사용자 가이드

# AWS Support

API 버전 2013-04-15

# AWS Support: 사용자 가이드

# Table of Contents

시작해 보세요 AWS Support ..... 1
지원 사례 및 사례 관리 생성 ..... 1
지원 사례 만들기 ..... 2
문제 설명 ..... 4
심각도 선택 ..... 5
예시: 계정 및 결제에 대한 지원 사례 생성 ..... 7
문제 해결 ..... 13
서비스 할당량 증가 생성 ..... 13
사례 업데이트, 해결 및 다시 열기 ..... 15
기존 지원 사례 업데이트 ..... 16
지원 사례 해결 ..... 17
해결된 사례 다시 열기 ..... 18
관련 사례 생성 ..... 19
사례 기록 ..... 21
AWS Support 권장 사항 ..... 22
AWS Support 권장 사항에 대한 액세스 관리 ..... 22
AWS Support 권장 사항 모니터링 및 로깅 ..... 24
SDK를 사용한 AWS 작업 ..... 28
AWS Support API 소개 ..... 30
지원 사례 관리 ..... 30
AWS Trusted Advisor ..... 31
엔드포인트 ..... 31
AWS SDK 지원 ..... 32
AWS Support 플랜 ..... 33
AWS Support 플랜의 특징 ..... 33
AWS Support 플랜 변경 ..... 35
관련 정보 ..... 35
AWS Trusted Advisor ..... 37
Trusted Advisor 권장 사항 시작하기 ..... 38
Trusted Advisor 콘솔에 로그인 ..... 38
검사 범주 보기 ..... 39
특정 검사 보기 ..... 41
검사 필터링 ..... 42
검사 결과 새로 고침 ..... 44

검사 결과 다운로드 ..... 44
조직 보기 ..... 45
기본 설정 ..... 45
Trusted Advisor API로 시작하기 ..... 47
웹 Trusted Advisor 서비스로 사용 ..... 48
사용 가능한 Trusted Advisor 검사 목록 가져오기 ..... 48
사용 가능한 Trusted Advisor 검사 목록을 새로 고치세요. ..... 49
상태 변경 Trusted Advisor 여부를 확인하기 위해 검사를 폴링합니다. ..... 49
Trusted Advisor 검사 결과 요청 ..... 51
Trusted Advisor 수표 세부 정보 보기 ..... 52
AWS Trusted Advisor에 대한 조직 보기 ..... 53
필수 조건 ..... 53
조직 보기 활성화 ..... 54
Trusted Advisor 검사 새로 고침 ..... 55
조직 보기 보고서 생성 ..... 55
보고서 요약 보기 ..... 59
조직 보기 보고서 다운로드 ..... 60
조직 보기 비활성화 ..... 65
IAM 정책을 사용하여 조직 보기에 대한 액세스 허용 ..... 67
다른 AWS 서비스를 사용하여 Trusted Advisor 보고서 보기 ..... 69
AWS Config에 의해 구동되는 Trusted Advisor 검사 보기 ..... 79
문제 해결 ..... 79
Trusted Advisor에서 Security Hub 컨트롤 보기 ..... 80
필수 조건 ..... 81
Security Hub 결과 보기 ..... 82
Security Hub 결과 새로 고침 ..... 83
Trusted Advisor에서 Security Hub 사용 중지 ..... 84
문제 해결 ..... 84
Trusted Advisor 수표 AWS Compute Optimizer 신청 ..... 87
관련 정보 ..... 88
AWS Trusted Advisor Priority 시작하기 ..... 89
사전 조건 ..... 90
Trusted Advisor Priority 사용 ..... 90
우선 순위 지정 권장 사항 보기 ..... 90
권장 사항 승인 ..... 93
권장 사항 취소 ..... 95

권장 사항 해결 ..... 97
권장 사항 다시 열기 ..... 99
권장 사항 세부 정보 다운로드 ..... 100
위임된 관리자 등록 ..... 101
위임된 관리자 등록 취소 ..... 101
Trusted Advisor Priority 알림 관리 ..... 102
Trusted Advisor Priority 사용 중지 ..... 103
AWS Trusted Advisor 참여(미리 보기) 시작하기 ..... 103
사전 조건 ..... 104
참여 대시보드 보기 ..... 104
참여 유형 카탈로그 보기 ..... 105
참여 요청 ..... 106
참여 편집 ..... 108
첨부 파일 및 메모 제출 ..... 110
참여 상태 변경 ..... 111
권장 참여와 요청 참여를 구분합니다. ..... 112
참여 검색 ..... 113
Trusted Advisor 레퍼런스 확인 ..... 114
비용 최적화 ..... 114
성능 ..... 150
보안 ..... 196
내결함성 ..... 234
서비스 한도 ..... 333
운영 우수성 ..... 353
로그 변경 대상 AWS Trusted Advisor ..... 392
검사 5개를 제거하고 검사 1개를 추가했습니다. ..... 392
내결함성 검사가 제거되었습니다. ..... 393
새로운 내결함성 검사 ..... 393
내결함성 및 보안 검사 업데이트 ..... 393
새로운 내결함성 검사 ..... 394
내결함성 검사 업데이트 ..... 394
보안 검사 업데이트 ..... 394
새로운 보안 및 성능 검사 ..... 394
새 보안 검사 ..... 395
새로운 내결함성 및 비용 최적화 검사 ..... 395
새로운 내결함성 검사 ..... 395

Amazon RDS에 대한 새로운 검사 ..... 395
새 API AWS Trusted Advisor ..... 395
Trusted Advisor 체크 제거 ..... 396
AWS Config 검사 통합: Trusted Advisor ..... 396
새로운 내결함성 검사 ..... 396
새로운 서비스 한도 검사 ..... 397
새로운 내결함성 검사 ..... 397
새로운 내결함성 및 성능 검사 ..... 397
새로운 내결함성 검사 ..... 398
새로운 내결함성 검사 ..... 398
Amazon ECS 내결함성 검사의 지역 확장 ..... 398
새로운 내결함성 검사 ..... 398
새로운 내결함성 검사 ..... 395
와의 통합 업데이트 Trusted AdvisorAWS Security Hub ..... 399
AWS Resilience Hub에 대한 새로운 내결함성 검사 ..... 395
콘솔 업데이트 Trusted Advisor ..... 400
Amazon EC2에 대한 새로운 검사 ..... 400
Trusted Advisor에 Security Hub 검사 추가 ..... 401
에서 검사를 추가했습니다. AWS Compute Optimizer ..... 401
노출된 액세스 키 검사 업데이트 ..... 401
AWS Direct Connect검사가 업데이트됨 ..... 402
AWS Security HubAWS Trusted Advisor 콘솔에 컨트롤이 추가되었습니다. ..... 403
Amazon EC2 및 AWS Well-Architected에 대한 새로운 검사 ..... 403
Amazon OpenSearch 서비스의 체크 이름 업데이트 ..... 404
Amazon Elastic Block Store 볼륨 스토리지에 대한 검사가 추가됨 ..... 404
에 대한 검사가 추가되었습니다. AWS Lambda ..... 405
Trusted Advisor 수표 제거 ..... 405
Amazon Elastic Block Store 검사가 업데이트됨 ..... 406
Trusted Advisor 수표 제거 ..... 407
Trusted Advisor 수표 제거 ..... 407
AWS Support 슬랙의 앱 ..... 408
필수 조건 ..... 409
AWS Support 앱 위젯에 대한 액세스 관리 ..... 409
AWS Support 앱에 대한 액세스 관리 ..... 411
Slack 작업 영역 승인 ..... 417
여러 계정 승인 ..... 419

Slack 채널 구성 ..... 419
Slack 채널 구성 업데이트 ..... 425
Slack에서 지원 사례 생성 ..... 426
Slack의 지원 사례에 회신 ..... 432
라이브 채팅 세션에 참여하세요 AWS Support ..... 434
Slack에서 지원 사례 검색 ..... 440
검색 결과 사용 ..... 442
Slack의 지원 사례 해결 ..... 444
Slack에서 지원 사례 다시 열기 ..... 444
서비스 할당량 증가 요청 ..... 445
AWS Support 앱에서 Slack 채널 구성 삭제 ..... 447
AWS Support 앱에서 Slack 작업 영역 구성 삭제 ..... 448
Slack의 AWS Support 앱 명령 ..... 449
Slack 채널 명령 ..... 449
실시간 채팅 채널 명령 ..... 450
AWS Support Center Console에서 AWS Support 앱 서신 보기 ..... 450
Slack 내 AWS Support 앱을 위한 AWS CloudFormation 리소스 만들기 ..... 451
AWS Support 앱 및 AWS CloudFormation 템플릿 ..... 451
조직을 위한 Slack 구성 리소스 생성 ..... 452
CloudFormation에 대해 자세히 알아보기 ..... 457
Terraform을 사용하여 AWS Support 앱 리소스 생성 ..... 457
보안 ..... 459
데이터 보호 ..... 460
지원 사례 보안 ..... 460
Identity and Access Management(IAM) ..... 461
고객 ..... 462
ID를 통한 인증 ..... 462
정책을 사용한 액세스 관리 ..... 465
IAM의 AWS Support 작동 방식 ..... 467
자격 증명 기반 정책 예시 ..... 469
서비스 링크 역할 사용 ..... 471
AWS 관리형 정책 ..... 478
AWS Support 센터 액세스 관리 ..... 527
플랜에 대한 액세스 관리 AWS Support ..... 531
액세스 관리: AWS Trusted Advisor ..... 535
AWS Trusted Advisor에 대한 예제 서비스 제어 정책 ..... 547

문제 해결 ... 549
사고 대응 ... 551
로그인 및 모니터링 AWS Support 및 AWS Trusted Advisor ... 551
규정 준수 확인 ... 552
복원력 ... 553
인프라 보안 ... 553
구성 및 취약성 분석 ... 554
코드 예시 ... 555
작업 ... 563
AddAttachmentsToSet ... 564
AddCommunicationToCase ... 570
CreateCase ... 577
DescribeAttachment ... 585
DescribeCases ... 590
DescribeCommunications ... 598
DescribeServices ... 606
DescribeSeverityLevels ... 613
DescribeTrustedAdvisorCheckRefreshStatuses ... 620
DescribeTrustedAdvisorCheckResult ... 621
DescribeTrustedAdvisorCheckSummaries ... 623
DescribeTrustedAdvisorChecks ... 625
RefreshTrustedAdvisorCheck ... 626
ResolveCase ... 627
시나리오 ... 633
사례 시작하기 ... 633
AWS Support의 모니터링 및 로깅 ... 691
다음을 통한 AWS Support 사례 모니터링 EventBridge ... 691
AWS Support 사례에 대한 EventBridge 규칙 생성 ... 692
AWS Support 이벤트 예제 ... 693
다음 사항도 참조하십시오. ... 696
AWS CloudTrail을 사용하여 AWS Support API 호출 로깅 ... 696
CloudTrail의 AWS Support 정보 ... 25
CloudTrail 로그 기록의 AWS Trusted Advisor 정보 ... 697
AWS Support 로그 파일 항목 이해 ... 698
CloudTrail을 사용하여 AWS Support 앱 API 호출 로깅 ... 700
CloudTrail의 AWS Support 앱 정보 ... 700

AWS Support 앱 로그 파일 항목 이해 ..... 701
Support 플랜의 모니터링 및 로깅 ..... 705
AWS CloudTrail을 사용하여 AWS Support 플랜 API 호출 로깅 ..... 705
CloudTrail의 AWS Support 플랜 정보 ..... 705
AWS Support 플랜 로그 파일 항목 이해 ..... 706
AWS Support 계획의 변경 사항에 대한 콘솔 작업 로깅 ..... 711
Trusted Advisor의 모니터링 및 로깅 ..... 715
다음을 통한 Trusted Advisor 검사 결과 모니터링 EventBridge ..... 716
Trusted Advisor 지표를 모니터링하여 CloudWatch 경보 생성 ..... 718
필수 조건 ..... 718
Trusted Advisor의 CloudWatch 지표 ..... 723
Trusted Advisor 지표 및 차원 ..... 729
를 AWS Trusted Advisor 사용하여 콘솔 작업 로깅 AWS CloudTrail ..... 731
Trusted Advisor 자세한 내용은 CloudTrail ..... 732
예: 로그 파일 항목 Trusted Advisor ..... 734
문제 해결 리소스 ..... 739
서비스별 문제 해결 ..... 739
문서 기록 ..... 744
이전 업데이트 ..... 766
AWS 용어집 ..... 770
..... dcclxxi

# 시작하기 AWS Support

AWS Support AWS 솔루션의 성공과 운영 상태를 지원하는 도구 및 전문 지식에 대한 액세스를 제공하는 다양한 계획을 제공합니다. 모든 지원 플랜을 통해 연중무휴 고객 서비스, AWS 설명서, 기술 문서 및 지원 포럼에 액세스할 수 있습니다. AWS 환경을 계획, 배포 및 개선하는 데 필요한 기술 지원 및 추가 리소스가 필요하면 AWS 사용 사례에 맞는 지원 계획을 선택할 수 있습니다.

참고

- 에서 지원 사례를 만들려면 AWS Management Console을 참조하십시오지원 사례 만들기.
- 다양한 AWS Support 플랜에 대한 자세한 내용은 AWS Support 플랜 비교 및 을 참조하십시오AWS Support 플랜 변경.
- Support 플랜은 지원 사례에 대해 서로 다른 응답 시간을 제공합니다. 심각도 선택 및 응답 시간 단원을 참조하세요.

주제


- 지원 사례 및 사례 관리 생성
- 서비스 할당량 증가 생성
- 사례 업데이트, 해결 및 다시 열기
- AWS Support 권장 사항
- AWS SupportAWS SDK와 함께 사용


## 지원 사례 및 사례 관리 생성

에서는 다음과 AWS Management Console같은 세 가지 유형의 고객 사례를 생성할 수 있습니다 AWS Support.

- 계정 및 결제 지원 사례는 모든 AWS 고객에게 제공됩니다. 결제 및 계정 관련 문의에 대한 도움을 받을 수 있습니다.
- 서비스 한도 증가 요청 역시 모든 AWS 고객이 이용할 수 있습니다. 이전에는 제한이라고 했던 기본 서비스 할당량에 대한 자세한 내용은 AWS 일반 참조에서 AWS 서비스 할당량을 참조하세요.
- 기술 지원 사례를 통해 서비스 관련 기술 문제 및 타사 애플리케이션(해당되는 경우)에 대한 기술 지원을 받을 수 있습니다. 기본 지원 플랜에 가입한 경우 기술 지원 사례를 생성할 수 없습니다.

참고

- 지원 플랜을 변경하려면 AWS Support 플랜 변경을(를) 참조하세요.
- 계정을 닫으려면 AWS Billing 사용 설명서의 계정 닫기를 참조하세요.
- 에 대한 AWS 서비스일반적인 문제 해결 주제를 찾으려면 을 참조하십시오문제 해결 리소스.
- Reseled AWS Partner Support에 AWS Partner Network속해 있는 고객의 경우 청구 관련 문제는 해당 고객에게 AWS Partner 직접 문의하십시오. AWS Support 청구 및 계정 관리와 같은 Reseld Support와 관련된 비기술적 문제에 대해서는 지원할 수 없습니다. 자세한 정보는 다음 주제를 참조하세요.
  - AWS 파트너가 조직의 AWS Support 플랜을 결정하는 방법
  - AWS Partner주도 지원

## 지원 사례 만들기

AWS Management Console의 지원 센터에서 지원 사례를 생성할 수 있습니다.

참고

- AWS 계정의 루트 사용자 또는 AWS Identity and Access Management (IAM) 사용자로 Support Center에 로그인할 수 있습니다. 자세한 정보는 AWS Support 센터 액세스 관리을 참조하세요.
- 지원 센터에 로그인하여 지원 사례를 만들 수 없는 경우 문의처(Contact Us) 페이지를 대신 사용할 수 있습니다. 이 페이지를 사용하여 결제 및 계정 문제에 대한 도움을 받을 수 있습니다.

지원 사례를 생성하려면

1. AWS Support Center Console에 로그인합니다.

> **Tip**
>
> 에서 물음표 아이콘
> (  )
> 을 선택한 다음 Support Center를 선택할 수도 있습니다. AWS Management Console

2. 사례 생성(Create case)을 선택하세요.
3. 다음 옵션 중 하나를 선택합니다:
   - 계정 및 결제(Account and billing)
   - 기술(Technical)
   - 서비스 할당량을 늘리려면 서비스 한도 증가를 원하십니까?(Looking for service limit increases?)를 선택한 다음 서비스 할당량 증가 생성의 지침을 따릅니다.
4. 서비스(Service), 범주(Category), 심각도(Severity)를 선택합니다.

> **Tip**
>
> 자주 묻는 질문에 있는 권장 해결 방법을 사용할 수 있습니다.

5. 다음 단계: 추가 정보(Next step: Additional information)를 선택합니다
6. 추가 정보(Additional information) 페이지의 제목(Subject)에 해당 문제에 대한 제목을 입력합니다.
7. 설명(Description)에서 프롬프트를 따라 다음과 같이 사례를 설명합니다:
   - 수신한 오류 메시지
   - 수행한 문제 해결 단계
   - 서비스에 액세스하는 방법:
     - AWS Management Console
     - AWS Command Line Interface (AWS CLI)
     - API 작업
8. (선택 사항) 파일 첨부(Attach files)를 선택하여 오류 로그 또는 스크린샷과 같은 관련 파일을 사례에 추가합니다. 최대 3개의 파일을 첨부할 수 있습니다. 각 파일의 크기는 최대 5MB까지입니다.
9. 다음 단계: 지금 해결하거나 문의하기를 선택합니다.
10. 문의처 페이지에서 선호하는 언어를 선택합니다.
11. 선호하는 연락 방법을 선택합니다. 다음 옵션 중 하나를 선택할 수 있습니다.

a. 웹(Web) - 지원 센터에서 답변을 받습니다.

b. 채팅(Chat) - 지원 에이전트와 실시간 채팅을 시작합니다. 채팅에 연결할 수 없는 경우 문제 해결 섹션을 참조하세요.

c. 전화(Phone) - 지원 상담원으로부터 전화를 받습니다. 이 옵션을 선택하는 경우 다음 정보를 입력합니다:

- 국가 또는 리전
- 전화번호
- (선택 사항) 확장

> **참고**
>
> - 표시되는 연락 옵션은 사례 유형 및 지원 플랜에 따라 다릅니다.
> - 초안 삭제(Discard draft)를 선택하여 지원 사례 초안을 지울 수 있습니다.

12. (선택 사항) Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있는 경우 추가 연락처(Additional contacts) 옵션이 나타납니다. 사례 상태가 변경될 때 알림을 받은 사람의 이메일 주소를 입력할 수 있습니다. IAM 사용자로 로그인한 경우 자체 이메일 주소를 포함하세요. 루트 계정 이메일 주소 및 암호로 로그인한 경우 이메일 주소를 입력할 필요가 없습니다

> **Note**
>
> Basic Support 플랜에 가입한 경우 추가 연락처(Additional contacts) 옵션은 제공되지 않습니다. 그러나 내 계정(My Account) 페이지의 대체 연락처(Alternate Contact) 섹션에 지정된 운영(Operations) 연락처는 사례 서신 사본을 수신하지만 특정 유형의 계정 및 결제 사례와 기술 사례에 대해서만 수신합니다.

13. 사례 세부 정보를 검토한 다음 제출(Submit)을 선택합니다. 사례 ID 번호와 요약이 표시됩니다.

## 문제 설명

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.

## 심각도 선택

항상 지원 플랜에서 허용하는 최고 심각도의 지원 사례를 생성하려는 경향이 있을 수 있는데, 자세한 내용은 단원을 참조하세요. 단일 리소스를 손실해도 애플리케이션에 영향을 미치지 않도록 서비스를 구축하는 방법에 대한 자세한 내용은 AWS에 내결함성 애플리케이션 구축 기술 문서를 참조하세요.

다음 표에는 심각도 수준, 응답 시간 및 문제 예가 나와 있습니다.

> 참고
>
> - 지원 사례를 만든 후에는 지원 사례에 대한 심각도 코드를 변경할 수 없습니다. 상황이 바뀌면 AWS Support 상담원에게 문의하여 지원 사례를 처리하세요.
> - 심각도 수준에 대한 자세한 내용은 AWS Support API 참조를 참조하세요.

| 심각도 | 심각도 수준 코드 | 최초 응답 시간 | 설명 및 지원 플랜 |
| --- | --- | --- | --- |
| 일반 지침 | `low` | 24시간 | 일반적인 개발 질문이 있거나 기능을 요청합니다. (*Developer, Business, Enterprise On-Ramp 또는 Enterprise Support 플랜) |
| 시스템 손상 | `normal` | 12시간 | 애플리케이션의 중요하지 않은 기능이 비정상적으로 작동하거나 시간에 민감한 개발 문제가 있습니다. (*Developer, Business, Enterprise On-Ramp 또는 Enterprise Support 플랜) |
| 프로덕션 시스템 손상 | `high` | 4시간 | 애플리케이션의 중요 기능이 손상되었거나 성능이 저하되었습니다. (Business, Enterprise On-Ramp 또는 Enterprise Support 플랜) |
| 프로덕션 시스템 중단 | `urgent` | 1시간 | 비즈니스가 큰 영향을 받습니다. 애플리케이션의 중요 기능을 사용할 수 없습니다. (Business, Enterprise On-Ramp 또는 Enterprise Support 플랜) |

| 심각도 | 심각도 수준 코드 | 최초 응답 시간 | 설명 및 지원 플랜 |
| --- | --- | --- | --- |
| 비즈니스 크리티컬 시스템 중단 | `critical` | 15분 | 비즈니스에 위험이 있습니다. 애플리케이션의 중요 기능을 사용할 수 없습니다(Enterprise Support 플랜). Enterprise On-Ramp Support 플랜의 경우 이 시간은 30분입니다. |

## 응답 시간

지정된 시간 내에 초기 요청에 응답하기 위해 최선을 다하고 있습니다. 각 AWS Support 플랜의 지원 범위에 대한 자세한 내용은 AWS Support 기능을 참조하십시오.

Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있는 경우 기술 지원을 위해 연중무휴 액세스할 수 있습니다. *Developer Support의 경우 지원 사례에 대한 응답 목표는 업무 시간을 기준으로 계산됩니다. 업무 시간은 일반적으로 고객 국가 기준 08:00~18:00로 정의되며, 공휴일 및 주말은 제외됩니다. 여러 시간대를 가진 국가에서는 이 시간이 달라질 수 있습니다. 고객 국가 정보는 AWS Management Console에 있는 My Account(내 계정) 페이지의 Contact Information(연락처 정보) 섹션에 있습니다.

> **Note**
>
> 지원 사례에 대한 기본 연락처 언어로 일본어를 선택하면 다음과 같이 일본어 지원이 제공될 수 있습니다.
>
> - 비기술적 지원 사례에 대한 고객 서비스가 필요하거나 개발자 지원 플랜에 가입하여 기술 지원이 필요한 경우, 공휴일과 주말을 제외하고 일본 표준시(GMT+9)로 정의된 일본 업무 시간 동안 일본어 지원을 이용할 수 있습니다.
> - Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있는 경우 일본어 기술 지원이 연중무휴 제공됩니다.
>
> 지원 사례의 기본 연락처 언어로 중국어를 선택하면 다음과 같이 중국어 지원이 제공될 수 있습니다.
>
> - 비기술적 지원 사례에 대한 고객 서비스가 필요한 경우 공휴일과 주말을 제외하고 오전 9시부터 오후 6시(GMT+8)까지 중국어 지원이 제공됩니다.

