이트 패치를 승인하고 14일 후에 다른 모든 심각도 및 분류를 승인합니다.

CloudFormation 스크립트:

이러한 스크립트는 위에서 설명한 기준 승인 설정을 사용하여 두 가용 영역 Windows HA EC2 애플리케이션에 대한 유지 관리 기간, 기준 및 패치 작업을 빌드하도록 설정됩니다.

- Windows Dev CFN 스택 예제: HA-Patching-Dev-Stack.json
- Windows Test CFN 스택 예제: HA-Patching-Test-Stack.json
- Windows Prod CFN 스택 예제: HA-Patching-Prod-Stack.json

패치 권장 사항 FAQs

Q: "0"일 익스플로잇에 대한 예정되지 않은 패치 적용은 어떻게 처리하나요?

A: SSM은 인스턴스의 OS에 현재 기본 기준을 사용하는 지금 패치 기능을 지원합니다. AMS는 0일 후에 모든 패치를 승인하는 기본 패치 기준 세트를 배포합니다. 그러나 지금 패치 기능을 사용하면이 명령이 AWS-RunPatchBaseline SSM 문서를 실행하므로 사전 패치 스냅샷이 생성되지 않습니다. 패치 적용 전에 수동 백업을 수행하는 것이 좋습니다.

Q: AMS는 Auto-Scaling Groups(ASGs)의 인스턴스에 대한 패치 적용을 지원하나요?

A: 아니요. 현재 Accelerate 고객에게는 ASG 패치가 지원되지 않습니다.

Q: 유지 관리 기간에 유의해야 할 제한 사항이 있나요?

A: 예, 몇 가지 제한 사항을 알고 있어야 합니다.

- 계정당 유지 관리 기간: 50
- 유지 관리 기간당 작업: 20
- 유지 관리 기간당 최대 동시 자동화 수: 20
- 동시 유지 관리 기간의 최대 수: 5

기본 SSM 제한의 전체 목록은 AWS Systems Manager 엔드포인트 및 할당량을 참조하세요.

AMS에서 패치 유지 관리 기간 생성

패치 유지 관리 기간은 대상 Amazon EC2 인스턴스에 대해 설정된 일정에 따라 AMS 패치 자동화를 실행합니다. 대상은 인스턴스 그룹의 태그로 정의됩니다. 패치 화요일 전후의 일 및 시간을 기준으로 일정을 설정하거나 cron 표현식을 사용하여 일정을 정의할 수 있습니다. 자세한 내용은 AWS Systems

Manager 사용 설명서의 참조: Systems Manager용 Cron 및 Rate 표현식을 참조하세요. 패치 적용 전에 AMS는 각 인스턴스의 루트 볼륨에 대한 스냅샷을 생성합니다. AMS가 패치가 인스턴스 상태에 영향을 미치는 것을 감지하거나 패치 적용으로 인한 애플리케이션 영향을 AMS에 알리는 경우 AMS는 이 스냅샷을 사용하여 루트 볼륨을 사전 패치 상태로 복원합니다.

AMS Accelerate 패치 유지 관리 기간 제한

AMS 패치 적용은 AWS Systems Manager (Systems Manager)를 사용합니다. Systems Manager 서비스 제한 외에도 AMS 패치 적용에는 패치 유지 관리 기간당 300개의 대상 인스턴스 제한이 있습니다. 인스턴스당 30분의 일반적인 패치 완료 시간을 고려하여 다음 표에는 유지 관리 기간 및 기간 수에 대한 예제가 나와 있습니다.

패치할 인스턴스	유지 관리 기간(시간)	동시 유지 관리 기간 필요
100	1	1
200	1	1
300	2	1
600	3	2
800	4	3
1200	6	4
1500	8	5

> **Important**
>
> 이 예제에서는 활성 상태인 다른 Systems Manager 유지 관리 기간이 없고 실행 중인 다른 자동화가 없다고 가정합니다.

제한에 대한 자세한 내용은 AWS Systems Manager 엔드포인트 및 할당량을 참조하세요.

주제

- AMS 콘솔에서 반복되는 “화요일 패치” 유지 관리 기간 생성(권장)

- AMS Accelerate CloudFormation 용를 사용하여 패치 유지 관리 기간 생성
- AMS Accelerate용 Systems Manager 콘솔에서 유지 관리 기간 생성
- AMS Accelerate용 Systems Manager 명령줄 인터페이스(CLI)를 사용하여 유지 관리 기간 생성

AMS 콘솔에서 반복되는 “화요일 패치” 유지 관리 기간 생성(권장)

Microsoft는 매월 두 번째 화요일에 운영 체제에 대한 패치를 릴리스합니다. 이를 패치 화요일이라고도 합니다. 패치 화요일을 기준으로 Windows 및 Linux 인스턴스 모두에 대한 패치 적용을 예약하는 것이 일반적입니다. 패치 화요일 이후 첫 번째 또는 두 번째 주말에 반복 패치 유지 관리 기간을 예약하려면 AMS 콘솔을 방문하여 다음 단계를 따르세요.

1. 패치 유지 관리 기간의 이름을 입력합니다.
2. [선택 사항] 패치 유지 관리 기간에 대한 설명을 입력합니다.
3. 패치 화요일을 기준으로 날짜를 선택합니다.
4. 패치 유지 관리 기간이 시작될 시간을 hh:mm로 입력합니다. 예를 들어 자정은 00:00이고 오후 11시는 23:00입니다. 그런 다음 시간대를 선택합니다.
5. [선택 사항] 필요에 맞게 기간을 변경합니다. AMS는 최소 4시간의 기간을 권장합니다.
6. 대상에 대한 패치 태그 키와 값을 입력합니다. 자세한 내용은 태그란 무엇입니까?를 참조하세요.
7. [선택 사항] 선택적 파라미터를 확장하여 동시성, 오류율 및 유지 관리 기간 컷오프를 조정합니다.
    1. 동시성은 동시에 패치되는 대상 인스턴스 수를 제어합니다. 예를 들어 10개의 대상 인스턴스에 대한 50% 동시성은 한 번에 5개 이하의 인스턴스를 패치하는 반면, 100% 동시성은 10개 인스턴스를 모두 한 번에 패치합니다.
    2. 오류율은 패치 적용이 일시 중지되기 전에 오류에 대한 허용 오차를 제어합니다. 예를 들어 10개의 대상 인스턴스에 대해 오류율이 100%이면 실패 횟수에 관계없이 모든 인스턴스가 패치되고, 5개의 인스턴스가 패치에 실패하면 50% 오류율이 패치 적용을 일시 중지합니다. AMS는 100% 오류율을 권장합니다.
    3. 패치 유지 관리 기간 컷오프는 패치 유지 관리 기간이 끝나기 몇 시간 전에 새 패치 적용 활동의 시작을 일시 중지하여 패치 유지 관리 기간의 위반을 방지합니다. 예를 들어 컷오프 1시간(권장)은 패치 유지 관리 기간이 끝나기 1시간 전에 새 패치 활동을 중단합니다.

> **Important**
>
> 다음 실행 시간을 확인합니다.

SSM 유지 관리 기간 콘솔을 방문하여 새로 생성된 패치 유지 관리 기간을 검색하고 다음 실행 시간을 확인합니다. 질문이 있거나 패치 유지 관리 기간을 편집해야 하는 경우 AMS 패치 전문가와 상담하기 위한 서비스 요청을 생성합니다.

CloudFormation을 사용하여 CRON 기반 패치 유지 관리 기간을 예약하려면 섹션을 참조하세요AMS Accelerate CloudFormation 용를 사용하여 패치 유지 관리 기간 생성.

AMS Accelerate CloudFormation 용를 사용하여 패치 유지 관리 기간 생성

를 사용하여 AMS Accelerate 패치 유지 관리 기간을 생성하려면 AWS CloudFormation먼저 Accelerate 계정에 로그인하고 대상 인스턴스가 있는를 AWS 리전 선택합니다. 그런 다음 https://console.aws.amazon.com/cloudformation 다음 단계를 따릅니다.

1. 두 개의 사용자 지정 Accelerate 패치 적용 CloudFormation 템플릿 중 하나를 선택합니다.

   - 패치 화요일 예약: Microsoft는 패치 화요일이라고도 하는 운영 체제에 대한 패치를 매월 두 번째 화요일에 릴리스하여 패치 화요일 이후 첫 번째 또는 두 번째 주말에 패치 유지 관리 기간을 예약합니다. Accelerate 콘솔에 로그인하면이 링크 PatchTuesdayScheduling CloudFormation 템플릿을 사용합니다.
   - CRON Scheduling: CRON을 사용하여 시작 날짜를 정의하는 패치 유지 관리 기간을 생성하려면이 링크 CRONScheduling CloudFormation 템플릿을 사용합니다. Systems Manager CRON 숫자는 1~7일입니다(System Manager CRON에 대한 자세한 내용은 참조: Systems Manager의 Cron 및 rate 표현식 참조).

   이러한 링크 중 하나를 선택하면 템플릿이 CloudFormation 콘솔에 자동으로 로드됩니다. 그런 다음 다음을 클릭합니다.
2. 스택 세부 정보 지정 페이지(스택 생성 페이지의 2단계)에 스택 이름과 템플릿 파라미터(표시된 기본 파라미터는 AMS 권장 기본값, 사용 사례의 날짜 및 시간 선택)를 입력합니다. 완료하면 다음을 클릭합니다.
3. 스택 옵션을 구성합니다(선택 사항). 옵션에 대한 자세한 내용은 AWS CloudFormation 스택 옵션 설정을 참조하세요. 완료하면 다음을 클릭합니다.
4. 스택 값을 검토합니다(선택 사항). 스택 세부 정보를 검토하여 비용을 추정하는 방법에 대한 자세한 내용은 스택 검토 및 스택 비용 추정을 참조하세요. 준비가 되면 스택 생성을 클릭합니다.

   스택을 생성하는 데 최대 1분이 걸릴 수 있습니다. 스택이 성공적으로 생성되면 패치 유지 관리 기간이 지정된 시간에 실행됩니다. CloudFormation 변경 세트(권장)를 생성 및 실행하거나(이 작업

에 대한 자세한 내용은 변경 세트를 사용하여 스택 생성 참조) Systems Manager 유지 관리 기간 콘솔()에서 패치 유지 관리 기간을 업데이트하여 패치 유지 관리 기간을 변경할 수 있습니다https://console.aws.amazon.com/systems-manager/maintenance-windows.

Namrata의 동영상을 보고 자세히 알아보기(5:41)

AMS Accelerate용 Systems Manager 콘솔에서 유지 관리 기간 생성

Systems Manager 콘솔에서 AMS Accelerate 유지 관리 기간을 생성하려면 다음 단계를 따릅니다.

1. 변경 관리 영역의 왼쪽 탐색 모음에서 유지 관리 기간을 클릭한 다음 화면 오른쪽 상단의 유지 관리 기간 생성을 클릭합니다. 양식을 작성합니다. 옵션에 대한 자세한 내용은 유지 관리 기간 생성(콘솔)을 참조하세요. 완료되면 유지 관리 기간 생성을 클릭합니다.

   유지 관리 기간 목록 페이지가 열립니다.
2. 새로 생성된 유지 관리 기간을 선택합니다.

   유지 관리 기간 세부 정보 페이지가 열립니다.
3. 대상 탭으로 이동하여 대상 등록을 선택합니다.

   대상 등록 페이지가 열립니다.
4. Accelerate 대상을 추가합니다. 대상에 대한 자세한 내용은 유지 관리 기간에 대상 할당(콘솔)을 참조하세요. 완료되면 대상 등록을 클릭합니다. 나중에 필요할 때 대상을 기록해 둡니다.

   유지 관리 기간 세부 정보 페이지가 새 대상이 포함된 목록과 함께 대상 탭에서 다시 열립니다.
5. 유지 관리 기간 세부 정보 페이지의 작업 탭에서 작업 등록을 선택한 다음 드롭다운 목록에서 자동화 작업 등록을 선택합니다. 양식을 작성합니다. 가속화 참고 사항:

   - 의미 있는 작업 이름을 제공합니다. 예: AcceleratePatch.
   - 자동화 문서 영역에서 검색 상자를 클릭하고 소유자를 선택한 다음 공유 문서를 선택합니다.
   - 검색 상자를 클릭하고 문서 이름 접두사 --> 같음을 선택한 다음 AWSManagedServices-PatchInstance를 입력하여 자동화 문서를 선택합니다. 그런 다음 라디오 버튼을 선택하여 AWSManagedServices-PatchInstance 문서를 선택합니다.
   - 문서 버전에서 런타임 시 기본 버전을 선택합니다.
   - 대상 섹션에서:
     - 대상 설정 기준:를 등록된 대상 그룹 선택으로 설정합니다.
     - 대상 목록에서 대상 탭에서 등록한 대상을 선택합니다.

- 입력 파라미터 섹션에서 양식을 입력합니다.
  - InstanceId: {{*TARGET_ID*}}
  - StartInactiveInstances: 패치 유지 관리 기간 동안 인스턴스가 중지된 경우 인스턴스를 `True` 시작합니다.

    > **Note**
    >
    > InstanceId 파라미터 값은 대소문자를 구분하며 StartInactiveInstances 파라미터 값은 True 또는 False일 수 있습니다.
    > 태그의 대상이 되면 중지된 인스턴스를 시작할 수 없습니다. 자세한 내용은 실행할 호출 없음을 참조하세요.

- 속도 제어 섹션에서 백분율을 선택합니다. AMS Accelerate는 자동화 오류에 관계없이 모든 인스턴스를 동시에 패치하려는 경우 동시성에 대해 100%, 오류 임계값에 대해 100%를 권장합니다. 예를 들어 대상 인스턴스의 절반을 로드 밸런싱 실행 상태로 유지하기 위해 한 번에 대상의 절반을 패치하려면 동시성을 50%로 설정합니다.
- IAM 서비스 역할 섹션에서 사용자 지정 서비스 역할 사용을 선택한 다음 ams_ssm_automation_role을 선택합니다.

자동화 작업 등록을 클릭합니다.

패치 유지 관리 기간이 생성됩니다. 설명 탭에서 다음 실행 시간을 볼 수 있습니다.

AMS Accelerate용 Systems Manager 명령줄 인터페이스(CLI)를 사용하여 유지 관리 기간 생성

명령줄 인터페이스를 사용하여 AMS Accelerate 유지 관리 기간을 생성하려면

1. SSM 자습서: 유지 관리 기간 생성 및 구성(AWS CLI)을 따릅니다. 다음은 자습서의 각 단계에 대한 패치 적용을 위한 샘플 CLI 명령입니다.

> **Note**
>
> 이 예제는 Linux 또는 macOS에만 해당됩니다. 로컬 시스템에서 `awscli`를 구성하는 것보다 더 간단한 명령도 실행할 수 AWS CloudShell 있습니다. 자세한 내용은 작업을 참조하세요 AWS CloudShell.

a. 자습서의 1단계에서 유지 관리 기간을 생성하려면:

```
aws ssm create-maintenance-window \
                --name Sample-Maintenance-Window \
                --schedule "cron(0 30 23 ? * TUE#2 *)" \
                --duration 4 \
                --cutoff 1 \
                --allow-unassociated-targets \
                --tags "Key=Environment,Value=Production"
```

성공적으로 완료되면 `window-id`가 반환됩니다.

b. 자습서의 2단계에서 대상 노드를 등록하려면:

```
aws ssm register-target-with-maintenance-window \
                --window-id "mw-xxxxxxxxx" \
                --resource-type "INSTANCE" \
                --target "Key=tag:Environment,Values=Prod"
```

성공적으로 완료되면이 반환`WindowTargetID`됩니다.

c. 자습서의 3단계에서 작업을 등록하려면:

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-xxxxxx" \
    --targets "Key=WindowTargetIds,Values=63d4f63c-xxxxxx-9b1d-xxxxxfff" \
    --task-arn "AWSManagedServices-PatchInstance" \
    --service-role-arn "arn:aws:iam::AWS-Account-ID:role/ams_ssm_automation_role"
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$DEFAULT
\",\"Parameters\":{\"InstanceId\":[\"{{TARGET_ID}}\"],\"StartInactiveInstances\":
[\"True\"]}}}" \
    --max-concurrency 50 \
    --max-errors 50 \
    --name "AutomationExample" \
    --description "Sample Description" \
    --task-type=AUTOMATION
```

후크가 있는 패치

AMS 패치 후크를 사용하여 패치 적용 전후에 운영 체제(OS) 수준 명령을 실행하도록 AMS 패치 적용을 구성할 수 있습니다. AMS 패치 후크를 사용하여 SSM 명령 문서를 실행하여 패치 적용 전에 서비스를 중지한 다음 패치 적용 후 서비스를 시작하거나 명령을 실행하여 패치 적용 후 애플리케이션이 정상인지 확인합니다.

AMS 패치 후크를 사용하려면 다음을 수행해야 합니다.

1. 패치 후크로 사용할 SSM 명령 문서를 생성합니다.
2. AMS 패치 유지 관리 기간을 생성하거나 기존 AMS 패치 유지 관리 기간을 사용합니다. 자세한 내용은 AMS 패치 유지 관리 기간을 참조하세요.
3. AMS 패치 후크에 SSM 명령 문서를 사용하도록 AMS 패치 유지 관리 기간을 구성합니다.

AMS 패치 후크 RACI

책임, 책임, 상담 및 정보에 입각한 RACI 매트릭스는 다양한 활동에 대해 고객 또는 AMS에 기본 책임을 할당합니다. 다음 표에는 AMS 패치 후크를 사용하는 애플리케이션의 활동에 대한 고객 및 AMS의 책임에 대한 개요가 나와 있습니다.

- R은 작업을 수행하기 위해 작업을 수행하는 책임 당사자를 나타냅니다.
- 는 책임 당사자를 의미합니다.
- C는 컨설팅, 일반적으로 주제 전문가로서 의견을 구하는 당사자, 양자 간 커뮤니케이션이 있는 당사자를 의미합니다.
- 나는 정보를 의미합니다. 진행 상황에 대한 정보를 받는 당사자로, 종종 작업 또는 결과물이 완료될 때만 정보를 받습니다.

활동	Customer	AMS
패치 전/후 SSM 명령 문서 및 문서 콘텐츠 생성	R	C
AMS 패치 적용을 위한 패치 후크 파라미터 구성	R	C

활동	Customer	AMS
패치 사전/사후 SSM 명령 문서 실행	정보	R
패치 후크 실패 분류 및 대응	정보	R
고객에게 패치 후크 실패 알림	정보	R
고객이 요청한 경우 사전 패치 상태로 롤백	C	R

패치 후크용 SSM 문서 생성

AMS 패치 후크는 패치 적용 중에 Amazon EC2 Systems Manager(SSM) 문서를 사용합니다. SSM 명령 문서를 생성하거나 패치가 발생하는 계정과 기존 SSM 명령 문서를 공유합니다. 제한을 포함하여 SSM 문서에 대한 자세한 내용은 SSM 문서 공유를 참조하세요.

SSM 명령 문서를 생성하려면 다음 단계를 따릅니다.

1. 문서 유형이 "명령"인 SSM 문서를 생성합니다.
2. 콘텐츠 섹션에 명령(들)을 입력합니다. 자세한 내용은 SSM 문서 콘텐츠 생성을 참조하세요.

> **Note**
>
> AMS 패치 후크에 대한 SSM 문서는 AWS CLI 또는를 사용하여 생성할 수도 있습니다 CloudFormation. AMS 패치 후크에 대한 SSM 문서를 생성하는 데 도움이 필요한 경우 Cloud Architect에 문의하세요.

SSM Command 문서를 AMS 패치 후크로 사용하도록 AMS 패치 유지 관리 기간 구성

AMS 패치 유지 관리 기간은 구성된 AMS 패치 자동화를 실행하는 Systems Manager 유지 관리 기간입니다.

패치 후크를 사용하도록 AMS 패치 유지 관리 기간을 편집하려면 다음 단계를 따르세요.

1. https://console.aws.amazon.com/systems-manager/ 왼쪽 탐색 창의 변경 관리 도구에서 유지 관리 기간을 선택합니다.

   기존 유지 관리 기간을 나열하는 페이지가 열립니다.

2. mw-로 시작하는 창 ID를 선택합니다.

   해당 유지 관리 기간의 세부 정보 페이지가 열립니다.

3. AMS-PatchInstance의 작업 ARN이 있는 작업 탭과 창 작업 ID를 선택하고 편집을 클릭합니다.

4. 아래로 스크롤하여 파라미터 섹션으로 이동하고 다음 파라미터를 업데이트합니다.

AMS 패치 후크 파라미터:

- PrePatchHook: 패치 적용 전에 실행하려는 "명령" 유형의 SSM 문서 이름입니다. 패치를 적용하기 전에 명령을 실행하지 않는 경우이 값을 비워 두거나 "AWS-Noop"(대소문자 구분)을 입력합니다.
- PostPatchHook: 패치 적용 후 실행할 유형이 "Command"인 SSM 문서의 이름입니다. 패치 후 명령을 실행하지 않는 경우이 값을 비워 두거나 "AWS-Noop"(대소문자 구분)을 입력합니다.
- ExecutePatchBasedOnPreHookStatus: PrePatchHook 실행의 성공 또는 실패를 기반으로 패치 적용을 실행하고 다음 중 하나를 선택합니다.
  - OnPreHookSuccess: PrePatchHook가 성공한 경우에만 AMS 패치 자동화를 실행합니다.
  - 항상: PrePatchHook가 성공하고 실패할 때 AMS 패치 자동화를 실행합니다.
  - OnPreHookFailure - PrePatchHook에 장애가 발생한 경우에만 AMS 패치 자동화를 실행합니다.
  - 안 함: AMS 패치 자동화를 실행하지 마십시오. 이는 PrePatchHook를 테스트할 때 유용할 수 있습니다.
- ExecutePostHookBasedOnPatchStatus: AMS 패치 자동화의 성공 또는 실패를 기반으로 패치 후 후크를 실행하고 하나를 선택합니다.
  - OnPatchSuccess: AMS 패치 자동화가 성공적으로 실행되는 경우에만 PostPatchHook를 실행합니다.
  - 항상: AMS 패치 자동화가 성공하고 실패하면 PostPatchHook를 실행합니다.
  - OnPatchFailure - AMS 패치 자동화에 실패한 경우에만 PostPatchHook를 실행합니다.

> **Note**
>
> 이러한 변수 중 하나라도 텍스트 상자가 누락된 경우 동일한 페이지의 자동화 문서 섹션까지 스크롤하여 다른 문서를 선택한 다음 원본 문서를 다시 선택하여이 문제를 해결합니다. 그러면 입력 파라미터가 새로 고쳐져 편집할 수 있습니다.

AMS Accelerate 패치 기준

패치 기준선은 인스턴스에 대한 설치가 승인되는 패치를 정의합니다. 패치 승인 또는 거부는 하나씩 지정할 수 있습니다. 또한 자동 승인 규칙을 생성하여 특정 유형의 업데이트(예: 필수 업데이트)가 자동 승인되도록 지정할 수도 있습니다. 거부된 목록은 규칙 및 승인 목록을 모두 재정의합니다.

기본 패치 기준

AMS Accelerate 패치 적용에 온보딩하면 다음 운영 체제의 AMS Accelerate 기본 패치 기준이 기본 패치 기준을 재정의합니다.

- Windows
- Amazon Linux 1
- Amazon Linux 2
- CentOS
- Suse
- Rhel
- Ubuntu

> **Important**
>
> 기본 패치 기준은 AMS에서 관리합니다. 변경 사항이 손실될 수 있으므로 기본 패치 기준을 편집하지 마십시오. 대신 사용자 지정 패치 기준을 생성합니다. AMS Accelerate를 사용한 사용자 지정 패치 기준 섹션을 참조하세요

> **Note**
>
> 제품 = *로 정의된 AMS Accelerate 패치 기준은 모든 패치가 모든 보안 및 분류의 인스턴스에 적용됨을 의미합니다.

AMS Accelerate를 사용한 사용자 지정 패치 기준

AMS Accelerate에서 사용자 지정 패치 기준을 사용하려면 먼저 패치 그룹이 있는지 확인한 다음 사용자 지정 기준을 생성합니다.

자세한 정보는 다음 자료를 참조하세요.

- 패치 그룹 작업
- 사용자 지정 패치 기준 생성(Windows)
- 사용자 지정 패치 기준 생성(Linux)
- 사용자 지정 패치 기준 업데이트 또는 삭제(콘솔)

AMS Accelerate의 온디맨드 패치를 위한 IAM 역할 생성

계정이 AMS Accelerate 패치에 온보딩되면 AMS Accelerate는 관리형 정책인 amspatchmanagedpolicy를 배포합니다. 이 정책에는 AMS 자동화 문서를 사용한 온디맨드 패치 적용에 필요한 권한이 포함되어 있습니다`AWSManagedServices-PatchInstance`. 이 자동화 문서를 사용하기 위해 계정 관리자는 사용자를 위한 IAM 역할을 생성합니다. 다음 단계를 따릅니다.

다음을 사용하여 역할을 생성합니다. AWS Management Console

1. 에 로그인 AWS Management Console 하고 IAM 콘솔을 엽니다.
2. 콘솔의 탐색 창에서 역할을 선택한 다음 역할 생성을 선택합니다.
3. Anotherrole AWS 계정 유형을 선택합니다.
4. 계정 ID에 리소스에 대한 액세스 권한을 부여하려는 AWS 계정 ID를 입력합니다.

   지정된 계정의 관리자는 해당 계정의 IAM 사용자에게 이 역할을 수임할 수 있는 권한을 부여할 수 있습니다. 이를 위해 관리자는 사용자 또는 그룹에 정책을 연결하여 thests:AssumeRoleaction에 대한 권한을 부여합니다. 이 정책은 역할의 Amazon 리소스 이름(ARN)을 리소스로 지정해야 합니다. 다음을 참조하십시오.

- 제어하지 않는 계정의 사용자에게 권한을 부여하고 사용자가이 역할을 프로그래밍 방식으로 수임하는 경우 외부 ID 필요를 선택합니다. 외부 ID는 나와 서드 파티 계정의 관리자 간에 합의한 숫자 또는 단어가 될 수 있습니다. 이 옵션은 요청에 correctsts:ExternalID가 포함된 경우에만 사용자가 역할을 수임할 수 있도록 하는 조건을 신뢰 정책에 자동으로 추가합니다. 자세한 내용은 AWS 리소스에 대한 액세스 권한을 타사에 부여할 때 외부 ID를 사용하는 방법을 참조하세요.
- 다중 인증(MFA)으로 로그인하는 사용자로 역할을 제한하려면 MFA 필요를 선택합니다. 이렇게 하면 MFA 로그인을 확인하는 역할의 신뢰 정책에 조건이 추가됩니다. 역할을 맡으려는 사용자는 구성된 MFA 디바이스에서 임시 일회용 암호로 로그인해야 합니다. MFA 인증이 없는 사용자는 역할을 수임할 수 없습니다. MFA에 대한 자세한 내용은 에서 다중 인증(MFA) 사용을 AWS 참조하세요.

5. 다음: 권한을 선택합니다.

   IAM에는 계정의 정책 목록이 포함됩니다. 권한 추가에서 필터 상자에 amspatchmanagedpolicy를 입력하고이 권한 정책의 확인란을 선택합니다. 다음을 클릭합니다.

6. 역할 세부 정보에서 PatchRole과 같은 역할 이름을 입력하고, 역할에 대한 설명을 추가하고(권장), 이 역할을 식별하는 데 도움이 되는 태그를 추가합니다. 역할 이름은 대소문자를 구분하지 않지만 내에서 고유해야 합니다 AWS 계정. 완료되면 역할 생성을 클릭합니다.

> **Note**
>
> 역할 이름은 생성한 후에는 편집할 수 없습니다.

AMS Accelerate의 패치 알림 및 패치 실패 이해

> **Important**
>
> 2025년 2월 1일부터 AMS 고객은 더 이상 관리형 계정의 빈 패치 유지 관리 기간에 대한 알림을 받지 않습니다.

패치 서비스 요청 및 이메일 알림

AMS는 다음 패치 유지 관리 기간 4일 전에 새 서비스 요청을 생성합니다. 예를 들어 App1 PROD라는 패치 유지 관리 기간이 실행되기 4일 전에 AMS는 계정 [계정 ID]용 App1 Prod에 대한 패치 유지 관리 기간 4월이라는 서비스 요청을 생성합니다. 예약된 패치를 조정해야 하는 경우 패치 서비스 요청을 사

용하여 AMS와 통신하거나 예정된 패치를 건너뜁니다. 서비스 요청이 생성되면 서비스 요청에 대한 링크가 포함된 이메일이 패치 알림 주소로 전송됩니다. AMS가 서비스 요청을 업데이트할 때마다 추가 이메일을 받게 됩니다.

> **Note**
>
> AMS는 패치 유지 관리 기간이 실행 예정 날짜로부터 4일 이내에 생성되더라도 새 서비스 요청을 생성합니다.
> 서비스 요청 알림을 받으려면 패치 유지 관리 기간이 "활성화됨" 상태여야 합니다.

패치 적용이 시작되기 1시간 전에 AMS는 패치 서비스 요청을 통해 사용자에게 알립니다. 패치 적용이 완료되면 AMS는 패치 관리자 콘솔에 대한 링크로 패치 서비스 요청을 업데이트합니다. 링크를 사용하여 패치 유지 관리 기간의 대상이 되는 인스턴스에 대한 패치 규정 준수를 확인합니다.

> **Note**
>
> 패치 관리자 콘솔의 링크는 인스턴스의 현재 규정 준수를 보여줍니다. AMS가 패치 적용을 완료하고 사용자가 링크에 액세스하는 시간 사이에 새 패치가 릴리스되면 패치 관리자는 인스턴스를 비준수로 표시합니다.

CloudWatch Events를 통한 패치 알림

AMS는 패치 프로세스 중에 다음을 포함하여 CloudWatch Events를 세 번 전송합니다.

- 패치 유지 관리 기간이 실행되기 4일 전.
- 패치 유지 관리 기간이 실행되기 1시간 전.
- 패치 유지 관리 기간이 완료되면

다음은 패치 유지 관리 기간 고급 알림 이벤트 스키마입니다.

```
{
    "version": "0",
    "id": "37004d81-458d-2cef-fe1c-8afa8af30406",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "145917996532",
```

```
    "time": "2021-05-20T02:00:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {
        "State": "PREEMPTIVE",
        "StartTime": "2021-05-24T02:00:00.000000",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\"}, {\"instanceId\":
 \"i-0000000aaaaaaaaab\"}]"
    }
}
```

다음 표에서는 패치 유지 관리 기간 사전 알림 이벤트 스키마를 설명합니다.

패치 알림 세부 정보

속성 이름	설명	샘플 값
State	패치 유지 관리 기간의 상태	PREEMPTIVE - 패치 적용 기간이 곧 시작됩니다.
상태	패치 유지 관리 기간의 상태	성공 - 모든 인스턴스가 실패 없이 패치되었습니다. FAILED - 하나 이상의 인스턴스가 패치에 실패했습니다.
StartTime	패치 유지 관리 기간의 ISO 형식 시작 시간	2021-02-03T22:14:05.814308
WindowArn	패치 적용 유지 관리 기간의 고유 식별자	arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235
Results	패치 창의 대상이 되는 인스턴스 목록	InstanceId - 대상 인스턴스의 인스턴스 ID

다음은 패치 유지 관리 기간 종료 이벤트 스키마입니다.

```
{"version": "0",
    "id": "0f25add5-44a9-0702-d2bc-bd2102affefe",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "123456789012",
    "time": "2021-02-03T22:14:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {"State": "[COMPLETED]",
        "Status": "SUCCESS",
        "StartTime": "2021-02-03T22:12:00.814308",
        "EndTime": "2021-02-03T22:14:05.814309",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "WindowExecutionId": "e32088eb-c05f-4c63-b766-6866e163c818",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\", \"status\":
 \"Success\", \"missing_critical_patch_count\": 0, \"missing_total_patch_count
\": 0} }, {\"instanceId\": \"i-0000000aaaaaaaaab\", \"status\": Success},
 \"missing_critical_patch_count\": 0, \"missing_total_patch_count\": 0}]"
    }
}
```

다음 표에서는 패치 유지 관리 기간 종료 이벤트 스키마를 설명합니다.

패치 기간 종료 세부 정보

속성 이름	설명	샘플 값
State	패치 유지 관리 기간의 상태	COMPLETED - 패치 적용 기간이 완료되었습니다.
상태	패치 유지 관리 기간의 상태	성공 - 모든 인스턴스가 실패 없이 패치되었습니다. FAILED - 하나 이상의 인스턴스가 패치에 실패했습니다.

속성 이름	설명	샘플 값
StartTime	패치 유지 관리 기간의 ISO 형식 시작 시간	2021-02-03T22:14:05.814308
EndTime	패치 유지 관리 기간의 ISO 형식 종료 시간	2021-02-03T23:14:05.814308
WindowArn	패치 유지 관리 기간의 고유 식별자입니다.	arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235
WindowExecutionId	SSM 유지 관리 기간 콘솔에서 볼 수 있는 창 실행 ID	e32088eb-c05f-4c63-b766-6866e163c818
Results	패치 창의 대상이 될 인스턴스 목록입니다.	InstanceId - 대상 인스턴스 ID 상태 - 인스턴스 패치 상태 missing_critical_patch_count - 인스턴스에서 누락된 중요 패치 수 missing_total_patch_count - 인스턴스에서 누락된 총 패치 수

CloudWatch Events 이벤트를 사용하여 패치 적용 유지 관리 기간 사전 알림이 전송될 때 알리는 CloudWatch 규칙을 트리거할 수 있습니다. 이렇게 하려면 다음 구성으로 CloudWatch 규칙을 구성합니다.

```
{
    "source": [
        "aws.managedservices"
    ],
    "detail-type": [
        "AMS Patch Window Execution State Change"
    ],
    "detail": {
        "State": ["PREEMPTIVE"]
```

```
    }
}
```

> **Note**
>
> 지원되지 않는 운영 체제가 있거나 유지 관리 기간 동안 중지된 인스턴스에 대해서는 패치 실패 알림이 생성되지 않습니다.

AMS의 패치 실패 조사

AWS Managed Services(AMS)는 패치 적용을 관리하고 패치 장애 수정을 포함합니다. 패치 적용이 실패하면 AMS 작업에 알림이 표시되고 문제를 해결하기 위한 AWS 및 AMS 모범 사례에 따라 문제 해결을 시도합니다.

패치가 실패하면 AMS는 AWS Managed Services - 인스턴스 <instance-id>에 대한 패치 인스턴스 실패라는 제목의 SSM OpsItem을 계정에 생성합니다.

그런 다음 AMS는 OpsItem을 조사합니다. AMS가 개입 없이 실패를 수정할 수 있는 경우 AMS는 OpsItem을 해결합니다. 개입이 필요한 경우 AMS는 조사 결과와 권장 수정 단계가 포함된 서비스 요청을 통해 사용자에게 알립니다. 문제를 해결하기 위한 조치를 취하지 않으면 AMS는 예약된 다음 패치 유지 관리 기간 동안 인스턴스 패치를 시도합니다.

> **Note**
>
> 패치 장애 OpsItems는 지원되지 않는 운영 체제가 있거나 패치 유지 관리 기간 동안 중지됨 상태인 인스턴스에 대해 생성되지 않습니다.

AMS Resource Scheduler를 사용한 비용 최적화

AWS 솔루션의 AMS Resource Scheduler는 사용되지 않는 리소스를 중지하고 용량이 필요할 때 리소스를 시작하여 AWS 및 AMS 비용을 줄이는 데 도움이 됩니다. 예를 들어 개발 환경에서 AWS 의 AMS Resource Scheduler를 사용하여 매일 업무 시간 외에 인스턴스를 자동으로 중지할 수 있습니다. 모든 인스턴스를 최대 사용률로 실행 상태로 두면이 솔루션이 인스턴스 사용률을 줄여 구성한 일정에 따라 전체 비용을 줄일 수 있습니다.

AWS Managed Services(AMS) Resource Scheduler를 사용하여 계정에서 Auto Scaling 그룹, Amazon EC2 인스턴스 및 Amazon RDS 인스턴스의 자동 시작 및 중지를 예약합니다. 이렇게 하면 리소스가 연중무휴로 실행되지 않는 인프라 비용을 줄일 수 있습니다. 이 솔루션은 AWS 인스턴스 스케줄러를 기반으로 구축되지만 AMS 고객 요구 사항에 맞는 추가 기능 및 사용자 지정이 포함되어 있습니다. 사용자 지정에는 Auto Scaling 그룹 예약 지원, Elastic Load Balancing 경보에 대한 CloudWatch 경보 억제기 지원, Amazon EC2에 대한 여러 AWS Systems Manager 유지 관리 기간 지원, 비용 절감 예측기, AMS의 운영 지원이 포함됩니다.

AMS Resource Scheduler는 기간과 일정을 사용합니다. 기간은 시작 시간, 종료 시간, 월의 일 등 리소스가 실행되어야 하는 시간을 정의합니다. 일정에는 SSM 유지 관리 기간, 시간대, 최대 절전 모드 등의 추가 구성과 함께 정의된 기간이 포함되며 리소스를 실행해야 하는 시기를 지정합니다. AMS 제공 AWS Systems Manager 자동화 실행서를 사용하여 이러한 기간 및 일정을 구성할 수 있습니다. 각 일정에는 인스턴스가 실행되어야 하는 시간(들)을 정의하는 기간이 하나 이상 포함되어야 합니다. 일정은 기간을 두 개 이상 포함할 수 있습니다. 일정에 둘 이상의 기간이 사용되는 경우 기간 규칙 중 하나 이상이 true이면 인스턴스 스케줄러가 적절한 시작 작업을 적용합니다. 일정 및 기간에 대한 자세한 내용은 AWS 인스턴스 스케줄러의 솔루션 구성 요소를 참조하세요.

AMS Resource Scheduler는 AWS 리소스 태그를 사용하여 일정을 하나 이상의 리소스에 연결하여 예약된 시작 및 중지 작업을 대상으로 지정합니다. 스케줄러에 구성된 태그 키(기본값은 `Schedule`)를 사용하여 리소스에 태그를 지정하고 일정 이름을 값으로 지정합니다. 비용 절감을 추적하고 보고하기 AWS Cost Explorer 위해 스케줄러의 비용 예측기 기능에 대해의 비용 할당 태그와 동일한 태그 키를 구성합니다.

AMS Resource Scheduler는 계정별로 활성화할 수 있는 옵트인 기능입니다.

AMS Resource Scheduler에서 리소스 사용

Amazon EC2

- Auto Scaling 그룹의 일부인 Amazon EC2 인스턴스는 태그가 지정된 경우에도 개별적으로 처리되지 않으며 AMS Resource Scheduler에서 건너뜁니다.
- 대상 인스턴스 루트 볼륨이 AWS KMS 고객 마스터 키(CMK)로 암호화된 경우 스케줄러가 이러한 인스턴스를 시작할 수 있도록 Resource Scheduler IAM 역할에 추가 `kms:CreateGrant` 권한을 추가해야 합니다. 보안 향상을 위해이 권한은 기본적으로 역할에 추가되지 않습니다. 이 권한이 필요한 경우 CMK 목록을 `UseCMK` 파라미터의 값으로 `ams-resource-scheduler`사용하여 CloudFormation 스택인를 업데이트하여 권한을 추가할 수 있습니다(KMS 별칭 `arn:`*`partition`*`:kms:`*`region`*`:`*`account-id`*`:key/`*`key-id`* 대신 형식으로 하나 이상의 CMK 키 ARNs 사용).
- Amazon EC2 인스턴스가 특정 소프트웨어 또는에서 관리하는 공급업체 라이선스로 구성된 경우 AWS License Manager Resource Scheduler는 인스턴스를 시작할 수 있도록 특정 AWS License Manager 라이선스에 대한 권한이 필요합니다. CloudFormation 스택()의 EC2 인스턴스 파라미터에 대한 AWS License Manager 라이선스 관리자 라이선스에 라이선스의 ARN(들) 목록을 추가하여 Resource Scheduler에 필요한 권한을 부여할 수 있습니다`ams-resource-scheduler`.

Amazon EC2 Auto Scaling

- AMS Resource Scheduler는 오토 스케일링의 개별 인스턴스가 아닌 Auto Scaling의 오토 스케일링을 시작하거나 중지합니다. 즉, 스케줄러는 Auto Scaling 그룹의 크기를 복원하거나(시작) 크기를 0(중지)으로 설정합니다.
- Auto Scaling에 그룹 내 인스턴스가 아닌 지정된 태그로 태그를 지정합니다.
- 중지하는 동안 AMS Resource Scheduler는 Auto Scaling 그룹의 최소, 원하는 및 최대 용량 값을 저장하고 최소 및 원하는 용량을 0으로 설정합니다. 시작하는 동안 스케줄러는 Auto Scaling 그룹 크기를 중지하는 동안과 동일하게 복원합니다. 따라서 Auto Scaling 그룹 인스턴스는 인스턴스의 종료 및 다시 시작이 Auto Scaling 그룹에서 실행되는 애플리케이션에 영향을 주지 않도록 적절한 용량 구성을 사용해야 합니다.
- 실행 기간 동안 Auto Scaling 그룹이 수정된 경우(최소 또는 최대 용량) 스케줄러는 새 Auto Scaling 그룹 크기를 저장하고 중지 일정이 끝날 때 그룹을 복원할 때 사용합니다.

Amazon RDS

- 스케줄러는 RDS 인스턴스를 중지하기 전에 스냅샷을 생성할 수 있습니다(Aurora DB 클러스터에는 적용되지 않음). 이 기능은 기본적으로 RDS 인스턴스 스냅샷 생성 AWS CloudFormation 템플릿 파라미터를 true로 설정하여 활성화됩니다. 스냅샷은 다음에 Amazon RDS 인스턴스가 중지되고 새 스냅샷이 생성될 때까지 유지됩니다.

- 스케줄러는 클러스터 또는 Amazon RDS Aurora 데이터베이스의 일부이거나 다중 가용 영역(다중 AZ) 구성에 있는 Amazon RDS 인스턴스를 시작/중지할 수 있습니다. 그러나 스케줄러가 Amazon RDS 인스턴스, 특히 다중 AZ 인스턴스를 중지할 수 없는 경우 Amazon RDS 제한을 확인합니다.
- Aurora 클러스터의 시작 또는 중지를 예약하려면 Aurora 클러스터 예약 템플릿 파라미터(기본값은 true)를 사용합니다. Aurora 클러스터(클러스터 내의 개별 인스턴스 아님)에는 초기 구성 중에 정의된 태그 키와 해당 클러스터를 예약하기 위한 태그 값으로 일정 이름을 지정해야 합니다.

> **Note**
>
> Resource Scheduler는 리소스가 시작 또는 중지되었는지 확인하지 않습니다. 관련 서비스에 대한 API 호출을 수행하고 계속 진행합니다. API 호출이 실패하면 조사를 위해 오류를 기록합니다.
>
> AMS Resource Scheduler는 AWS Backup 기간을 지원하지 않습니다. Resource Scheduler 일정으로 AWS Backup활성화된 RDS 인스턴스를 매핑하는 경우 백업이 예상대로 작동하려면 백업 기간이 일정의 실행 기간 내에 있어야 합니다.

온보딩 AMS 리소스 스케줄러

계정이 AMS Accelerate 운영 계획에 온보딩되면 계정이 AMS Resource Scheduler에 자동으로 온보딩되지 않습니다. 그러나 AMS Accelerate 운영 계획에 대한 계정 온보딩의 일환으로 또는 그 후 언제든지 Cloud Service Delivery Manager(CSDM)에 AMS Resource Scheduler에 계정을 온보딩하도록 요청할 수 있습니다. CSDM이 계정을 온보딩하면 기본 구성의 AMS Resource Scheduler 리소스가 포함된 CloudFormation 스택이 계정에 자동으로 프로비저닝됩니다.

계정에 AMS Resource Scheduler를 프로비저닝한 후 기본 구성을 검토하고 필요한 경우 기본 설정에 따라 태그 키, 시간대, 예약된 서비스 등과 같은 구성을 사용자 지정하는 것이 좋습니다. 권장 사용자 지정에 대한 자세한 내용은 AMS Resource Scheduler 사용자 지정다음 단원을 참조하십시오.

AMS Resource Scheduler 사용자 지정

온보딩하면 AMS Resource Scheduler가 AMS Accelerate 계정의 기본 AWS 리전`ams-resource-scheduler`에 이름이 인 CloudFormation 스택으로 배포됩니다. CloudFormation 스택 파라미터를 통해 기본 설정을 기반으로 AMS Resource Scheduler의 속성을 구성하고 스택 업데이트를 수행할 수 있습니다. CloudFormation 스택 업데이트에 대한 자세한 내용은 스택 직접 업데이트를 참조하세요.

최적의 기능을 위해 다음 속성을 사용자 지정하고 나머지는 기본적으로 그대로 두는 것이 좋습니다.

- 태그 이름: Resource Scheduler가 인스턴스 일정을 리소스와 연결하는 데 사용할 태그의 이름입니다. 기본값은 `Schedule`입니다.
- 예약할 서비스(들): Resource Scheduler가 관리할 수 있는 서비스의 쉼표로 구분된 목록입니다. 기본값은 “`ec2,rds,autoscaling`”입니다. 유효한 값은 "ec2", "rds" 및 "autoscaling"입니다.
- 기본 시간대: Resource Scheduler에서 사용할 기본 시간대를 지정합니다. 기본값은 `UTC`입니다.
- 암호화된 EBS 볼륨에 대한 CMK: Resource Scheduler에 권한을 부여할 수 있는 Amazon KMS 고객 관리형 키(CMK) ARNs의 쉼표로 구분된 목록입니다.
- EC2 인스턴스용 라이선스 관리자 라이선스: 해당 Resource Scheduler에 대한 AWS Licence Manager ARNs의 쉼표로 구분된 목록에 권한을 부여할 수 있습니다.

> **Note**
>
> AMS는 계정에서 AMS Resource Scheduler를 최신 상태로 유지하기 위해 기능 및 수정 사항을 릴리스합니다. 이 경우 스택 파라미터를 통해 AMS Resource Scheduler 스택에 대해 수행하는 모든 사용자 지정은 유지됩니다.
> AMS Resource Scheduler의 구성 요소 리소스를 직접 사용자 지정하지 않는 것이 좋습니다. 이렇게 하면 Resource Scheduler 기능과 이를 최신 상태로 유지하는 AMS의 기능에 영향을 미칩니다.

AMS Resource Scheduler 사용

AMS Accelerate 계정에서 AMS Resource Scheduler 기간을 사용하는 방법.

다음 AWS Systems Manager 자동화 실행서 세트를 사용하여 AMS Resource Scheduler에서 필요한 일정 및 기간을 관리합니다.

> **Note**
>
> 이러한 SSM 자동화 실행서는 계정의 기본 AWS 리전에서 사용할 수 있습니다.

- `AWSManagedServices-AddOrUpdatePeriod`
- `AWSManagedServices-AddOrUpdateSchedule`
- `AWSManagedServices-DeleteScheduleOrPeriod`
- `AWSManagedServices-DescribeScheduleOrPeriods`

- `AWSManagedServices-EnableOrDisableAMSResourceScheduler`

또한 AMS는 런북을 사용하기 위해 및가 `ams_resource_scheduler_ssm_automation_role` AWS Systems Manager 필요한 AWS Identity and Access Management 역할을 프로비저닝합니다. IAM 역할은 실행서 기능에 필요한 SSM 권한을 부여하는 최소 권한 인라인 정책으로 범위가 축소됩니다.

사전 조건

SSM 자동화 런북 및 AMS Resource Scheduler 사용을 시작하기 전에 다음 단계를 수행합니다.

자동화 실행서를 사용하여 AMS Resource Scheduler에서 일정 및 기간을 관리할 수 있도록 허용하려는 적절한 IAM 엔터티(사용자, 그룹 또는 역할)에 다음 정책을 연결합니다. IAM 엔터티에 계정에 관리자 또는 PowerUser 권한이 있는 경우이 정책은 필요하지 않습니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPassingResourceSchedulerRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/
ams_resource_scheduler_ssm_automation_role",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "ListAndDescribeAutomationExecutions",
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:DescribeAutomationStepExecutions"
            ],
            "Resource": "arn:aws:ssm:*:111122223333:automation-execution/*"
        },
```

```
        {
            "Sid": "ListAndDescribeResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocumentVersions",
                "ssm:DescribeDocument",
                "ssm:ListDocumentMetadataHistory",
                "ssm:DescribeDocumentParameters",
                "ssm:GetDocument",
                "ssm:DescribeDocumentPermission"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler"
            ]
        },
        {
            "Sid": "AllowExecutionOfResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler",
                "arn:aws:ssm:*:111122223333:automation-execution/*"
            ]
        },
        {
            "Sid": "AllowListingAllDocuments",
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
```

```
            "Resource": "*"
        },
        {
            "Sid": "AllowListingAllSSMExecutions",
            "Effect": "Allow",
            "Action": "ssm:DescribeAutomationExecutions",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingIAMRolesForStartingExecutionViaConsole",
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        }
    ]
}
```

AWS Systems Manager 콘솔에서 또는 AWS CLI를 사용하여 자동화를 실행할 수 있습니다. AWS CLI를 사용하는 경우 아직 설치 및 구성하지 않은 경우 PowerShell용 AWS 도구를 설치하고 구성해야 할 수 있습니다. 자세한 내용은 AWS 명령줄 도구 설치 또는 업그레이드를 참조하세요.