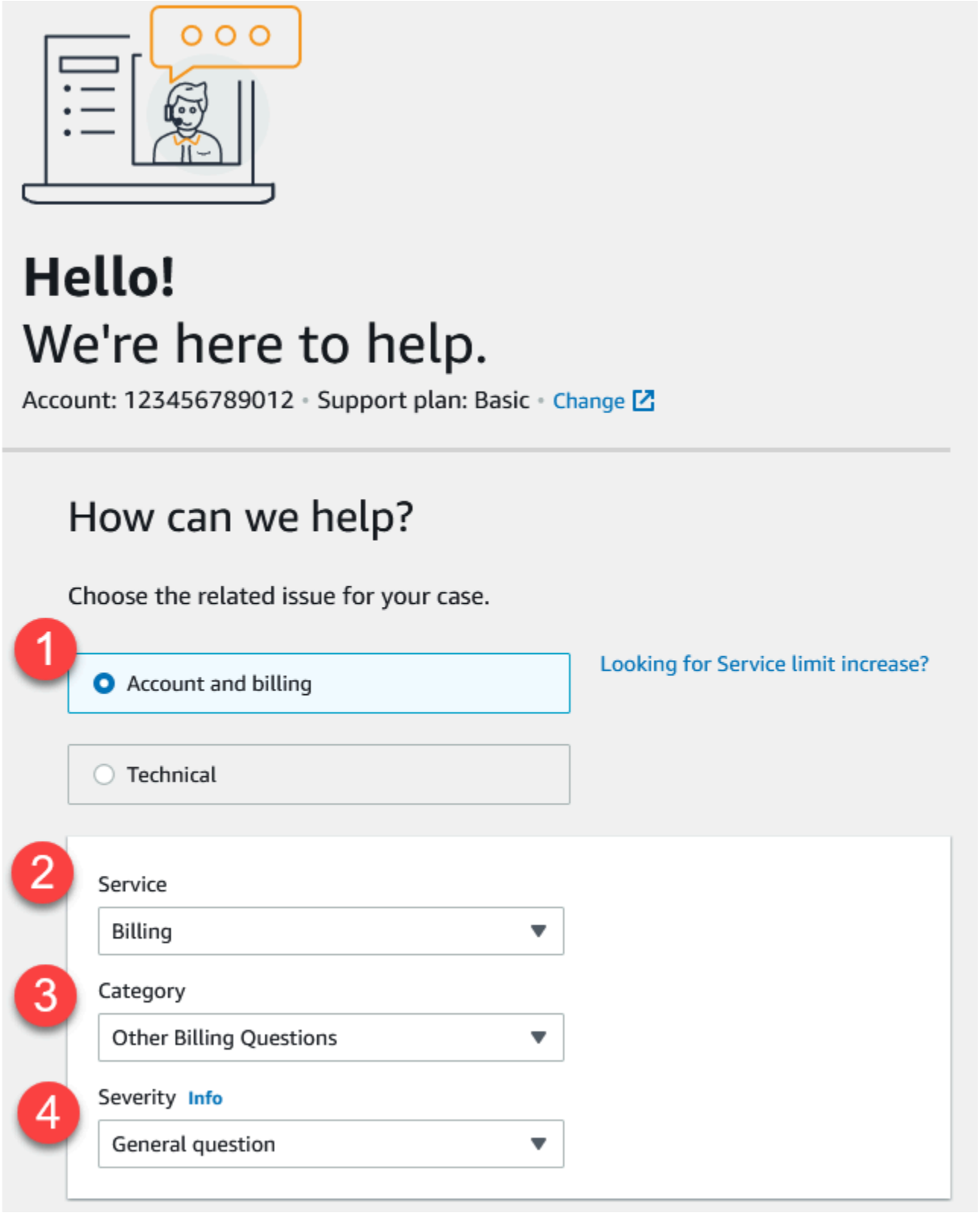
- 개발자 지원 플랜에 가입한 경우 공휴일과 주말을 제외하고 내 계정에 설정된 해당 국가의 일반적으로 오전 8시~오후 6시에 정의된 업무 시간 동안 중국어 기술 지원을 이용할 수 있습니다. 여러 시간대를 가진 국가에서는 이 시간이 달라질 수 있습니다.
- Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있는 경우 중국어 기술 지원이 연중무휴 제공됩니다.

지원 사례에 대한 선호 연락처 언어로 한국어를 선택하면 다음과 같이 한국어 지원이 제공될 수 있습니다.

- 비기술 지원 사례에 대한 고객 서비스가 필요한 경우, 휴일과 주말을 제외하고 한국 표준시(GMT+9)로 정의된 오전 9시~오후 6시 (GMT+9) 의 한국 업무 시간 동안 한국어 지원을 이용할 수 있습니다.
- 개발자 지원 플랜을 이용하는 경우 공휴일과 주말을 제외하고 내 계정에 설정된 해당 국가의 일반적으로 오전 8시~오후 6시에 정의된 업무 시간 동안 한국어 기술 지원을 이용할 수 있습니다. 여러 시간대를 가진 국가에서는 이 시간이 달라질 수 있습니다.
- Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있는 경우 한국어 기술 지원이 연중무휴 제공됩니다.

## 예시: 계정 및 결제에 대한 지원 사례 생성

다음 예시는 결제 및 계정 문제에 대한 지원 사례입니다.




1. 사례 생성(Create case) - 생성할 사례 유형을 선택합니다. 이 예시에서 사례 유형은계정 및 결제(Account and billing)입니다.

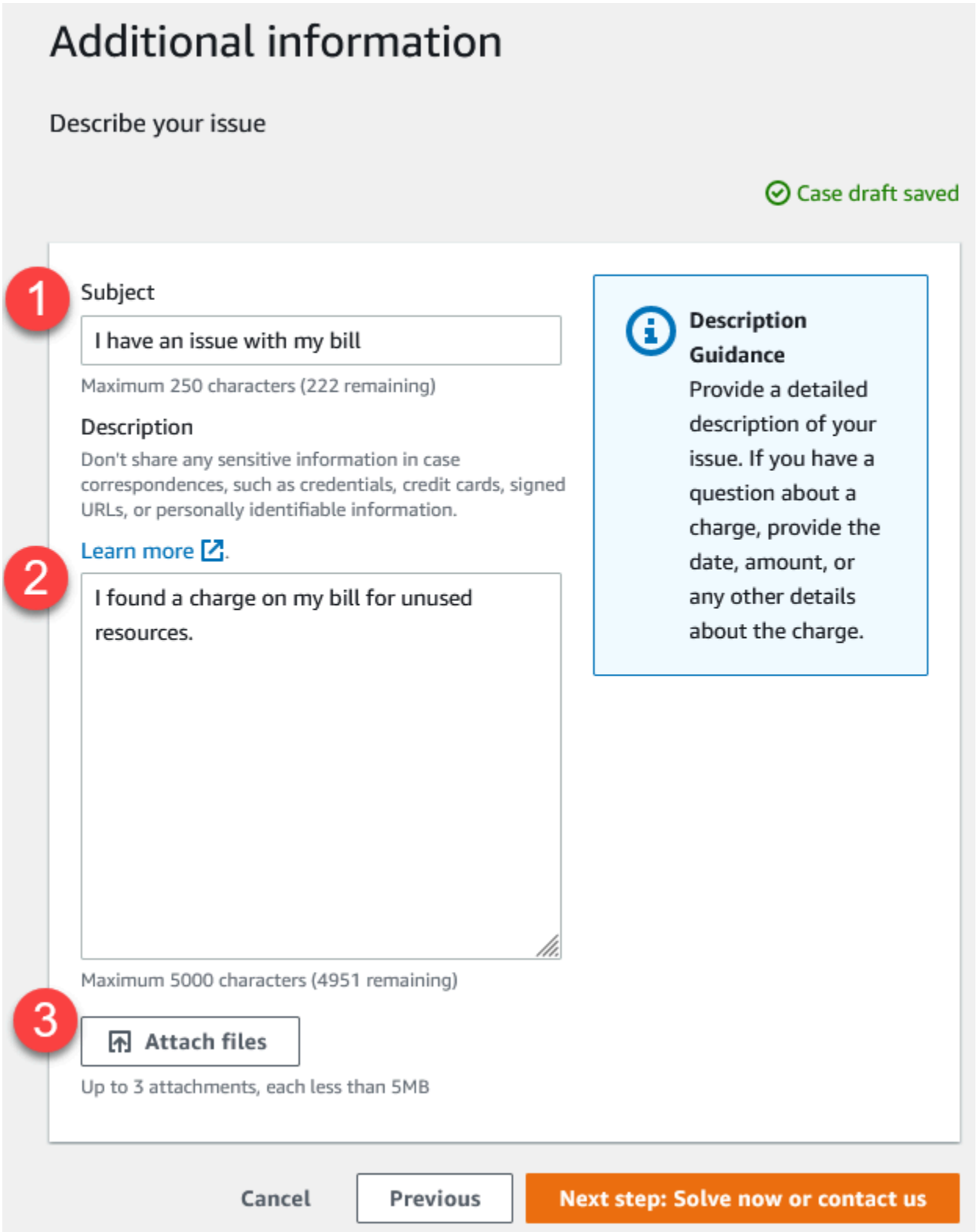
> **Note**
>
> 기본 지원 플랜에 가입한 경우 기술 지원 사례를 생성할 수 없습니다.

2. 서비스(Service) 질문이 여러 서비스에 영향을 미치는 경우 가장 적합한 서비스를 선택합니다.
3. 범주(Category) - 해당 사용 사례에 가장 적합한 범주를 선택하세요. 범주를 선택하면 아래에 문제 해결에 도움이 될 수 있는 정보 링크가 나타납니다.
4. Severity(심각도) - 유료 지원 플랜을 보유한 고객은 General guidance(일반 지침)(1일 응답 시간) 또는 System impaired(시스템 손상)(12시간 응답 시간) 심각도 수준을 선택할 수 있습니다. 또한 Business Support 플랜을 보유한 모든 고객은 프로덕션 시스템 손상(Production system impaired)(4시간 응답 시간) 또는 프로덕션 시스템 중단(Production system down)(1시간 응답 시간)을 선택할 수 있습니다. Enterprise On-Ramp 또는 Enterprise Support 플랜을 보유한 고객은 비즈니스에 중요한 시스템 중단(Enterprise Support의 경우 15분 응답 시간, Enterprise On-Ramp의 경우 30분 응답 시간)을 선택할 수 있습니다.

   응답 시간은 AWS Support의 첫 번째 응답에 관한 것입니다. 후속 응답에는 이 응답 시간이 적용되지 않습니다. 타사 문제의 경우 숙련된 직원의 가용성에 따라 응답 시간이 길어질 수 있습니다. 자세한 내용은 심각도 선택 단원을 참조하세요.

   > **Note**
   >
   > 범주 선택에 따라 추가 정보를 입력하라는 메시지가 표시될 수 있습니다.

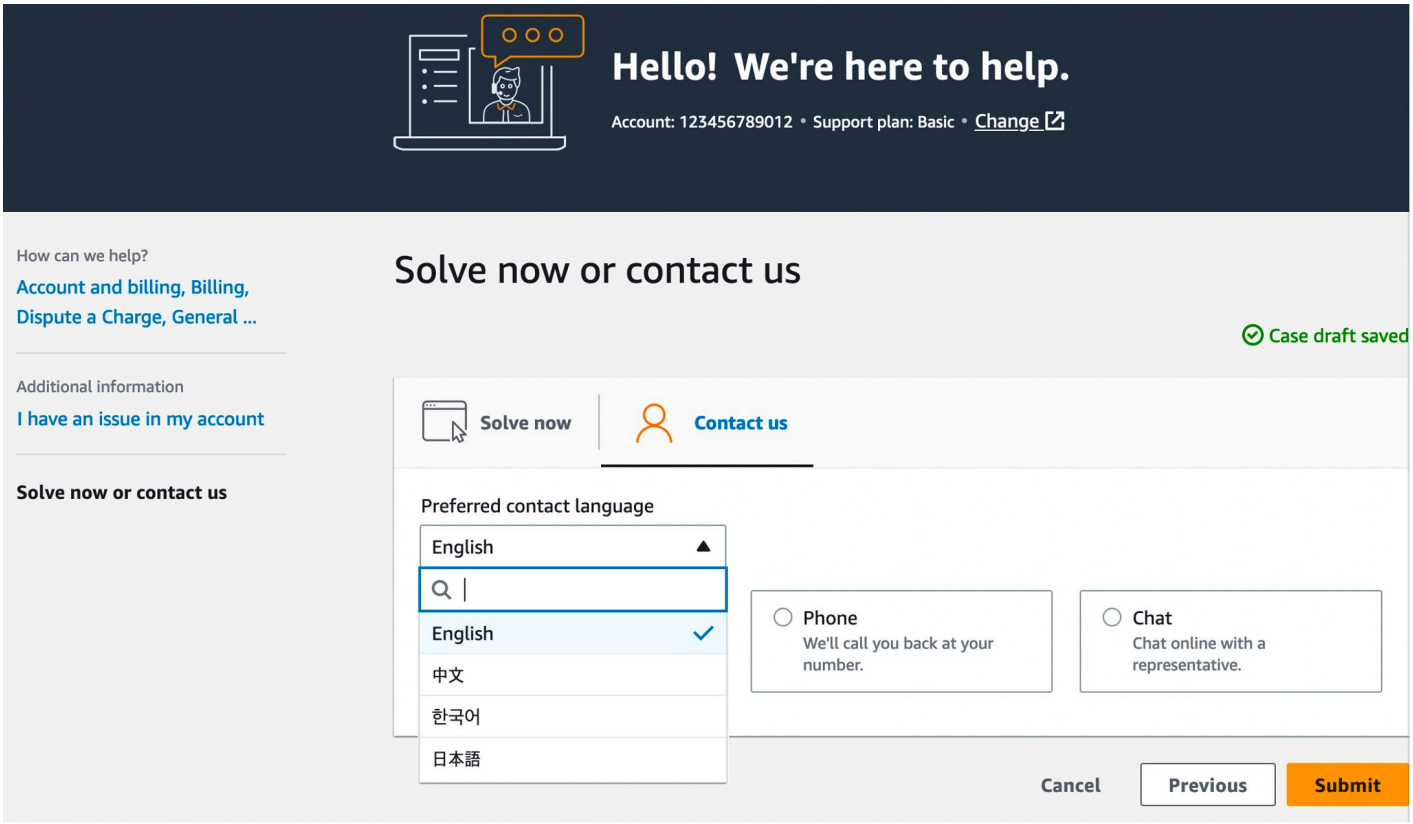
사례 유형과 분류를 지정한 후 설명과 연락 방법을 지정할 수 있습니다.




1. 제목(Subject) - 문제를 간략하게 설명하는 제목을 입력하세요.

2. 설명(Description) - 지원 사례에 대한 설명을 제공하세요. 이것은 AWS Support에 제공해야 하는 가장 중요한 정보입니다. 일부 서비스 및 범주 조합의 경우 관련 정보가 포함된 프롬프트가 나타납니다. 이러한 링크를 사용하여 문제를 해결할 수 있습니다. 자세히 알아보려면 문제 설명의 내용을 참조하세요.
3. 첨부 파일 – Support 에이전트가 사례를 더 빨리 해결하는 데 도움이 되는 스크린샷과 기타 파일을 첨부합니다. 최대 3개의 파일을 첨부할 수 있습니다. 각 파일의 크기는 최대 5MB까지입니다.

사례 세부 정보를 추가한 후 연락 방법을 선택할 수 있습니다.




1. 선호하는 언어 설정 - 선호하는 언어를 선택합니다. 현재 영어, 일본어 또는 한국어를 선택할 수 있습니다. 지원 플랜에는 기본 설정 언어의 사용자 지정 연락처 옵션이 표시됩니다.
2. 연락 방법을 선택합니다. 표시되는 연락 옵션은 사례 유형 및 지원 플랜에 따라 다릅니다.
   - 웹(Web)을 선택하는 경우 지원 센터(Support Center)를 통해 사례 진행 상황을 읽고 응답할 수 있습니다.
   - 채팅(Chat) 또는 전화(Phone)를 선택합니다. 전화(Phone)을 선택하는 경우 콜백 번호를 입력하라는 메시지가 표시됩니다.
3. 정보 작성을 완료하고 사례를 생성할 준비가 되면 제출(Submit) 버튼을 클릭하세요.

Note

지원 사례에 대한 기본 연락처 언어로 일본어를 선택하면 다음과 같이 일본어 지원이 제공될 수 있습니다.

- 비기술적 지원 사례에 대한 고객 서비스가 필요하거나 개발자 지원 플랜에 가입하여 기술 지원이 필요한 경우, 공휴일과 주말을 제외하고 일본 표준시(GMT+9)로 정의된 일본 업무 시간 동안 일본어 지원을 이용할 수 있습니다.
- Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있는 경우 일본어 기술 지원이 연중무휴 제공됩니다.

지원 사례의 기본 연락처 언어로 중국어를 선택하면 다음과 같이 중국어 지원이 제공될 수 있습니다.

- 비기술적 지원 사례에 대한 고객 서비스가 필요한 경우 공휴일과 주말을 제외하고 오전 9시부터 오후 6시(GMT+8)까지 중국어 지원이 제공됩니다.
- 개발자 지원 플랜에 가입한 경우 공휴일과 주말을 제외하고 내 계정에 설정된 해당 국가의 일반적으로 오전 8시~오후 6시에 정의된 업무 시간 동안 중국어 기술 지원을 이용할 수 있습니다. 여러 시간대를 가진 국가에서는 이 시간이 달라질 수 있습니다.
- Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있는 경우 중국어 기술 지원이 연중무휴 제공됩니다.

지원 사례에 대한 선호 연락처 언어로 한국어를 선택하면 다음과 같이 한국어 지원이 제공될 수 있습니다.

- 비기술 지원 사례에 대한 고객 서비스가 필요한 경우, 휴일과 주말을 제외하고 한국 표준시(GMT+9)로 정의된 오전 9시~오후 6시 (GMT+9) 의 한국 업무 시간 동안 한국어 지원을 이용할 수 있습니다.
- 개발자 지원 플랜을 이용하는 경우 공휴일과 주말을 제외하고 내 계정에 설정된 해당 국가의 일반적으로 오전 8시~오후 6시에 정의된 업무 시간 동안 한국어 기술 지원을 이용할 수 있습니다. 여러 시간대를 가진 국가에서는 이 시간이 달라질 수 있습니다.
- Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있는 경우 한국어 기술 지원이 연중무휴 제공됩니다.

# 문제 해결

지원 사례를 생성하거나 관리하는 데 어려움이 있는 경우 다음 문제 해결 정보를 참조하세요.

## 사례에 대한 실시간 채팅 창을 다시 열고 싶습니다.

기존 지원 사례에 회신하여 다른 채팅 창을 열 수 있습니다. 자세한 내용은 기존 지원 사례 업데이트 섹션을 참조하세요.

## 실시간 채팅에 연결할 수 없습니다

채팅 옵션을 선택했지만 채팅 창에 연결할 수 없는 경우, 먼저 다음을 확인하세요.

- 지원 센터에서 팝업 창을 허용하도록 브라우저를 구성했는지 확인합니다.

> **Note**
>
> 브라우저의 설정을 검토합니다. 자세한 내용은 Chrome 도움말과 Firefox 지원 웹 사이트를 참조하세요.

- AWS Support를 사용할 수 있도록 다음과 같이 네트워크를 구성했는지 확인합니다.
  - 네트워크가 `*.connect.us-east-1.amazonaws.com` 엔드포인트에 액세스할 수 있습니다.

> **Note**
>
> AWS GovCloud (US)의 경우 엔드포인트는 `*.connect-fips.us-east-1.amazonaws.com`입니다.

  - 방화벽이 웹 소켓 연결을 지원합니다.

그래도 채팅 창에 연결할 수 없는 경우 이메일 또는 전화 연락처 옵션을 사용하여 AWS Support에 문의하세요.

# 서비스 할당량 증가 생성

서비스 성능을 향상시키기 위해 서비스 할당량(이전에는 한도라고 함) 증가를 요청합니다.

> **Note**
>
> Service Quotas 서비스를 사용하여 서비스에 대한 증가를 직접 요청할 수도 있습니다. 현재 Service Quotas는 모든 서비스에 대해 서비스 할당량을 지원하지 않습니다. 자세한 내용은 Service Quotas 사용 설명서의 Service Quotas는 무엇입니까?를 참조하세요.

지원 사례를 생성하여 할당량 증가를 요청하려면

1. AWS Support Center Console에 로그인합니다.

   > **Tip**
   >
   > AWS Management Console에서 물음표 아이콘 (  ) 을 선택한 다음 지원 센터(Support Center)를 선택할 수도 있습니다.

2. 사례 생성(Create case)을 선택합니다.
3. 서비스 한도 증가를 원하십니까?(Looking for service limit increases?)를 선택합니다.
4. 증가를 요청하려면 프롬프트를 따릅니다. 가능한 옵션에는 다음이 포함됩니다.

   - 한도 유형
   - 심각도

   > **Note**
   >
   > 범주 선택에 따라 프롬프트에서 추가 정보를 요청할 수 있습니다.

5. 요청(Requests)에서 리전(Region)을 선택합니다.
6. 한도(Limit)에서 서비스 한도 유형을 선택합니다.
7. 새 한도 값(New limit value)에 원하는 값을 입력합니다.
8. (선택 사항) 다른 증가를 요청하려면 다른 요청 추가(Add another request)를 선택합니다.
9. 사례 설명(Case description)에 지원 사례를 설명합니다.
10. 문의 옵션(Contact options) 페이지에서 원하는 언어와 연락 방법을 선택합니다. 다음 옵션 중 하나를 선택할 수 있습니다.

    - 웹(Web) - 지원 센터에서 답변을 받습니다.

- 채팅(Chat) - 지원 에이전트와 실시간 채팅을 시작합니다. 채팅에 연결할 수 없는 경우 문제 해결 섹션을 참조하세요.
- 전화(Phone) - 지원 상담원으로부터 전화를 받습니다. 이 옵션을 선택하는 경우 다음 정보를 입력합니다.
  - 국가/리전
  - 전화번호
  - (선택 사항) 확장

11. Submit(제출)을 선택합니다. 사례 ID 번호와 요약이 표시됩니다.

# 사례 업데이트, 해결 및 다시 열기

지원 사례를 생성한 후 지원 센터에서 사례 상태를 모니터링할 수 있습니다. 새 사례는 할당되지 않음(Unassigned) 상태에서 시작됩니다. 지원 상담원이 사례에 대한 작업을 시작하면 상태가 작업 진행 중(Work in Progress)으로 변경됩니다. 지원 상담원이 귀하의 사례에 응답하여 자세한 정보를 요청(보류 중인 고객 작업(Pending Customer Action))하거나 사례를 조사 중임(보류 중인 아마존 작업(Pending Amazon Action))을 알릴 수 있습니다

사례가 업데이트되면 사례에 대한 대응 서신 및 지원 센터 내 링크가 포함된 이메일을 받게 됩니다. 이메일 메시지의 링크를 사용하여 지원 사례로 이동하세요. 이메일을 통해 사례 대응 서신에 응답할 수는 없습니다.

> 주의
>
> - 지원 사례를 제출한 AWS 계정에 로그인해야 합니다. AWS Identity and Access Management(IAM) 사용자로 로그인하는 경우, 지원 사례를 검토하려면 필요한 권한이 있어야 합니다. 자세한 내용은 AWS Support 센터 액세스 관리 단원을 참조하세요.
> - 며칠 이내에 사례에 응답하지 않으면 AWS Support가 사례를 자동으로 해결합니다.
> - 해결된 상태로 14일 이상이 지난 지원 사례는 다시 열 수 없습니다. 해결된 사례와 관련된 유사한 문제가 있는 경우 관련 사례를 생성할 수 있습니다. 자세한 내용은 관련 사례 생성 섹션을 참조하세요.