Navish의 비디오를 보고 자세히 알아보기(4:52)

AWS Managed Services Resource Scheduler에서 기간 및 일정 작업

AMS Resource Scheduler를 사용하여 AMS Accelerate 계정에서 일정 또는 기간을 추가, 업데이트 또는 삭제할 수 있습니다.

AMS Resource Scheduler에서 기간 추가 또는 업데이트

AMS 계정에서 Resource Scheduler 기간을 추가하거나 업데이트합니다.

필요한 데이터:

- 작업: 수행할 작업의 유형입니다. 기간을 추가하려면 "추가"를 사용하고, 기존 기간을 업데이트하려면 "업데이트"를 사용합니다.
- 이름: 마침표의 이름입니다. 새 기간을 추가하는 경우 고유한 값을 지정해야 합니다.
- AutomationAssumeRole: 실행서가 사용자를 대신하여 기간을 추가하거나 업데이트할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 ARN입니다. 역할을 로 지정합니다`ams_resource_scheduler_ssm_automation_role`.

- 설명(선택 사항): 해당 기간에 대한 의미 있는 설명입니다.
- BeginTime(선택 사항): 리소스를 시작하려는 HH:MM 형식의 시간입니다.
- EndTime(선택 사항): 리소스를 중지하려는 HH:MM 형식의 시간입니다.
- 월(선택 사항): 쉼표로 구분된 월 목록 또는 리소스를 실행해야 하는 하이픈으로 표시된 월 범위입니다.
- MonthDays(선택 사항): 쉼표로 구분된 월의 일 목록 또는 리소스를 실행해야 하는 하이픈으로 표시된 일 범위입니다.
- WeekDays(선택 사항): 리소스를 실행해야 하는 요일 또는 요일의 쉼표로 구분된 목록입니다.

이 작업을 수행하는 방법:

- AWSManagedServices-AddOrUpdatePeriod에서 문서를 봅니다(온보딩된 리전을 선택해야 할 수 있음).

  입력 파라미터 섹션에서 요구 사항을 지정한 다음 실행을 선택합니다. 작업이 완료되면 출력 탭에서 결과를 봅니다.
- AWS CLI:

  다음 명령을 실행하여 자동화를 시작합니다. *## ####* 자신의 정보로 바꿉니다.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdatePeriod" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"],
    "Description":["DESCRIPTION"],"BeginTime":["TIME"], "EndTime":["TIME"],
    "Months":["MONTH"],"MonthDays":["DAY"], "WeekDays":["DAY"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

예:

다음 예제에서는 AWS Systems Manager 콘솔을 사용하여 새 기간을 추가하는 방법을 보여줍니다. Period-Name 기간의 이름을 지정하고 매월 처음 15일 동안 월요일부터 금요일까지 오전 9AM-6PM시를 포함하도록 구성했습니다.

1. AWSManagedServices-AddOrUpdatePeriod에서 AWS Systems Manager 자동화 문서를 봅니다(온보딩된 리전을 선택해야 할 수 있음).

2. 파라미터 값을 입력합니다.

3. 실행을 클릭하고 자동화가 완료될 때까지 기다립니다.

AMS Resource Scheduler에서 일정 추가 또는 업데이트

AMS Accelerate 계정에서 Resource Scheduler 일정을 추가하거나 업데이트합니다.

필요한 데이터:

- 작업: 수행할 작업의 유형입니다. 일정을 추가하려면 "추가"를 사용하고, 기존 일정을 업데이트하려면 "업데이트"를 사용합니다.
- 이름: 일정의 이름입니다. 새 일정을 추가하는 경우 고유한 값을 지정해야 합니다.
- AutomationAssumeRole: 실행서가 사용자를 대신하여 일정을 추가하거나 업데이트할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 ARN입니다. 역할을 지정합니다`ams_resource_scheduler_ssm_automation_role`.
- 설명(선택 사항): 일정에 대한 의미 있는 설명입니다.
- 기간(선택 사항):이 일정에 사용할 쉼표로 구분된 기간 목록을 지정합니다. 각 기간은 이미 생성되어 있어야 합니다.
- RetainRunning(선택 사항): 실행 중인 퍼로드가 시작되기 전에 리소스가 수동으로 시작된 경우 Resource Scheduler가 실행 기간이 끝날 때 실행 중인 리소스를 중지하지 않도록 'true'를 지정합니다. 기본적으로 Resource Scheduler는 리소스를 중지합니다.
- StopNewInstances(선택 사항): Resource Scheduler가 실행 기간 외에 실행 중인 경우 처음으로 리소스에 태그를 지정할 때 리소스를 중지하지 않도록 'false'를 지정합니다. 기본적으로 Resource Scheduler는 리소스를 중지합니다.
- SSMMaintenanceWindow(선택 사항): 일정의 실행 기간으로 추가할 AWS Systems Manager(SSM) 유지 관리 기간의 쉼표로 구분된 목록을 지정합니다. 또한 "UseMaintenanceWindow" 속성을 "true"로 지정해야 합니다.
- TimeZone(선택 사항): Resource Scheduler에서 사용할 시간대를 지정합니다. 기본적으로 Resource Scheduler는 UTC를 사용합니다.
- UseMaintenanceWindow(선택 사항): Resource Scheduler가 Amazon RDS 인스턴스 일정의 실행 기간으로 Amazon Relational Database Service(RDS) 유지 관리 기간을 고려하거나 Amazon EC2 인스턴스 일정에 실행 기간으로 AWS Systems Manager(SSM) 유지 관리 기간을 추가하려면 "true"를 지정합니다.

- UseMetrics(선택 사항): "true"를 지정하여 일정 수준에서 CloudWatch 지표를 활성화하고 "false"를 지정하여 CloudWatch 지표를 비활성화합니다. 이 속성을 지정하면 스택 수준에서 설정된 CloudWatch 지표 설정이 재정의됩니다.

이 작업을 수행하는 방법:

- AWSManagedServices-AddOrUpdateSchedule에서 문서를 봅니다(온보딩된 리전을 선택해야 할 수 있음).

  입력 파라미터 섹션에서 요구 사항을 지정한 다음 실행을 선택합니다. 작업이 완료되면 출력 탭에서 결과를 봅니다.

- AWS CLI:

  다음 명령을 실행하여 자동화를 시작합니다. *## ####* 자신의 정보로 바꿉니다.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdateSchedule" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"], "Description":
["DESCRIPTION"],
    "Hibernate":["true or false"],"Enforced":["true or false"],
    "OverrideStatus":["running or stopped"],"Periods":["PERIOD-A, PERIOD-B"],
    "RetainRunning":["true or false"],"StopNewInstances":["true or false"],
    "SSMMaintenanceWindow":["WINDOW-NAME"],"TimeZone":["TIMEZONE"],
    "UseMaintenanceWindow":["true or false"],"UseMetrics":["true or false"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

예:

다음 예제에서는 AMS Resource Scheduler에 대한 일정을 추가하는 방법을 보여줍니다. 이 예제에서는 CustomPeriod를 사용하여 이름이 CustomSchedule인 일정을 추가합니다. CustomPeriod

1. AWSManagedServices-AddOrUpdateSchedule에서 AWS Systems Manager 자동화 문서를 봅니다(온보딩된 리전을 선택해야 할 수 있음).

2. 파라미터 값을 입력합니다.

3. 실행을 클릭하고 자동화가 완료될 때까지 기다립니다.

AMS Resource Scheduler에서 기간 또는 일정 삭제

AMS Accelerate 계정에서 Resource Scheduler 기간 또는 일정을 삭제하려면 다음 데이터가 필요합니다.

- ConfigurationType: 삭제할 구성의 유형입니다. 기간을 삭제하려면 "기간"을 사용하고 일정을 삭제하려면 "일정"을 사용합니다.
- 이름: 삭제하려는 일정 또는 기간의 이름입니다.
- AutomationAssumeRole: 실행서가 사용자를 대신하여 일정 또는 기간을 삭제할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 ARN입니다. 역할을 지정합니다`ams_resource_scheduler_ssm_automation_role`.

이 작업을 수행하는 방법:

- AWSManagedServices-DeleteScheduleOrPeriod에서 문서를 봅니다(온보딩된 리전을 선택해야 함).

  입력 파라미터 섹션에서 요구 사항을 지정한 다음 실행을 선택합니다. 작업이 완료되면 출력 탭에서 결과를 봅니다.
- AWS CLI:

  다음 명령을 실행하여 자동화를 시작합니다. *## ####* 자신의 정보로 바꿉니다.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DeleteScheduleOrPeriod" --document-version "\$DEFAULT"
--parameters '{"ConfigurationType":["period" or "schedule"],"Name":["NAME"],
    "AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}' --region ONBOARDED_REGION
```

예:

다음 예제에서는 AWS Systems Manager 콘솔을 사용하여 기간을 삭제하는 방법을 보여줍니다.

1. AWSManagedServices-DeleteScheduleOrPeriod에서 AWS Systems Manager 자동화 문서를 봅니다(온보딩된 리전을 선택해야 할 수 있음).

2. 파라미터 값을 입력합니다.

3. 실행을 클릭하고 자동화가 완료될 때까지 기다립니다.

AMS Resource Scheduler에서 기간 또는 일정 설명

AMS Accelerate 계정에서 Resource Scheduler 기간 또는 일정을 설명(세부 정보 보기)하려면 다음 데이터가 필요합니다.

- ConfigurationType: 설명할 구성 유형입니다. 모든 기간을 설명하려면 "기간"을 사용하고, 모든 일정을 설명하려면 "일정"을 사용합니다.
- AutomationAssumeRole: 실행서가 사용자를 대신하여 일정 또는 기간을 설명할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 ARN입니다. 역할을 지정합니다`ams_resource_scheduler_ssm_automation_role`.

이 작업을 수행하는 방법:

- AWSManagedServices-DescribeScheduleOrPeriods에서 문서를 봅니다(온보딩된 리전을 선택해야 할 수 있음).
  1. 입력 파라미터 섹션에서 요구 사항을 지정한 다음 실행을 선택합니다.
  2. 작업이 완료되면 출력 탭에서 결과를 봅니다.
- AWS CLI:
  1. 다음 명령을 실행하여 자동화를 시작합니다. *## ####* 자신의 정보로 바꿉니다.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DescribeScheduleOrPeriods" --document-version "\$DEFAULT"
                --parameters '{"ConfigurationType":["period" or
 "schedule"],"AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}'
                --region ONBOARDED_REGION
```

예:

다음 예제에서는 AWS Systems Manager 콘솔을 사용하여 기간을 설명하는 방법을 보여줍니다.

1. AWSManagedServices-DescribeScheduleOrPeriods에서 AWS Systems Manager 자동화 문서를 봅니다(온보딩된 리전을 선택해야 할 수 있음).

2. 파라미터 값을 입력합니다.

3. 실행을 클릭하고 자동화가 완료될 때까지 기다립니다.

AMS Resource Scheduler에 리소스 태그 지정

AMS Resource Scheduler에 대한 리소스에 태그를 지정합니다.

AMS Resource Schedule에 일정 및 기간을 추가한 후에는 Resource Scheduler 태그 이름을 태그 키로, 사용자 지정 태그 이름을 태그 값으로, 일정 이름을 태그로 지정해야 합니다. AMS Accelerate 계정의 리소스에 태그를 지정하는 방법에 대한 자세한 내용은 섹션을 참조하세요AMS Accelerate의 태그 지정.

> **Note**
>
> 리소스 태거를 사용하여 리소스에 태그를 지정하는 경우 리소스 태거에 적용된 모든 태그의 키 접두사가 'ams:rt:'이므로 Resource Scheduler의 기본 Tag 키를 접두사 'ams:rt:'로 사용자 지정해야 합니다. 그렇지 않으면 리소스 태거로 태그가 지정된 리소스는 Resource Scheduler에서 관리하지 않습니다. Resource Scheduler의 기본 태그 키 사용자 지정에 대한 자세한 내용은 섹션을 참조하세요AMS Resource Scheduler 사용자 지정.

AMS Resource Scheduler의 비용 예측기

비용 절감을 추적하기 위해 AMS Resource Scheduler는 스케줄러에서 관리하는 Amazon EC2 및 Amazon RDS 리소스에 대한 예상 비용 절감을 시간당 계산하는 구성 요소를 제공합니다. 그러면이 비용 절감 데이터가 CloudWatch 지표(AMS/ResourceScheduler)로 게시되어 이를 추적하는 데 도움이 됩니다. 비용 절감 예측기는 인스턴스 실행 시간에 대한 절감액만 추정합니다. 리소스와 관련된 데이터 전송 비용과 같은 다른 비용은 고려하지 않습니다.

비용 절감 예측기는 Resource Scheduler에서 활성화됩니다. 시간당 실행되며에서 비용 및 사용량 데이터를 검색합니다 AWS Cost Explorer. 해당 데이터에서 각 인스턴스 유형에 대한 시간당 평균 비용을 계산한 다음 예약 없이 실행되는 경우 하루 종일 비용을 프로젝션합니다. 비용 절감은 예상 비용과 지정된 날짜 동안 Cost Explorer에서 실제로 보고한 비용 간의 차이입니다.

예를 들어 인스턴스 A가 오전 9시에서 오후 5시까지 실행되도록 Resource Scheduler로 구성된 경우 해당 날짜의 8시간입니다. Cost Explorer는 비용을 1 USD로, 사용량을 8로 보고합니다. 따라서 시간당 평균 비용은 0.125 USD입니다. 인스턴스가 Resource Scheduler로 예약되지 않은 경우 인스턴스는 해당 날짜에 24시간 동안 실행됩니다. 이 경우 비용은 24x0.125 = 3 USD였습니다. Resource Scheduler를 사용하면 2 USD의 비용 절감을 달성할 수 있습니다.

비용 절감 예측기가 Cost Explorer에서 Resource Scheduler에서 관리하는 리소스에 대해서만 비용 및 사용량을 검색하려면 Resource Scheduler가 리소스를 대상으로 지정하는 데 사용하는 태그 키를 결제

대시보드에서 비용 할당 태그로 활성화해야 합니다. 계정이 조직에 속한 경우 조직의 관리 계정에서 태그 키를 활성화해야 합니다. 이에 대한 자세한 내용은 사용자 정의 비용 할당 태그 및 사용자 정의 비용 할당 태그 활성화를 참조하세요.

태그 키가 비용 할당 태그로 활성화되면 AWS 결제는 Resource Scheduler에서 관리하는 리소스의 비용 및 사용량을 추적하기 시작하고 해당 데이터를 사용할 수 있게 되면 비용 절감 예측기는 비용 절감을 계산하고 CloudWatch의 `AMS/ResourceScheduler` 지표 네임스페이스에 데이터를 게시하기 시작합니다.

비용 할당 태그가 활성화되지 않은 경우 예측기는 절감액을 계산하고 활성화된 경우에도 지표를 게시할 수 없습니다.

> **Note**
>
> Cost Savings Estimator는 계산 시 예약 인스턴스, 절감형 플랜 등과 같은 할인을 허용하지 않습니다. 예측기는 Cost Explorer에서 사용 비용을 받아 리소스의 시간당 평균 비용을 계산합니다. 자세한 내용은 AWS 비용 데이터세트 이해: 치트 시트를 참조하세요.

AMS Resource Scheduler의 경보 억제기

AMS Resource Scheduler는 Elastic Load Balancing, Application Load Balancer 또는 Network Load Balancer 뒤에 있는 인스턴스에 대한 경보를 `AMSAlarmSuppressor` 억제하는 별도의 Lambda 함수로 배포되는 CloudWatch 경보 억제기와 함께 제공됩니다 Load Balancer. 함수는 5분마다 실행되며 계정에 있는 모든 경보를 검색하고 네임스페이스를 기반으로 그룹화합니다. 예: `AWS/ELB`, `AWS/ApplicationELB`, `AWS/NetworkELB`. 각 경보 그룹에 대해 억제기는 경보 차원에서 로드 밸런서 이름 및/또는 대상 그룹(ALB/NLB의 경우)을 찾고, 로드 밸런서 및/또는 대상 그룹에 등록된 인스턴스를 찾고, 인스턴스 상태를 확인하여 AMS Resource Scheduler에서 인스턴스를 예약했는지 확인합니다. Resource Scheduler에서 인스턴스를 예약하고 Resource Scheduler에서 인스턴스를 중지하면 억제기가 경보를 표시하여 인스턴스를 비활성화합니다. 등록된 인스턴스 목록에서 하나 이상의 인스턴스가 실행 중인 경우 억제기는 해당 경보를 표시하여 활성화로 표시된 경보를 활성화하고 비활성화로 표시된 경보를 비활성화합니다. 이에 대한 로그는 `/aws/lambda/AMSAlarmSuppressor` 로그 그룹에 저장됩니다.

AMS Accelerate에서의 로그 관리

AMS Accelerate는 로그를 수집하도록 지원되는 AWS 서비스를 구성합니다. 이러한 로그는 AMS Accelerate에서 계정 내 리소스의 규정 준수 및 감사를 보장하는 데 사용됩니다.

AMS Accelerate는 AWS에서 운영 우수성을 달성하는 데 도움이 되는 다양한 운영 서비스를 제공합니다. 연중무휴 24시간 헬프데스크, 사전 모니터링, 보안, 패치 적용, 로깅 및 백업을 포함한 몇 가지 주요 운영 기능을 통해 AMS가 AWS 클라우드에서 전반적인 운영 우수성을 달성하는 데 어떻게 도움이 되는지 빠르게 이해하려면 AMS 참조 아키텍처 다이어그램을 참조하세요.

주제

- 로그 관리 - AWS CloudTrail
- 로그 관리 - Amazon EC2
- 로그 관리 - Amazon VPC 흐름 로그

로그 관리 - AWS CloudTrail

AWS CloudTrail는 규정 준수, 운영 감사, 위험 감사 등 계정 거버넌스에 사용되는 서비스입니다. CloudTrail을 사용하면 AWS 인프라 전반의 작업과 관련된 계정 활동을 로깅, 지속적인 모니터링 및 유지할 수 있습니다.

AMS Accelerate를 사용하려면 계정의 모든 리소스에 대한 감사 및 규정 준수를 관리하기 위한 AWS CloudTrail 로깅이 필요합니다. 온보딩 중에 다음 옵션 중 하나를 선택할 수 있습니다.

- AMS 배포 추적:이 옵션을 선택하면 AMS는 계정의 기존 추적과 관계없이 기본 AWS 리전에서 CloudTrail 다중 리전 추적을 생성, 배포 및 관리합니다.
- 자체 추적 가져오기: 자체 계정 또는 조직 CloudTrail 추적을 제공하기로 선택한 경우 Cloud Architect(CA)와 협력하여 Accelerate에 필요한 구성을 충족하는지 확인해야 합니다. 이 옵션을 선택했지만 자체 추적을 제공하지 않는 경우 Accelerate는 자체 CloudTrail 추적을 자동으로 배포하여 지속적인 보안 및 감사 범위를 유지합니다. 나중에 자체 추적을 제공하는 경우 AMS는 배포된 추적을 제거하여 중복성과 추가 비용을 방지합니다. 이 접근 방식은 계정에서 단일 활성 CloudTrail 추적을 유지하고 중복 로깅 비용을 방지하는 데 도움이 됩니다.

> **Note**
>
> 계정에 기존 CloudTrail 추적이 있고 온보딩 중에 AMS 관리형 추적을 특별히 구성하거나 요청하지 않은 경우 AMS Accelerate는 계정에서 AMS 배포 추적을 자동으로 제거합니다. 이렇게 하면 중복 로깅을 방지하고 리소스 사용을 최적화하며 추가 비용을 절감할 수 있습니다.

AMS Accelerate는 Accelerate 배포된 CloudTrail 추적을 위한 Amazon S3 버킷을 이벤트 전송 대상으로 생성하고 AWS Key Management Service (AWS KMS) 암호화를 사용합니다. AMS Accelerate 운영자는 조사 및 진단 목적으로 추적 이벤트에 액세스합니다. 계정에 이미 활성화된 기존 CloudTrail 추적이 있는 경우 온보딩 중에 Accelerate가 Accelerate 관리형 추적을 배포하도록 선택한 경우이 추적은 이에 추가됩니다.

AMS Accelerate는 Accelerate 배포된 CloudTrail 추적을 포함한 CloudTrail 계정 추적이 올바르게 설정되고 암호화되도록 AWS Config 규칙을 배포합니다. 자세한 내용은 AWS Config를 참조하세요. 사용되는 규칙은 다음과 같으며 이를 설명하는 AWS 설명서 링크로 제공됩니다.

- multi-region-cloudtrail-enabled. AMS Accelerate CloudTrail이 올바른 구성으로 올바르게 설정되었는지 확인합니다.
- cloud-trail-encryption-enabled. AWS CloudTrail 가 AWS KMS 고객 마스터 키(CMK) 암호화와 함께 서버 측 암호화(SSE)를 사용하도록 구성되어 있는지 확인합니다.
- cloud-trail-log-file-validation-enabled. 활성화되면가 AWS CloudTrail 로그가 포함된 서명된 다이제스트 파일을 생성하는지 확인합니다. 모든 추적에서 파일 검증을 활성화하는 것이 좋습니다.
- s3-bucket-default-lock-enabled. 활성화되면는 Amazon S3 버킷에 잠금이 활성화되어 있는지 확인합니다.
- s3-bucket-logging-enabled. 활성화되면 Amazon S3 버킷에 대한 로깅이 활성화되어 있는지 확인합니다.