주제


- 기존 지원 사례 업데이트
- 지원 사례 해결

- 해결된 사례 다시 열기
- 관련 사례 생성
- 사례 기록

## 기존 지원 사례 업데이트

지원 에이전트에게 자세한 정보를 제공하도록 사례를 업데이트할 수 있습니다. 예를 들어 서신에 회신하고, 다른 실시간 채팅을 시작하고, 이메일 수신자를 추가하는 등의 작업을 수행할 수 있습니다. 단, 사례를 생성한 후 사례의 심각도는 업데이트할 수 없습니다. 자세한 내용은 심각도 선택 섹션을 참조하세요.

기존 지원 사례를 업데이트하려면

1. AWS Support Center Console에 로그인합니다.

   > **Tip**
   >
   > AWS Management Console에서 물음표 아이콘
   > (  )
   > 을 선택한 다음 지원 센터(Support Center)를 선택할 수도 있습니다.

2. 지원 사례 열기(Open support cases)에서 지원 사례의 제목(Subject)을 선택합니다.
3. 답변(Reply)을 선택합니다. 서신(Correspondence) 섹션에서도 다음과 같이 변경할 수 있습니다.
   - 지원 에이전트가 요청한 정보 제공
   - 첨부 파일 업로드
   - 선호하는 연락 방법 변경
   - 사례 업데이트를 받을 이메일 주소 추가
4. Submit(제출)을 선택합니다.

> **Tip**
>
> 채팅 창을 닫은 후 다른 실시간 채팅을 시작하려면 지원 사례에 답변(Reply)을 추가하고 채팅(Chat)을 선택한 다음 제출(Submit)을 선택합니다. 새 팝업 채팅 창이 열립니다.

# 지원 사례 해결

응답에 만족하거나 문제가 해결되면 지원 센터에서 사례를 해결할 수 있습니다.

지원 사례 해결를 해결하려면

1. AWS Support Center Console에 로그인합니다.

   > **Tip**
   >
   > AWS Management Console에서 물음표 아이콘
   > (  )
   > 을 선택한 다음 지원 센터(Support Center)를 선택할 수도 있습니다.

2. 지원 사례 열기(Open support cases)를 선택하고 해결 하려는 지원 사례의 제목(Subject)을 선택합니다.
3. (선택 사항) 응답(Reply)을 선택하고 대응 서신(Correspondence) 섹션에서 사례 해결 이유를 입력한 다음 제출(Submit)을 선택합니다. 예를 들어 나중에 참조할 수 있도록 문제를 해결한 방법에 대한 정보를 직접 입력할 수 있습니다.
4. 사례 해결(Resolve case)을 선택합니다.
5. 대화 상자에서 확인(Ok)을 선택하여 사례를 해결합니다.

> **Note**
>
> AWS Support가 사례를 해결하면 사용자는 피드백 링크를 사용하여 AWS Support에 대해 경험한 정보를 더 자세히 제공할 수 있습니다.

Example : 피드백 링크

다음 스크린샷은 지원 센터 내 사례의 대응 서신에서 피드백 링크를 보여 줍니다.

Please let us know if we helped resolve your issue:

If YES, click here:
https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-Yes

If NO, click here:
https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-No

## 해결된 사례 다시 열기

동일한 문제가 다시 발생하면 원래 사례를 다시 열 수 있습니다. 문제가 다시 발생한 시기와 사용자가 시도한 문제 해결 단계에 대한 세부 정보를 제공하세요. 지원 상담원이 이전 대응 서신을 참조할 수 있도록 관련 사례 번호를 포함하세요.

주의

- 문제가 해결된 날로부터 최대 14일 이내에 지원 사례를 다시 열 수 있습니다. 그러나 14일 이상 비활성 상태인 사례는 다시 열 수 없습니다. 새 사례 또는 관련 사례를 만들 수 있습니다. 자세한 내용은 관련 사례 생성 단원을 참조하세요.
- 현재 문제와는 다른 정보가 있는 기존 사례를 다시 열면 지원 상담원이 새 사례 생성을 사용자에게 요청할 수 있습니다.

해결된 사례를 다시 열려면

1. AWS Support Center Console에 로그인합니다.

   Tip

   AWS Management Console에서 물음표 아이콘 ( ) 을 선택한 다음 지원 센터(Support Center)를 선택할 수도 있습니다.

2. 모든 사례 보기(View all cases)를 선택한 다음 다시 열려는 지원 사례의 제목(Subject) 또는 사례 ID(Case ID)를 선택합니다.
3. 사례 다시 열기(Reopen case)를 선택합니다.

4. 대응 서신(Correspondence)에서 응답(Reply)에 사례 세부 정보를 입력합니다.
5. (선택 사항) 파일 선택(Choose files)을 선택하여 사례에 파일을 첨부할 수 있습니다. 최대 3개의 파일을 첨부할 수 있습니다.
6. 연락 방법(Contact method)에서 다음 옵션 중 한 가지를 선택합니다.
   - 웹(Web) - 이메일 및 지원 센터로 알림을 받습니다.
   - 채팅(Chat) - 지원 상담원과 온라인으로 채팅할 수 있습니다.
   - 전화(Phone) - 지원 상담원으로부터 전화를 받습니다.
7. (선택 사항) 추가 연락처(Additional contacts)에서, 사례 대응 서신을 받을 다른 사용자의 이메일 주소를 입력합니다.
8. 사례 세부 정보를 검토하고 제출(Submit)을 선택합니다.

## 관련 사례 생성

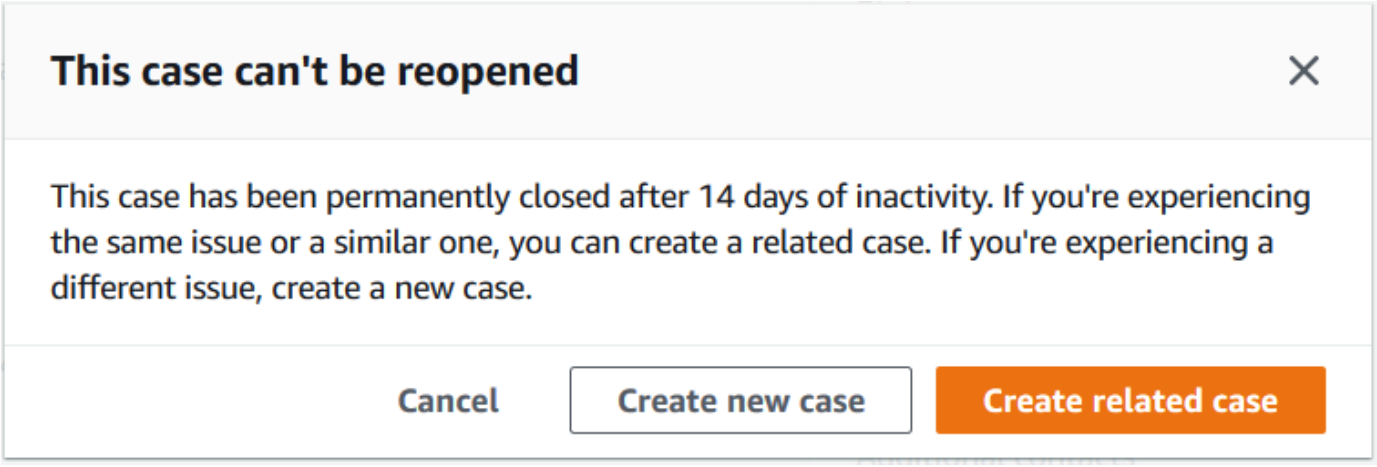
14일 동안 사용하지 않으면 해결된 서비스 사례를 다시 열 수 없습니다. 해결된 사례와 관련된 유사한 문제가 있는 경우 관련 사례를 생성할 수 있습니다. 이 관련 사례에는 이전에 해결된 사례에 대한 링크가 포함되므로 지원 상담원이 이전 사례 세부 정보 및 대응 서신을 검토할 수 있습니다. 다른 문제가 발생하는 경우 새 사례를 생성하는 것이 좋습니다.

관련 사례를 생성하려면

1. AWS Support Center Console에 로그인합니다.

   > **Tip**
   >
   > AWS Management Console에서 물음표 아이콘 (  )을 선택한 다음 지원 센터(Support Center)를 선택할 수도 있습니다.

2. 모든 사례 보기(View all cases)를 선택한 다음 다시 열려는 지원 사례의 제목(Subject) 또는 사례 ID(Case ID)를 선택합니다.
3. 사례 다시 열기(Reopen case)를 선택합니다.
4. 대화 상자에서 관련 사례 만들기(Create related case)를 선택합니다.. 이전 사례 정보가 관련 사례에 자동으로 추가됩니다. 다른 문제가 있는 경우 신규 사례 만들기(Create new case)를 선택합니다.

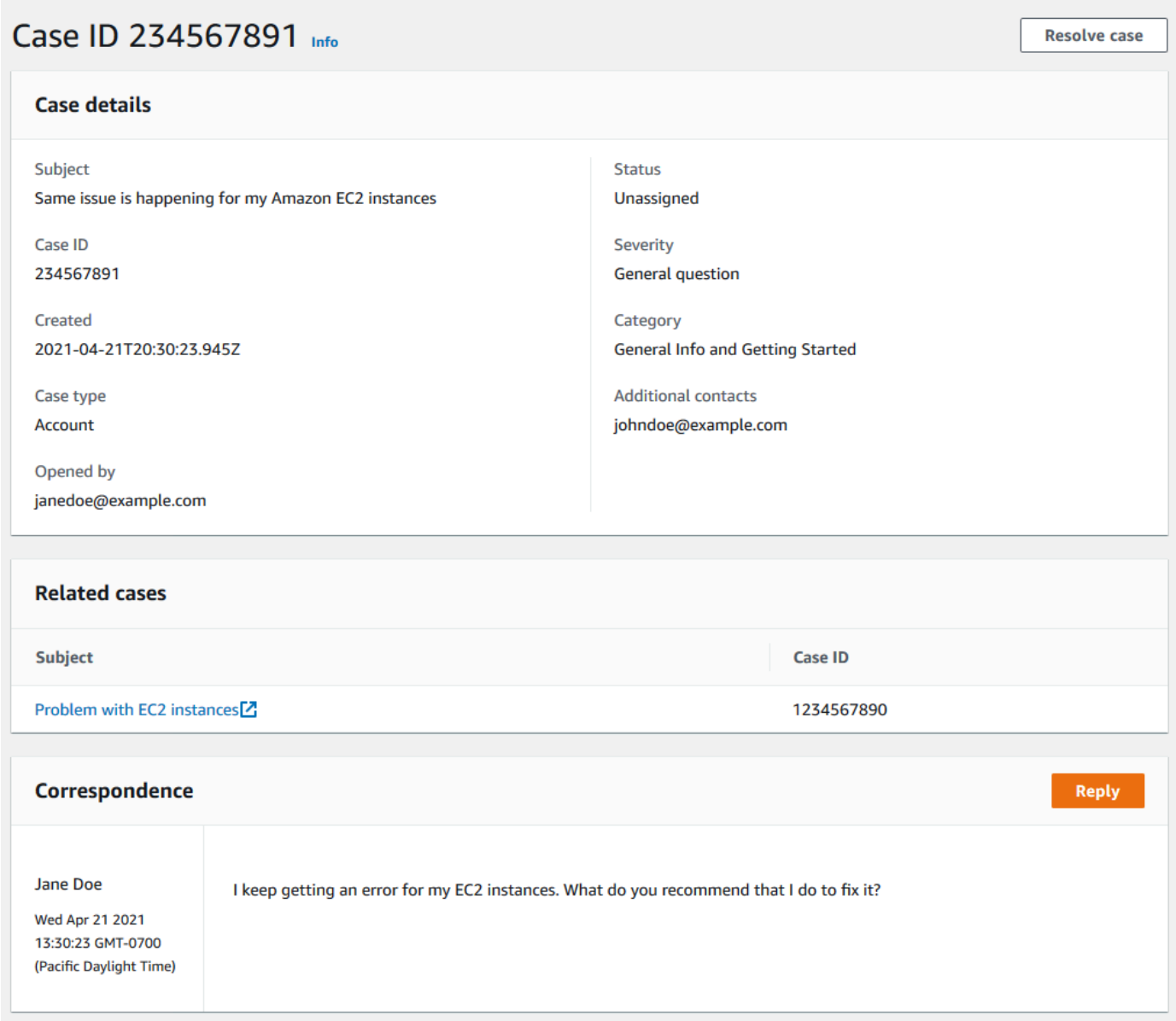



5. 동일한 단계를 거쳐 사례를 생성하세요. 지원 사례 만들기 단원을 참조하세요.

> **Note**
>
> 기본적으로 관련 사례는 이전 사례와 동일한 유형(Type), 범주(Category), 및 심각도(Severity)를 가집니다. 필요에 따라 사례 세부 정보를 업데이트할 수 있습니다.

6. 사례 세부 정보를 검토하고 제출(Submit)을 선택합니다.

사례를 생성하면 다음 예시와 같이 이전 사례가 관련 사례(Related cases) 섹션에 표시됩니다.




# 사례 기록

사례 생성 후 최대 24개월까지 사례 기록 정보를 볼 수 있습니다.

# AWS Support 권장 사항

> **Note**
>
> AWS Support 권장 사항은 서비스 약관에 정의된 '미리 보기 서비스'로 제공됩니다. AWS 미리 보기 서비스는 변경 및 취소될 수 있습니다. 자세히 알아보기

AWS Support 권장 사항은 AWS Support 센터 콘솔에서 케이스 생성 플로우를 진행하는 동안 계정 및 기술 문제에 대한 맞춤형 문제 해결 지원을 제공합니다. AWS Support 권장 사항은 사례 세부 정보 및 로그인한 계정을 기반으로 문제 해결을 위한 맞춤형 솔루션으로 응답합니다.

AWS Support 권장 사항은 문제를 분석하기 위해 승인된 정책/사용자 권한 범위 내에서 AccountID, AWS 리소스 식별자 또는 오류 메시지와 같은 정보를 쿼리합니다. 자세히 알아보기

주제

- AWS Support 권장 사항에 대한 액세스 관리
- AWS Support 권장 사항 모니터링 및 로깅

## AWS Support 권장 사항에 대한 액세스 관리

> **Note**
>
> AWS Support 권장 사항은 서비스 약관에 정의된 '미리 보기 서비스'로 제공됩니다. AWS 미리 보기 서비스는 변경 및 취소될 수 있습니다. 자세히 알아보기

사례 생성 흐름 중에 AWS Support 센터 콘솔에서 AWS Identity and Access Management (IAM) 을 사용하여 AWS Support 권장 사항에 대한 액세스를 관리할 수 있습니다.

주제

- AWS Support 권장 사항 조치
- 권장 사항에 대한 IAM 정책 예시 AWS Support

## AWS Support 권장 사항 조치

IAM 정책에서 전체 액세스를 제공하거나, 전체 액세스를 거부하거나, 특정 작업에 대한 액세스를 제공/거부하도록 AWS Support 권장 사항 작업을 지정할 수 있습니다.

| 작업 | 설명 |
| --- | --- |
| `StartSupportTroubleshooting` | 센터 콘솔의 사례 생성 흐름 중에 계정 또는 기술 문제를 진단하고 해결하는 데 도움이 되는 문제 해결 안내 세션을 시작하십시오. AWS Support |
| `GetSupportTroubleshootingResponse` | 로 StartSupportTroubleshooting 시작한 문제 해결 세션에서 현재 상태와 결과를 검색하십시오. 추가 정보에 대한 대화식 요청과 이전 응답을 기반으로 한 문제 해결을 위한 권장 사항을 포함합니다. |

## 권장 사항에 대한 IAM 정책 예시 AWS Support

다음 예제 정책을 사용하여 AWS Support 권장 사항에 대한 액세스를 관리할 수 있습니다.

AWS Support 권장 사항에 대한 전체 액세스 권한

다음 정책은 사용자에게 AWS Support 권장 사항에 대한 전체 액세스를 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportrecommendations:StartSupportTroubleshooting",
                "supportrecommendations:GetSupportTroubleshootingResponse"
            ],
            "Resource": "*"
        }
    ]
}
```

권장 사항에 AWS Support 대한 액세스 거부

다음 정책은 사용자가 AWS Support 권장 사항에 액세스하는 것을 허용하지 않습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "supportrecommendations:*",
            "Resource": "*"
        }
    ]
}
```

# AWS Support 권장 사항 모니터링 및 로깅

> **Note**
>
> AWS Support 권장 사항은 서비스 약관에 정의된 '미리 보기 서비스'로 제공됩니다. AWS 미리 보기 서비스는 변경 및 취소될 수 있습니다. 자세히 알아보기

모니터링은 AWS Support 권장 사항 및 기타 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. AWS AWS Support 권장 사항을 관찰하고, 문제 발생 시 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- AWS CloudTrail계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 호출이 이루어졌는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

주제

- 로깅 AWS Support 권장 사항 호출 AWS CloudTrail

# 로깅 AWS Support 권장 사항 호출 AWS CloudTrail

> **Note**
>
> AWS Support 권장 사항은 서비스 약관에 정의된 '미리 보기 서비스'로 제공됩니다. AWS 미리 보기 서비스는 변경 및 취소될 수 있습니다. 자세히 알아보기

AWS Support 권장 사항은 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합됩니다. CloudTrail AWS Support 권장 사항에 대한 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 AWS Support 센터 콘솔에서의 통화 및 AWS Support 권장 사항에 대한 코드 호출이 포함됩니다.

트레일을 생성하면 추천 CloudTrail 이벤트를 포함하여 Amazon Simple Storage Service (Amazon S3) 버킷으로 이벤트를 AWS Support 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다.

에서 수집한 CloudTrail 정보를 사용하여 AWS Support 권장 사항에 대한 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

구성 및 활성화 방법을 CloudTrail 포함하여 자세한 내용은 사용 AWS CloudTrail 설명서를 참조하십시오.

AWS Support 권장 사항 정보는 다음을 참조하십시오. CloudTrail

CloudTrail 계정을 만들 때 AWS 계정에서 활성화됩니다. AWS Support 권장 사항에서 지원되는 이벤트 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. AWS 계정에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

AWS Support 추천 이벤트를 포함하여 AWS 계정에서 진행 중인 이벤트 기록을 보려면 트레일을 만드세요. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 지역에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합

- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 AWS Support 권장 사항 호출은 에 의해 기록됩니다 CloudTrail. 모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 연동 사용자를 위한 임시 보안 인증으로 요청을 생성하였는지.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail 사용자 ID 요소를 참조하십시오.

또한 여러 AWS 지역 및 여러 AWS 계정의 AWS Support 권장 사항 로그 파일을 단일 Amazon S3 버킷으로 집계할 수 있습니다.

AWS Support 권장 사항 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일은 하나 이상의 로그 항목을 포함합니다. 이벤트는 모든 소스로부터 단일 요청을 나타냅니다. 여기에는 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보가 포함됩니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

Example : **`StartSupportTroubleshooting`**에 대한 로그 항목

다음 예제는 `StartSupportTroubleshooting` 작업에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    },
    "eventTime": "2023-09-11T16:34:13Z",
    "eventSource": "supportrecommendations.amazonaws.com",
    "eventName": "StartSupportTroubleshooting",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "message": "..."
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : **GetSupportTroubleshootingResponse**에 대한 로그 항목

다음 예제는 GetSupportTroubleshootingResponse 작업에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    },
    "eventTime": "2023-09-11T16:34:13Z",
    "eventSource": "supportrecommendations.amazonaws.com",
    "eventName": "GetSupportTroubleshootingResponse",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "conversationId": "..."
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
```

```
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

# AWS SupportAWS SDK와 함께 사용

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

| SDK 설명서 | 코드 예시 |
| --- | --- |
| AWS SDK for C++ | AWS SDK for C++ 코드 예제 |
| AWS CLI | AWS CLI 코드 예제 |
| AWS SDK for Go | AWS SDK for Go 코드 예제 |
| AWS SDK for Java | AWS SDK for Java 코드 예제 |
| AWS SDK for JavaScript | AWS SDK for JavaScript 코드 예제 |
| AWS SDK for Kotlin | AWS SDK for Kotlin 코드 예제 |
| AWS SDK for .NET | AWS SDK for .NET 코드 예제 |
| AWS SDK for PHP | AWS SDK for PHP 코드 예제 |
| AWS Tools for PowerShell | PowerShell 코드 예제를 위한 도구 |
| AWS SDK for Python (Boto3) | AWS SDK for Python (Boto3) 코드 예제 |
| AWS SDK for Ruby | AWS SDK for Ruby 코드 예제 |
| AWS SDK for Rust | AWS SDK for Rust 코드 예제 |
| AWS SDK for SAP ABAP | AWS SDK for SAP ABAP 코드 예제 |

| SDK 설명서 | 코드 예시 |
| --- | --- |
| AWS SDK for Swift | AWS SDK for Swift 코드 예제 |

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

# AWS Support API 소개

이 AWS Support API는 AWS지원 센터의 일부 기능에 대한 액세스를 제공합니다.

이 API는 현재 다음과 같은 두 가지 그룹의 작업을 제공합니다.

- 지원 사례 관리 작업을 통해 생성에서 해결에 이르기까지 AWS 지원 사례의 전체 수명 주기를 관리할 수 있습니다.
- AWS Trusted Advisor 검사에 액세스하기 위한 AWS Trusted Advisor 작업

> **Note**
>
> 해당 AWS Support API를 사용하려면 Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있어야 합니다. 자세히 알아보려면 AWS Support의 내용을 참조하세요.

AWS Support에서 제공하는 작업 및 데이터 유형에 대한 자세한 내용은 AWS Support API 참조 섹션을 참조하세요.

주제


- 지원 사례 관리
- AWS Trusted Advisor
- 엔드포인트
- AWS SDK 지원


## 지원 사례 관리

API를 사용하여 다음 작업을 수행할 수 있습니다.

- 지원 사례 열기
- 최근 지원 사례에 대한 목록 및 세부 정보 획득
- 해결된 사례를 포함하여 날짜와 사례 식별자별로 지원 사례 검색 범위 필터링
- 사례에 통신 수단 및 파일 첨부를 추가하고 사례 대응용으로 이메일 수신자를 추가합니다. 최대 3개의 파일을 첨부할 수 있습니다. 각 파일의 크기는 최대 5MB까지입니다
- 사례 해결

AWS SupportAPI는 지원 사례 관리 작업에 대한 CloudTrail 로깅을 지원합니다. 자세히 알아보려면 AWS CloudTrail을 사용하여 AWS Support API 호출 로깅의 내용을 참조하세요.

예를 들어 지원 사례의 전체 수명 주기를 관리하는 방법을 설명하는 코드 예제는 Code examples for AWS Support using AWS SDKs 섹션을 참조하세요.

## AWS Trusted Advisor

Trusted Advisor 작업으로 다음 과제를 수행할 수 있습니다.

- Trusted Advisor 검사의 이름과 식별자를 얻습니다.
- AWS 계정 및 리소스에 대해 Trusted Advisor 검사를 실행하도록 요청합니다.
- Trusted Advisor 검사에 대한 요약 및 세부 정보를 얻습니다.
- Trusted Advisor 검사 새로고침
- Trusted Advisor 검사의 각의 상태를 가져옵니다.

AWS SupportAPI는 Trusted Advisor 작업 CloudTrail 로깅을 지원합니다. 자세히 알아보려면 CloudTrail 로그 기록의 AWS Trusted Advisor 정보의 내용을 참조하세요.

Amazon CloudWatch Events를 사용하여 검사 결과의 변경 사항을 모니터링할 수 Trusted Advisor 있습니다. 자세히 알아보려면 Amazon을 통한 AWS Trusted Advisor 검사 결과 모니터링 EventBridge의 내용을 참조하세요.

예를 들어 Trusted Advisor 작업을 사용하는 방법을 보여 주는 Java 코드는 웹 Trusted Advisor 서비스로 사용 단원을 참조하십시오.

## 엔드포인트

AWS Support는 전역적 서비스입니다. 즉, 사용하는 모든 엔드포인트가 지원 센터 콘솔에서 지원 사례를 업데이트합니다.

예를 들어 미국 동부(버지니아 북부) 엔드포인트를 사용하여 사례를 만들면 미국 서부(오레곤) 또는 유럽(아일랜드) 엔드포인트를 사용하여 동일한 사례에 대한 대응 서신을 추가할 수 있습니다.

AWS Support API에 다음 엔드포인트를 사용할 수 있습니다.

- 미국 동부(버지니아 북부) – https://support.us-east-1.amazonaws.com
- 미국 서부(오레곤) – https://support.us-west-2.amazonaws.com

- 유럽(아일랜드) – https://support.eu-west-1.amazonaws.com

> **Important**
>
> - 테스트 지원 사례를 생성하기 위해 CreateCase작업을 호출하는 경우 제목 줄 (예: TEST Case) 을 포함하는 것이 좋습니다. 무시하십시오. 테스트 지원 케이스를 모두 작성한 후 ResolveCase오퍼레이션을 호출하여 문제를 해결하세요.
> - AWS Support API에서 AWS Trusted Advisor 작업을 호출하려면 미국 동부(버지니아 북부) 엔드포인트를 사용해야 합니다. 현재, 미국 서부(오레곤) 및 유럽(아일랜드) 엔드포인트에서는Trusted Advisor 작업이 지원되지 않습니다.

AWS 엔드포인트에 대한 자세한 내용은 Amazon Web Services 일반 참조의 AWS Support 엔드포인트 및 할당량을 참조하세요.

# AWS SDK 지원

AWS Command Line Interface(AWS CLI) 및 AWS 소프트웨어 개발 키트(SDK)에는 AWS Support API에 대한 지원이 포함됩니다.

AWS SupportAPI를 지원하는 언어 목록을 보려면 작업 이름 (예:) 을 선택하고 CreateCase, 참조 항목 섹션에서 원하는 언어를 선택합니다.

# AWS Support 플랜

비즈니스 요구 사항에 따라 계정의 AWS Support 플랜을 변경할 수 있습니다.

주제


- AWS Support 플랜의 특징
- AWS Support 플랜 변경


## AWS Support 플랜의 특징

AWS Support 다섯 가지 지원 플랜을 제공합니다.

- 기본
- 개발자
- 업무
- Enterprise On-Ramp
- 엔터프라이즈

기본(Basic) 플랜은 계정 및 결제 관련 질문과 서비스 할당량 증가에 대한 지원을 제공합니다. 다른 플랜은 장기 계약 없이 다양한 기술 지원 사례를 pay-by-the-month 가격 책정과 함께 제공합니다.

모든 AWS 고객은 자동으로 다음과 같은 Basic Support 기능에 연중무휴 액세스할 수 있습니다.

- 계정 및 ne-on-one 청구 질문에 대한 응답 없음
- 지원 포럼
- 서비스 상태 점검
- 문서, 백서 및 모범 사례 가이드

개발자 지원(Developer Support) 플랜을 보유한 고객은 다음과 같은 추가 기능에 액세스할 수 있습니다.

- 모범 사례 안내
- 고객 PC 진단 도구
- 빌딩 블록 아키텍처 지원: AWS 제품, 기능, 서비스를 함께 사용하는 방법에 대한 지침

- 권한이 있는 모든 사용자가 열 수 있는 지원 사례를 무제한으로 지원합니다.

또한 Business, Enterprise On-Ramp 또는 Enterprise Support 플랜을 보유한 고객은 다음 기능에 액세스할 수 있습니다.

- 사용 사례 지침 — 특정 요구 사항을 가장 잘 지원하기 위해 사용할 AWS 제품, 기능 및 서비스
- AWS Trusted Advisor— 고객 환경을 검사하여 비용을 절감하고 AWS Support, 보안 격차를 해소하고, 시스템 신뢰성 및 성능을 개선할 기회를 식별하는 기능입니다. 모든 Trusted Advisor 검사 항목에 액세스할 수 있습니다.
- 지원 센터와 상호 작용하기 위한 AWS Support API 및 Trusted Advisor. AWS Support API를 사용하면 지원 사례 관리 및 Trusted Advisor 작업을 자동화할 수 있습니다.
- 서드 파티 소프트웨어 지원 – Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 운영 체제 및 구성에 도움이 됩니다. 또한 에서 가장 인기 있는 타사 소프트웨어 구성 요소의 성능에 대한 도움을 받을 수 AWS있습니다. 기본(Basic) 또는 개발자 지원(Developer Support) 플랜 고객은 서드 파티 소프트웨어 지원을 이용할 수 없습니다.
- 기술 지원 사례를 열 수 있는 AWS Identity and Access Management (IAM) 사용자를 무제한으로 지원합니다.

또한 Enterprise On-Ramp 또는 Enterprise Support 플랜을 보유한 고객은 다음 기능에 액세스할 수 있습니다.

- 애플리케이션 아키텍처 지침 - 특정 사용 사례, 워크로드 또는 애플리케이션에 맞춰 서비스를 구성하는 컨설팅 지침입니다.
- 인프라 이벤트 관리 – AWS Support 와의 단기간 계약을 통해 사용 사례를 깊이 이해할 수 있습니다. 분석 후 이벤트에 대한 아키텍처 및 확장 지침을 제공합니다.
- 테크니컬 어카운트 관리자 - 특정 사용 사례 및 애플리케이션에 대해 테크니컬 어카운트 관리자(TAM)와 협력합니다.
- 화이트 글로브 사례 전달.
- 관리 사업 평가.

각 지원 플랜의 기능 및 가격에 대한 자세한 내용은 AWS Support 플랜 AWS Support비교를 참조하십시오. 연중무휴 24시간 전화 및 채팅 지원과 같은 일부 기능은 일부 언어로만 사용 가능합니다.

# AWS Support 플랜 변경

AWS Support 플랜 콘솔을 사용하여 지원 플랜을 변경할 수 있습니다 AWS 계정. 지원 플랜을 변경하려면 AWS Identity and Access Management (IAM) 권한이 있거나 계정에 루트 사용자로 로그인해야 합니다. 자세한 내용은 플랜에 대한 액세스 관리 AWS Support 및 AWSAWS Support 플랜의 관리형 정책 단원을 참조하세요.

지원 플랜을 변경하려면

1. https://console.aws.amazon.com/support/plans/home 에서 AWS Support 플랜 콘솔에 로그인합니다.
2. (선택 사항) AWS Support Plans 페이지에서 지원 플랜을 비교합니다. 요금에 대한 자세한 내용은 pricing detail(요금 세부 정보) 페이지를 참조하세요.
3. (선택 사항) AWS Support pricing example에서 See examples(예시 참조)를 선택한 다음 지원 플랜 옵션 중 하나를 선택하여 예상 비용을 확인합니다.
4. 플랜을 결정할 때 원하는 플랜에 대해 Review downgrade(다운그레이드 검토) 또는 Review upgrade(업그레이드 검토)를 선택합니다.

   > 참고
   >
   > - 유료 지원 플랜에 가입하는 경우 AWS Support를 최소 1개월 이상 구독해야 합니다. 자세한 내용은 AWS Support FAQ를 참조하십시오.
   > - Enterprise On-Ramp 또는 Enterprise Support 플랜을 보유한 경우 Change plan confirmation(플랜 변경 확인) 대화 상자에서 AWS Support에 문의하여 지원 플랜을 변경하세요.

5. Change plan confirmation(플랜 변경 확인) 대화 상자에서 지원 항목을 확장하여 계정에서 추가하거나 제거하려는 기능을 볼 수 있습니다.

   Pricing(요금)에서 새 지원 플랜에 대해 예상되는 일회성 요금을 볼 수 있습니다.
6. Accept and agree(수락 및 동의)를 선택합니다.

## 관련 정보

AWS Support 플랜에 대한 자세한 내용은 AWS Support FAQ를 참조하십시오. 지원 플랜 콘솔에서 Contact us(문의처)를 선택할 수도 있습니다.

계정을 닫으려면 AWS Billing 사용 설명서의 Closing an Account(계정 닫기)를 참조하세요.

# AWS Trusted Advisor

Trusted Advisor 수십만 명의 AWS 고객에게 서비스를 제공하면서 배운 모범 사례를 활용합니다. Trusted Advisor AWS 환경을 검사한 다음 비용을 절감하고, 시스템 가용성 및 성능을 개선하거나, 보안 격차를 줄이는 데 도움이 되는 기회가 있을 때 권장 사항을 제시합니다.

Basic 또는 Developer Support 플랜을 사용하는 경우 Trusted Advisor 콘솔을 사용하여 서비스 제한 범주의 모든 검사와 보안 범주의 6개 검사에 액세스할 수 있습니다.

비즈니스, 엔터프라이즈 온램프 또는 Enterprise Support 플랜을 사용하는 경우 Trusted Advisor 콘솔과 AWS Trusted Advisor API를 사용하여 모든 Trusted Advisor 검사에 액세스할 수 있습니다. Amazon CloudWatch Events를 사용하여 Trusted Advisor 검사 상태를 모니터링할 수도 있습니다. 자세한 설명은 Amazon을 통한 AWS Trusted Advisor 검사 결과 모니터링 EventBridge 섹션을 참조하세요.

Trusted Advisor 에서 액세스할 수 있습니다 AWS Management Console. Trusted Advisor 콘솔 액세스 제어에 대한 자세한 내용은 을 참조하십시오액세스 관리: AWS Trusted Advisor.

자세한 내용은 Trusted Advisor을(를) 참조하세요.

주제

- Trusted Advisor 권장 사항 시작하기
- Trusted Advisor API로 시작하기
- 웹 Trusted Advisor 서비스로 사용
- AWS Trusted Advisor에 대한 조직 보기
- AWS Config에 의해 구동되는 AWS Trusted Advisor 검사 보기
- AWS Trusted Advisor에서 AWS Security Hub 컨트롤 보기
- Trusted Advisor 수표 AWS Compute Optimizer 신청
- AWS Trusted Advisor Priority 시작하기
- AWS Trusted Advisor 참여(미리 보기) 시작하기
- AWS Trusted Advisor 참조 확인
- 로그 변경 대상 AWS Trusted Advisor

# Trusted Advisor 권장 사항 시작하기

Trusted Advisor 콘솔의 Trusted Advisor 권장 사항 페이지를 사용하여 검사 결과를 검토한 다음 권장 단계에 따라 문제를 해결할 수 있습니다. AWS 계정 예를 들어, Trusted Advisor 는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 등의 사용하지 않는 리소스는 월별 청구 금액을 줄이기 위해 삭제할 것을 권장할 수 있습니다.

AWS Trusted Advisor API를 사용하여 Trusted Advisor 검사에 대한 작업을 수행할 수도 있습니다. 자세한 내용은 AWS Trusted Advisor API 참조를 참조하십시오.

주제


- Trusted Advisor 콘솔에 로그인
- 검사 범주 보기
- 특정 검사 보기
- 검사 필터링
- 검사 결과 새로 고침
- 검사 결과 다운로드
- 조직 보기
- 기본 설정


## Trusted Advisor 콘솔에 로그인

Trusted Advisor 콘솔에서 검사 및 각 검사의 상태를 볼 수 있습니다.

> **Note**
>
> Trusted Advisor 콘솔에 액세스하려면 AWS Identity and Access Management (IAM) 권한이 있어야 합니다. 자세한 정보는 액세스 관리: AWS Trusted Advisor을 참조하세요.

콘솔에 로그인하려면 Trusted Advisor

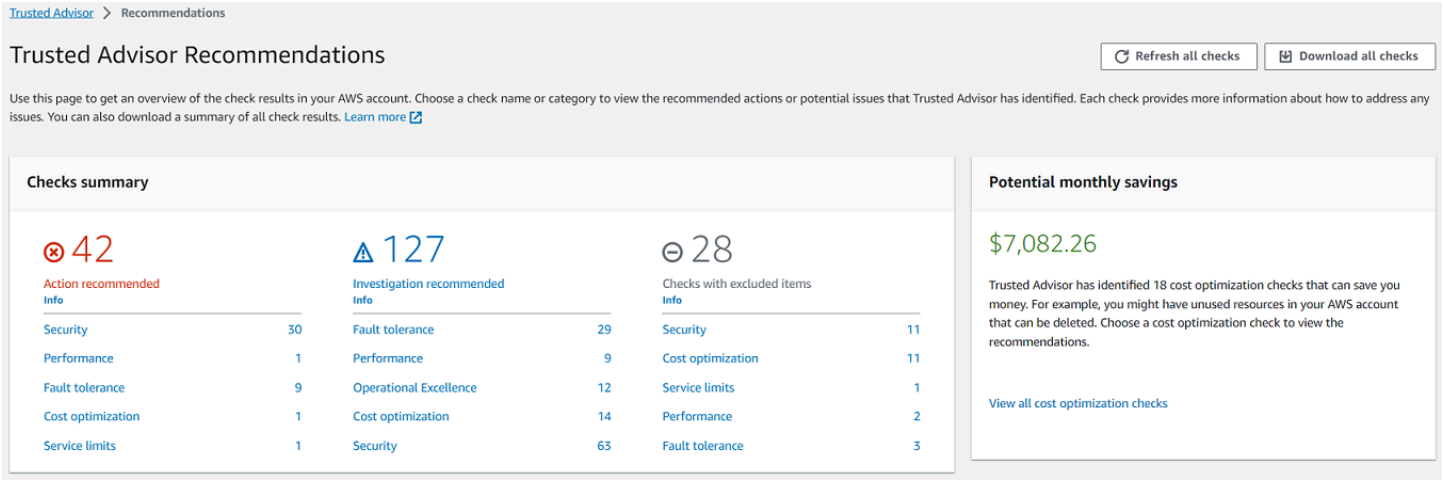
1. https://console.aws.amazon.com/trustedadvisor/home 에서 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor 권장 사항 페이지에서 각 검사 범주에 대한 요약을 봅니다.

- 조치 권장 (빨간색) - 확인을 위한 조치를 Trusted Advisor 권장합니다. 예를 들어 IAM 리소스에 대한 보안 문제를 감지하는 검사에서 긴급하게 단계를 진행할 것을 권장할 수 있습니다.
- 조사 권장(노란색) – Trusted Advisor 가 검사 가능한 문제를 감지합니다. 예를 들어 검사에서 리소스가 할당량에 도달했다면 사용되지 않는 리소스를 삭제하는 방법을 권장할 수 있습니다.
- 제외된 항목이 있는 검사(회색) – 제외된 항목(예: 검사에서 무시할 리소스)이 있는 검사의 수입니다. 예를 들어, 이것은 검사에서 평가하고 싶지 않은 Amazon EC2 인스턴스일 수 있습니다.

3. Trusted Advisor 권장 사항 페이지에서 다음을 수행할 수 있습니다.
   - 계정의 모든 검사를 새로 고치려면 모든 검사 새로 고침(Refresh all checks)을 선택합니다.
   - 모든 검사 결과를 포함하는.xls 파일을 만들려면 모든 검사 다운로드(Download all checks)를 선택합니다.
   - 검사 요약에서 보안 등의 검사 범주를 선택하여 결과를 봅니다.
   - 잠재적 월별 비용 절감에서 계정에서 절약할 수 있는 금액과 권장 사항에 대한 비용 최적화 검사를 확인할 수 있습니다.
   - 최근 변경 사항(Recent changes)에서, 지난 30일 이내의 상태를 확인하기 위해 변경 사항을 검토할 수 있습니다. 검사 이름을 선택하여 해당 검사에 대한 최신 결과를 보거나 화살표 아이콘을 선택하여 다음 페이지를 봅니다.

Example : Trusted Advisor 권장 사항

다음 예제는 AWS 계정에 대한 검사 결과의 요약을 보여줍니다.




# 검사 범주 보기

다음 검사 범주에 대한 검사 설명 및 결과를 볼 수 있습니다.

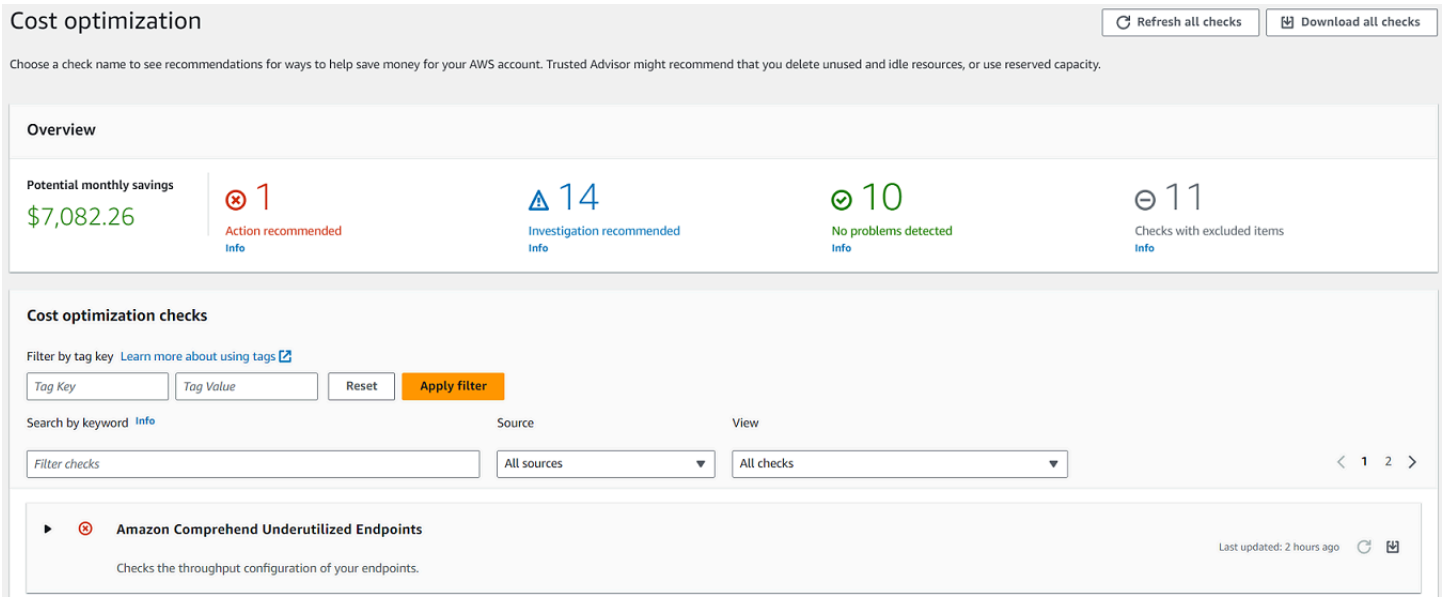
- 비용 최적화 - 잠재적으로 비용을 절약할 수 있는 권장 사항입니다. 해당 검사는 사용되지 않는 리소스와, 청구 금액을 줄일 수 있는 기회를 강조 표시합니다.
- 성능(performance) - 애플리케이션의 속도와 응답성을 향상할 수 있는 권장 사항입니다.
- 보안 - AWS 솔루션의 보안을 강화할 수 있는 보안 설정에 대한 권장 사항입니다.
- 내결함성 — AWS 솔루션의 복원력을 높이는 데 도움이 되는 권장 사항. 이러한 검사를 통해 중복성 부족과 리소스 과다 사용을 확인할 수 있습니다.
- 서비스 한도 - 계정 사용량을 확인하고 계정이 AWS 서비스 및 리소스 한도(할당량이라고도 함)에 도달하거나 한도를 초과하는지 확인합니다.
- 운영 우수성 — AWS 환경을 대규모로 효과적으로 운영하는 데 도움이 되는 권장 사항.

검사 범주를 보려면

1. https://console.aws.amazon.com/trustedadvisor/home 에서 Trusted Advisor 콘솔에 로그인합니다.
2. 탐색 창에서 검사 범주를 선택합니다.
3. 범주 페이지에서 각 검사 범주에 대한 요약을 봅니다.
   - 조치 권장 (빨간색) - 확인을 위한 조치를 Trusted Advisor 권장합니다.
   - 조사 권장(노란색) – Trusted Advisor 가 검사 대상이 될 수 있는 문제를 감지합니다.
   - 감지된 문제 없음 (녹색) — 검사 시 문제가 Trusted Advisor 감지되지 않습니다.
   - 제외된 항목(회색) - 제외된 항목(예: 검사에서 무시할 리소스)이 있는 검사의 수입니다.
4. 각 검사에 대해 새로 고침 아이콨
   ( )
   을 사용하여 해당 검사를 새로 고치세요.
5. 다운로드 아이콘
   ( )
   을 선택하여 해당 검사 결과를 포함하는.xls 파일을 만드세요

Example : 비용 최적화 범주

다음 예는 문제가 없는 검사 10개 (녹색) 를 보여줍니다.




# 특정 검사 보기

검사를 확장하면 전체 검사 설명, 영향을 받는 리소스, 권장 단계 및 추가 정보 링크를 볼 수 있습니다.

특정 검사를 보려면

1. https://console.aws.amazon.com/trustedadvisor/home 에서 Trusted Advisor 콘솔에 로그인합니다.
2. 탐색 창에서 검사 범주를 하나 선택합니다.
3. 검사 이름을 선택하여 설명 및 다음 세부 정보를 봅니다.
   - 알림 기준(Alert Criteria) - 검사 상태가 변경될 때의 임계값을 설명합니다.
   - 권장 작업(Recommended Action) - 이 검사에 권장되는 작업에 대해 설명합니다.
   - 추가 리소스(Additional Resources) - 관련 AWS 문서의 목록을 만듭니다.
   - 계정에서 영향을 받는 항목을 나열하는 테이블입니다. 검사 결과에서 이러한 항목을 포함하거나 제외할 수 있습니다.
4. (선택 사항) 검사 결과에 나타나지 않도록 항목을 제외하려면 다음을 수행하세요.
   a. 항목을 선택하고 제외 및 새로 고침(Exclude & Refresh)을 선택합니다.
   b. 제외된 모든 항목을 보려면 제외된 항목(Excluded items)을 선택합니다.
5. (선택 사항) 검사에서 항목을 다시 평가할 수 있도록 항목을 포함하려면 다음을 수행하세요.