AMS Accelerate는 AWS KMS 를 사용하여 계정에 Accelerate 배포된 CloudTrail 추적에 대해 로깅된 이벤트를 암호화합니다. 이 키는 계정 관리자, AMS Accelerate 운영자 및 CloudTrail에서 제어하고 액세스할 수 있습니다. 에 대한 자세한 내용은 AWS Key Management Service 기능 제품 설명서를 AWS KMS참조하세요.

CloudTrail 로그 액세스 및 감사

AMS Accelerate 배포 CloudTrail 추적에 대한 CloudTrail 로그는 계정 내의 Amazon S3 버킷에 저장됩니다. Amazon S3 버킷에 저장된 추적 데이터는 CloudTrail 리소스가 프로비저닝될 때 생성된 AWS KMS 키를 사용하여 암호화됩니다.

Amazon S3 버킷은 ams-***aaws ## id***-cloudtrail-***AWS ##***(예: ams-a123456789-cloudtrail-us-east-1a)의 이름 지정 패턴을 활용하며 모든 이벤트는 AWS/CloudTrail 접두사와 함께 저장됩니다. 기본 버킷에 대한 모든 액세스가 로깅되고 감사 목적으로 로그 객체가 암호화되고 버전이 지정됩니다.

변경 사항 추적 및 로그 쿼리에 대한 자세한 내용은 섹션을 참조하세요AMS Accelerate 계정의 변경 사항 추적.

CloudTrail 로그 보호 및 유지

AMS Accelerate를 사용하면 Accelerate 배포 CloudTrail 추적에 대한 거버넌스 모드를 사용하여 Amazon S3 객체 잠금을 활성화하여 사용자가 특별한 권한 없이 객체 버전을 덮어쓰거나 삭제하거나 잠금 설정을 변경할 수 없도록 합니다. 자세한 내용은 Amazon S3 객체 잠금을 참조하세요.

기본적으로이 버킷의 모든 로그는 무기한 보관됩니다. 보존 기간을 변경하려면 AWS Support 센터를 통해 서비스 요청을 제출하여 다른 보존 정책을 설정할 수 있습니다.

Amazon EC2 로그 액세스

를 사용하여 Amazon EC2 인스턴스 로그에 액세스할 수 있습니다 AWS Management Console. 인스턴스 및 AWS 서비스에서 생성된 로그는 AMS Accelerate에서 관리하는 각 계정에서 사용할 수 있는 CloudWatch Logs에서 사용할 수 있습니다. 로그 액세스에 대한 자세한 내용은 CloudWatch Logs 설명서를 참조하세요.

Amazon EC2 로그 유지

Amazon EC2 인스턴스 로그는 기본적으로 무기한 보관됩니다. 보존 기간을 변경하려면 AWS Support 센터를 통해 서비스 요청을 제출하여 다른 보존 정책을 설정할 수 있습니다.

로그 관리 - Amazon EC2

AMS Accelerate는 AMS Accelerate 관리형으로 식별한 모든 Amazon EC2 인스턴스에 CloudWatch 에이전트를 설치합니다. 이 에이전트는 시스템 수준 로그를 Amazon CloudWatch Logs로 전송합니다. 자세한 내용은 Amazon CloudWatch Logs란 무엇입니까?를 참조하세요.

다음 로그 파일은 CloudWatch Logs로 전송되어 로그와 동일한 이름의 로그 그룹으로 전송됩니다. 각 로그 그룹 내에는 Amazon EC2 인스턴스 ID에 따라 이름이 지정된 각 Amazon EC2 인스턴스에 대한 로그 스트림이 생성됩니다.

Linux

- /var/log/amazon/ssm/amazon-ssm-agent.log
- /var/log/amazon/ssm/errors.log
- /var/log/audit/audit.log
- /var/log/auth.log
- /var/log/cloud-init-output.log
- /var/log/cron
- /var/log/dnf.log
- /var/log/dpkg.log
- /var/log/maillog
- /var/log/messages
- /var/log/secure
- /var/log/spooler
- /var/log/syslog
- /var/log/yum.log
- /var/log/zypper.log

자세한 내용은 CloudWatch 에이전트 구성 파일 수동 생성 또는 편집을 참조하세요.

Windows

- AmazonSSMAgentLog
- AmazonCloudWatchAgentLog
- AmazonSSMErrorLog
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEventLog

- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

자세한 내용은 빠른 시작: CloudWatch Logs 에이전트를 사용하여 CloudWatch Logs로 로그를 전송하도록 Windows Server 2016을 실행하는 Amazon EC2 인스턴스 활성화를 참조 CloudWatch 하세요.

로그 관리 - Amazon VPC 흐름 로그

VPC 흐름 로그는 VPC의 네트워크 인터페이스로 들어오고 나가는 IP 트래픽에 대한 정보를 캡처하는 기능입니다. 흐름 로그 데이터는 Amazon CloudWatch logs 또는 Amazon S3에 게시할 수 있습니다. 흐름 로그 데이터 수집은 네트워크 처리량 또는 지연 시간에 영향을 주지 않습니다. 네트워크 성능에 영향을 주지 않고 흐름 로그를 생성하거나 삭제할 수 있습니다.

흐름 로그는 다음과 같은 여러 작업에 도움이 될 수 있습니다.

- 지나치게 제한적인 보안 그룹 규칙 진단
- 인스턴스에 도달하는 트래픽 모니터링
- 네트워크 인터페이스를 오가는 트래픽 방향 결정

Accelerate 계정에서 새로 생성된 각 VPC에 대해 VPC 흐름 로그를 활성화할 필요는 없습니다. AMS는 ams-nist-cis-vpc-flow-logs-enabled Config 규칙을 사용하여 VPC에 흐름 로그가 있는지 자동으로 감지합니다. VPC 흐름 로그가 활성화되지 않은 경우 AMS는 사용자 지정 필드가 있는 VPC 흐름 로그를 생성하여 자동으로 문제를 해결합니다. 이러한 추가 필드를 사용하면 AMS 및 고객이 VPC 트래픽을 더 잘 모니터링하고, 네트워크 종속성을 이해하고, 네트워크 연결 문제를 해결하고, 네트워크 위협을 식별할 수 있습니다.

흐름 로그 보기 및 검색에 대한 자세한 내용은 흐름 로그 작업을 참조하세요.

AMS Accelerate 계정의 변경 사항 추적

Important

Change Record 서비스는 2025년 7월 1일부터 더 이상 사용되지 않습니다.
새 계정은 변경 레코드 서비스에 온보딩할 수 없습니다.
AMS Accelerate 계정에서 CloudTrail 데이터를 쿼리하려면 다음 서비스를 사용할 수 있습니다.

- 에서 이벤트 기록을 AWS CloudTrail선택하고 조회 속성을 사용하여 이벤트를 필터링합니다. 시간 범위 필터를 사용하여 `s3.amazon.aws.com` 지정된의 이벤트 소스별로 이벤트 기록을 필터링하거나 사용자 이름별로 이벤트 기록을 필터링하도록 선택할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록 작업을 참조하세요.
- AWS CloudTrail Lake를 사용하여 쿼리를 통해 데이터를 수집합니다. 에서 Lake를 AWS CloudTrail 선택한 다음 Query를 선택합니다. 자체 쿼리를 생성하거나, 쿼리 생성기를 사용하거나, 샘플 쿼리를 사용하여 이벤트 기반 데이터를 수집할 수 있습니다. 예를 들어 지난 주에 Amazon EC2 인스턴스를 삭제한 사람에게 질문할 수 있습니다. 자세한 내용은 AWS CloudTrail 소스에서 데이터 레이크 생성 및 CloudTrailLake 쿼리를 참조하세요.
- 에서 Amazon Athena 테이블을 생성하고 스토리지 위치를 추적 AWS CloudTrail 과 연결된 Amazon S3 버킷으로 설정합니다. 추적과 Amazon S3 버킷의 홈 리전이 동일한지 확인합니다. Amazon Athena에서 쿼리 편집기를 사용하여 Accelerate가 Athena 콘솔과 함께 사용하기 위해 제공하는 기본 쿼리를 실행합니다. CloudTrail 로그를 쿼리하기 위해에 Athena 테이블을 생성하는 방법에 대한 자세한 내용은 쿼리 AWS CloudTrail 로그를 참조하세요.

주제

- 변경 레코드 보기
- 기본 쿼리
- 레코드 권한 변경

AWS Managed Services는 Amazon Athena(Athena) 콘솔 및 AMS Accelerate 로그 관리를 사용하여 쿼리 가능한 인터페이스를 제공하여 AMS Accelerate Operations 팀 및 AMS Accelerate 자동화의 변경 사항을 추적하는 데 도움이 됩니다.

Athena는 표준 구조화 쿼리 언어(SQL)를 사용하여 Amazon S3의 데이터를 분석하는 데 사용할 수 있는 대화형 쿼리 서비스입니다(Amazon Athena용 SQL 참조 참조). Athena는 서버리스 서비스이므로 관

리할 인프라가 없으며 실행한 쿼리에 대해서만 비용을 지불하면 됩니다. AMS Accelerate는 CloudTrail 로그를 통해 일일 파티션이 있는 Athena 테이블을 생성하고 기본 AWS 리전 및 ams-change-record 작업 그룹 내에서 쿼리를 제공합니다. 기본 쿼리 중 하나를 선택하고 필요에 따라 실행할 수 있습니다. Athena 작업 그룹에 대한 자세한 내용은 작업 그룹 작동 방식을 참조하세요.

> **Note**
>
> 조직 관리자가 온보딩 중에 계정의 CloudTrail 이벤트를 쿼리하고 분석하기 위해 Athena를 사용하기 위한 IAM 역할을 배포하지 않는 한 CloudTrail Accelerate만 Athena를 사용하여 Accelerate에 대한 CloudTrail 이벤트를 쿼리할 수 있습니다.

변경 레코드를 사용하면 다음과 같은 질문에 쉽게 답할 수 있습니다.

- (AMS Accelerate Systems 또는 AMS Accelerate Operators)가 계정에 액세스한 사용자
- 계정에서 AMS Accelerate가 변경한 사항
- AMS Accelerate가 계정에서 변경을 수행한 시기
- 계정의 변경 사항을 볼 수 있는 위치
- AMS Accelerate가 계정에서 변경해야 하는 이유
- 쿼리를 수정하여 비 AMS 변경 사항에 대한 모든 질문에 대한 답변을 얻는 방법

변경 레코드 보기

Athena 쿼리를 사용하려면 AWS 관리 콘솔에 로그인하고 기본 AWS 리전의 Athena 콘솔로 이동합니다.

> **Note**
>
> 단계를 수행하는 동안 Amazon Athena 시작하기 페이지가 표시되면 시작하기를 클릭합니다. 이는 변경 레코드 인프라가 이미 마련되어 있는 경우에도 나타날 수 있습니다.

1. Athena 콘솔의 상단 탐색 패널에서 작업 그룹을 선택합니다.
2. ams-change-record 작업 그룹을 선택한 다음 작업 그룹 전환을 클릭합니다.
3. 데이터베이스 콤보 상자에서 ams-change-record-database를 선택합니다. ams-change-record-database에는 ams-change-record-table 테이블이 포함되어 있습니다.

4. 상단 탐색 패널에서 저장된 쿼리를 선택합니다.
5. 저장된 쿼리 창에는 AMS Accelerate가 제공하는 쿼리 목록이 표시되며,이 쿼리를 실행할 수 있습니다. 저장된 쿼리 목록에서 실행할 쿼리를 선택합니다. 예를 들어 ams_session_accesses_v1 쿼리입니다.

   사전 설정된 AMS Accelerate 쿼리의 전체 목록은 섹션을 참조하세요기본 쿼리.
6. 필요에 따라 쿼리 편집기 상자에서 날짜/시간 필터를 조정합니다. 기본적으로 쿼리는 마지막 날의 변경 사항만 확인합니다.
7. 쿼리 실행을 선택합니다.

기본 쿼리

AMS Accelerate는 Athena 콘솔 내에서 사용할 수 있는 몇 가지 기본 쿼리를 제공합니다. 기본 쿼리는 다음 표에 나열되어 있습니다.

> **Note**
>
> - 모든 쿼리는 날짜/시간 범위를 선택적 필터로 수락합니다. 모든 쿼리는 기본적으로 지난 24시간 동안 실행됩니다. 예상 입력은 다음 하위 섹션인 단원을 참조하십시오쿼리에서 날짜/시간 필터 수정.
> - 변경할 수 있거나 변경해야 하는 파라미터 입력은 쿼리에 각진 중괄호와 함께 *<PARAMETER_NAME>*으로 표시됩니다. 자리 표시자와 각형 중괄호를 파라미터 값으로 바꿉니다.
> - 모든 필터는 선택 사항입니다. 쿼리에서 일부 선택적 필터는 줄 시작 부분에 이중 대시(--)로 주석 처리됩니다. 모든 쿼리는 기본 파라미터와 함께 쿼리 없이 실행됩니다. 이러한 선택적 필터에 파라미터 값을 지정하려면 줄의 시작 부분에서 이중 대시(--)를 제거하고 원하는 대로 파라미터를 바꿉니다.
> - 모든 쿼리는 출력`IAM SessionId`에서 `IAM PincipalId` 및를 반환합니다.
> - 쿼리 실행에 대해 계산된 비용은 계정에 대해 생성되는 CloudTrail 로그 수에 따라 달라집니다. 비용을 계산하려면 AWS Athena 요금 계산기를 사용합니다.

미리 준비된 쿼리

용도/설명	입력	결과
쿼리 이름: ams_access_session_query_v1		
AMS Accelerate 액세스 세션 추적 특정 AMS Accelerate 액세스 세션에 대한 정보를 제공합니다. 쿼리는 IAM 보안 주체 ID를 선택적 필터로 수락하고 이벤트 시간, 계정 액세스에 대한 비즈니스 요구 사항, 요청자 등을 반환합니다. 줄의 주석 처리를 취소하고 자리 표시자 IAM PrincipalId를 쿼리 편집기의 특정 ID로 대체하여 특정 *IAM PrincipalId* 주체 ID를 기준으로 필터링할 수 있습니다. 쿼리의 WHERE 절에서 useragent 필터 줄을 제거하여 비 AMS 액세스 세션을 나열할 수도 있습니다.	(선택 사항) IAM PrincipalId : 액세스하려는 리소스의 IAM 보안 주체 식별자입니다. 형식은 *UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* 입니다. 자세한 내용은 고유 식별자를 참조하세요. 이 필터 없이 쿼리를 실행하여 필터링하려는 정확한 IAM PrincipalId를 확인할 수 있습니다.	• EventTime: 액세스 권한을 얻는 시간 • EventName: AWS 이벤트 이름 (AssumeRole) • EventRegion: 요청을 가져오는 AWS 리전 • EventId: CloudTrail 이벤트 ID • BusinessNeed 유형: 계정에 액세스하기 위한 비즈니스 사유 유형입니다. 허용되는 값은 SupportCase, OpsItem, Issue, Text입니다. • BusinessNeed: 비즈니스에서 계정에 액세스해야 합니다. 지원 사례 ID, 운영 항목 ID 등을 예로 들 수 있습니다. • 요청자: 계정에 액세스하는 운영자 ID 또는 계정에 액세스하는 자동화 시스템입니다. • RequestAccessType: 요청자 유형(시스템, OpsConsole, OpsAPI, Unset)
쿼리 이름: ams_events_query_v1		
AMS Accelerate에서 수행한 모든 변경 작업 추적 해당 AMS Accelerate 역할 필터를 사용하여 계정	(선택 사항) 날짜/시간 범위만 해당됩니다. 쿼리에서 날짜/시간 필터 수정을(를) 참조하세요.	• AccountId: AWS 계정 ID • RoleArn: 요청자의 RoleArn • EventTime: 액세스 권한을 얻는 시간 • EventName: AWS 이벤트 이름 (AssumeRole)

용도/설명	입력	결과
에서 수행된 모든 쓰기 작업을 반환합니다. 쿼리의 WHERE 절에서 useridentity.arn 필터 라인을 제거하여 비 AMS 역할이 수행한 변경 작업을 추적할 수도 있습니다.		• EventRegion: 요청을 가져오는 AWS 리전 • EventId: CloudTrail 이벤트 ID • RequestParameters: 요청에 대한 요청 파라미터 • ResponseElements: 응답에 대한 응답 요소입니다. • UserAgent: AWS CloudTrail 사용자 에이전트
쿼리 이름: ams_instance_access_sessions_query_v1		

용도/설명	입력	결과
AMS Accelerate로 인스턴스 액세스 추적 AMS Accelerate 인스턴스 액세스 목록을 반환합니다. 모든 레코드에는 이벤트 시간, 이벤트 리전, 인스턴스 ID, IAM 보안 주체 ID, IAM 세션 ID, SSM 세션 ID가 포함됩니다. IAM 보안 주체 ID를 사용하여 `ams_access_sessions_query_v1` Athena 쿼리를 사용하여 인스턴스에 액세스하는 데 필요한 비즈니스 요구 사항에 대한 자세한 정보를 얻을 수 있습니다. SSM 세션 ID를 사용하여 세션의 시작 및 종료 시간, 로그 세부 정보, 인스턴스 AWS 리전의 AWS Session Manager 콘솔 사용 등 인스턴스 액세스 세션에 대한 자세한 정보를 얻을 수 있습니다. 사용자는 쿼리의 WHERE 절에서 사용자 ID 필터 줄을 제거하여 비 AMS 인스턴스 액세스를 나열할 수도 있습니다.	`datetime range`만 해당합니다. 쿼리에서 날짜/시간 필터 수정을(를) 참조하세요.	• InstanceId: 인스턴스 ID • SSMSession ID: SSM 세션 ID • RoleArn: 요청자의 RoleArn • EventTime: 액세스 권한을 얻는 시간 • EventName: AWS 이벤트 이름 (AssumeRole) • EventRegion: 요청을 가져오는 AWS 리전 • EventId: CloudTrail 이벤트 ID

쿼리 이름: `ams_privilege_escalation_events_query_v1`

용도/설명	입력	결과
AMS 및 비 AMS 사용자에 대한 권한(에스컬레이션) 이벤트 추적 권한 에스컬레이션으로 직접 또는 잠재적으로 이어질 수 있는 이벤트 목록을 제공합니다. 쿼리는 ActionedBy를 선택적 필터로 수락하고 EventName, EventId, EventTime 등을 반환합니다. 이벤트와 연결된 모든 필드도 반환됩니다. 해당 이벤트에 해당하지 않는 경우 필드는 비어 있습니다. ActionedBy 필터는 기본적으로 비활성화되어 있습니다. 활성화하려면 해당 줄에서 "-- "를 제거합니다. 기본적으로 ActionedBy 필터는 비활성화되어 있습니다(모든 사용자의 권한 에스컬레이션 이벤트가 표시됨). 특정 사용자 또는 역할에 대한 이벤트를 표시하려면 WHERE 절의 사용자 ID 필터 줄에서 이중 대시(--)를 제거하고 자리 표시자 *ACTIONEDBY_PUT_USER_NAME_HERE* 를 IAM 사용자 또는 역할 이름으	(선택 사항) `ACTIONEDBY_PUT_USER_NAME` : actionedBy 사용자의 사용자 이름입니다. 이는 IAM 사용자 또는 역할일 수 있습니다. 예를 들어 ams-access-admin입니다. (선택 사항) `datetime range`. 쿼리에서 날짜/시간 필터 수정을(를) 참조하세요.	• AccountId: 계정 ID • ActionedBy: ActionedBy 사용자 이름 • EventTime: 액세스 권한을 얻는 시간 • EventName: AWS 이벤트 이름(AssumeRole). • EventRegion: 요청을 가져오는 AWS 리전 • EventId: CloudTrail 이벤트 ID

용도/설명	입력	결과
로 바꿉니다. 필터 없이 쿼리를 실행하여 필터링할 정확한 사용자를 결정할 수 있습니다.		
쿼리 이름: ams_resource_events_query_v1		
특정 리소스 AMS 또는 비 AMS에 대한 쓰기 이벤트 추적 특정 리소스에서 수행된 이벤트 목록을 제공합니다. 쿼리는 필터의 일부로 리소스 ID를 수락하고 (쿼리의 WHERE 절에서 자리 표시자 *RESOURCE_INFO* 대체) 해당 리소스에 대해 수행된 모든 쓰기 작업을 반환합니다.	(필수) RESOURCE_INFO : 리소스 식별자는 계정의 모든 AWS 리소스에 대한 ID일 수 있습니다. 리소스 ARNs과 혼동하지 마세요. 예를 들어 EC2 인스턴스의 인스턴스 ID, DynamoDB 테이블의 테이블 이름, CloudWatch Log의 logGroupName 등이 있습니다. (선택 사항) datetime range. 쿼리에서 날짜/시간 필터 수정을(를) 참조하세요.	• AccountId: 계정 ID • ActionedBy: ActionedBy 사용자 이름 • EventTime: 액세스 권한을 얻는 시간 • EventName: AWS 이벤트 이름 (AssumeRole). • EventRegion: 요청을 가져오는 AWS 리전 • EventId: CloudTrail 이벤트 ID
쿼리 이름: ams_session_events_query_v1		

용도/설명	입력	결과
특정 세션 동안 AMS Accelerate에서 수행한 쓰기 작업 추적 특정 세션에서 수행된 이벤트 목록을 제공합니다. 쿼리는 필터의 일부로 IAM 보안 주체 ID를 수락하고(쿼리의 WHERE 절에서 자리 표시자 *PRINCIPAL_ID* 대체) 해당 리소스에 대해 수행된 모든 쓰기 작업을 반환합니다.	(필수) PRINCIPAL_ID : 세션의 보안 주체 ID입니다. 형식은 *UNIQUE_ID ENTIFIER :RESOURCE_NAME* 입니다. 자세한 내용은 고유 식별자를 참조하세요. 쿼리 "ams_session_ids_by_requester_v1"을 실행하여 요청자의 IAM 보안 주체 IDs 있습니다. 이 필터 없이 쿼리를 실행하여 필터링할 정확한 IAM PrincipalId를 결정할 수도 있습니다. (선택 사항) datetime range. 쿼리에서 날짜/시간 필터 수정을(를) 참조하세요.	• AccountId: 계정 ID • ActionedBy: ActionedBy 사용자 이름 • EventTime: 액세스 권한을 얻는 시간 • EventName: AWS 이벤트 이름 (AssumeRole) • EventRegion: 요청을 가져오는 AWS 리전 • EventId: CloudTrail 이벤트 ID
쿼리 이름: ams_session_ids_by_requester_v1		
특정 요청자의 IAM 보안 주체/세션 IDs. 쿼리는 "requester"(쿼리의 WHERE 절에서 자리 표시자 *###* 대체)를 수락하고 지정된 시간 범위 동안 해당 요청자가 모든 IAM 보안 주체 ID를 반환합니다.	(필수) Requester : 계정에 액세스하는 연산자 ID(예: 연산자의 별칭) 또는 계정에 액세스하는 자동화 시스템(예: OsConfiguration, AlarmManager 등). (선택 사항) datetime range. 쿼리에서 날짜/시간 필터 수정을(를) 참조하세요.	• IAM PrincipalId - 세션의 IAM PrincipalId입니다. 형식은 *UNIQUE_ID ENTIFIER :RESOURCE_NAME* 입니다. 자세한 내용은 고유 식별자를 참조하세요. 이 필터 없이 쿼리를 실행하여 필터링할 정확한 IAM PrincipalId를 결정할 수 있습니다. • IAM SessionId - 액세스 세션의 IAM 세션 ID • EventTime: 액세스 권한을 얻는 시간

쿼리에서 날짜/시간 필터 수정

모든 쿼리는 날짜/시간 범위를 선택적 필터로 허용합니다. 모든 쿼리는 기본적으로 지난 1일 동안 실행됩니다.