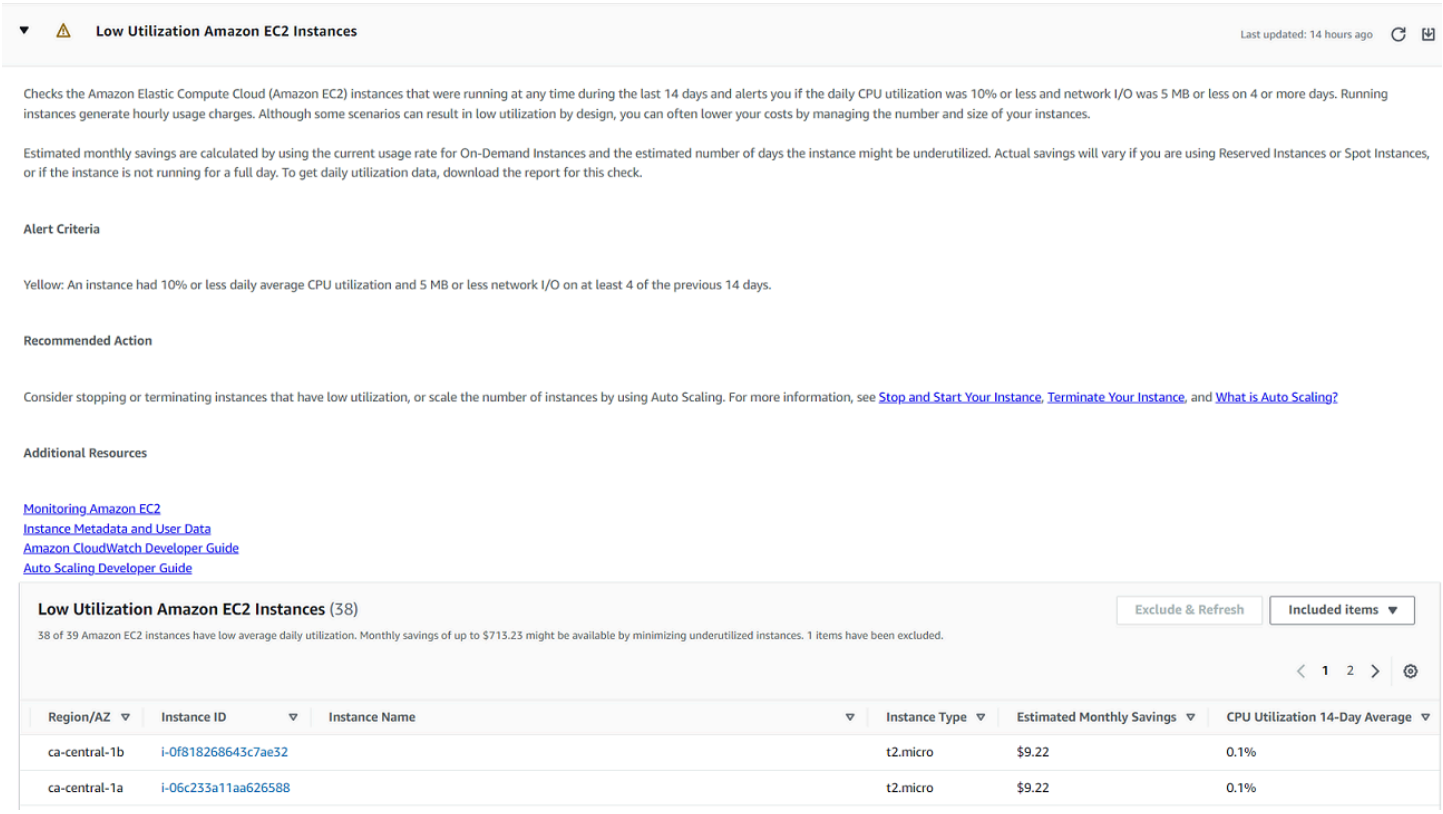
a. 제외된 항목(Excluded items)을 선택하고, 항목을 선택한 다음, 포함 및 새로고침(nclude & Refresh)을 선택합니다.

b. 포함된 모든 항목을 보려면 포함된 항목(Included items)을 선택합니다.

6. 설정 아이콘 ( ) 을 선택합니다. Preferences(기본 설정) 대화 상자에서 표시할 항목 수 또는 속성을 지정한 다음 Confirm(확인)을 선택합니다.

Example : 비용 최적화 검사

다음의 사용률이 낮은 Amazon EC2 인스턴스(Low Utilization Amazon EC2 Instances)검사는 계정에서 영향을 받는 인스턴스를 나열합니다. 이 검사는 사용량이 적은 Amazon EC2 인스턴스 38개를 식별하고 리소스를 중지하거나 종료할 것을 권장합니다.




# 검사 필터링

검사 범주 페이지에서, 보려는 검사 결과를 지정할 수 있습니다. 예를 들어 계정에서 오류가 감지된 검사를 기준으로 필터링하여 긴급한 문제를 먼저 조사할 수 있습니다.

계정의 항목 (예: AWS 리소스) 을 평가하는 검사가 있는 경우 태그 필터를 사용하여 지정된 태그가 있는 항목만 표시할 수 있습니다.

검사를 필터링하려면

1. https://console.aws.amazon.com/trustedadvisor/home 에서 Trusted Advisor 콘솔에 로그인합니다.
2. 탐색 창이나 Trusted Advisor 권장 사항 페이지에서 검사 범주를 선택합니다.
3. 키워드로 검색하려면 검사 이름이나 설명의 키워드를 입력하여 결과를 필터링합니다.
4. 보기(View)목록에서, 보려는 검사를 지정합니다.
   - 모든 검사(All checks) - 이 범주에 대한 모든 검사를 나열합니다.
   - 작업 권장(Action recommended) - 작업를 취하도록 권장하는 검사를 나열합니다. 해당 검사는 빨간색으로 강조 표시됩니다.
   - 조사 권장(Investigation recommended) - 가능한 조치를 취하도록 권장하는 검사를 나열합니다. 해당 검사는 노란색으로 강조 표시됩니다.
   - 문제가 감지되지 않음(No problems detected)— 문제가 없는 검사를 나열합니다. 해당 검사는 녹색으로 강조 표시됩니다.
   - 제외된 항목이 있는 검사(Checks with excluded items) - 검사 결과에서 항목을 제외하도록 지정한 검사를 나열합니다.
5. Amazon EC2 인스턴스 또는 AWS CloudTrail 트레일과 같은 AWS 리소스에 태그를 추가한 경우 검사 시 지정된 태그가 있는 항목만 표시되도록 결과를 필터링할 수 있습니다.

   태그 기준으로 필터링(Filter by tag)에 태그 키와 값을 입력한 다음 필터 적용(앱ly filter)을 선택합니다.
6. 검사 테이블에서, 지정된 키와 값을 가진 항목만 검사 결과에 표시됩니다.
7. 태그별 필터를 지우려면 재설정(Reset)을 선택합니다.

## 관련 정보

의 태깅에 대한 자세한 내용은 다음 Trusted Advisor주제를 참조하십시오.

- AWS Support 다음에 대한 태깅 기능을 활성화합니다. Trusted Advisor
- AWS 일반 참조에서 AWS 리소스 태그 지정

# 검사 결과 새로 고침

검사를 새로 고쳐 계정에 대한 최신 결과를 얻을 수 있습니다. Developer 또는 Basic Support 플랜을 사용 중인 경우 Trusted Advisor 콘솔에 로그인하여 확인 내용을 새로 고칠 수 있습니다. 비즈니스, Enterprise On-Ramp 또는 Enterprise Support 플랜을 사용하는 경우 계정 점검 내용이 매주 Trusted Advisor 자동으로 새로 고쳐집니다.

수표를 새로 고치려면 Trusted Advisor

1. https://console.aws.amazon.com/trustedadvisor 에서 AWS Trusted Advisor 콘솔로 이동합니다.
2. Trusted Advisor 권장 사항 또는 검사 범주 페이지에서 모든 검사 새로 고침을 선택합니다.

또한 다음과 같은 방법으로도 특정 검사를 새로 고침할 수 있습니다.

- 개별 검사에 대해 새로 고침 아이콘
  ( )
  을 선택합니다.
- RefreshTrustedAdvisorCheck API 작업을 사용합니다.

> 참고
>
> - Trusted Advisor 신뢰성 검사의 고위험 문제와 같은 일부 검사를 하루에 여러 번 자동으로 새로 AWS Well-Architected 고칩니다. 계정에 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 이러한 자동 새로 고침 검사의 경우 새로 고침 아이콘
>   ( )
>   을 선택하여 수동으로 결과를 새로 고칠 수 없습니다.
> - 계정을 AWS Security Hub 활성화한 경우 Trusted Advisor 콘솔을 사용하여 Security Hub 컨트롤을 새로 고칠 수 없습니다. 자세한 정보는 Security Hub 결과 새로 고침을 참조하세요.

# 검사 결과 다운로드

검사 결과를 다운로드하여 계정에 대한 Trusted Advisor 개요를 확인할 수 있습니다. 모든 검사 또는 특정 검사의 결과를 다운로드할 수 있습니다.

Trusted Advisor 권장 사항에서 검사 결과를 다운로드하려면

1. https://console.aws.amazon.com/trustedadvisor 에서 AWS Trusted Advisor 콘솔로 이동하십시오.
   - 모든 검사 결과를 다운로드하려면 Trusted Advisor 권장 사항 또는 검사 범주 페이지에서 모든 검사 다운로드를 선택합니다.
   - 특정 검사의 결과를 다운로드하려면 검사 이름을 선택하고 다운로드 아이콘 ( ) 을 선택합니다.
2. .xls 파일을 저장하거나 엽니다. 이 파일은 검사 이름, 설명, 상태, 영향을 받는 리소스 등 Trusted Advisor 콘솔의 요약 정보와 동일한 정보를 포함합니다.

## 조직 보기

조직 보기 기능을 설정하여 AWS 조직의 모든 구성원 계정에 대한 보고서를 만들 수 있습니다. 자세한 정보는 AWS Trusted Advisor에 대한 조직 보기을 참조하세요.

## 기본 설정

Trusted Advisor관리 페이지에서 Trusted Advisor를 비활성화할 수 있습니다.

알림(Notifications) 페이지에서 검사 요약에 대한 주간 이메일 메시지를 구성할 수 있습니다. 알림 기본 설정 지정를 참조하세요.

내 기관 페이지에서 을 사용하여 신뢰할 수 있는 액세스를 활성화하거나 비활성화할 수 AWS Organizations있습니다. 이는 AWS Trusted Advisor에 대한 조직 보기 기능 및 Trusted Advisor 우선순위 및 Trusted Advisor 참여에 필요합니다.

### 알림 기본 설정 지정

검사 결과 및 언어에 대한 주간 Trusted Advisor 이메일 메시지를 받을 수 있는 사람을 지정합니다. 일주일에 한 번 Trusted Advisor 권장 사항에 대한 확인 요약에 대한 이메일 알림을 받게 됩니다.

Trusted Advisor 권장 사항에 대한 이메일 알림에는 Trusted Advisor Priority에 대한 결과가 포함되지 않습니다. 자세한 정보는 Trusted Advisor Priority 알림 관리을 참조하세요.

알림에 대한 기본 설정을 지정하려면

1. https://console.aws.amazon.com/trustedadvisor/home 에서 Trusted Advisor 콘솔에 로그인합니다.

2. 탐색 창의 Preferences(기본 설정)에서 Notifications(알림)를 선택합니다.
3. Recommendations(권장 사항)에서 검사 결과에 대해 알릴 대상을 선택합니다. AWS Billing and Cost Management 콘솔의 계정 설정 페이지에서 연락처를 추가 및 제거할 수 있습니다.
4. 언어(Language)에서 이메일 메시지에 사용할 언어를 선택합니다.
5. Save your preferences(기본 설정 저장)를 선택합니다.

## 조직 보기 설정

로 AWS Organizations계정을 설정하면 조직의 모든 구성원 계정에 대한 보고서를 만들 수 있습니다. 자세한 정보는 AWS Trusted Advisor에 대한 조직 보기을 참조하세요.

## 비활성화 Trusted Advisor

이 서비스를 비활성화하면 계정에 대한 확인이 Trusted Advisor 수행되지 않습니다. Trusted Advisor 콘솔에 액세스하거나 API 작업을 사용하려고 시도하는 모든 사용자에게 액세스 거부 오류 메시지가 표시됩니다.

비활성화하려면 Trusted Advisor

1. https://console.aws.amazon.com/trustedadvisor/home 에서 Trusted Advisor 콘솔에 로그인합니다.
2. 탐색 창의 Preferences(기본 설정)에서 Manage Trusted Advisor를 선택합니다.
3. Trusted Advisor에서 Enabled(활성)를 해제합니다. 이 작업을 수행하면 계정에 Trusted Advisor 있는 모든 체크가 비활성화됩니다.
4. 그런 다음 계정에서 AWSServiceRoleForTrustedAdvisor Trusted Advisor 수동으로 삭제할 수 있습니다. 자세한 정보는 Trusted Advisor에 대한 서비스 링크 역할 삭제을 참조하세요.

## 관련 정보

에 대한 Trusted Advisor자세한 내용은 다음 항목을 참조하십시오.

- 어떻게 사용을 시작하나요 Trusted Advisor?
- AWS Trusted Advisor 참조 확인

# Trusted Advisor API로 시작하기

AWS Trusted Advisor API 참조는 Trusted Advisor API 작업 및 데이터 유형에 대한 자세한 정보가 필요한 프로그래머를 위한 것입니다. 이 API를 사용하면 사용자 계정 또는 AWS 조직 내 모든 계정에 대한 Trusted Advisor 권장 사항에 액세스할 수 있습니다. Trusted Advisor API는 JSON 형식으로 결과를 반환하는 HTTP 메서드를 사용합니다.

> **Note**
>
> - API를 사용하려면 비즈니스, 엔터프라이즈 온램프 또는 엔터프라이즈 지원 플랜이 있어야 합니다. Trusted Advisor
> - 비즈니스, Enterprise On-Ramp 또는 Enterprise Support 플랜이 없는 계정에서 AWS Trusted Advisor API를 호출하면 액세스 거부 예외가 발생합니다. 지원 플랜 변경에 대한 자세한 내용은 AWS Support를 참조하십시오.

AWS Trusted Advisor API를 사용하여 검사 목록과 해당 설명, 권장 사항, 권장 사항 및 권장 사항 리소스를 가져올 수 있습니다. 권장 사항의 수명 주기를 업데이트할 수도 있습니다. 권장 사항을 관리하려면 다음 API 작업을 사용하십시오.

- ListChecks, ListRecommendationsGetRecommendation, 및 ListRecommendationResourcesAPI 작업을 사용하여 권장 사항과 해당 계정 및 리소스를 볼 수 있습니다.
- UpdateRecommendationLifecycleAPI 작업을 사용하면 Trusted Advisor Priority에서 관리하는 권장 사항의 수명 주기를 업데이트할 수 있습니다.
- BatchUpdateRecommendationResourceExclusionAPI 작업을 사용하여 Trusted Advisor 결과에서 하나 이상의 리소스를 포함하거나 제외할 수 있습니다.
- ListOrganizationRecommendations,, GetOrganizationRecommendationListOrganizationRecommendationResourcesListOrganizationRecommer 및 UpdateOrganizationRecommendationLifecycleAPI 호출은 Trusted Advisor Priority에서 관리하는 권장 사항만 지원합니다. 이러한 권장 사항을 우선 순위가 지정된 권장 사항이라고도 합니다. Trusted Advisor Priority를 활성화한 경우 관리 또는 위임된 관리자 계정에서 우선 순위가 지정된 권장 사항을 보고 관리할 수 있습니다. 우선 순위가 활성화되지 않은 경우 요청 시 액세스 거부 예외가 발생합니다.

자세한 내용은 AWS Support 사용 설명서를 참조하십시오 AWS Trusted Advisor .

요청 인증에 대해서는 서명 버전 4 서명 프로세스를 참조하십시오.

# 웹 Trusted Advisor 서비스로 사용

> **Note**
>
> Trusted Advisor 2024년에는 AWS Trusted Advisor Support API에서 작업을 지원하지 않을 예정입니다. 새 AWS Trusted Advisor API를 사용하여 모범 사례 검사 및 권장 사항에 프로그래밍 방식으로 액세스하세요.

이 AWS Support 서비스를 사용하면 상호 작용하는 AWS Trusted Advisor애플리케이션을 작성할 수 있습니다. 이 항목에서는 검사 목록을 가져와 Trusted Advisor 검사 중 하나를 새로 고친 다음 검사의 세부 결과를 가져오는 방법을 보여 줍니다. 이러한 작업은 Java로 설명되어 있습니다. 다른 언어 지원에 대한 정보는 Amazon Web Services용 도구를 참조하십시오.

주제

- 사용 가능한 Trusted Advisor 검사 목록 가져오기
- 사용 가능한 Trusted Advisor 검사 목록을 새로 고치세요.
- 상태 변경 Trusted Advisor 여부를 확인하기 위해 검사를 폴링합니다.
- Trusted Advisor 검사 결과 요청
- Trusted Advisor 수표 세부 정보 보기

## 사용 가능한 Trusted Advisor 검사 목록 가져오기

다음 Java 코드 스니펫은 모든 Trusted Advisor API 작업을 호출하는 데 사용할 수 있는 AWS Support 클라이언트 인스턴스를 만듭니다. 그런 다음 코드는 DescribeTrustedAdvisorChecksAPI 작업을 호출하여 Trusted Advisor 검사 목록과 해당 `CheckId` 값을 가져옵니다. 이 정보를 사용하여 사용자가 실행하거나 새로 고치려는 검사를 선택할 수 있게 허용하는 사용자 인터페이스를 구축할 수 있습니다.

```
private static AWSSupport createClient()
{
    return AWSSupportClientBuilder.defaultClient();
}
// Get the List of Available Trusted Advisor Checks
public static void getTAChecks() {
```

```
    // Possible language parameters: "en" (English), "ja" (Japanese), "fr" (French),
 "zh" (Chinese)
    DescribeTrustedAdvisorChecksRequest request = new
 DescribeTrustedAdvisorChecksRequest().withLanguage("en");
    DescribeTrustedAdvisorChecksResult result =
 createClient().describeTrustedAdvisorChecks(request);
    for (TrustedAdvisorCheckDescription description : result.getChecks()) {
        // Do something with check description.
        System.out.println(description.getId());
        System.out.println(description.getName());
    }
}
```

## 사용 가능한 Trusted Advisor 검사 목록을 새로 고치세요.

다음 Java 코드 스니펫은 데이터를 새로 고치는 Trusted Advisor 데 사용할 수 있는 AWS Support 클라이언트 인스턴스를 만듭니다.

```
// Refresh a Trusted Advisor Check
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation.
// Specifying the check ID of a check that is automatically refreshed causes an
 InvalidParameterValue error.
public static void refreshTACheck(final String checkId) {
    RefreshTrustedAdvisorCheckRequest request = new
 RefreshTrustedAdvisorCheckRequest().withCheckId(checkId);
    RefreshTrustedAdvisorCheckResult result =
 createClient().refreshTrustedAdvisorCheck(request);
    System.out.println("CheckId: " + result.getStatus().getCheckId());
    System.out.println("Milliseconds until refreshable: " +
 result.getStatus().getMillisUntilNextRefreshable());
    System.out.println("Refresh Status: " + result.getStatus().getStatus());
}
```

## 상태 변경 Trusted Advisor 여부를 확인하기 위해 검사를 폴링합니다.

최신 상태 데이터를 생성하는 Trusted Advisor 검사 실행 요청을 제출한 후 DescribeTrustedAdvisorCheckRefreshStatusesAPI 작업을 사용하여 검사 실행 진행 상황과 검사에 사용할 새 데이터가 준비되면 이를 요청합니다.

다음 Java 코드 조각은 CheckId 변수에 해당하는 값을 사용하여 다음 단원에서 요청된 검사 상태를 가져옵니다. 또한 코드는 이 Trusted Advisor 서비스를 여러 가지 다른 용도로 사용하는 방법을 보여줍니다.

1. DescribeTrustedAdvisorCheckRefreshStatusesResult 인스턴스에 포함된 객체를 통과하여 getMillisUntilNextRefreshable을 호출할 수 있습니다. 반환된 값을 사용하여 코드로 점검 항목을 새로 고칠 것인지 여부를 테스트할 수 있습니다.
2. timeUntilRefreshable이 0이라면 검사 항목의 새로 고침을 요청할 수 있습니다.
3. 반환된 상태를 사용하여 상태 변경 사항을 계속 폴링할 수 있습니다. 코드 조각은 폴링 간격을 권장하는 값인 10초로 설정합니다. 상태가 enqueued 또는 in_progress인 경우 반복 작업을 반환하며 다른 상태를 요청합니다. 호출이 successful을 반환하면 반복 작업이 종료됩니다.
4. 마지막으로, 코드는 검사를 통해 생성된 정보를 통과하는 데 사용할 수 있는 DescribeTrustedAdvisorCheckResultResult 데이터 형식의 인스턴스를 반환합니다.

참고: 요청 상태를 폴링하기 전에 단일 새로 고침 요청을 사용하십시오.

```
// Retrieves TA refresh statuses. Multiple checkId's can be submitted.
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String...
 checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request =
            new
 DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result =
            createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
}
// Retrieves a TA check status, and checks to see if it has finished processing.
public static boolean isTACheckStatusInTerminalState(final String checkId) {
    // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
    TrustedAdvisorCheckRefreshStatus status = getTARefreshStatus(checkId).get(0);
    // Valid statuses are:
    // 1. "none", the check has never been refreshed before.
    // 2. "enqueued", the check is waiting to be processed.
    // 3. "processing", the check is in the midst of being processed.
    // 4. "success", the check has succeeded and finished processing - refresh data is
 available.
    // 5. "abandoned", the check has failed to process.
    return status.getStatus().equals("abandoned") ||
 status.getStatus().equals("success");
```

```
}
// Enqueues a Trusted Advisor check refresh. Periodically polls the check refresh
 status for completion.
public static TrustedAdvisorCheckResult getFreshTACheckResult(final String checkId)
 throws InterruptedException {
    refreshTACheck(checkId);
    while(!isTACheckStatusInTerminalState(checkId)) {
        Thread.sleep(10000);
    }
    return getTACheckResult(checkId);
}
// Retrieves fresh TA check data whenever possible.
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation. This method
// is only functional for checks that can be refreshed using the
 RefreshTrustedAdvisorCheck operation.
public static void pollForTACheckResultChanges(final String checkId) throws
 InterruptedException {
    String checkResultStatus = null;
    do {
        TrustedAdvisorCheckResult result = getFreshTACheckResult(checkId);
        if (checkResultStatus != null && !checkResultStatus.equals(result.getStatus()))
 {
            break;
        }
        checkResultStatus = result.getStatus();
        // The rule refresh has completed, but due to throttling rules the checks may
 not be refreshed again
        // for a short period of time.
        // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
        TrustedAdvisorCheckRefreshStatus refreshStatus =
 getTARefreshStatus(checkId).get(0);
        Thread.sleep(refreshStatus.getMillisUntilNextRefreshable());
    } while(true);
    // Signal that a TA check has changed check result status here.
}
```

## Trusted Advisor 검사 결과 요청

원하는 세부 결과에 대한 검사를 선택한 후 DescribeTrustedAdvisorCheckResult API 작업을 사용하여 요청을 제출합니다.

> **Tip**
>
> Trusted Advisor 검사의 이름과 설명은 변경될 수 있습니다. 검사를 고유하게 식별하려면 코드에 검사 ID를 지정하는 것이 좋습니다. DescribeTrustedAdvisorChecksAPI 작업을 사용하여 검사 ID를 가져올 수 있습니다.

다음 Java 코드 조각은 이전의 코드 조각에서 얻은 `result` 변수가 참조하는 `DescribeTrustedAdvisorChecksResult` 인스턴스를 사용합니다. 사용자 인터페이스를 통해 대화식으로 검사 항목을 정의하는 대신 해당 조각의 실행 요청을 제출한 후 각 `result.getChecks().get(0)` 호출에서 인덱스 값 0을 지정하여 실행할 목록의 첫 번째 검사 요청을 제출합니다. 그 다음, 해당 코드는 `checkResult`라는 `DescribeTrustedAdvisorCheckResultResult` 인스턴스로 전달되는 `DescribeTrustedAdvisorCheckResultRequest` 인스턴스를 정의합니다. 이 데이터 유형의 멤버 구조를 사용하여 검사 결과를 볼 수 있습니다.

```
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
    DescribeTrustedAdvisorCheckResultRequest request = new
 DescribeTrustedAdvisorCheckResultRequest()
            // Possible language parameters: "en" (English), "ja" (Japanese),
 "fr" (French), "zh" (Chinese)
            .withLanguage("en")
            .withCheckId(checkId);
    DescribeTrustedAdvisorCheckResultResult requestResult =
 createClient().describeTrustedAdvisorCheckResult(request);
    return requestResult.getResult();
}
```

참고: Trusted Advisor 검사 결과를 요청해도 업데이트된 결과 데이터는 생성되지 않습니다.

## Trusted Advisor 수표 세부 정보 보기

다음 Java 코드 스니펫은 이전 섹션에서 반환된 `DescribeTrustedAdvisorCheckResultResult` 인스턴스를 반복하여 검사에서 플래그가 지정된 리소스 목록을 가져옵니다. Trusted Advisor

```
// Show ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
```

```
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

# AWS Trusted Advisor에 대한 조직 보기

조직 보기를 사용하면 Trusted Advisor 검사를 AWS Organizations의 모든 계정에 대하여 검토할 수 있습니다. 이 기능을 활성화한 후 보고서를 만들어 기관의 모든 멤버 계정에 대한 검사 결과를 집계할 수 있습니다. 보고서에는 검사 결과 요약과 각 계정의 영향을 받는 자원에 대한 정보가 포함됩니다. 예를 들어 보고서를 사용하여 조직의 어떤 계정이 IAM 사용 검사에 AWS Identity and Access Management(IAM)를 사용 중인지 또는 Amazon S3 버킷 권한 검사에 권장되는 Amazon Simple Storage Service(Amazon S3) 버킷 작업이 있는지 식별할 수 있습니다.

주제


- 필수 조건
- 조직 보기 활성화
- Trusted Advisor 검사 새로 고침
- 조직 보기 보고서 생성
- 보고서 요약 보기
- 조직 보기 보고서 다운로드
- 조직 보기 비활성화
- IAM 정책을 사용하여 조직 보기에 대한 액세스 허용
- 다른 AWS 서비스를 사용하여 Trusted Advisor 보고서 보기


## 필수 조건

조직 보기를 사용하려면 다음 요구 사항을 충족해야 합니다.

- 귀하의 계정이 AWS 조직의 멤버여야 합니다.
- 조직에서 Organizations의 모든 기능을 활성화해야 합니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하세요.
- 조직의 관리 계정에 Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있어야 합니다. 지원 플랜은 AWS Support 센터 또는 지원 플랜 페이지에서 찾을 수 있습니다. AWS Support 플랜 비교를 참조하세요.

- 관리 계정의 사용자(또는 동등하게 수임한 역할)로 로그인해야 합니다. IAM 사용자 또는 IAM 역할로 로그인하는 경우 필요한 권한을 가진 정책이 있어야 합니다. IAM 정책을 사용하여 조직 보기에 대한 액세스 허용 단원을 참조하세요.

## 조직 보기 활성화

사전 조건을 충족한 후에 조직 보기를 활성화하려면 다음 단계를 따르세요. 이 기능을 활성화하면 다음과 같이 진행됩니다.

- Trusted Advisor가 조직에서 신뢰할 수 있는 서비스로 활성화됩니다. 자세한 내용은 AWS Organizations 사용 설명서의 다른 AWS 서비스로 신뢰할 수 있는 액세스 활성화를 참조하세요.
- `AWSServiceRoleForTrustedAdvisorReporting` 서비스 연결 역할이 조직의 관리 계정에 생성됩니다. 이 역할에는 Trusted Advisor가 사용자를 대신하여 Organizations를 호출하는 데 필요한 권한이 포함되어 있습니다. 이 서비스 연결 역할은 잠겨 있으므로 수동으로 삭제할 수 없습니다. 자세한 내용은 Trusted Advisor의 서비스 링크 역할 사용 단원을 참조하세요.

Trusted Advisor 콘솔에서 조직 보기를 활성화합니다.

조직 보기를 활성화하려면

1. 조직의 관리 계정에 관리자로 로그인한 다음 https://console.aws.amazon.com/trustedadvisor의 AWS Trusted Advisor 콘솔을 엽니다.
2. 탐색 창의 Preferences(기본 설정)에서 Organization(조직)을 선택합니다.
3. Enable trusted access with AWS Organizations에서 Enabled(활성화됨)를 설정합니다.

> **Note**
>
> 관리 계정에 대해 조직 보기를 사용하도록 설정하면 일부 멤버 계정에 대해 동일한 검사가 제공되지 않습니다. 예를 들어 멤버 계정이 모두 Basic Support가 있는 경우 해당 계정은 관리 계정과 동일한 검사를 사용할 수 없습니다. AWS Support 계획에 따라 계정이 사용할 수 있는 Trusted Advisor 검사가 결정됩니다.

# Trusted Advisor 검사 새로 고침

조직에 대한 보고서를 만들기 전에 Trusted Advisor 검사의 상태를 새로 고치는 것이 좋습니다. Trusted Advisor 검사를 새로 고치지 않고 보고서를 다운로드할 수 있지만 보고서에 최신 정보가 없을 수 있습니다.

Business, Enterprise On-Ramp 또는 Enterprise Support 플랜을 보유한 경우 Trusted Advisor에서는 매주 계정의 검사 내용을 자동으로 새로 고칩니다.

> **Note**
>
> 조직의 계정에 개발자(Developer) 또는 기본(Basic) 지원 플랜이 있는 경우 해당 계정의 사용자는 Trusted Advisor 콘솔에 로그인하여 검사를 새로 고쳐야 합니다. 조직의 관리 계정에서 모든 계정에 대한 검사를 새로 고칠 수는 없습니다.

Trusted Advisor 검사를 새로 고치려면

1. https://console.aws.amazon.com/trustedadvisor의 AWS Trusted Advisor콘솔로 이동합니다.
2. Trusted Advisor 권장 사항 페이지에서 모든 검사 새로 고침을 선택합니다. 이렇게 하면 계정에 속한 모든 검사를 새로 고칩니다.

다음과 같은 방법으로 특정 검사를 새로 고칠 수 있습니다.

- RefreshTrustedAdvisorCheck API 작업을 사용합니다.
- 개별 검사에 대해 새로 고침 아이콘 ( ) 을 선택합니다.

# 조직 보기 보고서 생성

조직 보기를 활성화한 후 보고서를 만들어 Trusted Advisor 조직에 대한 검사 결과를 검토할 수 있습니다.

최대 50개의 보고서를 생성할 수 있습니다. 이 할당량을 초과하는 보고서를 만드는 경우 Trusted Advisor가 가장 오래된 보고서를 삭제합니다. 삭제된 보고서는 복구할 수 없습니다.

조직 보기 보고서를 생성하려면

1. 조직의 관리 계정에 로그인한 다음 https://console.aws.amazon.com/trustedadvisor의 AWS Trusted Advisor 콘솔을 엽니다.
2. 탐색 창에서 조직 보기(Organizational View)를 선택합니다.
3. 보고서 생성(Create report)을 선택합니다.
4. 기본적으로 보고서에는 모든 AWS 리전, 검사 범주, 검사 및 리소스 상태가 포함되어 있습니다. 보고서 생성(Create report) 페이지에서 필터 옵션을 사용하여 보고서를 사용자 지정할 수 있습니다. 예를 들어, 리전(Region)에서 모두(All) 옵션을 지우고 개별 리전을 보고서에 포함할 수 있습니다.

   a. 보고서의 이름을 입력합니다.

   b. 형식(Format)에서 JSON 또는 CSV를 선택합니다.

   c. 리전(Region)에서 AWS 리전을 지정하거나 모두(All)를 선택합니다.

   d. 검사 범주(Check category)에서 검사 범주를 선택하거나 모두(All)를 선택합니다.

   e. 검사(Checks)에서 해당 범주에 대한 특정 검사를 선택하거나 모두(All)를 선택합니다.

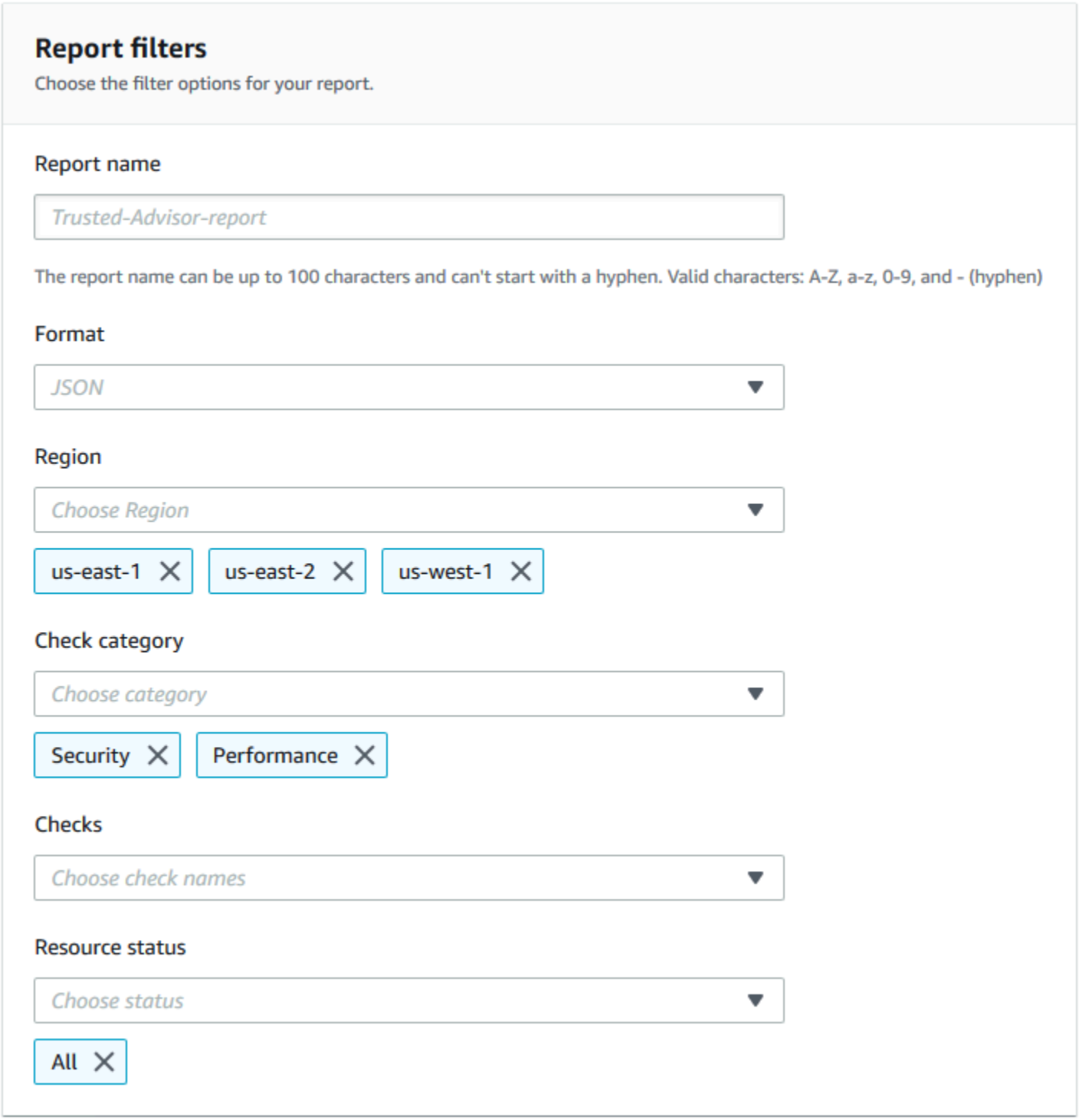
   > **Note**
   >
   > 검사 범주(Check category) 필터는 검사(Checks) 필터를 재정의합니다. 예를 들어 보안(Security) 범주를 선택한 다음 특정 검사 이름을 선택하면 보고서에 해당 범주에 대한 모든 검사 결과가 포함됩니다. 특정 검사에 대해서만 보고서를 생성하려면 검사 범주(Check category)에서 모두(All)를 기본값으로 두고 검사 이름을 선택합니다.

   f. 리소스 상태(Resource status)에서 필터링할 상태(예: 경고(Warning))를 선택하거나 모두(All)를 선택합니다.
5. AWS 조직에서 보고서에 포함할 조직 단위(OU)를 선택합니다. OU에 대한 자세한 내용은 AWS Organizations사용 설명서의 조직 단위 관리를 참조하세요.
6. 보고서 생성(Create report)을 선택합니다.

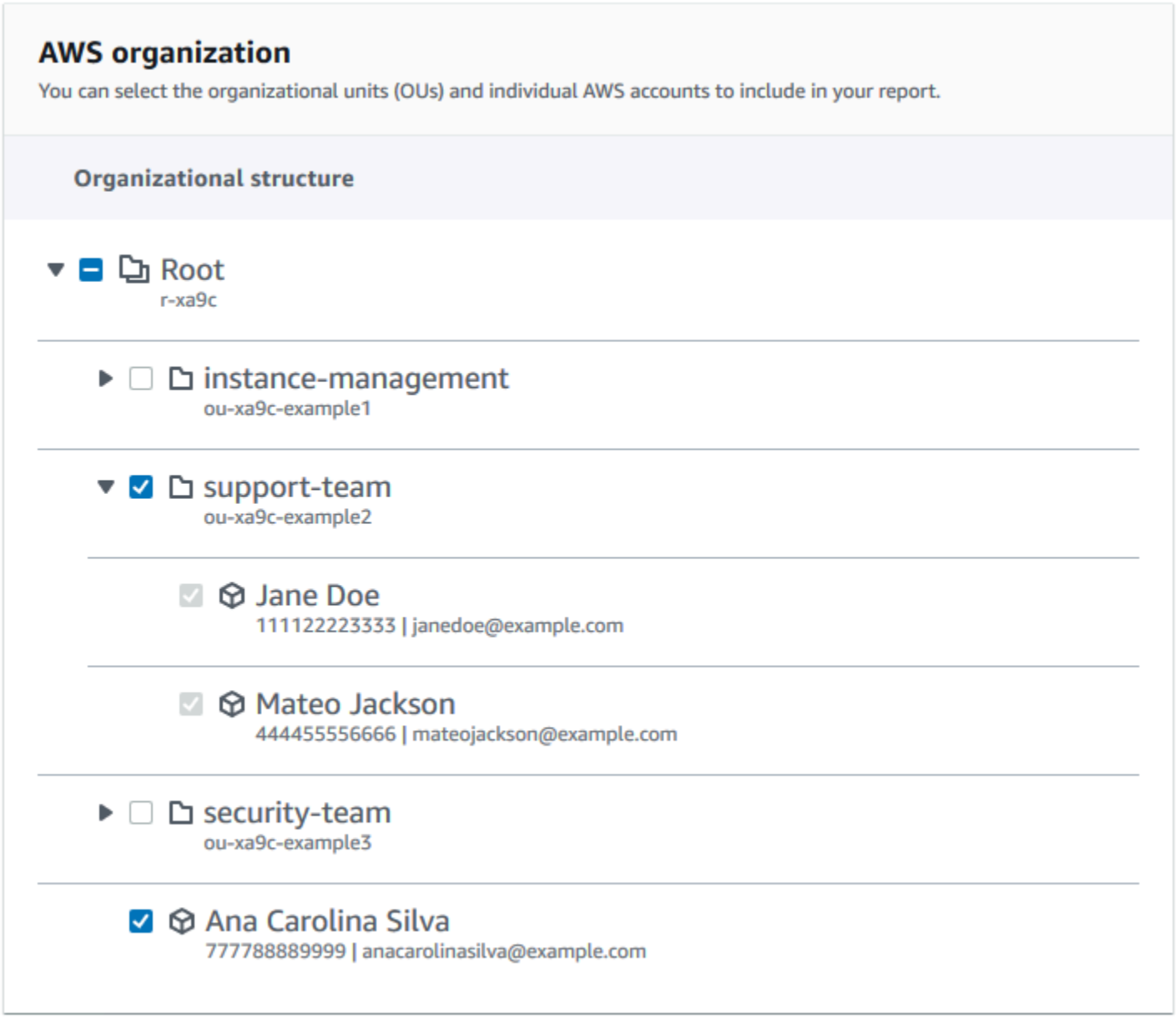
Example : 보고서 필터 옵션 생성

다음 예제에서는 다음에 대한 JSON 보고서를 생성합니다.

- 3개의 AWS 리전
- 모든 보안 및 성능 검사




다음 예제에서 보고서에는 조직에 속하는 지원 팀(support-team) OU 및 1개의 AWS 계정이 포함되어 있습니다.




주의

- 보고서를 생성하는 데 걸리는 시간은 조직의 계정 수와 각 계정의 리소스 수에 따라 달라집니다.
- 현재 보고서가 6시간 넘게 실행 중인 경우가 아니라면 두 개 이상의 보고서를 동시에 생성할 수 없습니다.
- 페이지에 보고서가 표시되지 않으면 페이지를 새로 고치세요.

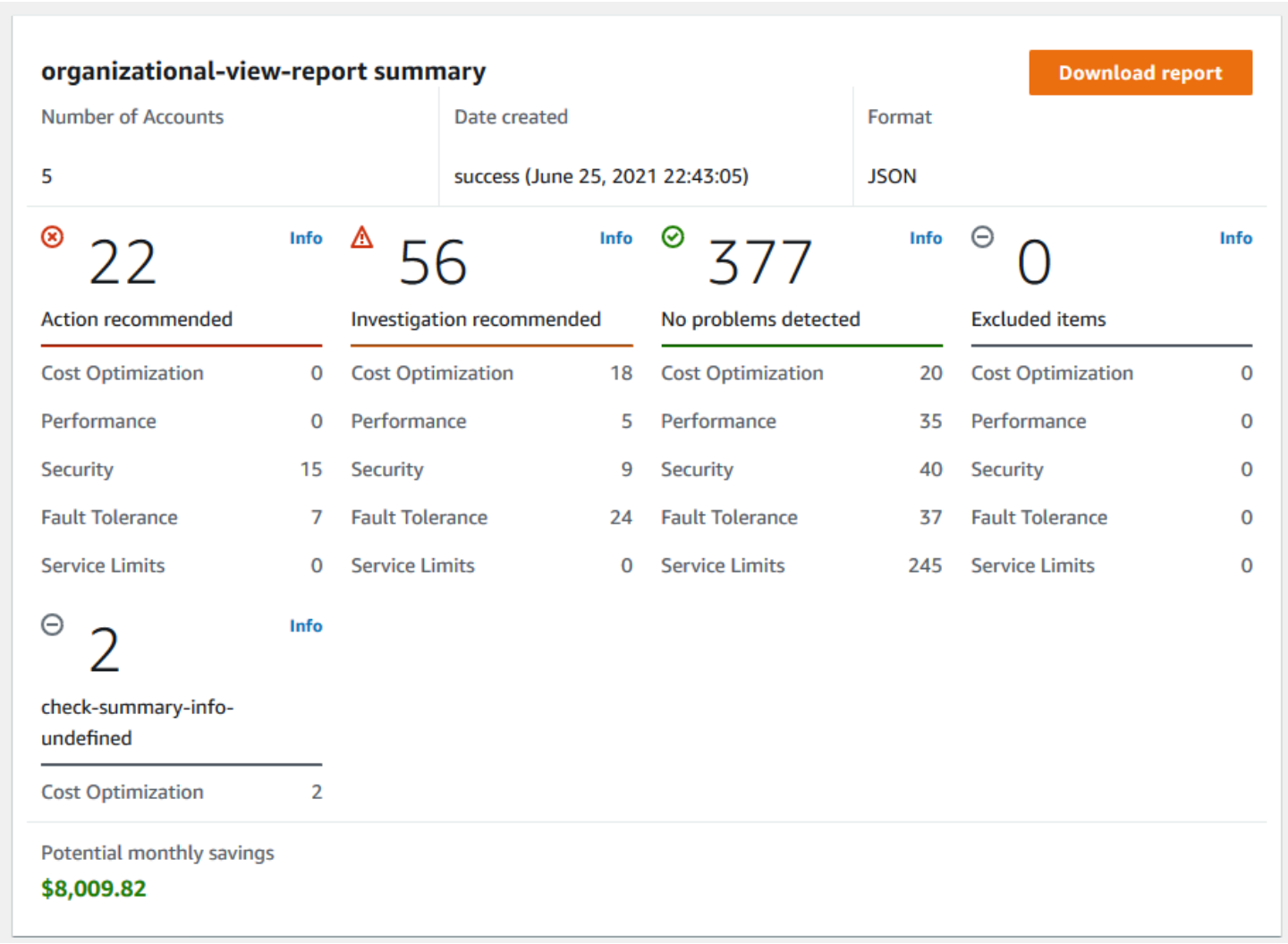
# 보고서 요약 보기

보고서가 준비되면 Trusted Advisor 콘솔에서 보고서 요약을 볼 수 있습니다.. 이렇게 하면 조직 전체의 검사 결과 요약을 빠르게 볼 수 있습니다.

보고서 요약을 보려면

1. 조직의 관리 계정에 로그인한 다음 https://console.aws.amazon.com/trustedadvisor에서 AWS Trusted Advisor 콘솔을 엽니다.
2. 탐색 창에서 조직 보기(Organizational View)를 선택합니다.
3. 보고서 이름을 선택합니다.
4. 요약(Summary) 페이지에서 각 범주의 검사 상태를 봅니다. 보고서 다운로드(Download report)를 선택할 수도 있습니다.

Example : 조직에 대한 보고서 요약




## 조직 보기 보고서 다운로드

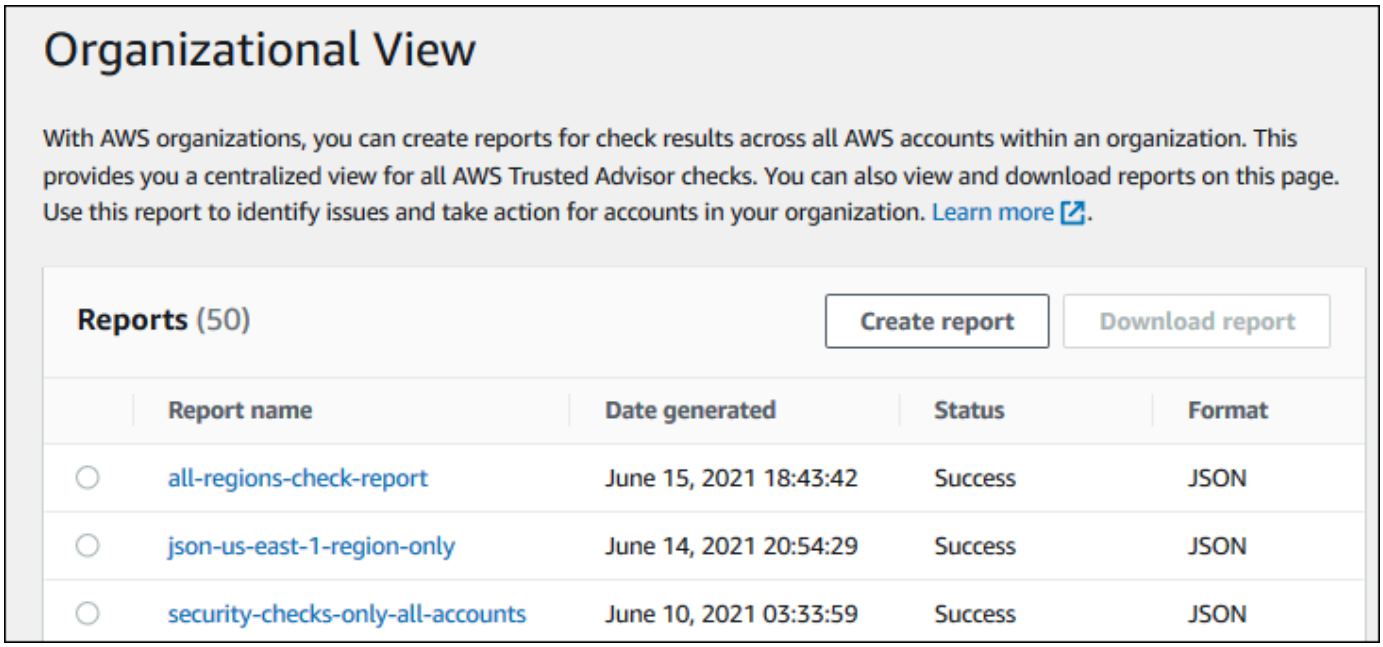
보고서가 준비되면 Trusted Advisor 콘솔에서 다운로드합니다. 보고서는 다음 세 개의 파일을 포함하는 .zip 파일입니다.

- `summary.json` - 각 검사 범주의 검사 결과 요약을 포함합니다.
- `schema.json` - 보고서의 지정된 검사에 대한 스키마를 포함합니다.
- 리소스 파일 (.json 또는.csv) - 조직의 리소스에 관한 검사 상태에 대한 자세한 정보가 들어 있습니다.

조직 보기 보고서를 다운로드하려면

1. 조직의 관리 계정에 로그인한 다음 https://console.aws.amazon.com/trustedadvisor에서 AWS Trusted Advisor 콘솔을 엽니다.
2. 탐색 창에서 조직 보기(Organizational View)를 선택합니다.

   조직 보기(Organizational View 페이지에 다운로드할 수 있는 보고서가 표시됩니다.
3. 보고서를 선택하고 보고서 다운로드(Download report)를 선택한 다음 파일을 저장합니다. 한 번에 하나의 보고서만 다운로드할 수 있습니다.




4. 파일 압축을 풉니다.
5. 텍스트 편집기를 사용하여 `.json` 파일을 열거나 스프레드시트 애플리케이션을 사용하여 `.csv` 파일을 엽니다.

> **Note**
>
> 보고서가 5MB 이상인 경우 여러 파일을 받을 수 있습니다.

Example : summary.json 파일

`summary.json` 파일에는 조직의 계정 수와 각 범주의 검사 상태가 표시됩니다.

Trusted Advisor는 검사 결과에 다음의 색상 코드를 사용합니다.

- `Green` – Trusted Advisor가 검사에서 문제를 감지하지 않습니다.
- `Yellow` – Trusted Advisor가 검사에서 가능한 문제를 감지합니다.
- `Red` – Trusted Advisor가 오류를 감지하고 검사에 대한 작업을 권장합니다.
- `Blue` – Trusted Advisor가 검사 상태를 확인할 수 없습니다.

다음 예제에서는 두 개의 검사가 `Red`이고, 하나가 `Green`이고, 하나가 `Yellow`입니다.