날짜/시간 필드에 사용되는 형식은 yyyy/MM/dd(예: 2021/01/01)입니다. 날짜만 저장하고 전체 타임스탬프는 저장하지 않습니다. 전체 타임스탬프의 경우 ISO 8601 형식 yyyy-MM-ddT HH:mm:ssZ(예: 2021-01-01T23:59:59Z)로 타임스탬프를 저장하는 필드 eventime을 사용합니다. 그러나 테이블은 날짜/시간 필드에 분할되므로 날짜/시간 필터와 이벤트/시간 필터를 모두 쿼리에 전달해야 합니다. 다음 예시를 참조하세요.

> **Note**
>
> 범위를 수정할 수 있는 허용되는 모든 방법을 보려면 현재 날짜 및 시간 함수 및 연산자에 사용되는 Athena 엔진 버전을 기반으로 하는 최신 Presto 함수 설명서를 참조하여 범위를 수정할 수 있는 허용되는 모든 방법을 확인하세요.

날짜 수준: 지난 1일 또는 지난 24시간(기본값) 예: CURRENT_DATE='2021/01/01' 인 경우 필터는 현재 날짜에서 하루를 빼서 날짜/시간 > '2020/12/31'로 형식을 지정합니다.

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
```

날짜 수준: 지난 2개월 예:

```
datetime > date_format(date_add('month', - 2, CURRENT_DATE), '%Y/%m/%d')
```

날짜 수준: 2일 사이 예:

```
datetime > '2021/01/01'
       AND
       datetime < '2021/01/10'
```

타임스탬프 수준: 지난 12시간 예:

스캔한 파티션 데이터는 1일 동안 지속된 다음 지난 12시간 내의 모든 이벤트를 필터링합니다.

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
       AND
```

```
      eventtime > date_format(date_add('hour', - 12, CURRENT_TIMESTAMP), '%Y-%m-%dT%H:
%i:%sZ')
```

타임스탬프 수준: 2개 사이의 타임스탬프 예:

2021년 1월 1일 오후 12시에서 2021년 1월 10일 오후 3시 사이에 이벤트를 가져옵니다.

```
datetime > '2021/01/01' AND datetime < '2021/01/10'
      AND
      eventtime > '2021-01-01T12:00:00Z' AND eventtime < '2021-01-10T15:00:00Z'
```

기본 쿼리 예제

ams_access_session_query_v1

```
Name: ams_access_session_query_v1

Description: >-
   The query provides more information on specific AMS access session.
   The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   By default; the query filter last day events only, the user can change the datetime
 filter to search for more wide time range.
   By default; the IAM PrincipalId filter is disabled. To enable it, remove "-- " from
 that line.

AthenaQueryString: |-
   /*
     The query provides list of AMS access sessions during specific time range.
     The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
     If you want to only show access sessions for a particular IAM principal ID, remove
 the double-dash (--) from
     the "IAM Principal ID" filter line in the WHERE clause of the query, and replace
 the placeholder "<IAM PrincipalId>" with the specific ID that you want.
     You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.
```

```
    By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
    remove the "useragent" filter in the WHERE clause of the query.

    For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
  */

  SELECT
     json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
     json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionId",
     eventtime AS "EventTime",
     eventname AS "EventName",
     awsregion AS "EventRegion",
     eventid AS "EventId",
     json_extract_scalar(requestparameters, '$.tags[0].value') AS "BusinessNeed",
     json_extract_scalar(requestparameters, '$.tags[1].value') AS "BusinessNeedType",
     json_extract_scalar(requestparameters, '$.tags[2].value') AS "Requester",
     json_extract_scalar(requestparameters, '$.tags[3].value') AS "AccessRequestType"
  FROM
      "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
  WHERE
     datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
     AND eventname = 'AssumeRole'
     AND useragent = 'access.managedservices.amazonaws.com'
     -- AND  json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId')
 = '<IAM PrincipalId>'
  ORDER BY eventtime

InsightsQueryString: |-
  # The query provides list of AMS access sessions during specific time range.
  # The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
  #
  # By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
  # If you want to only show access sessions for a particular IAM principal ID, remove
 the # (#) from
  # the "IAM Principal ID" filter of the query, and replace the placeholder "<IAM
 PrincipalId>" with the specific ID that you want.
```

```
  # You can run the query without the filter to determine the exact IAM PrincipalId
you want to filter with.
  #
  # By default; the query only shows AMS access sessions. If you also want to show
non-AMS access sessions,
  # remove the "useragent" filter from the query.
  #
  # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
in your AMS Accelerate accounts -> Default Queries

  filter eventName="AssumeRole" AND userAgent="access.managedservices.amazonaws.com"
  # | filter responseElements.assumedRoleUser.assumedRoleId= "<IAM PrincipalId>"
  | sort eventTime desc
  | fields
     responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
     responseElements.credentials.accessKeyId as IAMSessionId,
     eventTime as EventTime,
     eventName as EventName,
     awsRegion as EventRegion,
     eventID as EventId,
     requestParameters.tags.0.value as BusinessNeed,
     requestParameters.tags.1.value as BusinessNeedType,
     requestParameters.tags.2.value as Requester,
     requestParameters.tags.3.value as AccessRequestType
```

ams_events_query_v1

```
ams_events_query_v1.yaml
/*
  The query provides list of events to track write actions for all AMS changes.
  The query returns all write actions done on the account using that AMS role filter.

  By default, the query filters the last day's events only; you can change the
"datetime" filter to search for a wider time range.

  You can also track mutating actions done by non-AMS roles by removing the
"useridentity.arn" filter lines from the WHERE clause of the query.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
your AMS Accelerate accounts -> Default Queries
*/
```

```
SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   useridentity.arn AS "RoleArn",
   eventid AS "EventId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventsource AS "EventService",
   eventtime AS "EventTime",
   requestparameters As "RequestParameters",
   responseelements AS "ResponseElements",
   useragent AS "UserAgent"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   readonly <> 'true'
   AND
   (
      LOWER(useridentity.arn) LIKE '%/ams%'
      OR LOWER(useridentity.arn) LIKE '%/customer_ssm_automation_role%'
   )
ORDER BY eventtime
```

ams_instance_access_sessions_query_v1

```
ams_instance_access_sessions_query_v1
/*
  The query provides list of AMS Instance accesses during specific time range.

  The query returns the list of AMS instance accesses; every record includes the event
 time, the event AWS Region, the instance ID, the IAM session ID, and the SSM session
 ID.
  You can use the IAM Principal ID to get more details on the business need for
 accessing the instance by using ams_access_session_query_v1 athena query.
  You can use the SSM session ID to get more details on the instance access session,
 including the start and end time of the session and log details, using the AWS Session
 Manager Console in the instance's AWS Region.

  You can also list non-AMS instance accesses by removing the "useridentity" filter
 line in the WHERE clause of the query.
```

```
  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   json_extract_scalar(requestparameters, '$.target') AS "InstanceId",
   json_extract_scalar(responseelements, '$.sessionId') AS "SSM SessionId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventsource AS "EventService",
   eventtime AS "EventTime"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   useridentity.sessionContext.sessionIssuer.arn like '%/ams_%'
   AND eventname = 'StartSession'
ORDER BY eventtime
```

ams_privilege_escalation_events_query_v1

```
ams_privilege_escalation_events_query_v1.yaml
/*
  The query provides list of events that can directly or potentially lead to a
 privilege escalation.

  The query accepts ActionedBy as an optional filter and returns EventName, EventId,
 EventTime, ... etc.
  All fields associated with the event are also returned. Some fields are blank if not
 applicable for that event.
  You can use the IAM Session ID to get more details about events happened in that
 session by using ams_session_events_query_v1 query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  By default, the ActionedBy filter is disabled (it shows privilege escalation events
 from all users).
```

```
  To show events for a particular user or role, remove the double-dash (--) from the
 useridentity filter line in the WHERE clause of the query
  and replace the placeholder "<ACTIONEDBY_PUT_USER_NAME_HERE>" with an IAM user or
 role name.
  You can run the query without the filter to determine the exact user you want to
 filter with.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventtime AS "EventTime",
   json_extract_scalar(requestparameters, '$.userName') AS "UserName",
   json_extract_scalar(requestparameters, '$.roleName') AS "RoleName",
   json_extract_scalar(requestparameters, '$.groupName') AS "GroupName",
   json_extract_scalar(requestparameters, '$.policyArn') AS "PolicyArn",
   json_extract_scalar(requestparameters, '$.policyName') AS "PolicyName",
   json_extract_scalar(requestparameters, '$.permissionsBoundary') AS
 "PermissionsBoundary",
   json_extract_scalar(requestparameters, '$.instanceProfileName') AS
 "InstanceProfileName",
   json_extract_scalar(requestparameters, '$.openIDConnectProviderArn') AS
 "OpenIDConnectProviderArn",
   json_extract_scalar(requestparameters, '$.serialNumber') AS "SerialNumber",
   json_extract_scalar(requestparameters, '$.serverCertificateName') AS
 "ServerCertificateName",
   json_extract_scalar(requestparameters, '$.accessKeyId') AS "AccessKeyId",
   json_extract_scalar(requestparameters, '$.certificateId') AS "CertificateId",
   json_extract_scalar(requestparameters, '$.newUserName') AS "NewUserName",
   json_extract_scalar(requestparameters, '$.newGroupName') AS "NewGroupName",
   json_extract_scalar(requestparameters, '$.newServerCertificateName') AS
 "NewServerCertificateName",
   json_extract_scalar(requestparameters, '$.name') AS "SAMLProviderName",
   json_extract_scalar(requestparameters, '$.sAMLProviderArn') AS "SAMLProviderArn",
   json_extract_scalar(requestparameters, '$.sSHPublicKeyId') AS "SSHPublicKeyId",
```

```
   json_extract_scalar(requestparameters, '$.virtualMFADeviceName') AS
 "VirtualMFADeviceName"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   (
     -- More event names can be found at https://docs.aws.amazon.com/IAM/latest/
UserGuide/list_identityandaccessmanagement.html
     eventname LIKE 'Add%' OR
     eventname LIKE 'Attach%' OR
     eventname LIKE 'Delete%' AND eventname != 'DeleteAccountAlias' OR
     eventname LIKE 'Detach%' OR
     eventname LIKE 'Create%' AND eventname != 'CreateAccountAlias' OR
     eventname LIKE 'Put%' OR
     eventname LIKE 'Remove%' OR
     eventname LIKE 'Update%' OR
     eventname LIKE 'Upload%' OR
     eventname = 'DeactivateMFADevice' OR
     eventname = 'EnableMFADevice' OR
     eventname = 'ResetServiceSpecificCredential' OR
     eventname = 'SetDefaultPolicyVersion'
   )
   AND eventsource = 'iam.amazonaws.com'
ORDER BY eventtime
```

ams_resource_events_query_v1

```
Name: ams_resource_events_query_v1

Description: >-
   The query provides list of events done on specific resource.
   The query accepts resource id as part of the filters, and return all write actions
 done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of events done on specific resource.

     The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the WHERE clause of the query),
```

```
    and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
    Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.

    By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

    For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
  */

  SELECT
     useridentity.principalId AS "IAM PrincipalId",
     useridentity.accesskeyid AS "IAM SessionId",
     useridentity.accountid AS "AccountId",
     reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
     eventname AS "EventName",
     awsregion AS "EventRegion",
     eventid AS "EventId",
     eventsource AS "EventService",
     eventtime AS "EventTime"
  FROM
      "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
  WHERE
     datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
     AND readonly <> 'true'
     AND
     (
        requestparameters LIKE '%<RESOURCE_INFO>%'
        OR responseelements LIKE '%<RESOURCE_INFO>%'
     )
  ORDER BY eventtime

InsightsQueryString: |-
  # The query provides list of events done on specific resource.
  #
  # The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the filter of the query),
  # and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
  # Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.
  #
```

```
  # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
in your AMS Accelerate accounts -> Default Queries

  filter readOnly=0
  | parse @message '"requestParameters":{*}' as RequestParameters
  | parse @message '"responseElements":{*}' as ResponseElements
  # | filter RequestParameters like "RESOURCE_INFO" or ResponseElements like
"<RESOURCE_INFO>"
  | fields
     userIdentity.principalId as IAMPrincipalId,
     userIdentity.accessKeyId as IAMSessionId,
     userIdentity.accountId as AccountId,
     userIdentity.arn as ActionedBy,
     eventName as EventName,
     awsRegion as EventRegion,
     eventID as EventId,
     eventSource as EventService,
     eventTime as EventTime
  | display IAMPrincipalId, IAMSessionId, AccountId, ActionedBy, EventName,
EventRegion, EventId, EventService, EventTime
  | sort eventTime desc
```

ams_session_events_query_v1

```
Name: ams_session_events_query_v1

Description: >-
   The query provides list of events done on specific session.
   The query accepts IAM Principal Id as part of the filters, and return all write
actions done on that resource.
   By default; the query list the accesses for last day, the user can change the time
range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides a list of events executed on a specific session.

     The query accepts the IAM principal ID as part of the filters (replace the
placeholder "<PRINCIPAL_ID>" in the WHERE clause of the query),
     and returns all write actions done on that resource.

     By default, the query filters the last day's events only; you can change the
"datetime" filter to search for a wider time range.
```

```
     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventsource AS "EventService",
      eventtime AS "EventTime",
      requestparameters As "RequestParameters",
      responseelements AS "ResponseElements",
      useragent AS "UserAgent"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate   WHERE
      useridentity.principalid = '<PRINCIPAL_ID>'
      AND datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides a list of events executed on a specific session.
   #
   # The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the filter of the query),
   # and returns all write actions done on that resource.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0 AND userIdentity.principalId = "<IAM Principal>"
   | sort eventTime desc
   | fields
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventSource as EventService,
```

```
      eventTime as EventTime,
      userAgent as UserAgent
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
```

ams_session_ids_by_requester_v1

```
Name: ams_session_ids_by_requester_v1

Description: >-
   The query provides list of IAM Principal/Session Ids for specific requester.
   The query accepts requester and return all IAM Principal/Session Ids by that
 requester during specific time range.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of IAM Principal IDs for a specific requester.

     The query accepts the requester (replace placeholder "<Requester>" in the WHERE
 clause of the query),
     and returns all IAM Principal IDs by that requester during a specific time range.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionIId",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND json_extract_scalar(requestparameters, '$.tags[2].value') = '<Requester>'
   ORDER BY eventtime
```

```
InsightsQueryString: |-
   # The query provides list of IAM Principal IDs for a specific requester.
   #
   # The query accepts the requester (replace placeholder "<Requester>" in the filter
 of the query),
   # and returns all IAM Principal IDs by that requester during a specific time range.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   filter eventName="AssumeRole" AND requestParameters.tags.2.value="<Requester>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime
```

레코드 권한 변경

변경 레코드 쿼리를 실행하려면 다음 권한이 필요합니다.

- 아테나
  - athena:GetWorkGroup
  - athena:StartQueryExecution
  - athena:ListDataCatalogs
  - athena:GetQueryExecution
  - athena:GetQueryResults
  - athena:BatchGetNamedQuery
  - athena:ListWorkGroups
  - athena:UpdateWorkGroup
  - athena:GetNamedQuery
  - athena:ListQueryExecutions
  - athena:ListNamedQueries
- AWS KMS
  - kms:Decrypt

  - AWS KMS Accelerate가 SSE-KMS 암호화를 사용하여 CloudTrail 추적 이벤트 Amazon S3 버킷 데이터 스토어를 사용하는 경우 AMSCloudTrailLogManagement의 키 ID 또는 AWS KMS 키 ID(들). Amazon S3
- AWS Glue
  - glue:GetDatabase
  - glue:GetTables
  - glue:GetDatabases
  - glue:GetTable
- Amazon S3 읽기 액세스
  - Amazon S3 버킷 CloudTrail 데이터 스토어: ams-a*AccountId*-cloudtrail-*primary region* 또는 Amazon S3 버킷 이름, CloudTrail 추적 이벤트 Amazon S3 버킷 데이터 스토어.
- Amazon S3 쓰기 액세스
  - Athena 이벤트 쿼리 결과 Amazon S3 버킷: ams-a*AccountId* athena-results-*primary region*

AWS Systems Manager Accelerate의

AWS Systems Manager 문서(SSM 문서)는 Systems Manager가 AWS 리소스에서 수행하는 작업을 정의합니다. Systems Manager에는 런타임 시 파라미터를 지정하여 사용할 수 있는 사전 구성된 문서가 12개 이상 포함되어 있습니다. 문서는 JavaScript Object Notation(JSON) 또는 YAML을 사용하며 사용자가 지정하는 단계와 파라미터를 포함합니다.

AWS Managed Services(AMS)는 SSM 문서의 신뢰할 수 있는 게시자입니다. AMS가 소유한 SSM 문서는 온보딩된 AMS 계정과만 공유되며, 항상 예약된 접두사(AWSManagedServices-*)로 시작하고, Amazon이 소유한 Systems Manager 콘솔에 표시됩니다. SSM 문서 개발 및 게시를 위한 AMS 프로세스는 AWS 모범 사례를 따르며 문서 수명 주기 전반에 걸쳐 여러 피어 검토가 필요합니다. SSM 문서 공유의 AWS 모범 사례에 대한 자세한 내용은 공유 SSM 문서 모범 사례를 참조하세요.

사용 가능한 AMS Accelerate SSM 문서

AMS Accelerate SSM 문서는 AMS Accelerate 고객만 사용할 수 있으며 계정 운영을 위한 운영 워크플로를 자동화하는 데 사용됩니다.

에서 사용 가능한 AMS Accelerate SSM 문서를 보려면 AWS Management Console

1. AWS Systems Manager 콘솔에서 Systems Manager콘솔을 엽니다.
2. 나와 공유를 선택합니다.
3. 검색 창에서 문서 이름 접두사를 기준으로 필터링한 다음 같음을 기준으로 값을 AWSManagedServices-로 설정합니다.

   AWS CLI 지침은 공유 SSM 문서 사용을 참조하세요.

AMS Accelerate SSM 문서 버전

SSM 문서는 버전 관리를 지원합니다. AMS Accelerate SSM 문서는 고객의 계정에서 수정할 수 없으며 다시 공유할 수 없습니다. 계정을 운영하기 위해 AMS Accelerate에서 중앙에서 관리하고 유지 관리합니다.

버전 번호는 특정 AWS 리전에서 문서를 업데이트할 때마다 증가합니다. 새 리전을 사용할 수 있게 되면 두 리전의 동일한 문서 콘텐츠의 버전 번호가 다를 수 있습니다. 이는 일반적이며 동작이 다르다는 의미는 아닙니다. 두 AMS Accelerate SSM 문서를 비교하려면 AWS CLI해시를와 비교하는 것이 좋습니다.

```
aws ssm describe-document \
--name AWSManagedServices-DOCUMENTNAME \
--output text --query "Document.Hash"
```

해시가 일치하면 두 개의 SSM 문서가 동일합니다.

Systems Manager 요금

AMS Accelerate SSM 문서 액세스와 관련된 비용은 없습니다. 런타임 비용은 SSM 문서 유형, 단계 및 런타임 기간에 따라 달라집니다. 자세한 내용은 AWS Systems Manager 요금을 참조하세요.

AMS Accelerate 사용 설명서의 문서 기록

다음 표에서는 AMS Accelerate 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
컨트롤 플레인 업그레이드를 위한 경보 관리자 설명서 업데이트	2026년 2월에 완료된 컨트롤 플레인 마이그레이션을 반영하도록 경보 관리자 설명서가 업데이트되었습니다. • Accelerate Alarm Manager - 리전 제한 공지 제거, 구성 경고에 대한 강조 추가, 적용되는 변경 사항에 대한 타이밍 설명 제거 • 구성 프로파일 가속화: 모니터링 - ConfigurationID에 대한 모순되는 설명 제거 • 구성 프로파일 가속화: 의사 파라미터 대체 - 새 리소스 유형에 대한 의사파라미터를 추가하고 EC2 인스턴스 및 디스크, Elasticsearch 도메인 및 Elastic Load Balancing에 대한 기존 설명을 업데이트했습니다. • 경보 구성 가속화 예제 - Linux에서 디스크 경로 파라미터가 더 이상 지원되지 않으므로 Linux 디스크 경보 예제에서 경로 차원을 제거했습니다. • 컨트롤 플레인 업그레이드와 함께 보고 기능이 더 이상 사	2026년 3월 31일

	용되지 않으므로 더 이상 사용되지 않는 페이지 "Alarm Manager에서 모니터링하는 리소스 수 보기"가 제거되었습니다. • Accelerate용 리소스 인벤토리 - 컨트롤 플레인 아키텍처 변경 사항을 반영하는 새 리소스 인벤토리 파일을 참조하도록 업데이트됨	
가속화를 위한 리소스 인벤토리 업데이트	AMS 인프라의 규정 준수 제어에 대한 세부 정보가 추가되었습니다.	2026년 3월 27일
Compute Optimizer 권장 사항 부울 값 업데이트	표준 규칙과의 일관성을 위해 모든 부울 파라미터 값을 대문자(True/False)에서 소문자(true/false)로 업데이트했습니다.	2026년 3월 24일
교차 계정 정책에 대한 AMS-STD-002 포인트 6.11 업데이트	타사 계정에 대한 쓰기 액세스 권한이 있는 교차 계정 정책을 위험 수락으로 구성할 수 있음을 명확히 했습니다.	2026년 3월 24일
업데이트된 AWS Health 모니터링 참고 사항	알림은 AMS Operations의 조치가 필요한 AWS Health 이벤트에 대해서만 전송됨을 명확히 했습니다.	2026년 3월 24일
ONTAP 볼륨 용량 자동 문제 해결 추가	자동 문제 해결 테이블에 AMSFSXONTAPVolumeCapacityUtilization 알림을 추가하고 ONTAP 볼륨 용량 문제 해결 자동화를 설명하는 새 섹션을 추가했습니다.	2026년 3월 24일

Resource Scheduler 일정 기간 필드 레이블 업데이트	일정 추가 절차에서 필드 레이블을 "Schedules"에서 "Periods"로 수정했습니다.	2026년 3월 11일
AMS 섹션의 기준 모니터링에서 알림 업데이트	Amazon EC2 인스턴스 - 모든 OSs.	2026년 1월 22일
고객 보안 위험 관리 프로세스 섹션 업데이트	위험 수락 유효성, 검토 및 옵트아웃 정보로 고객 보안 위험 관리 프로세스 섹션을 업데이트했습니다.	2026년 1월 15일
AMS 알림 자동 문제 해결의 Amazon RDS 스토리지 부족 이벤트 문제 해결 자동화 섹션 업데이트	트리거 이벤트에 따라 수정으로 수정된 속성에 대한 정보로 Amazon RDS 스토리지 부족 이벤트 수정 자동화 섹션을 업데이트했습니다.	2026년 1월 15일
온디맨드 작업 섹션에 대한 표 업데이트	작업 온디맨드 섹션을 업데이트된 콘텐츠로 업데이트했습니다.	2026년 1월 7일
Security Hub CSPM에 대한 정보로 AMS의 신뢰할 수 있는 수정자 섹션에 새 콘텐츠를 업데이트하고 추가했습니다.	AMS 섹션에서 신뢰할 수 있는 수정자를 Security Hub CSPM에 대한 정보로 업데이트하고 신뢰할 수 있는 수정자가 지원하는 Security Hub CSPM 권장 사항을 새 페이지로 추가했습니다.	2025년 12월 11일