```
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountIds": ["123456789012","111122223333","111111111111"],
        "checkIds": "All",
        "categories": [
            "security",
            "performance"
        ],
        "statuses": "All",
        "regions": [
            "us-west-1",
            "us-west-2",
            "us-east-1"
        ],
        "organizationalUnitIds": [
            "ou-xa9c-EXAMPLE1",
            "ou-xa9c-EXAMPLE2"
        ]
    },
    "categoryStatusMap": {
        "security": {
            "statusMap": {
                "ERROR": {
                    "name": "Red",
                    "count": 2
                },
                "OK": {
                    "name": "Green",
                    "count": 1
                },
                "WARN": {
                    "name": "Yellow",
                    "count": 1
```

```
                }
            },
            "name": "Security"
        }
    },
    "accountStatusMap": {
        "123456789012": {
            "security": {
                "statusMap": {
                    "ERROR": {
                        "name": "Red",
                        "count": 2
                    },
                    "OK": {
                        "name": "Green",
                        "count": 1
                    },
                    "WARN": {
                        "name": "Yellow",
                        "count": 1
                    }
                },
                "name": "Security"
            }
        }
    }
}
```

Example : schema.json 파일

schema.json 파일에는 보고서의 검사에 대한 스키마가 포함됩니다. 다음 예제에는 IAM 암호 정책(Yw2K9puPzl)과 IAM 키 교체(DqdJqYeRm5) 검사의 ID 및 속성이 포함되어 있습니다.

```
{
    "Yw2K9puPzl": [
        "Password Policy",
        "Uppercase",
        "Lowercase",
        "Number",
        "Non-alphanumeric",
        "Status",
        "Reason"
    ],
```

```
    "DqdJqYeRm5": [
        "Status",
        "IAM User",
        "Access Key",
        "Key Last Rotated",
        "Reason"
    ],
    ...
}
```

Example : resources.csv 파일

`resources.csv` 파일에는 조직의 리소스에 대한 정보가 포함됩니다. 이 예에서는 다음과 같이 보고서에 나타나는 일부 데이터 열을 보여 줍니다.

- 영향을 받는 계정의 계정 ID
- Trusted Advisor 검사 ID
- 리소스 ID
- 보고서의 타임스탬프
- Trusted Advisor 검사의 전체 이름
- Trusted Advisor 검사 범주
- 상위 조직 단위(OU) 또는 루트의 계정 ID

| AccountId | CheckId | ResourceId | TimeStamp | CheckName | Category |
|---|---|---|---|---|---|
| 1.11122E+11 | Qch7DwouX1 | LnW14f1M40NMjmMLvY5 | 1.58983E+12 | Low Utilization Amazon EC2 Instances | Cost Optimizing |
| 1.11122E+11 | HCP4007jGY | dJrQZXw36ZdswBeo9WUl | 1.58983E+12 | Security Groups - Specific Ports Unrestricted | Security |
| 1.11122E+11 | HCP4007jGY | 1hzakmTbWd5UmAM_a0L | 1.58983E+12 | Security Groups - Specific Ports Unrestricted | Security |
| 4.44456E+11 | 1iG5NDGVre | dJrQZXw36ZdswBeo9WUl | 1.58983E+12 | Security Groups - Unrestricted Access | Security |
| 4.44456E+11 | 1iG5NDGVre | 1hzakmTbWd5UmAM_a0L | 1.58983E+12 | Security Groups - Unrestricted Access | Security |
| 4.44456E+11 | Pfx0RwqBli | vioZmlba45kf2JWIe_W0j5 | 1.58983E+12 | Amazon S3 Bucket Permissions | Security |
| 4.44456E+11 | Pfx0RwqBli | wAvASS3YOwy6WWxIBHf | 1.58983E+12 | Amazon S3 Bucket Permissions | Security |
| 1.23457E+11 | Pfx0RwqBli | LIc4zRaUSiIGRSlmqaMa5V | 1.58983E+12 | Amazon S3 Bucket Permissions | Security |
| 1.23457E+11 | Pfx0RwqBli | gWB27TMXof2evYzMSYBg | 1.58983E+12 | Amazon S3 Bucket Permissions | Security |
| 7.77789E+11 | Pfx0RwqBli | M3LBsF0e15Cl9MxppapcX | 1.58983E+12 | Amazon S3 Bucket Permissions | Security |
| 7.77789E+11 | Yw2K9puPzl | 47DEQpj8HBSa-_TImW-5J | 1.58983E+12 | IAM Password Policy | Security |
| 7.77789E+11 | H7lgTzjTYb | 1xHQ5ovV8bS0H1Z-t7Kbib | 1.58983E+12 | Amazon EBS Snapshots | Fault Tolerance |
| 7.77789E+11 | wuy7G1zxql | 10F6p6VAF0F-MuL6Dc-dl1 | 1.58983E+12 | Amazon EC2 Availability Zone Balance | Fault Tolerance |

검사 결과가 리소스 수준에 있는 경우에만 리소스 파일에 항목이 포함됩니다. 다음과 같은 이유로 보고서에 검사가 표시되지 않을 수 있습니다.

- 루트 계정의 MFA 등의 일부 검사는 리소스가 없으므로 보고서에 나타나지 않습니다. 리소스가 없는 검사는 `summary.json` 파일에 대신 나타납니다.
- 일부 검사는 `Red` 또는 `Yellow`일 때만 리소스를 보여줍니다. 모든 리소스가 `Green`이면 보고서에 표시되지 않을 수 있습니다.
- 검사가 필요한 서비스에 대해 계정이 활성화되지 않은 경우 보고서에 검사가 나타나지 않을 수 있습니다. 예를 들어 조직에서 Amazon Elastic Compute Cloud 예약 인스턴스를 사용하지 않는 경우 보고서에 Amazon EC2 Reserved Instance Lease Expiration 검사가 보고서에 표시되지 않습니다.
- 계정이 검사 결과를 새로 고치지 않았습니다. 이런 일은 기본(Basic) 또는 개발자(Developer) 지원 플랜을 사용하는 사용자가 Trusted Advisor 콘솔에 처음으로 로그인할 때 발생할 수 있습니다 Business, Enterprise On-Ramp 또는 Enterprise Support 플랜을 보유한 경우 사용자가 검사 결과를 보려면 계정 등록 시점부터 최대 1주일이 걸릴 수 있습니다. 자세한 내용은 Trusted Advisor 검사 새로 고침 섹션을 참조하세요.
- 조직의 관리 계정에서만 검사에 대한 권장 사항을 활성화한 경우 보고서에 조직의 다른 계정에 대한 리소스가 포함되지 않습니다.

리소스 파일의 경우 Microsoft Excel과 같은 일반적인 소프트웨어를 사용하여.csv 파일 형식을 열 수 있습니다. .csv 파일을 사용하여 조직의 모든 계정에 걸쳐 모든 검사를 한 번에 분석할 수 있습니다. 애플리케이션에서 보고서를 사용하려면 보고서를.json 파일로 대신 다운로드할 수 있습니다.

.json 파일 형식은 여러 데이터 집합을 사용한 집계 및 고급 분석 등의 고급 사용 사례에서.csv 파일 형식보다 더 많은 유연성을 제공합니다. 예를 들어, .Amazon Athena와 같은 AWS 서비스에서 SQL 인터페이스를 사용하여 보고서에 대한 쿼리를 실행할 수 있습니다. Amazon QuickSight를 사용하여 대시보드를 만들고 데이터를 시각화할 수도 있습니다. 자세한 내용은 다른 AWS 서비스를 사용하여 Trusted Advisor 보고서 보기 단원을 참조하세요.

## 조직 보기 비활성화

이 절차에 따라 조직 보기를 비활성화합니다. 이 기능을 비활성화하려면 조직의 관리 계정에 로그인하거나 필요한 권한이 있는 역할을 수임해야 합니다. 조직의 다른 계정에서는 이 기능을 비활성화할 수 없습니다.

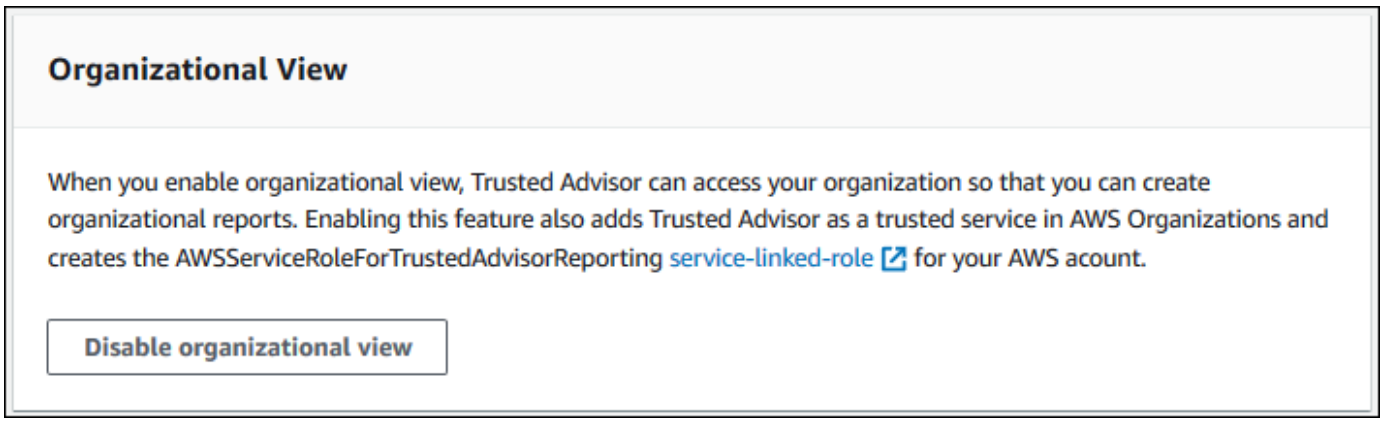
이 기능을 비활성화하면 다음과 같이 진행됩니다.

- Trusted Advisor가 Organizations의 신뢰할 수 있는 서비스로서 제거됩니다.
- 조직의 관리 계정에서 `AWSServiceRoleForTrustedAdvisorReporting` 서비스 연결 역할이 잠금 해제됩니다. 즉, 필요한 경우 수동으로 삭제할 수 있습니다.

- 조직에 대한 보고서를 만들거나 보거나 다운로드할 수 없습니다. 이전에 만든 보고서에 액세스하려면 Trusted Advisor 콘솔에서 조직 보기를 다시 활성화해야 합니다. 조직 보기 활성화 단원을 참조하세요.

Trusted Advisor에 대한 조직 보기를 비활성화하려면

1. 조직의 관리 계정에 로그인한 다음 https://console.aws.amazon.com/trustedadvisor에서 AWS Trusted Advisor 콘솔을 엽니다.
2. 탐색 창에서 Preferences(기본 설정)를 선택합니다.
3. 조직 보기(Organizational View)를 선택하고조직 보기 비활성화(Disable organizational view)를 선택합니다.




조직 보기를 비활성화하면 Trusted Advisor가 더 이상 조직의 다른 AWS 계정에서 검사를 집계하지 않습니다. 그러나 `AWSServiceRoleForTrustedAdvisorReporting` 서비스 연결 역할은 IAM 콘솔, IAM API 또는 AWS Command Line Interface(AWS CLI)를 통해 삭제할 때까지 조직의 관리 계정에 남아 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스에 연결 역할 삭제 단원을 참조하세요.

> **Note**
>
> 다른 AWS 서비스를 사용하여 조직 보기 보고서에서 데이터를 쿼리하고 시각화할 수 있습니다. 자세한 정보는 다음 자료를 참조하세요.
>
> - AWS 관리 및 거버넌스 블로그에서 규모에 따른 AWS Trusted Advisor 권장 사항AWS Organizations 보기
> - 다른 AWS 서비스를 사용하여 Trusted Advisor 보고서 보기

# IAM 정책을 사용하여 조직 보기에 대한 액세스 허용

다음 AWS Identity and Access Management(IAM) 정책을 사용하여 계정의 사용자 또는 역할이 AWS Trusted Advisor의 조직 보기에 액세스할 수 있도록 허용할 수 있습니다.

Example : 조직 보기에 대한 모든 액세스 권한

다음 정책은 조직 보기 기능에 대한 모든 액세스를 허용합니다. 이 권한이 있는 사용자는 다음을 수행할 수 있습니다.

- 조직 보기 사용 및 사용 중지
- 보고서 작성, 보기 및 다운로드.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:DescribeServiceMetadata",
                "trustedadvisor:DescribeOrganizationAccounts",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateReportStatement",
```

```
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:GenerateReport"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageOrganizationalViewStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess",
                "trustedadvisor:SetOrganizationAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleStatement",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting"
        }
    ]
}
```

Example : 조직 보기에 대한 읽기 액세스

다음 정책은 Trusted Advisor에 대해 조직 보기에 대한 읽기 전용 액세스를 허용합니다. 이러한 권한이 있는 사용자는 기존 보고서를 보거나 다운로드할 수만 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
```