지원되는 리전 업데이트	아시아 태평양(말레이시아) 리전에서 사용할 수 없는 서비스에 대한 다음 섹션에 참고 사항이 추가되었습니다. • Amazon Macie로 모니터링 • AMS Accelerate에서 Amazon EKS 모니터링 및 인시던트 관리 • SSM 에이전트 자동 설치 • 경보 관리자 가속화	2025년 10월 24일
업데이트된 로그 관리 - AWS CloudTrail 섹션	AWS CloudTrail 로깅에 대한 새로운 정보 및 참고 사항입니다.	2025년 9월 25일
Trusted Remediator에서 지원하는 새로운 Trusted Advisor 비용 최적화 검사 4개 추가	다음과 같은 비용 최적화 검사가 추가되었습니다. • c1z7kmr00n - 인스턴스에 대한 Amazon EC2 비용 최적화 권장 사항 • c1z7kmr02n - 볼륨에 대한 Amazon EBS 비용 최적화 권장 사항 • c1z7kmr03n - DB 인스턴스에 대한 Amazon RDS 비용 최적화 권장 사항 • c1z7kmr05n - 함수에 대한 AWS Lambda 비용 최적화 권장 사항	2025년 9월 22일
변경 레코드 서비스에 대한 사용 중단 참고 사항 업데이트	대체 솔루션을 사용하여 Change Record 서비스에 대한 사용 중단 정보를 업데이트했습니다.	2025년 9월 11일

Trusted Remediator에서 지원하는 업데이트된 Trusted Advisor 보안 검사	검사 Hs4Ma3G108에 대해 지원되는 사전 구성된 파라미터 및 제약 조건 업데이트 - CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 함	2025년 9월 5일
Trusted Remediator에서 지원하는 업데이트된 Trusted Advisor 보안 검사	Hs4Ma3G184 버전 2를 추가하도록 Trusted Advisor 보안 검사를 업데이트했습니다. Application Load Balancer 및 Classic Load Balancer 로깅을 활성화해야 합니다.	2025년 9월 5일
신뢰할 수 있는 수정자 섹션에서 지원하는 Trusted Advisor 운영 우수성 검사 업데이트	지원되는 새 검사 c1fd6b96l4 Amazon S3 액세스 로그 활성화를 추가하도록 Trusted Remediator에서 지원하는 Trusted Advisor 운영 우수성 검사가 업데이트되었습니다.	2025년 8월 28일
Compute Optimizer에 대한 새 콘텐츠를 포함하도록 신뢰할 수 있는 수정자 섹션 업데이트	지원되는 AWS Compute Optimizer 권장 사항에 대한 새 콘텐츠를 포함하도록 신뢰할 수 있는 수정자 섹션을 업데이트했습니다.	2025년 8월 18일
TOC 용어집 링크 제거됨	AWS 용어집.	2025년 8월 8일
TOC 용어집 링크 제거됨	AWS 용어집.	2025년 8월 8일
패치 일일 보고서의 새 필드	인스턴스 태그: Amazon EC2 인스턴스 ID와 연결된 태그입니다.	2025년 8월 8일

새로운 신뢰할 수 있는 수정자 검사	Trusted Advisor Trusted Remediator Hs4Ma3G120–AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime, Hs4Ma3G230–AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 및 c18d2gz150–AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime에서 지원하는 Trusted Remediator 보안 검사에서 지원하는 비용 최적화 검사입니다. Trusted Advisor Hs4Ma3G120 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime Hs4Ma3G230AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime	2025년 8월 8일
포인트 3.2에서 IAM 표준 업데이트	언어를 명확히 하고 태그 지정에 대한 언급을 제거했습니다.	2025년 7월 25일
Accelerate에서 리소스 태거 구성 프로파일 업데이트	Accelerate의 리소스 태거 구성 프로필에 새 AvailabilityZone 필터가 추가되었습니다.	2025년 7월 25일
Accelerate에서 인시던트 보고서, 서비스 요청 및 결제 질문을 업데이트했습니다.	Plus 및 Premium 서비스 티어에 대한 참조를 서비스 SLA 링크로 대체했습니다.	2025년 7월 25일

Accelerate에서 인시던트 관리를 업데이트했습니다.	운영 센터에 대한 정보가 업데이트되었습니다.	2025년 7월 25일
AMS 패턴 페이지를 올바른 링크로 업데이트했습니다.	SLA 및 SLO 링크를 수정했습니다.	2025년 7월 25일
알림 옵트아웃 옵션 업데이트	태그를 추가하면 두 개의 알림을 추가로 옵트아웃할 수 있습니다.	2025년 7월 25일
백업을 위한 새로운 기능	새 태그를 사용하여 백업 볼트에 대한 알림을 사용자 지정합니다.	2025년 7월 25일
Accelerate에서 지원되는 구성에 대한 섹션 업데이트	Accelerate에서 지원되는 운영 체제 및 지원되는 지원 종료(EOS) 운영 체제에 대해 지원되는 구성을 업데이트했습니다.	2025년 6월 26일
Accelerate에서 패치 관리를 위한 태그 관리 페이지 제거	이 기능은 더 이상 사용되지 않으므로 Accelerate에서 패치 관리를 위한 태그 관리 페이지가 제거되었습니다.	2025년 6월 19일
대체 패치 리포지토리에 대한 패치 관리 중요 보안 참고 사항입니다.	AMS Accelerate에서 대체 패치 리포지토리를 사용하기 위한 중요 보안 참고 사항 및 모범 사례입니다.	2025년 6월 10일
AMS Accelerate 변경 레코드 사용 중단.	AMS Accelerate Change Record 서비스는 2025년 7월 1일부터 더 이상 사용되지 않습니다.	2025년 5월 27일
지원되는 운영 체제 업데이트.	AMS Accelerate 지원 운영 체제가 업데이트되고, 일부는 추가되고, 일부는 제거됩니다.	2025년 5월 22일

중동(UAE) 리전 지원 서비스에 대한 참고 사항입니다.	중동(UAE) 리전의 일부 서비스에 대한 제한된 지원.	2025년 5월 22일
내부 전용 APIs	일부 CloudWatch 로그에 나타나는 내부 전용 APIs.	2025년 5월 22일
누락된 로그 위치가 추가되었습니다.	일부 누락된 Windows 로그 위치가 추가되었습니다.	2025년 5월 22일
AMS Accelerate Trusted Remediator 업데이트.	새 파라미터인 `preconfigured-parameters` 를 사용하여 신뢰할 수 있는 수정자에서 Trusted Advisor 검사를 사용자 지정하는 방법.	2025년 5월 22일
AMS Accelerate Trusted Remediator FAQ 및 업데이트.	지원되는 Trusted Advisor 검사에 대한 몇 가지 업데이트, 신뢰할 수 있는 수정자 FAQ("신뢰할 수 있는 수정자는 계정에 어떤 리소스를 배포합니까?" 추가됨) 등이 있습니다. Trusted Advisor Trusted Remediator에서 지원하는 검사를 참조하세요.	2025년 5월 8일
AMS Accelerate Standard 보안 제어 업데이트.	"보안 그룹 공유" 제어가 추가되었습니다.	2025년 5월 8일
모니터링 알림 업데이트를 가속화합니다.	추가 알림이 추가되고 알림 이름이 메모 열에 추가되었습니다.	2025년 4월 28일
리소스 인벤토리를 가속화합니다.	리소스 인벤토리 스프레드시트 파일(압축됨)이 업데이트됩니다.	2025년 4월 24일
로그 위치를 가속화합니다.	추가 로그 위치가 추가되었습니다.	2025년 4월 24일

보안 인시던트 대응을 위한 새로운 역할과 책임(RACI)을 가속화합니다.	보안 인시던트 대응을 위한 RACI.	2025년 3월 27일
새로운 Amazon RDS 자동 수정 알림을 가속화합니다.	알림 ID:- 0224, 요청된 할당된 스토리지가 구성된 최대 스토리지 임계값에 도달하거나 초과할 때 트리거됩니다.	2025년 3월 27일
온보딩 가속화 역할 템플릿 업데이트.	AWS GovCloud 리전을 지원하도록 AMS Accelerate 온보딩 역할 템플릿이 업데이트되었습니다.	2025년 3월 25일
새로운 자동 수정 RDS 알림을 가속화합니다.	RDS-EVENT-0224가 추가되었습니다.	2025년 3월 17일
새로운 기능 가속화: 인시던트 알림.	AppRegistry를 사용하여 애플리케이션을 생성하고 해당 애플리케이션에 대한 인시던트 알림을 사용자 지정할 수 있습니다.	2025년 3월 13일
RDS 경보 모니터링 임계값에 대한 업데이트를 가속화합니다.	RDS 평균 CPU 사용률 경보 임계값이 75%에서 90%로 변경되었습니다.	2025년 2월 20일
알림 테이블의 AMS 자동 문제 해결에 대한 업데이트를 가속화합니다.	알림 수정 테이블이 새 콘텐츠로 확장되었습니다.	2025년 2월 20일
새로운 기능 가속화: 경보를 유지합니다.	자동 삭제 대신 CloudWatch에 경보를 유지하도록 경보 관리자를 구성할 수 있습니다.	2025년 2월 20일

집계된 보고서 보기를 위한 새 데이터 옵션으로 셀프 서비스 보고서 업데이트	다음 셀프 서비스 보고서에 `Trusted AWS Organization account enabled by the customer` 대한 새 필드 이름: `Admin Account ID`, 데이터 세트 필드 이름: `aws_admin_account_id` 및 정의:를 포함하는 데이터 옵션을 추가했습니다. • 패치 보고서(일별) • 백업 보고서(일별) • 인시던트 보고서(주별) • Resource Tagger 대시보드 • 보안 구성 규칙 대시보드	2025년 1월 28일

Trusted Remediator에서 지원하는 추가 AWS Trusted Advisor 검사 추가	이제 Trusted Remediator에서 다음 Trusted Advisor 검사를 지원합니다.
	• 비용 최적화
	  • c1cj39rr6v - Amazon S3 불완전 멀티파트 업로드 중단 구성
	• 보안
	  • Hs4Ma3G199 - RDS DB 인스턴스는 CloudWatch Logs에 로그를 게시해야 합니다.
	  • Hs4Ma3G326 - Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
	  • Hs4Ma3G272 - 사용자에게 SageMaker AI 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
	  • Hs4Ma3G325 - EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
	  • HHs4Ma3G118 - VPC 기본 보안 그룹은 인바운드 또는 아웃바운드 트래픽을 허용하지 않아야 합니다.
	  • Hs4Ma3G127 - API Gateway REST 및 WebSocket API 실행 로깅을 활성화해야 합니다.
	  • Hs4Ma3G124 - Amazon EC2 인스턴스는 인스턴스
		2025년 1월 28일

메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

- 내결함성
  - c1qf5bt013 - Amazon RDS DB 인스턴스에 스토리지 Auto Scaling이 꺼져 있음
  - 7qGXsKIUw - Classic Load Balancer 연결 드레이닝
  - c18d2gz106 - Amazon EBS가 AWS Backup 플랜에 포함되지 않음
  - c18d2gz107 - AWS Backup계획에 포함되지 않은 Amazon DynamoDB 테이블
  - cc18d2gz117 - Amazon EFS가 AWS Backup플랜에 포함되지 않음
  - c18d2gz105 - Network Load Balancer 교차 로드 밸런싱
  - c1qf5bt026 - Amazon RDS synchronous_commit 파라미터가 꺼져 있음
  - c1qf5bt030 - Amazon RDS innodb_flush_log_at_trx_commit 파라미터가 1이 아님

    - c1qf5bt031 - Amazon RDS sync_binlog 파라미터가 꺼져 있음
    - c1qf5bt036 - Amazon RDS innodb_default_row_format 파라미터 설정이 안전하지 않음
    - c18d2gz144 - Amazon EC2 세부 모니터링이 활성화되지 않음
- 운영 우수성
    - c18d2gz125 - Amazon API Gateway가 실행 로그를 로깅하지 않음
    - c18d2gz168 - 로드 밸런서에 대해 Elastic Load BalancingDeletion 보호가 활성화되지 않음
    - c1qf5bt012 - Amazon RDS 성능 개선 도우미가 꺼져 있음
- 성능
    - c1qf5bt021 - 최적 값보다 작은 값을 사용하는 Amazon RDS innodb_change_buffering 파라미터
    - c1qf5bt025 - Amazon RDS autovacuum 파라미터가 꺼져 있음
    - c1qf5bt028 - Amazon RDS enable_indexonlyscan 파라미터가 꺼져 있음

	• c1qf5bt029 - Amazon RDS enable_indexscan 파라미터가 꺼져 있음 • c1qf5bt032 - Amazon RDS innodb_stats_persistent 파라미터가 꺼져 있음 • c1qf5bt037 - Amazon RDSgeneral_logging 파라미터가 켜져 있음	
업데이트된 리소스 인벤토리 스프레드시트	리소스 인벤토리 스프레드시트가 업데이트되었습니다.	2025년 1월 23일
새로운 AMS 기능: 집계된 셀프 서비스 보고서	집계된 셀프 서비스 보고(SSR)를 사용하면 조직 수준, 교차 계정에서 집계된 기존 셀프 서비스 보고서를 볼 수 있습니다.	2025년 1월 21일
새로운 Accelerate 패치 기능: 패치 후크	이 기능을 사용하여 패치 적용 전후에 운영 체제 수준 명령을 실행하도록 SSM 명령 문서로 "후크"를 구성합니다.	2025년 1월 16일
모니터링 작동 방식 섹션 업데이트	인시던트가 아닌 리소스 또는 인스턴스 ID별로 알림 알림을 구성하여 새 기능에 대한 정보를 추가했습니다.	2025년 1월 8일
EKS 모니터링 및 인시던트 관리의 온보딩 섹션 업데이트	알림 신호가 일시 중지되고 재개되는 시기를 명확히 하기 위해 온보딩 절차 노트를 업데이트했습니다.	2024년 12월 19일
신뢰할 수 있는 수정자에 추가된 멤버 계정 로그	멤버 계정 로그를 사용하여 각 멤버 계정의 계정 ID AWS 리전, 온보딩 및 실행 시간을 찾을 수 있습니다.	2024년 12월 19일

SSM 에이전트 사용을 위한 사전 조건	아웃바운드 트래픽 차단에 대한 콘텐츠가 업데이트됩니다.	2024년 12월 4일
이제 아시아 태평양(홍콩)에서 EKS에 대한 모니터링 및 인시던트 관리 가속화가 지원됩니다. AWS 리전	아시아 태평양(홍콩)은 이제 EKS용 모니터링 및 인시던트 관리 가속화에서 지원됩니다.	2024년 11월 21일
온디맨드 작업 제공 표 업데이트	현재 위치 업그레이드에는 다음 운영 체제가 지원됩니다. • Microsoft Windows 2016에서 Microsoft Windows 2022 이상으로	2024년 11월 11일
이제 EKS에 대한 모니터링 및 인시던트 관리 가속화가 아프리카(케이프타운)에서 지원됩니다 AWS 리전.	이제 EKS용 모니터링 및 인시던트 관리 가속화에서 아프리카(케이프타운) 지원	2024년 11월 4일
온디맨드 작업 제공 표 업데이트	현재 위치 업그레이드에는 다음 운영 체제가 지원됩니다. • Microsoft Windows 2012 R2에서 Microsoft Windows 2016 이상으로 • Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로 • Red Hat Enterprise Linux 8에서 Red Hat Enterprise Linux 9로 • Oracle Linux 7에서 Oracle Linux 8로	2024년 11월 1일
업데이트된 퀵 스타트 템플릿	다이어그램, 템플릿 파라미터 및 yaml 템플릿 파일을 업데이트했습니다.	2024년 10월 28일

Trusted Advisor AMS에서 신뢰할 수 있는 수정자에 추가된 검사	이제 Trusted Remediator에서 다음 Trusted Advisor 검사를 사용할 수 있습니다. • Z4AUBRNSmz - 연결되지 않은 탄력적 IP 주소 • c18d2gz128 - 수명 주기 정책이 구성되지 않은 Amazon ECR 리포지토리 • c18d2gz138 - DynamoDB Point-in-time으로 복구 • Hs4Ma3G323 - DynamoDBtables블에는 삭제 방지 기능이 활성화되어 있어야 합니다. • Hs4Ma3G247 - Amazon EC2 Transit Gateway가 VPC 연결 요청을 자동으로 수락해서는 안 됩니다. • Hs4Ma3G308 - Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. • Hs4Ma3G299 - Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. • Hs4Ma3G306 - Amazon DocumentDB 수동 클러스터 스냅샷은 퍼블릭이 아니어야 합니다. • Hs4Ma3G109 - CloudTrail 로그 파일 검증을 활성화해야 합니다.	2024년 10월 25일

	• Hs4Ma3G217 - CodeBuild 프로젝트 환경에는 로깅 AWS Configuration4가 있어야 합니다. • Hs4Ma3G158 - SSM 문서는 공개되어서는 안 됩니다. • Hs4Ma3G319 - Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.	
지원되는 구성 업데이트	지원되는 Oracle Linux 운영 체제를 9.0-9.3, 8.0-8.9, 7.5-7.9로 업데이트했습니다.	2024년 10월 24일
AMS Accelerate에서 오프보드에 새 섹션 추가	AMS Accelerate에서 오프보드에 추가된 경보 관리자 및 리소스 태거 종속성을 오프보드하는 방법에 대한 지침입니다.	2024년 10월 24일
이제 Resource Tagger 대시보드를 사용할 수 있습니다.	이제 셀프 서비스 보고에서 Resource Tagger 대시보드를 사용할 수 있습니다.	2024년 9월 26일
이제 태그 기반 알림에 여러 이메일 주소를 포함할 수 있습니다.	이제 태그 기반 알림에서 여러 이메일 주소가 지원됩니다.	2024년 9월 20일
이제 AMS Accelerate 제한이 AMS 패치 관리에 포함됩니다.	AMS Accelerate 제한은 패치 관리 - 패치 유지 관리 기간 생성에 포함됩니다.	2024년 8월 30일
AMS Accelerate 계정 검색 업데이트	Amazon EC2 인스턴스 평가를 위해 계정 검색의 새 섹션이 추가되었습니다.	2024년 8월 29일

이제 Ubuntu 운영 체제에서 AMS Accelerate 기본 패치 기준을 사용할 수 있습니다.	이제 Ubuntu 운영 체제에서 AMS Accelerate 기본 패치 기준을 사용할 수 있습니다.	2024년 8월 22일
AMS Accelerate 계정 검색 업데이트	운영 검사 테이블의 AWS CloudTrail 평가 섹션에 4개의 새 AWS API 호출이 추가되었습니다.	2024년 8월 2일
신뢰할 수 있는 수정자가 이제 추가 검사를 지원합니다.	Trusted Remediator는 이제 보안 검사 Hs4Ma3G192를 지원합니다. RDS DB 인스턴스는 퍼블릭 액세스를 금지해야 합니다.	2024년 7월 30일
이제 AMS에서 Amazon Route 53 Resolver DNS 방화벽 지원	이제 AMS에서 Amazon Route 53 Resolver DNS 방화벽 지원	2024년 7월 30일
AMS Accelerate onboarding_role_minimal.zip에 이제 Terraform 코드 포함	이제 AMS Accelerate onboarding_role_minimal.zip에 Terraform 코드가 포함되어 있습니다.	2024년 7월 30일
보안 구성 규칙 대시보드	이제 셀프 서비스 보고에서 보안 구성 규칙 대시보드를 사용할 수 있습니다.	2024년 7월 24일
AMS Accelerate는 이제 Oracle Linux 8.9, RHEL 8.10 및 RHEL 9.4를 지원합니다.	AMS Accelerate는 이제 Oracle Linux 8.9, RHEL 8.10 및 RHEL 9.4를 지원합니다.	2024년 7월 5일
AMS Accelerate 계정 검색 프로세스가 업데이트되었습니다.	AMS Accelerate에 온보딩 AWS 계정 할 때 사용되는 계정 검색 프로세스가 업데이트됩니다.	2024년 7월 1일

이제 신뢰할 수 있는 수정자를 사용할 수 있습니다.	이제 AWS Trusted Advisor 검사 문제 해결을 자동화하는 AWS Managed Services 솔루션인 Trusted Remediator를 사용할 수 있습니다.	2024년 6월 24일
보안 인시던트 대응의 Amazon Route 53 Resolver DNS 방화벽 이벤트.	이제 AMS가 보안 인시던트 대응에서 Amazon Route 53 Resolver DNS 방화벽 이벤트를 모니터링합니다.	2024년 6월 21일
지원되는 운영 체제 업데이트	AMS Accelerate는 이제 AlmaLinux 8.3-8.9, 9.0-9.2를 지원합니다(AlmaLinux는 x86 아키텍처에서만 지원됨).	2024년 6월 19일
이제 기본값이 충족되면 자동 인스턴스 프로파일 제한이 증가합니다.	이제 AMS는 기본 제한인 10에 도달하면 기본 인스턴스 프로파일 제한을 20으로 늘립니다.	2024년 6월 18일
이제 AMS SSM 에이전트 자동 설치 기능이 기본적으로 활성화됩니다.	AMS SSM 에이전트 자동 설치 기능은 6/03/2024 이후에 온보딩된 계정에 대해 기본적으로 활성화됩니다.	2024년 6월 7일
보안 FAQ가 보안 관리에 추가되었습니다.	이제 AMS 운영 엔지니어 또는 자동화가 계정에 액세스할 때 사용되는 보안 모범 사례, 제어, 액세스 모델 및 감사 메커니즘에 대한 일반적인 질문을 다루는 보안 FAQ를 사용할 수 있습니다.	2024년 6월 3일
이제 Amazon EKS용 모니터링 및 인시던트 관리에서 추가 AWS 리전을 지원합니다.	이제 Amazon EKS용 모니터링 및 인시던트 관리에서 세 개의 추가 AWS 리전을 지원합니다.	2024년 5월 23일

이제 패치 유지 관리 기간 전에 서비스 요청 패치 알림이 전송됩니다.	AMS Accelerate 패치 적용은 패치 유지 관리 기간 4일 전에 새 서비스 요청을 생성합니다. 서비스 요청을 사용하여 AMS와 통신하여 패치를 조정하거나 패치를 건너뛸 수 있습니다.	2024년 5월 3일
AMS Accelerate EKS 모니터링 기준 알림 테이블에 추가된 알림 임계값입니다.	이제 Amazon EKS 모니터링을 위한 기준 알림 테이블에서 자세한 알림 임계값을 사용할 수 있습니다.	2024년 5월 3일
업데이트됨: 경보 관리자 구성 프로필.	Alarm Manager를 사용하여 이상 탐지 경보를 생성하는 방법에 대한 참고 사항이 추가되었습니다.	2024년 4월 25일
Resource Tagger 구성 프로필에 추가.	이제 Resource Tagger에서 DynamoDB 테이블 및 Amazon S3 버킷을 사용할 수 있습니다.	2024년 4월 25일
계획된 이벤트 관리(PEM) 정보 섹션이 추가되었습니다.	PEM 서비스 상품에 대한 자세한 내용은 이제 AMS Accelerate 사용 설명서에서 확인할 수 있습니다.	2024년 4월 25일
AMS는 Red Hat Enterpise Linux(RHEL) 9.x를 지원합니다.	AMS는 Red Hat Enterprise Linux(RHEL) 9.x를 지원합니다.	2024년 4월 25일
AMS Accelerate는 모든 AWS 리전 구성에 대한 보고를 지원합니다.	AMS Accelerate는 모든 AWS 리전 구성에 대해 SSM 인벤토리 보고를 지원합니다.	2024년 4월 25일
업데이트됨: AWS 관리형 정책.	AWSManagedServices DeploymentToolkitPolicy를 새 ECR 권한으로 업데이트했습니다.	2024년 4월 4일

업데이트됨: 리소스 태거 구성 프로필 섹션	ResourceType 목록에 `AWS::EFS::FileSystem` 가 추가되었습니다.	2024년 3월 21일
업데이트됨: Accelerate 섹션의 인시던트 보고서 및 서비스 요청.	Accelerate에서 주제 제목을 인시던트 보고서, 서비스 요청 및 결제 질문으로 변경했습니다. 새로운 섹션인 결제 질문을 추가했습니다.	2024년 3월 21일
업데이트됨: 서비스 요청 관리 작동 방식 섹션.	AMS가 기능 요청 또는 버그가 포함된 서비스 요청을 처리하는 방법에 대한 설명을 추가했습니다.	2024년 3월 21일
업데이트됨: CloudFormation 섹션을 사용하여 aws_managedservices_onboarding_role 역할 생성	역할을 생성하는 명령을 추가했습니다 AWS CloudShell.	2024년 3월 21일
업데이트됨: (선택 사항) 빠른 시작 템플릿	템플릿을 다운로드하는 명령을 추가했습니다 AWS CloudShell.	2024년 3월 21일
경보 관리자 구성 프로필에 사용할 수 있는 새 리소스 유형입니다.	경보 관리자 구성 프로필에 Amazon FSx, Amazon EFS 및 Elasticsearch에 대한 리소스 유형이 추가되었습니다.	2024년 3월 21일
구성 프로필에 사용할 수 있는 추가 가상 파라미터 대체입니다.	Amazon EFS 및 Amazon FSx 가상 파라미터 대체가 추가되었습니다.	2024년 3월 21일
서비스 설명 주제의 기능에 새 섹션을 추가했습니다.	AMS Accelerate 기능에 새 섹션인 서비스 요청 관리를 추가했습니다.	2024년 3월 21일

셀프 서비스 보고 주간 인시던트 보고서에 추가된 새 열	인시던트가 생성되거나 해결된 분기, 월, 주 또는 날짜를 기준으로 인시던트를 필터링할 수 있도록 주간 인시던트 보고서에 새 열이 추가되었습니다.	2024년 3월 11일

이전 업데이트

다음 표에서는 2024년 3월 이전의 AMS Accelerate 가이드 설명서에 대한 중요한 변경 사항을 설명합니다.

변경	설명	Date
AMS Accelerate CloudTrail 추적 온보딩 개선 사항	AMS Accelerate CloudTrail 추적 온보딩 개선 사항: • 모든 버킷 정책을 단일 블록으로 수집 • 정책 설명에서 두 번째 AWS 조직 ID 제거 • 고객 환경 요구 사항 명확히 설명 자세한 내용은 구성을 검토하고 업데이트하여 AMS Accelerate가 CloudTrail 추적을 사용할 수 있도록 합니다. 단원을 참조하십시오.	2024년 2월 23일
업데이트됨: 계정 온보딩 프로세스.	단계를 더 명확하게 하기 위해 계정 온보딩 프로세스 섹션을 재구성했습니다. 또한 온보딩 기능을 위한 선택적 Quick Start 템플릿을 추가했습니다. (선택 사항) Accelerate의 빠른 시작 템플릿을(를) 참조하세요.	2024년 2월 22일
업데이트됨: AMS Accelerate 오프보딩.	`ams-access-management` CloudFormation 스택 및 `ams-access-management` IAM 역할이 오프보딩 프로세스에 의해 삭제되	2024년 2월 22일

변경	설명	Date
	지 않음을 나타내도록 AMS Accelerate 오프보딩 고려 사항 섹션을 업데이트했습니다. AMS Accelerate 오프보딩 효과을(를) 참조하세요.	
업데이트됨: Accelerate의 구성 규정 준수.	이러한 용어가 혼동되지 않도록 '인시던트 보고서'를 '서비스 요청'으로 변경했습니다. Accelerate의 구성 규정 준수을(를) 참조하세요.	2024년 2월 22일
업데이트됨: Accelerate의 계정 검색.	Accelerate의 계정 검색을 재구성하여 관련 섹션으로 사전 조건을 더 잘 그룹화했습니다. 1단계. Accelerate의 계정 검색을(를) 참조하세요.	2024년 2월 22일
이름이 변경됨: AMS 호스트 관리로 AMS 패치 보고.	AMS 호스트 관리로 AMS 패치 보고의 이름을 바꾸고 보고서인 패치 세부 정보 보고서의 이름을 SSM 에이전트 담당률 보고서로 바꿨습니다. AMS 호스트 관리 보고서을(를) 참조하세요.	2024년 2월 22일
업데이트된 온디맨드 작업 카탈로그	에서 "상태"에 대한 참조를 제거하도록 오퍼링 테이블의 온디맨드 작업 카탈로그를 업데이트했습니다`Amazon EKS cluster maintenance .` 온디맨드 AMS 작업 요청을(를) 참조하세요.	2024년 2월 22일
업데이트된 AMS 이벤트 라우터	AMS 이벤트 라우터 섹션에서 `AMSCoreRule` 를 업데이트했습니다. AMS에서 Amazon EventBridge 관리형 규칙 사용을(를) 참조하세요.	2024년 2월 22일

변경	설명	Date
지원되는 운영 체제를 업데이트했습니다.	SUSE Linux Enterprise Server 15 SP5를 포함하도록 지원되는 운영 체제를 업데이트했습니다. 지원되는 구성을(를) 참조하세요.	2024년 2월 22일
EC2 볼륨 사용량 수정 자동화 업데이트	EC2 볼륨 사용량 수정 자동화 섹션을 올바른 용량 확장 일정으로 업데이트했습니다. EC2 볼륨 사용량 수정 자동화을(를) 참조하세요.	2024년 2월 22일
업데이트됨: 구성을 검토하고 업데이트하여 Accelerate가 CloudTrail 추적을 사용할 수 있도록 합니다.	AMS Accelerate Organization CloudTrail S3 버킷 정책 섹션을 업데이트했습니다. 구성을 검토하고 업데이트하여 AMS Accelerate가 CloudTrail 추적을 사용할 수 있도록 합니다. 섹션을 참조하세요	2024년 2월 15일
새로운 기능 추가: SSM 에이전트 자동 설치	SSM 에이전트 자동 설치에 대한 새 섹션 추가 SSM 에이전트 자동 설치을(를) 참조하세요.	2024년 1월 26일
업데이트됨: 지원되는 구성	지원되는 버전에 대한 정보 추가 AWS Control Tower 지원되는 구성을(를) 참조하세요.	2024년 1월 26일
업데이트됨: AMS 패치 보고.	AMS 패치 보고에서 다음 세 섹션을 제거했습니다. • 패치 인스턴스 세부 정보 요약 보고서 • 패치 세부 정보 보고서 • 누락된 패치가 보고하는 인스턴스 AMS 호스트 관리 보고서을(를) 참조하세요.	2023년 12월 22일

변경	설명	Date
업데이트됨: 온보딩 사전 조건을 가속화합니다.	AMS Accelerate 온보딩에 필요한 지원 계획을 업데이트했습니다. 온보딩 사전 조건 가속화을(를) 참조하세요.	2023년 12월 15일
업데이트됨: 패치 유지 관리 창을 생성합니다.	이 기능은 더 이상 사용되지 않으므로 기본 패치 주기 섹션을 제거했습니다. AMS에서 패치 유지 관리 기간 생성을(를) 참조하세요.	2023년 12월 13일
업데이트됨: Accelerate의 알림 설정.	알림에 사용되는 이메일을 명확히 했습니다. 자세한 정보는 Accelerate의 알림 설정을 참조하세요.	2023년 12월 12일
업데이트됨: `AMSAccelerateCustomerAccessPolicies` 템플릿.	구문 오류를 수정하도록 `AMSAccelerateCustomerAccessPolicies` 템플릿을 업데이트했습니다. 자세한 정보는 AMS 기능을 사용할 수 있는 권한을 참조하세요.	2023년 12월 12일
추가됨: 변경 요청 보안 검토	보안 관리 아래에 변경 요청 보안 검토 섹션을 새로 추가했습니다. 자세한 정보는 변경 요청 보안 검토을 참조하세요.	2023년 12월 11일
업데이트: resource_inventory.xlsx	보안 분석가 역할을 포함하도록 resource_inventory.xlsx를 업데이트했습니다. 자세한 정보는 Accelerate의 리소스 인벤토리을 참조하세요.	2023년 11월 17일

변경	설명	Date
업데이트됨: ams-access-admin-operations 역할 설명	ams-access-admin-operations 설명이 업데이트되었습니다. 자세한 내용은 AMS가 계정에 액세스하는 이유와 시간 및 AMS Accelerate에서 자격 증명으로 인증 섹션을 참조하세요.	2023년 11월 17일
업데이트됨: AMS Accelerate 오프보딩 고려 사항	오프보딩 후 Amazon GuardDuty 및 AWS Config 규칙에서 사용할 수 있는 항목을 명확히 하기 위해 보안 섹션을 업데이트했습니다. 자세한 정보는 AMS Accelerate 오프보딩 효과을 참조하세요.	2023년 11월 17일
추가됨: Amazon EKS에 대한 모니터링 및 인시던트 관리	Amazon EKS용 모니터링 및 인시던트 관리는 Amazon EKS 리소스에서 장애, 성능 저하 및 보안 문제를 모니터링합니다. 자세한 정보는 AMS Accelerate에서 Amazon EKS 모니터링 및 인시던트 관리을 참조하세요.	2023년 11월 14일
업데이트됨: 태그 지정	고객 제공 태그 지정에 대한 정보가 추가되었습니다. 자세한 정보는 Accelerate의 고객 제공 태그을 참조하세요.	2023년 11월 7일
업데이트됨: 리소스 태거 구성 프로필	AWS::AutoScaling::AutoScalingGroup, AWS::EKS::Cluster, AWS::Elasticsearch ::Domain 및 AWS::FSx::FileSystem을 필터 섹션에 추가했습니다. 자세한 정보는 AMS Accelerate의 리소스 태거 구성 프로파일을 참조하세요.	2023년 10월 27일
업데이트됨: 서비스 설명	지원되는 운영 체제에 Ubuntu 22.04가 추가되었습니다. 서비스 설명 섹션을 참조하세요	2023년 9월 29일

변경	설명	Date
업데이트됨: AMS Accelerate 온보딩 사전 조건	CloudFormation 템플릿을 포함하도록 AMS Accelerate VPC 엔드포인트에 메모를 추가했습니다. 온보딩 사전 조건 가속화을(를) 참조하세요.	2023년 9월 29일
업데이트됨: 감지	AMS Accelerate 보안 응답에서 엔드포인트 보호 유형을 제거했습니다. 감지을(를) 참조하세요.	2023년 9월 29일
업데이트됨: AMS의 기준 모니터링에서 알림	기준 모니터링의 알림 테이블에 AWS Outposts가 추가되었습니다. 감지 monitoring-default-metrics 참조하세요.	2023년 9월 29일
업데이트됨:를 사용하여 aws_managedservices_onboarding_role 역할 생성 CloudFormation	스택 세부 정보 지정에 대한 스크린샷이 업데이트되었습니다. 가속화 CloudFormation 를 위해 `aws_managedservices_onboarding_role` 를 사용하여 생성을(를) 참조하세요.	2023년 9월 29일
업데이트됨: AMS Accelerate에서 배포한 Amazon EventBridge 관리형 규칙	새 AMS Accelerate Amazon EventBridge 관리형 규칙 AMSCoreRule이 추가되었습니다. AMS Accelerate Amazon EventBridge 관리형 규칙 AMSAccessRolesRule을 업데이트하여 새 역할을 추가했습니다. 자세한 정보는 AMS에서 배포한 Amazon EventBridge 관리형 규칙을 참조하세요.	2023년 9월 19일
업데이트됨: 경보 관리자 구성 프로필	AWS Outposts 가상 파라미터 대체 식별자가 추가되었습니다. AMS Accelerate의 모니터링 및 이벤트 관리을(를) 참조하세요.	2023년 9월 11일
업데이트됨: 리소스 태거 구성 프로필	AWS Outposts 리소스 유형이 추가되었습니다. 구성 프로파일 가속화: 가상 파라미터 대체을(를) 참조하세요.	2023년 9월 11일

변경	설명	Date
업데이트됨: 지원되는 서비스	CloudWatch 경보로 모니터링하는 서비스 섹션에 Amazon Elastic File System을 추가했습니다. 자세한 정보는 서비스 설명을 참조하세요.	2023년 9월 6일
업데이트됨: 패치 모니터링 및 장애 해결	패치 오케스트레이터 사용 섹션에 다음 참고 사항이 추가되었습니다. “운영 체제가 지원되지 않거나 유지 관리 기간 동안 중지된 인스턴스에 대해서는 패치 실패 알림이 생성되지 않습니다.” 자세한 정보는 AMS Accelerate의 패치 관리 이해을 참조하세요.	2023년 9월 6일
업데이트됨: 맬웨어 이벤트에 대한 응답 런북을 명확히 함	보안 인시던트 대응을 위한 맬웨어 이벤트에 대한 대응 런북을 명확히 했습니다. 자세한 정보는 AMS의 보안 인시던트 대응을 참조하세요.	2023년 9월 6일
업데이트됨: Transit Gateway에 Accelerate 계정 연결	새 Accelerate 계정 VPC를 AMS 다중 계정 랜딩 존 네트워크에 연결(TGW VPC 연결 생성)하는 단계를 명확히 했습니다. 자세한 내용은 Accelerate 계정 withTransit Gateway 연결을 참조하세요.	2023년 9월 5일
업데이트됨: AMS의 기준 모니터링에서 알림	더 이상 사용되지 않는 두 경보 AMSReadLatencyAlarm 및 AMSWriteLatencyAlarm에 대한 참조를 제거했습니다. 자세한 정보는 AMS의 기준 모니터링 알림을 참조하세요.	2023년 9월 5일
추가됨: AMS 이벤트 라우터	AMS 이벤트 라우터에 대한 설명서가 추가되었습니다. 자세한 내용은 섹션을 참조AMS에서 Amazon EventBridge 관리형 규칙 사용하세요.	2023년 9월 5일

변경	설명	Date
업데이트됨: Alarm Manager 가상 파라미터 목록입니다.	경보 관리자 가상 파라미터 목록을 업데이트했습니다. EC2 인스턴스 이름 파라미터가 EC2 인스턴스 및 EC2 디스크 경보 구성에 추가되었습니다. 자세한 정보는 구성 프로파일 가속화: 가상 파라미터 대체을 참조하세요.	2023년 8월 29일
추가됨: AMS 액세스 오프보딩	AMS 액세스 오프보딩 시 고려 사항이 추가되었습니다. AMS Accelerate 오프보딩 효과을(를) 참조하세요.	2023년 8월 24일
추가됨: AMS 보안 인시던트 대응	AMS 보안 인시던트 대응 사용에 대한 설명서가 추가되었습니다. AMS의 보안 인시던트 대응을(를) 참조하세요.	2023년 8월 18일
업데이트됨: AMS Accelerate 액세스 역할	역할 이름의 오타를 수정했습니다. AWS Identity and Access Management AMS Accelerate의을(를) 참조하세요.	2023년 8월 10일
업데이트됨: 정책 설명	하드코딩된 역할 이름을 와일드카드로 대체했습니다. 구성을 검토하고 업데이트하여 AMS Accelerate가 CloudTrail 추적을 사용할 수 있도록 합니다.을(를) 참조하세요.	2023년 8월 10일
업데이트됨: EFS 알림이 포함된 모니터링된 서비스 목록입니다.	AMS 기준 모니터링을 위한 새로운 EFS 알림으로 모니터링 서비스 목록을 업데이트했습니다. 4개의 새로운 EFS 알림 유형이 추가되었습니다. 자세한 정보는 AMS의 기준 모니터링 알림을 참조하세요.	2023년 8월 3일
업데이트됨: 리소스 인벤토리 테이블 가속화	ams-backup-config-rule-stack 및 관련 리소스를 제거했습니다. Accelerate의 리소스 인벤토리을(를) 참조하세요.	2023년 7월 18일

변경	설명	Date
업데이트됨: AMS Accelerate 액세스 역할	ams-backup-config-rule-st-amsBackupAlertConfigRule-<8자리 해시> 및 ams-backup-config-rule-st-amsBackupPlanConfigRuleH-<8자리 해시> 역할을 제거했습니다. AWS Identity and Access Management AMS Accelerate의을(를) 참조하세요.	2023년 7월 18일
업데이트됨: 모니터링되는 RDS 알림 목록입니다.	AMS 기준 모니터링을 위한 RDS 알림 목록을 업데이트했습니다. 새로운 RDS 알림 유형 9개가 추가되었고 기존 RDS 알림 유형 3개가 제거되었습니다. 자세한 정보는 AMS의 기준 모니터링 알림을 참조하세요.	2023년 6월 19일
신규: AMS Accelerate 액세스 역할	AMS 보안에 대한 새 액세스 역할이 추가되었습니다.	2023년 6월 16일
신규: 이제 AMS Accelerate CloudTrail 로그 관리에서 고객 CloudTrail 추적을 사용할 수 있습니다.	배포된 추적 가속화 또는 고객 관리형 CloudTrail 계정 또는 조직 추적과의 통합을 포함하여 CloudTrail 로그 관리에 지원되는 가속화 옵션을 업데이트했습니다. 자세한 정보는 구성을 검토하고 업데이트하여 AMS Accelerate가 CloudTrail 추적을 사용할 수 있도록 합니다.을 참조하세요.	2023년 6월 9일
업데이트됨: AMS Accelerate Config 규칙 응답 구성 보고서.	AWS Config 규칙 응답 구성 보고서에 대한 요청 시 보고를 업데이트했습니다. 요청 시 보고에 대한 업데이트 가속화를 참조하세요. AMS Config 규칙 응답 구성 보고서을(를) 참조하세요.	2023년 5월 26일
업데이트됨: 서비스 결제 시작일 정책.	에서 결제 시작일에 대한 정의를 업데이트했습니다AMS 키 용어.	2023년 5월 15일

변경	설명	Date
업데이트: AWS 관리형 정책.	AWSManagedServicesDeploymentToolkitPolicy를 새 CFN 및 ECR 권한으로 업데이트하고 와일드카드를 사용하여 기존 작업의 범위를 좁혔습니다. 서비스 연결 역할에 대한 업데이트 가속화를 참조하세요. 서비스 연결 역할에 대한 업데이트 가속화을(를) 참조하세요.	2023년 5월 9일
업데이트됨: 역할 정책 링크에 액세스합니다.	이제 Accelerate S3 버킷 위치에서 직접 액세스 역할을 다운로드할 수 있습니다. AMS가 계정에 액세스하는 이유와 시간 및 AWS Identity and Access Management AMS Accelerate의 섹션을 참조하세요.	
업데이트됨: 월별 결제 셀프 서비스 보고서.	참고 추가: 월별 결제 보고서는 Management Payer 계정(AMS Advanced 다중 계정 랜딩 존)에서만 사용할 수 있지만 연결된 모든 AMS Accelerate 관리 계정에서 사용할 수 있습니다. 결제 보고서(월별)을(를) 참조하세요.	2023년 4월 13일
업데이트됨: 알림 목록.	CloudTrail 참조를 제거했습니다. AMS Accelerate에서의 로그 관리을(를) 참조하세요.	2023년 4월 13일
업데이트됨: 알림 목록.	3개의 새 SSM 에이전트 알림이 추가되었습니다. AMS의 기준 모니터링 알림을(를) 참조하세요.	2023년 4월 13일
업데이트됨: 사전 조건 가속화.	Accelerate는 4개의 AWS Support 플랜 중 하나가 있어야 하며 개발자 플랜은 제외됨을 명확히 했습니다. 온보딩 사전 조건 가속화을(를) 참조하세요.	2023년 4월 13일

변경	설명	Date
업데이트됨: 서비스 연결 역할 정책 가속화.	Contacts Service 정책 zip 파일이 업데이트되었습니다. AWS AMS Accelerate에 대한 관리형 정책을(를) 참조하세요.	2023년 4월 13일
업데이트됨: AMS Resource Scheduler.	잘못된 역할 이름인 AWSManagedServices-DescribeScheduleOrPeriod가 AWSManagedServices-DescribeScheduleOrPeriods로 수정되었습니다. AMS Resource Scheduler를 사용한 비용 최적화을(를) 참조하세요.	2023년 4월 13일
업데이트: AWS 관리형 정책.	단일 또는 여러 계정에서 사용자 지정 응답을 업데이트하기 위한 지침사용자 지정 조사 결과 응답으로 업데이트되었습니다.	2023년 4월 13일
업데이트됨: Resource Tagger	실수로 동일한 이름으로 AMS 관리형 구성을 재정의할 수 있으므로 "새 구성의 이름 지정(제공된 예제의 SampleConfigurationBlock)"에 대한 경고가 추가되었습니다. AMS Accelerate의 Resource Tagger 사용 사례을(를) 참조하세요.	2023년 3월 16일
업데이트됨: 패치 RACI	패치 적용을 위한 RACI에 대한 몇 가지 업데이트 및 설명입니다. 서비스 설명을(를) 참조하세요.	2023년 3월 16일
업데이트됨: 배포 툴킷 SLR JSON의 작업	정책 및 작업이 업데이트되었습니다. 참조: AMS Accelerate에 서비스 연결 역할 사용.	2023년 3월 16일
업데이트됨: 자동 문제 해결	EC2 볼륨 자동화에 대한 LVM 지원이 제거되었습니다. 참조: 알림의 AMS 자동 문제 해결.	2023년 3월 16일
업데이트됨: 온보딩 가속화.	역할, 특히 최소 역할 사용을 명확히 했습니다AMS 역할을 생성하기 위한 템플릿.	2023년 3월 16일

변경	설명	Date
업데이트됨: 셀프 서비스 보고.	일일 백업 보고서는 이제 기본 및 보조 리전을 지원합니다. 둘 다의 리소스 리전 필드에 보고됩니다백업 보고서(일별).	2023년 3월 16일
업데이트됨: 패치 지침	AMS에서 관리하는 기본 패치 기준을 사용자 지정하지 않도록 경고가 추가되었습니다. 대신 새 사용자 지정 패치 기준을 생성합니다. 기본 패치 기준 및 단원을 참조하십시오AMS Accelerate를 사용한 사용자 지정 패치 기준.	2023년 3월 16일
서비스 종료 정책이 업데이트되었습니다.	에서 서비스 종료 및 서비스 종료 날짜의 정의를 업데이트했습니다AMS 키 용어. 해지 신청은 지난 달 20일 이전에 발행되어야 합니다.	2023년 3월 16일
업데이트: AWS 관리형 정책.	정책 이름을 명확히 함: AMS Accelerate의 서비스 연결 역할에 문의.	2023년 2월 16일
New: AWS managed 정책.	정책 추가: AMS Accelerate의 서비스 연결 역할에 문의.	2023년 2월 16일
업데이트됨: 구성 규정 준수.	에서 철자가 잘못된 단어를 수정했습니다Accelerate의 구성 규정 준수.	2023년 2월 16일
새 콘텐츠: 지원되지 않는 OSes	AMS가 지원되지 않는 운영 체제(OSes)에 제공하는 서비스에 대한 정보가 추가되었습니다. 섹션을 참조하세요Accelerate에서 지원되지 않는 운영 체제의 기능.	2023년 2월 16일
업데이트됨: 패치 창 생성	CloudShell 사용에 대한 링크를에 추가했습니다AMS Accelerate용 Systems Manager 명령줄 인터페이스(CLI)를 사용하여 유지 관리 기간 생성.	2023년 2월 16일
업데이트된 콘텐츠: 온보딩 관리 리소스	에서 압축된 JSON 템플릿을 업데이트했습니다AMS 역할을 생성하기 위한 템플릿.	2023년 2월 16일

변경	설명	Date
새 콘텐츠: 구성 규정 준수	새 주제 추가: 사용자 지정 조사 결과 응답.	2023년 2월 16일
New: AWS managed 정책.	정책 추가: AMS Accelerate에 대한 Amazon EventBridge 규칙 서비스 연결 역할.	2023년 2월 7일
업데이트: AWS 관리형 정책.	새 S3 권한`AWSManagedServices DeploymentToolkitPolicy` 으로를 업데이트했습니다. 서비스 연결 역할에 대한 업데이트 가속화을(를) 참조하세요.	2023년 1월 30일
새로운 옵트인 리전: CPT.	이제 Capetown(CPT) 옵트인 리전에서 AMS Accelerate를 사용할 수 있습니다. 옵트인하려면 관리를 AWS 리전 참조하세요.	2023년 1월 12일
업데이트됨: 서비스 설명.	CloudWatch 경보로 모니터링되는 FSx 서비스를에 추가했습니다서비스 설명.	2023년 1월 12일
업데이트됨: 기본 지표 모니터링.	에 FSx 경보 6개를 추가했습니다AMS의 기준 모니터링 알림.	2023년 1월 12일
업데이트됨: AMS 패턴.	에 Cloudwatch 경보 알림 사용자 지정을 추가했습니다AMS 패턴.	2023년 1월 12일
업데이트됨: 관리 리소스 온보딩.	에서에 대한 행을 추가하여 템플릿 테이블`ams-onboarding-ssm-execution-role` 을 업데이트했습니다AMS 역할을 생성하기 위한 템플릿.	2023년 1월 12일
업데이트됨: 구성 규정 준수.	에서 사용자 지정 문제 해결 요청(중요 상자)에 대한 추가 세부 정보입니다Accelerate의 구성 규정 준수.	2023년 1월 12일
업데이트됨: Service-linked-role 권한.	이전 또는 중복 권한을 제거했습니다. AMS Accelerate에 서비스 연결 역할 사용을(를) 참조하세요.	2022년 12월 15일

변경	설명	Date
업데이트됨: 패치 관리, 유지 관리 기간.	콘솔 지침, 5단계, 유지 관리 기간 생성에 대한 지침을 추가했습니다. AMS Accelerate용 Systems Manager 콘솔에서 유지 관리 기간 생성을(를) 참조하세요.	2022년 12월 15일
신규: 패치 관리 섹션.	패치 화요일 유지 관리 기간에 대한 섹션을 추가했습니다. AMS 콘솔에서 반복되는 “화요일 패치” 유지 관리 기간 생성(권장)을(를) 참조하세요.	2022년 12월 15일
업데이트됨: AMS Resource Scheduler.	CloudFormation 스택 이름을 업데이트했습니다. AMS Resource Scheduler에서 리소스 사용을(를) 참조하세요.	2022년 12월 15일
업데이트됨: 백업을 위해 리소스에 태그를 지정합니다.	AMS Resource Tagger 사용에 대한 지침이 추가되었습니다. 리소스에 태그를 지정하여 AMS 백업 계획 적용을(를) 참조하세요.	2022년 12월 15일
업데이트됨: 백업 계획을 선택합니다.	연속 백업을 제공하는 계획을 나타냅니다. AMS 백업 계획 선택을(를) 참조하세요.	2022년 12월 15일
업데이트됨: AMS Resource Scheduler.	기간 또는 일정을 삭제하기 위한 AWS CLI 예제를 업데이트했습니다. AWS Managed Services Resource Scheduler에서 기간 및 일정 작업을(를) 참조하세요.	2022년 12월 15일
업데이트: AWS 관리형 정책.	를 추가했습니다`AWSManagedServices DeploymentToolkitPolicy` . AWS AMS Accelerate에 대한 관리형 정책을(를) 참조하세요.	2022년 12월 15일
신규: AMS 새 서비스 연결 역할인 AWSServiceRoleForManagedServices_DetectiveControlsConfig를 설명하는 섹션이 추가되었습니다.	GovCloud 리전 및 권한이 추가되었습니다. Detective는 AMS Accelerate의 서비스 연결 역할을 제어합니다.을(를) 참조하세요.	2022년 12월 15일

변경	설명	Date
신규: AWS관리형 정책	AWS관리형 정책인 AWSManagedServices_AlarmManagerPermissionsBoundary를 서비스 연결 역할 정책인 AWSManagedServices_AlarmManager_ServiceRolePolicy에서 사용하여 서비스 연결 역할인 AWSServiceRoleForManagedServices_AlarmManager에서 생성된 IAM 역할의 권한을 제한하는 방법을 설명하는 섹션이 추가되었습니다. AWS AMS Accelerate에 대한 관리형 정책을(를) 참조하세요.	2022년 12월 15일
업데이트됨: 온디맨드 작업.	추가된 제품: EC2 작업의 SQL Server 및 AMI 구축 및 판매. 온디맨드 작업을(를) 참조하세요.	2022년 11월 10일
업데이트됨: 모니터링 및 이벤트 관리.	서비스 알림 및 인시던트 보고서에 대한 설명을 업데이트했습니다. 모니터링 작동 방식을(를) 참조하세요.	2022년 11월 10일
업데이트됨: 서비스 연결 역할 리전	GovCloud 리전 및 권한이 추가되었습니다. AMS Accelerate에 서비스 연결 역할 사용을(를) 참조하세요.	2022년 11월 10일
신규: 서비스 연결 역할입니다.	새 역할 추가: `AWSServiceRoleForAMSDetectiveControls` . Detective는 AMS Accelerate의 서비스 연결 역할을 제어합니다.을(를) 참조하세요.	2022년 11월 10일
업데이트됨: 액세스 관리.	개선된 지침으로 하위 섹션을 업데이트했습니다. AMS Accelerate의 액세스 관리을(를) 참조하세요.	2022년 11월 10일
업데이트됨: 서비스 설명.	RACI 매트릭스에서 AMS 패턴을 업데이트했습니다. 서비스 설명을(를) 참조하세요.	2022년 11월 10일
업데이트됨: AMS 패턴.	고객은 패턴 배포에 대한 책임이 있습니다. AMS 패턴을(를) 참조하세요.	2022년 11월 10일

변경	설명	Date
업데이트됨: 오프보딩.	오프보딩 중에 특정 백업 및 모니터링 리소스에 발생하는 상황에 대한 세부 정보가 추가되었습니다. AMS Accelerate에서 오프보드을(를) 참조하세요.	2022년 11월 10일
업데이트됨: 패치 관리.	IAM 정책에 대한 지침을 업데이트하고 단축했습니다. AMS Accelerate의 온디맨드 패치를 위한 IAM 역할 생성을(를) 참조하세요.	2022년 11월 10일
신규: 아키텍처 다이어그램에 대한 링크입니다.	AMS 참조 아키텍처 다이어그램에 대한 링크를 다양한 주제에 추가했습니다. 예제는 AMS Accelerate의 모니터링 및 이벤트 관리을 참조하세요.	2022년 11월 10일
신규: 온디맨드 작업 제공	"랜딩 존 액셀러레이터 작업"이 추가되었습니다. 온디맨드 작업을(를) 참조하세요.	2022년 10월 13일
업데이트: 관리 모니터링. 알림은 서비스 요청이 아닌 인시던트 보고서를 생성합니다.	모니터링 작동 방식.	2022년 10월 13일
신규: Accelerate-custom CFN 템플릿을 사용하여 패치 유지 관리 기간 생성	CloudFormation 패치 창 구성 템플릿. AMS에서 패치 유지 관리 기간 생성을(를) 참조하세요.	2022년 9월 15일
업데이트됨: 오프보딩	Accelerate의 백업 계획은 오프보딩 후 더 이상 작동하지 않는다는 점을 강조했습니다. AMS Accelerate에서 오프보드을(를) 참조하세요.	2022년 9월 15일
업데이트됨: CloudWatch 구성 변경 세부 정보	Windows 및 Linux 예제에서 실수를 수정했습니다. CloudWatch 구성 변경 세부 정보을(를) 참조하세요.	2022년 9월 15일
업데이트됨: AMS Resource Scheduler 사용	비용 할당 태그에 대한 지침이 추가되었습니다. AMS Resource Scheduler의 비용 예측기을(를) 참조하세요.	2022년 9월 15일

변경	설명	Date
업데이트됨: AMS Config 규칙 라이브러리	규칙 테이블에 `ams-eks-` 두 가지 구성 규칙이 추가되었습니다. AMS Config 규칙 라이브러리을(를) 참조하세요.	2022년 9월 15일
업데이트됨: 백업 관리	백업 계획 제목 및 설명에서 잘못된 레이블 PITR(point-in-time-recovery)을 제거했습니다. AMS 백업 계획 선택을(를) 참조하세요.	2022년 9월 15일
업데이트됨: Accelerate Service 설명	구성 규칙 및 카나리아에 대한 설명을 업데이트했습니다. 서비스 설명을(를) 참조하세요.	2022년 9월 15일
업데이트됨: 서비스 설명, 지원되는 구성	Windows 2008 R2의 end-of-service 날짜가 제거되었습니다. Accelerate는 Windows 2008을 지원하지 않습니다. 지원되는 구성을(를) 참조하세요.	2022년 8월 11일
업데이트됨: 서비스 설명, 역할 및 책임	RACI 테이블을 업데이트했습니다. 네트워킹 섹션의 마지막 행에서 ELB 액세스 로그를 제거했습니다. Accelerate 고객에 대해서는 ELB 액세스 로그를 활성화하지 않습니다. 역할 및 책임을(를) 참조하세요.	2022년 8월 11일
업데이트됨: 구성 규정 준수	규칙 테이블, 프레임워크 열의 오타를 수정했습니다. NIST-CSF가 NIST-CIS로 잘못 나열되었습니다. Accelerate의 구성 규정 준수을(를) 참조하세요.	2022년 8월 11일
신규: 오프보딩 가속화	오프보딩을 위한 고려 사항 및 프로세스입니다. Offboarding AMS Accelerate를 참조하세요.	2022년 8월 11일
업데이트됨: 사전 설치된 SSM 에이전트의 운영 체제 목록	목록에 "Ubuntu Linux 18.04 및 20.04"가 추가되었습니다. 가속화할 EC2 인스턴스 온보딩을(를) 참조하세요.	2022년 8월 11일

변경	설명	Date
신규: Resource Scheduler	AMS Resource Scheduler를 사용하면 필요에 따라 리소스만 중지하고 시작하여 비용을 최적화할 수 있습니다. AMS Resource Scheduler를 사용한 비용 최적화을(를) 참조하세요.	2022년 7월 14일
업데이트됨: Resource Scheduler에 대한 서비스 설명	새로운 Resource Scheduler 제품에 대한 서비스 설명의 여러 섹션이 업데이트되었습니다. 서비스 설명을(를) 참조하세요.	2022년 7월 14일
신규: AMS 패턴	AMS는 AMS 관리형 환경의 사용 사례 패밀리를 해결하는 일반화된 솔루션인 패턴 템플릿을 제공합니다. 첫 번째 제공 패턴: AMS 패턴.	2022년 7월 14일
신규: 비용 최적화 참고 사항	리소스 사용에 따라 비용이 어떻게 증가할 수 있는지 설명하는 참고 사항이 추가되었습니다. Accelerate의 리소스 인벤토리을(를) 참조하세요.	2022년 7월 14일
업데이트됨: AMS Config 규칙	에서 테이블을 재구성했습니다AMS Config 규칙 라이브러리. HTML 테이블의 열 수가 적기 때문에 한 눈에 더 쉽게 읽을 수 있습니다. 다운로드 가능한 스프레드시트에는 정렬 및 필터링을 허용하는 추가 열이 있습니다.	2022년 7월 14일
업데이트됨: 액세스 관리	에서 샘플 CloudFormation 템플릿을 업데이트했습니다AMS 기능을 사용할 수 있는 권한. 이제 `AMSAccelerateAdminAccess` 정책에 `AmsResourceSchedulerPassRolePolicy` 및 `IAMReadOnlyPolicy` 정책이 포함됩니다.	2022년 7월 14일
업데이트됨: 셀프 서비스 보고	KMS 키로 AWS Glue 메타데이터를 암호화하기 위한 지침이 추가되었습니다. 에서 중요로 레이블이 지정된 상자를 참조하세요셀프 서비스 보고서.	2022년 7월 14일

변경	설명	Date
업데이트됨: AMS 기준 모니터링	DeleteRecoveryPoint 백업 알림이 추가되었습니다. AMS의 기준 모니터링 알림	2022년 7월 14일
업데이트됨: 지원되는 운영 체제	Amazon Linux 2에 대한 지원 종료 날짜가 추가되었습니다. 서비스 설명	2022년 7월 14일
업데이트됨: AMS 보고	옵트인 리전에 대한 참고 사항이 추가되었습니다. 보고서 및 옵션	2022년 7월 14일
리소스 스케줄러	리소스 중지 및 시작 시간을 예약하여 비용 최적화를 지원하는 AMS Resource Scheduler 온보딩 및 사용에 대한 정보가 추가되었습니다. 또한 Resource Scheduler에 대한 언급을 포함하도록 Accelerate 서비스 설명을 업데이트했습니다. 또한는 Amazon Linux 2 지원 지원 종료일을 2024년으로 업데이트했습니다. AMS Resource Scheduler를 사용한 비용 최적화 및 서비스 설명를 참조하세요.	2022년 6월 30일
새 경보	AWS Backup 경보를 추가했습니다. AMS의 기준 모니터링 알림	2022년 6월 21일
새로운 내용	서비스 연결 역할 콘텐츠가 추가되었습니다. AMS Accelerate에 서비스 연결 역할 사용	2022년 6월 16일
	AWS OOD(Orption on Demand) 카탈로그에 Network Firewall Operations가 추가되었습니다. 온디맨드 작업	2022년 6월 16일
	문제 관리 기능 설명이 추가되었습니다. 서비스 설명	2022년 6월 16일
	특정 옵트인 리전에서가 지원하지 않는 구성 규칙 세트에 대한 참고 사항이 추가되었습니다. Accelerate의 구성 규정 준수	2022년 6월 16일

변경	설명	Date
콘텐츠 업데이트	구성 규정 준수. "AMS Config Rule library" -> "Table of rules"가 ZIP으로만 업데이트 및 제거되었습니다. Accelerate의 구성 규정 준수	2022년 6월 16일
	에스컬레이션 이메일을 제거했습니다. 에스컬레이션 경로	2022년 6월 16일
	주제 목록을 아래 열린 단락으로 이동했습니다. AMS Accelerate란 무엇입니까?	2022년 6월 16일
	자동 문제 해결 콘텐츠를 업데이트했습니다. 알림의 AMS 자동 문제 해결	2022년 6월 16일
업데이트된 콘텐츠: 서비스 설명	의 AMS Config 규칙에서 모니터링하는 서비스 목록에 EKS를 추가했습니다지원되는 서비스. 의 RACI 테이블에서 모니터링 설명을 업데이트했습니다역할 및 책임.	2022년 5월 12일
업데이트된 콘텐츠: 구성 규정 준수	EKS 관련 구성 규칙이 추가되었습니다. Accelerate의 구성 규정 준수을(를) 참조하세요.	2022년 5월 12일
업데이트된 콘텐츠: 시작하기, 계정 검색	에 최신 버전의 AwsAccountDiscoveryCli 스크립트(계정 검색 변경 로그 zip 파일)가 추가되었습니다1단계. Accelerate의 계정 검색.	2022년 5월 12일
업데이트된 콘텐츠: 모니터링, 기본 지표	ALB 관련 지표의 트리거 조건을 업데이트했습니다. AMS의 기준 모니터링 알림을(를) 참조하세요.	2022년 5월 12일
업데이트된 콘텐츠: 온보딩 패치 적용	명시적 패치 적용 사전 조건 추가: EBS에 옵트인해야 합니다. Accelerate의 온보딩 패치을(를) 참조하세요.	2022년 5월 12일

변경	설명	Date
업데이트된 콘텐츠: 리소스 인벤토리 테이블 가속화	ams-detective-controls-config-rules-cdk 규칙을 변경하고 ams-detective-controls-recorder-cdk 및 ams-detective-controls-infrastructure-cdk에 대한 규칙을 추가했습니다. Accelerate의 리소스 인벤토리을(를) 참조하세요.	2022년 4월 14일
업데이트된 콘텐츠: 구성 규정 준수	업계 표준, 구성 규칙 및 응답 유형에 대한 소개. 고객이 개별 구성 규칙 또는 응답을 선택하지 않음을 강조합니다Accelerate의 구성 규정 준수.	2022년 4월 14일
업데이트된 콘텐츠: 서비스 설명	역할 및 책임에서 기존 변경 범위 섹션을 이동했습니다. 역할 및 책임을(를) 참조하세요.	2022년 4월 14일
업데이트된 콘텐츠: 태그 지정 및 모니터링	태그 지정 및 모니터링`AWS::Synthetics:Canary` 에 허용되는 리소스 유형 목록에가 추가되었습니다. AMS Accelerate의 리소스 태거 구성 프로파일 및 구성 프로파일 가속화: 가상 파라미터 대체 섹션을 참조하세요.	2022년 4월 14일
업데이트된 콘텐츠: 사전 조건 가속화	에 SSM 필수 버킷 권한을 추가했습니다Accelerate의 Amazon EC2 Systems Manager.	2022년 4월 14일
새 콘텐츠: 패치 및 모니터링	Cloudformation을 사용하여 태그 지정 및 모니터링 구성을 배포하는 샘플 코드가 추가되었습니다. CloudFormation for Accelerate를 사용하여 구성 프로파일 배포 및 CloudFormation 를 사용하여 구성 변경 가속화 배포 섹션을 참조하세요.	2022년 3월 10일
업데이트된 콘텐츠: 패치 유지 관리 콘솔	콘솔 인터페이스AMS Accelerate용 Systems Manager 콘솔에서 유지 관리 기간 생성와 일치하도록의 단계를 재정렬했습니다.	2022년 3월 10일

변경	설명	Date
업데이트된 콘텐츠: 패치 유지 관리 CLI	에 대한 CLI 파라미터(일정, 기간 및 마감) 업데이트 AMS Accelerate용 Systems Manager 명령줄 인터페이스(CLI)를 사용하여 유지 관리 기간 생성	2022년 3월 10일
새 콘텐츠: Auto Instance Config	의 정의를 `AMSInstanceProfile BasePolicy` 에 추가 IAM 권한 변경 세부 정보	2022년 3월 10일
새 콘텐츠: 온보딩	에 샘플 Linux 명령 추가 Accelerate의 아웃바운드 인터넷 연결	2022년 3월 10일
새 콘텐츠: 온보딩	에 최소 권한 옵션을 추가했습니다AMS 역할을 생성하기 위한 템플릿.	2022년 3월 10일
업데이트된 콘텐츠: 에스컬레이션 가속화 지침	에 지침, 링크 및 이메일 연락처 추가 에스컬레이션 경로	2022년 3월 10일
업데이트된 콘텐츠: 지원되는 구성	AMS는 2023년 3월 14일에 RHEL 6 및 CentOs 대한 지원을 종료할 것으로 예상됩니다. 지원되는 구성 섹션을 참조하세요	2022년 3월 10일
업데이트된 콘텐츠: 리소스 테이블	Accelerate의 리소스 인벤토리 리소스 테이블에 AMS 액세스 IAM 역할 추가	2022년 3월 10일
업데이트된 콘텐츠: 온보딩 및 백업	Accelerate AWS Backup 의 온보딩 및에 옵트인 AWS Backup 하기 위한 지침 추가 AMS Accelerate의 연속성 관리	2022년 3월 10일
업데이트된 콘텐츠: 액세스 관리	Accelerate 지침에서 고급 관련 지침을 제거했습니다AMS에서 루트 사용자 계정을 사용하는 방법 및 시기.	2022년 3월 10일
업데이트된 콘텐츠: 지원되는 구성	AMS는 이제 Oracle Linux 8.3 및 Ubuntu 18.04 및 20.04를 지원합니다. 지원되는 구성을(를) 참조하세요.	2022년 2월 28일

변경	설명	Date
업데이트된 콘텐츠: 서비스 수준 계약	에서 다운로드 가능한 서비스 수준 계약을 업데이트했습니다지원되는 서비스.	2022년 2월 28일
업데이트된 콘텐츠: 액세스 관리	AMS 운영자 콘솔 역할에 대한 AMS가 계정에 액세스하는 방법 FAQs와 이를 수정하거나 삭제하지 않도록 경고로 업데이트되었습니다.	2022년 2월 28일
업데이트된 콘텐츠: Alarm Manager	구성 프로파일 가속화: 모니터링 업데이트됨 Alarm Manager는 더 이상 단일 지표 경보로 제한되지 않습니다.	2022년 2월 28일
업데이트된 콘텐츠: 시작하기	2단계. Accelerate의 온보딩 관리 리소스 업데이트됨 온보딩 리소스에 대한 액세스를 최소화하는 IAM 역할이 추가되었습니다.	2022년 2월 28일
새 콘텐츠: 서비스 설명의 변경 범위	AMS Accelerate가 수행하지 않는 경계와 작업을 강조하는 새 섹션AMS Accelerate에서 수행한 변경 범위이 추가되었습니다.	2022년 2월 10일
업데이트된 콘텐츠: 시작하기	새로운 온보딩 프로세스는 사용자 지정 전에 기본 기능 및 구성을 설정하는 것으로 시작됩니다. 하위 섹션에는 기능별 목표 및 관련 링크가 포함되어 있습니다. AMS Accelerate 시작하기을(를) 참조하세요.	2022년 2월 10일
업데이트된 콘텐츠: AMS Backup Management.	가독성을 위해 AMS Accelerate의 연속성 관리장을 단축하고 재구성했습니다.	2022년 2월 10일
업데이트된 콘텐츠: 태그 지정	CloudFormation 및 기타 도구의 코드 샘플을 수용하기 위한 태그 지정 도구 섹션이 추가되었습니다. AMS Accelerate의 태그 지정을(를) 참조하세요.	2022년 2월 10일
업데이트된 콘텐츠: 기준 모니터링	RedShift 클러스터 경보의 트리거 조건이 개선되면 유지 관리 중에 잘못된 경보가 줄어듭니다. AMS의 기준 모니터링 알림을(를) 참조하세요.	2022년 2월 10일

변경	설명	Date
업데이트된 콘텐츠: 패치 적용	유지 관리 기간을 등록하도록 샘플 CLI 명령을 업데이트했습니다. AMS Accelerate용 Systems Manager 명령줄 인터페이스(CLI)를 사용하여 유지 관리 기간 생성을(를) 참조하세요.	2022년 2월 10일
업데이트된 content: AWS Config Rules Inventory.	Config Rules Inventory 테이블`ams-nist-cis-ec2-security-group-attached-to-eni` 에서 더 이상 사용되지 않는 AWS 구성 규칙을 제거했습니다. 규칙 테이블을(를) 참조하세요.	2022년 1월 27일
새 콘텐츠: 패치 유지 관리 기간 생성.	명령줄에서 패치 유지 관리 기간을 생성하기 위한 SSM 자습서 및 샘플 명령에 대한 링크를 추가했습니다. AMS Accelerate용 Systems Manager 명령줄 인터페이스(CLI)를 사용하여 유지 관리 기간 생성을(를) 참조하세요.	2022년 1월 27일
새 콘텐츠: Resource Tagger는 새 Auto Scaling 그룹(ASG) 리소스 유형을 인식합니다.	Resource Tagger 구성 프로필로 필터링할 수 있는 리소스 유형에 Auto Scaling 그룹을 추가했습니다. 구문 및 구조을(를) 참조하세요.	2022년 1월 13일
새 콘텐츠: 추가 백업 계획 및 볼트.	랜섬웨어 공격을 포함한 고위험 시나리오를 완화하기 위한 새로운 백업 계획 및 볼트가 추가되었습니다. AMS 볼트에서 백업 보기 및 AMS 볼트에서 백업 보기 섹션을 참조하세요.	2022년 1월 13일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.