```
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        }
    ]
}
```

또한 사용자 고유의 IAM 정책을 만들 수도 있습니다. 자세한 내용은 IAM 사용 설명서에서 IAM 정책 생성을 참조하세요.

> **Note**
>
> 계정에서 AWS CloudTrail을(를) 활성화한 경우 로그 항목에 다음 역할이 나타날 수 있습니다.
>
> - `AWSServiceRoleForTrustedAdvisorReporting` - Trusted Advisor가 조직의 계정에 액세스하는 데 사용하는 서비스 연결 역할입니다.
> - `AWSServiceRoleForTrustedAdvisor` - Trusted Advisor가 조직의 서비스에 액세스하는 데 사용하는 서비스 연결 역할입니다.
>
> 서비스 연결 역할에 대한 자세한 내용은 Trusted Advisor의 서비스 링크 역할 사용 단원을 참조하세요.

## 다른 AWS 서비스를 사용하여 Trusted Advisor 보고서 보기

이 자습서를 따라 다른 AWS 서비스를 사용하여 데이터를 업로드하고 볼 수 있습니다. 이 주제에서는 보고서를 저장하기 위한 Amazon Simple Storage Service(Amazon S3) 버킷을 생성하고 계정에 리소스를 생성하기 위한 AWS CloudFormation 템플릿을 생성합니다. 그런 다음 Amazon Athena를 사용하여 보고서에 대한 쿼리를 분석 또는 실행하거나 Amazon QuickSight를 사용하여 대시보드에서 해당 데이터를 시각화할 수 있습니다.

보고서 데이터를 시각화하기 위한 정보 및 예제는 AWS 관리 및 거버넌스 블로그에서 AWS Organizations로 규모에 따른 AWS Trusted Advisor 권장 사항 보기를 참조하세요.

## 필수 조건

이 자습서를 사용하기 전에 다음 요구 사항을 충족하는지 확인하세요.

- 관리자 권한이 있는 AWS Identity and Access Management(IAM) 사용자로 로그인합니다.
- 미국 동부 (버지니아 북부) AWS 리전을 사용하여 빠르게 AWS 서비스 및 리소스를 설정하세요.
- Amazon QuickSight 계정을 생성합니다. 자세한 내용은 Amazon QuickSight 사용 설명서의 Amazon QuickSight에서 데이터 분석 시작하기를 참조하세요.

## 보고서를 Amazon S3에 업로드합니다.

`resources.json` 보고서를 다운로드한 후 파일을 Amazon S3에 업로드합니다. 미국 동부(버지니아 북부) 리전의 버킷을 사용해야 합니다.

Amazon S3 버킷에 보고서를 업로드하려면

1. https://console.aws.amazon.com/deepracer에서 AWS Management Console 콘솔에 로그인합니다.
2. 리전 선택기(Region selector)를 사용하여 미국 동부(버지니아 북부) 리전을 선택합니다.
3. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
4. 버킷 목록에서 S3 버킷을 선택한 다음 이름을 복사합니다. 이 이름은 다음 절차에서 사용합니다.
5. *`## ##(bucket-name)`* 페이지에서 폴더 생성(Create folder)을 선택하고 **`folder1`**을 이름으로 입력한 후 저장(Save)을 선택합니다.
6. folder1을 선택합니다.
7. folder1에서 업로드(Upload)를 선택하고 `resources.json` 파일을 선택합니다.
8. 다음(Next)을 선택하고 기본 옵션을 그대로 둔 채 업로드(Upload)를 선택합니다.

> **Note**
>
> 이 버킷에 새 보고서를 업로드하는 경우 보고서를 업로드할 때마다 `.json` 파일의 이름을 다시 지정하여 기존 보고서를 덮어쓰지 않도록 합니다. 예를 들어 타임스탬프를 `resources-timestamp.json`, `resources-timestamp2.json` 등의 각 파일에 추가할 수 있습니다.

## AWS CloudFormation을 사용한 리소스 생성

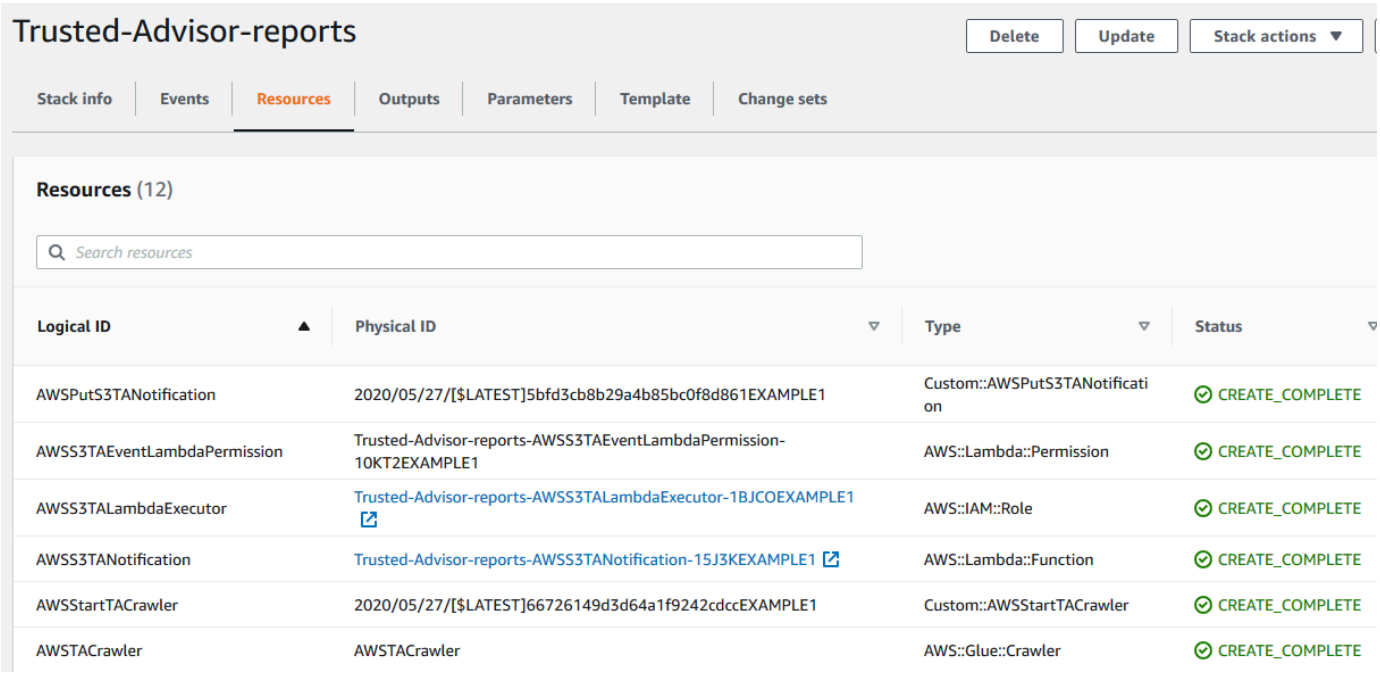
보고서를 Amazon S3에 업로드한 후 다음 YAML 템플릿을 AWS CloudFormation에 업로드합니다. 이 템플릿은 다른 서비스가 S3 버킷에서 보고서 데이터를 사용할 수 있도록 AWS CloudFormation이 계정에 대해 어떤 리소스를 생성할지를 지정합니다. 템플릿은 IAM, AWS Lambda 및 AWS Glue에 대한 리소스를 생성합니다

AWS CloudFormation을 사용하여 리소스를 만들려면

1. trusted-advisor-reports-template.zip 파일을 다운로드합니다.
2. 파일 압축을 풉니다.
3. 텍스트 편집기에서 템플릿 파일을 엽니다.
4. `BucketName` 및 `FolderName` 파라미터에서, *`your-bucket-name-here`* 및 *`folder1`*에 대한 값을 계정의 버킷 이름 및 폴더 이름으로 바꿉니다.
5. 파일을 저장합니다.
6. https://console.aws.amazon.com/cloudformation에서 AWS CloudFormation 콘솔을 엽니다.
7. 아직 설정하지 않았다면 리전 선택기(Region selector)에서 미국 동부(버지니아 북부) 리전을 선택합니다.
8. 탐색 창에서 스택(Stacks)을 선택합니다.
9. 스택 생성(Create stack)을 선택한 다음 새 리소스 사용(스탠더드)(With new resources (standard))을 선택합니다.
10. 스택 생성(Create stack) 페이지의 템플릿 지정(Specify template)에서 템플릿 파일 업로드(Upload a template file)를 선택한 후 파일 선택(Choose file)을 선택합니다.
11. YAML 파일을 선택한 후 다음(Next)을 선택합니다.
12. 스택 세부 정보 지정(Specify stack details) 페이지에서 **`Organizational-view-Trusted-Advisor-reports`** 등의 스택 이름을 입력한 후 다음(Next)을 선택합니다.
13. 스택 옵션 구성(Configure stack options) 페이지에서 기본 옵션을 유지하고 다음(Next)을 선택합니다.
14. **`Organizational-view-Trusted-Advisor-reports`** 검토(Review) 페이지에서, 선택한 옵션을 검토하세요. 페이지 하단에서 AWS CloudFormation이 IAM 리소스를 생성할 수 있음을 확인합니다(I acknowledge that might create IAM resources) 확인란을 선택합니다.
15. 스택 생성(Create stack)을 선택합니다.

    스택을 만드는 데 약 5분이 걸립니다.

16. 스택이 성공적으로 생성되면 리소스(Resources) 탭이 다음 예제처럼 표시됩니다.



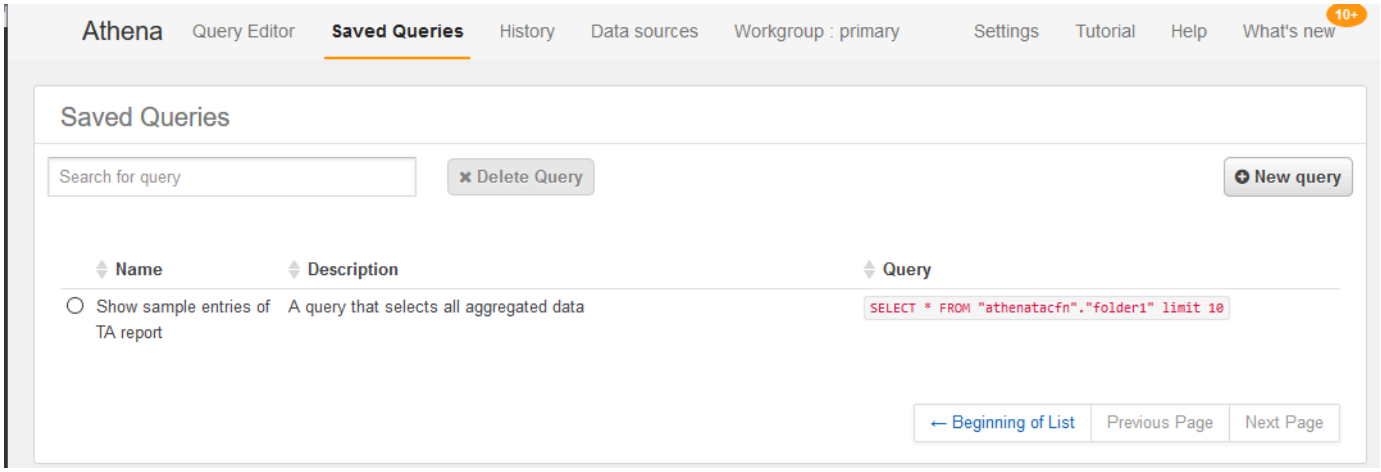

## Amazon Athena에서 데이터 쿼리

리소스를 확보한 후에는 Athena에서 데이터를 볼 수 있습니다. Athena를 사용하여 쿼리를 만들고 조직의 계정에 대한 특정 검사 결과 조회 등 보고서 결과를 분석합니다.

> **주의**
>
> - 미국 동부(버지니아 북부) 리전을 사용하세요.
> - Athena를 처음 사용하는 경우 보고서에 대한 쿼리를 실행하려면 먼저 쿼리 결과 위치를 지정해야 합니다. 이 위치에 대해 다른 S3 버킷을 지정하는 것이 좋습니다. 자세한 내용은 Amazon Athena 사용 설명서의 쿼리 결과 위치 지정을 참조하세요.

Athena에서 데이터를 쿼리하려면

1. https://console.aws.amazon.com/athena/에서 Athena 콘솔을 엽니다.
2. 아직 설정하지 않았다면 리전 선택기(Region selector)에서 미국 동부(버지니아 북부) 리전을 선택합니다.
3. 저장된 쿼리(Saved Queries)를 선택한 후 검색 필드에 **`Show sample`**을 입력합니다.
4. 표시되는 쿼리를 선택하세요(예: TA 보고서의 샘플 항목 표시(Show sample entries of TA report)).



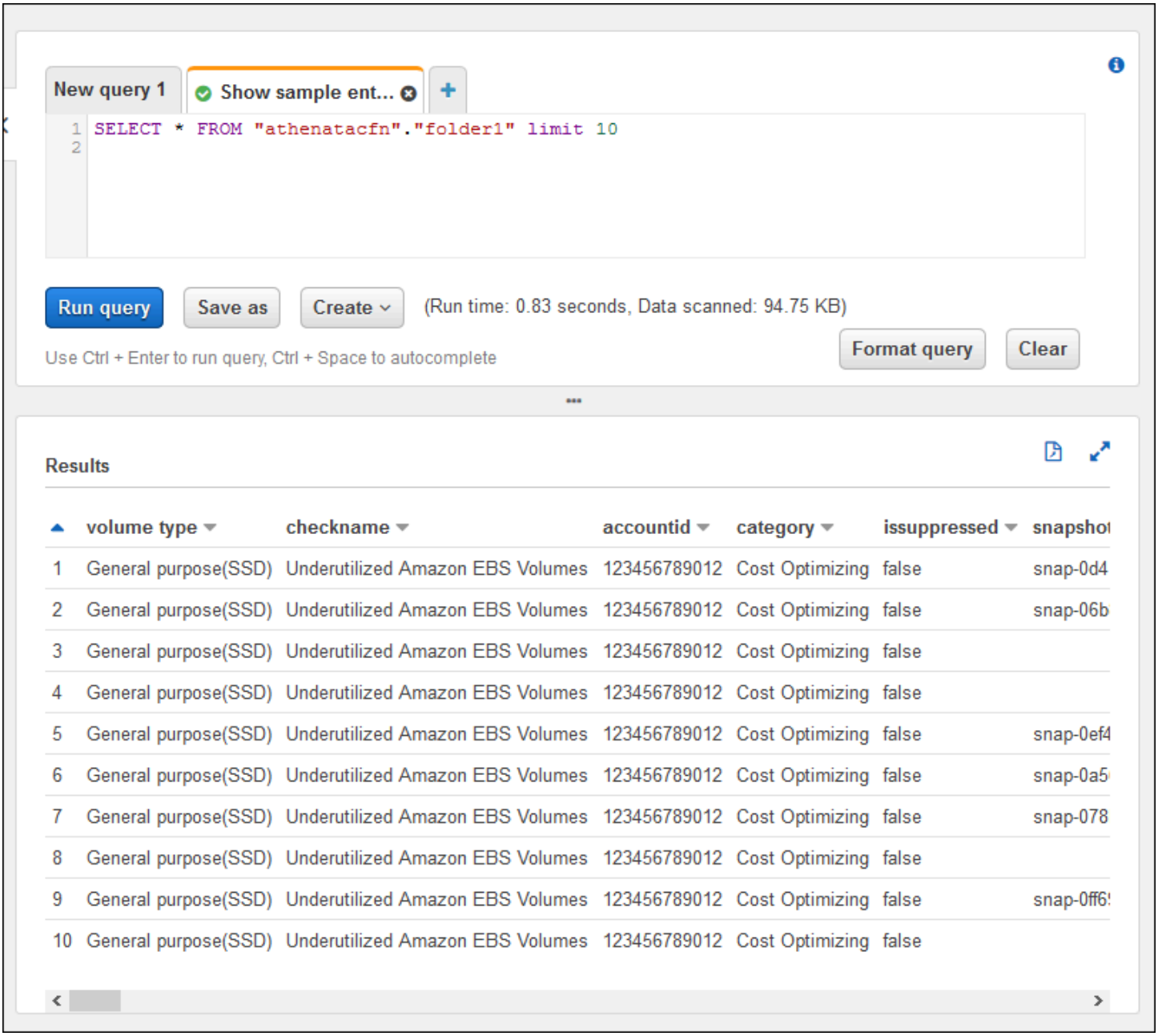

이 쿼리는 다음과 같이 표시됩니다.

```
SELECT * FROM "athenatacfn"."folder1" limit 10
```

5. 쿼리 실행을 선택합니다. 쿼리 결과가 나타납니다.

Example : Athena 쿼리

다음 예에서는 보고서에서 10개의 샘플 항목을 보여 줍니다.




자세한 내용은 Amazon Athena 사용 설명서의 Amazon Athena를 사용하여 SQL 쿼리 실행을 참조하세요.

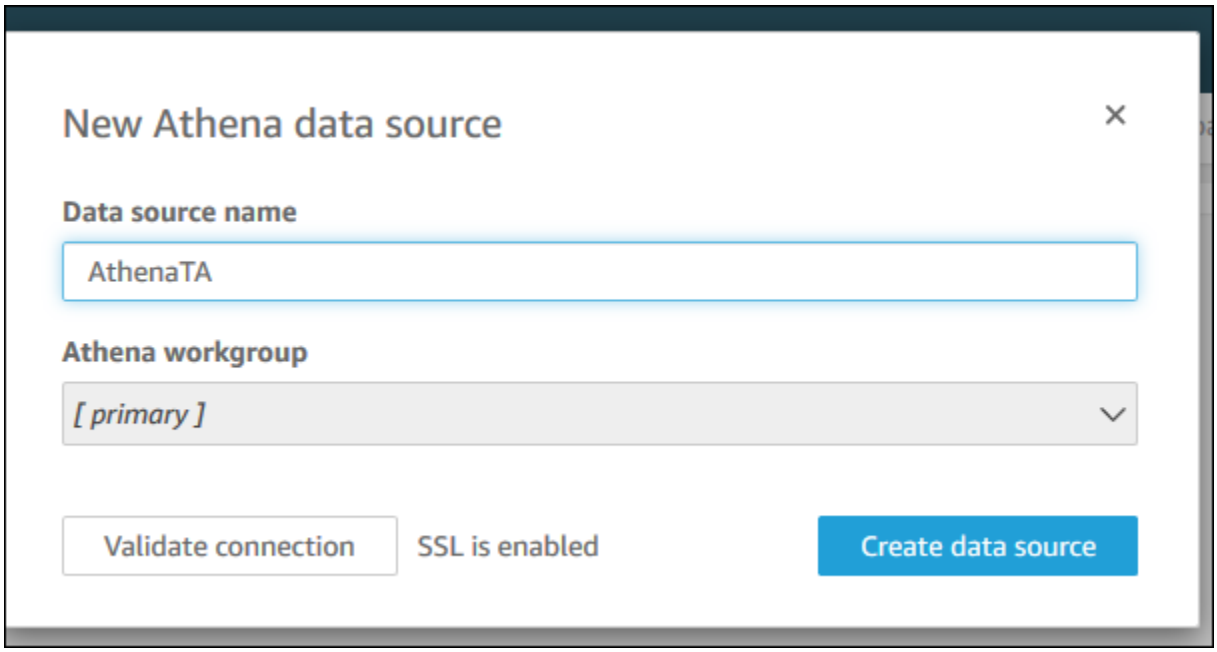
## Amazon QuickSight에서 대시보드 만들기

대시보드에서 데이터를 보고 보고서 정보를 시각화할 수 있도록 Amazon QuickSight를 설정할 수도 있습니다.

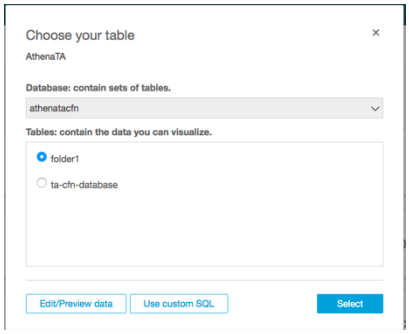
> **Note**
>
> 미국 동부(버지니아 북부) 리전을 사용해야 합니다.

Amazon QuickSight에서 대시보드를 생성하려면

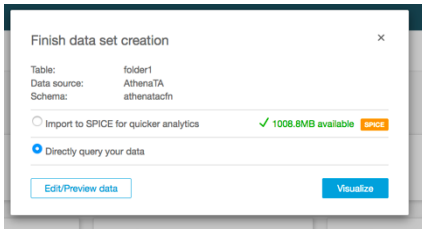
1. Amazon QuickSight 콘솔로 이동하여 계정(account)에 로그인합니다.
2. 새로운 분석(New analysis), 새 데이터 집합(New dataset)을 선택한 다음 Athena를 선택합니다.
3. 새 Athena 데이터 원본(New Athena data sourc) 대화 상자에서 AthenaTA 등의 데이터 원본 이름을 입력한 다음 데이터 원본 생성(Create data source)을 선택합니다.




4. 테이블 선택(Choose your table) 대화 상자에서 athenatacfn 테이블을 선택하고 folder1을 선택한 다음 선택(Select)을 선택합니다.




5. 데이터 집합 생성 완료(Finish data set creation) 대화 상자에서 직접 데이터 쿼리(Directly query your data)를 선택한 다음 시각화(Visualize)를 선택합니다.




이제 Amazon QuickSight에서 대시보드를 만들 수 있습니다. 자세한 내용은 Amazon QuickSight 사용 설명서의 대시보드 작업을 참조하세요.

Example : Amazon QuickSight 대시보드

다음 예제 대시보드는 다음과 같은 Trusted Advisor 검사에 대한 정보를 표시합니다.

- 영향을 받는 계정 ID
- AWS 리전별 요약
- 검사 범주
- 검사 상태
- 각 계정에 대한 보고서의 항목 수

> **Note**
>
> 대시보드를 만드는 동안 권한 오류가 발생한 경우 Amazon QuickSight에서 Athena를 사용할 수 있는지 확인하세요. 자세한 내용은 Amazon QuickSight 사용 설명서의 Amazon Athena에 연결할 수 없음을 참조하세요.

보고서 데이터 시각화에 대한 자세한 정보와 예제는 AWS 관리 및 거버넌스 블로그에서 AWS Organizations로 규모에 따른 AWS Trusted Advisor 권장 사항 보기를 참조하세요..

## 문제 해결

이 자습서에 문제가 있는 경우 다음 문제 해결 팁을 참조하세요.

내 보고서에 최신 데이터가 표시되지 않음

보고서를 만들 때 조직 보기 기능이 조직에서 Trusted Advisor 검사를 자동으로 새로 고치지 않습니다. 최신 검사 결과를 얻으려면 관리 계정과, 조직의 각 멤버 계정에 대해 검사를 새로 고치세요. 자세한 내용은 Trusted Advisor 검사 새로 고침 단원을 참조하세요.

보고서에 중복 열이 있음

보고서에 중복 열이 있는 경우 Athena 콘솔이 테이블에 다음 오류를 표시할 수 있습니다.

```
HIVE_INVALID_METADATA: Hive metadata for table folder1 is invalid: Table
descriptor contains duplicate columns
```

예를 들어 보고서에 이미 있는 열을 추가한 경우 Athena 콘솔에서 보고서 데이터를 보려고 할 때 문제가 발생할 수 있습니다. 다음 단계를 수행하여 이 문제를 해결할 수 있습니다.

중복 열 찾기

AWS Glue 콘솔을 사용하여 스키마를 보고 보고서에 중복 열이 있는지 빠르게 식별할 수 있습니다.

중복 열을 찾으려면

1. AWS Glue 콘솔(https://console.aws.amazon.com/glue/)을 엽니다.
2. 아직 설정하지 않았다면 리전 선택기(Region selector)에서 미국 동부(버지니아 북부) 리전을 선택합니다.
3. 탐색 창에서 테이블(Tables)을 선택합니다.

4. ***folder1*** 등의 폴더 이름을 선택한 다음 Schema(스키마)에서 열 이름(Column name)의 값을 봅니다.

   중복 열이 있는 경우 Amazon S3 버킷에 새 보고서를 업로드해야 합니다. 다음 새 보고서 업로드 단원을 참조하세요.

새 보고서 업로드

중복 열을 식별한 후에는 기존 보고서를 새 보고서로 바꾸는 것이 좋습니다. 이렇게 하면 이 자습서에서 만든 리소스가 조직의 최신 보고서 데이터를 사용할 수 있습니다.

새 보고서를 업로드하려면

1. 아직 새로 고치지 않았다면 조직의 계정에 대해 Trusted Advisor 검사를 새로 고치세요. Trusted Advisor 검사 새로 고침 단원을 참조하세요.
2. Trusted Advisor 콘솔에서 다른 JSON 보고서를 생성하고 다운로드합니다. 조직 보기 보고서 생성 단원을 참조하세요. 이 자습서에서는 JSON 파일을 사용해야 합니다.
3. AWS Management Console에 로그인한 후 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
4. Amazon S3 버킷을 선택하고 ***folder1*** 폴더를 선택합니다.
5. 이전의 ***resources***`.json` 보고서를 선택하고 삭제(Delete)를 선택합니다.
6. 객체 삭제(Delete objects) 페이지의 객체를 영구적으로 삭제하시겠습니까?(Permanently delete objects?)에서 **`permanently delete`**를 입력한 다음 객체 삭제(Delete objects)를 선택합니다.
7. S3 버킷에서 업로드(Upload)를 클릭한 다음 새 보고서를 지정합니다. 이 작업은 Athena 테이블과 AWS Glue 크롤러 리소스를 최신 보고서 데이터로 자동으로 업데이트합니다. 리소스를 새로 고치는 데 몇 분 정도 걸릴 수 있습니다.
8. Athena 콘솔에 새 쿼리를 입력합니다. Amazon Athena에서 데이터 쿼리 단원을 참조하세요.

> **Note**
>
> 이 자습서로도 문제가 해결되지 않는 경우 AWS Support Center에서 기술 지원 사례를 생성할 수 있습니다..

# AWS Config에 의해 구동되는 AWS Trusted Advisor 검사 보기

AWS Config은(는) 원하는 설정에 맞게 리소스 구성을 지속적으로 평가, 감사 및 감정하는 서비스입니다. AWS Config은(는) 관리형 규칙을 제공합니다. AWS Config은(는) 미리 정의되고 사용자 정의 가능한 이 규칙을 사용하여 AWS 리소스 구성이 공통 모범 사례를 준수하는지 평가합니다.

AWS Config 콘솔에서 관리형 규칙의 구성 및 활성화를 통해 안내해 줍니다. AWS Command Line Interface(AWS CLI) 또는 AWS Config API를 사용하여 JSON 코드를 전달하고 그 코드로 관리형 규칙의 구성을 정의할 수도 있습니다. 관리형 규칙의 동작을 필요에 맞게 사용자 지정할 수 있습니다. 규칙의 파라미터를 사용자 지정하여 리소스가 규칙을 준수하기 위해 보유해야 하는 속성을 정의할 수 있습니다. AWS Config 활성화에 대한 자세한 내용은 AWS Config 개발자 안내서를 참조하세요.

AWS Config 관리형 규칙은 모든 카테고리에서 일련의 Trusted Advisor 검사를 수행합니다. 특정 관리형 규칙을 활성화하면 해당 Trusted Advisor 검사가 자동으로 활성화됩니다. 특정 AWS Config 관리형 규칙으로 구동되는 Trusted Advisor 검사를 확인하려면 AWS Trusted Advisor 참조 확인을(를) 참조하세요.

AWS Config 구동 확인은 AWS Business Support, AWS Enterprise On-Ramp 및 AWS Enterprise Support 계획을 보유한 고객에게 제공됩니다. AWS Config 및 이러한 AWS 지원 플랜 중 하나를 사용하도록 설정하면 배포된 해당 AWS Config 관리형 규칙이 제공하는 권장 사항이 자동으로 표시됩니다.

> **Note**
>
> 이러한 검사에 대한 결과는 AWS Config 관리형 규칙에 대한 변경으로 인해 발생하는 업데이트에 따라 자동으로 새로 고쳐집니다. 새로 고침 요청은 허용되지 않습니다. 현재 이러한 검사에서 리소스를 제외할 수 없습니다.

## 문제 해결

이 통합에 문제가 있는 경우 다음 문제 해결 정보를 참조하세요.

목차


- AWS Config에 대한 레코딩 및 관리형 규칙을 활선화했지만 해당 Trusted Advisor 확인을 표시하지 않았습니다.
- 동일한 AWS Config 관리형 규칙을 두 번 배포했는데 Trusted Advisor에 어떤 내용이 표시되나요?
- AWS 지역의 AWS Config에 대한 레코딩을 해제했습니다. Trusted Advisor에서 무엇을 볼 수 있나요?

### AWS Config에 대한 레코딩 및 관리형 규칙을 활선화했지만 해당 Trusted Advisor 확인을 표시하지 않았습니다.

AWS Config 규칙이 평가 결과를 생성하면 거의 실시간으로 Trusted Advisor에서 결과를 볼 수 있습니다. 이 기능을 사용하는 데 문제가 있는 경우, AWS Support 센터에서 기술 지원 사례를 생성합니다.

### 동일한 AWS Config 관리형 규칙을 두 번 배포했는데 Trusted Advisor에 어떤 내용이 표시되나요?

설치한 각 관리형 규칙의 Trusted Advisor 검사 결과에는 별도의 항목이 표시됩니다.

### AWS 지역의 AWS Config에 대한 레코딩을 해제했습니다. Trusted Advisor에서 무엇을 볼 수 있나요?

AWS 지역의 AWS Config에 대한 리소스 기록을 끄면 Trusted Advisor이(가) 해당 지역의 해당 관리형 규칙 및 검사에 대한 데이터를 더 이상 수신하지 않습니다. 기존 관리형 규칙 결과는 레코더 보존 정책에 따라 AWS Config 후 및 Trusted Advisor 후 AWS Config이(가) 만료될 때까지 그대로 유지됩니다. 관리형 규칙을 삭제하면 일반적으로 Trusted Advisor 검사 데이터가 거의 실시간으로 삭제됩니다.

## AWS Trusted Advisor에서 AWS Security Hub 컨트롤 보기

AWS 계정에서 AWS Security Hub를 사용 설정하면 Trusted Advisor 콘솔에서 보안 컨트롤 및 결과를 볼 수 있습니다. Security Hub 컨트롤을 사용하여 Trusted Advisor 검사를 사용하는 것과 동일한 방식으로 계정의 보안 취약성을 식별할 수 있습니다. 검사 상태, 영향을 받은 리소스 목록을 확인한 다음 Security Hub 권장 사항에 따라 보안 문제를 해결할 수 있습니다. 이 기능을 사용하여 하나의 편리한 위치에서 Trusted Advisor 및 Security Hub의 보안 권장 사항을 찾을 수 있습니다.

주의

- Trusted Advisor에서 AWS Foundational Security Best Practices 보안 표준의 컨트롤을 볼 수 있습니다. 단, 범주: 복구 > 복원성(Category: Recover > Resilience)이 있는 제어는 예외입니다. 지원되는 컨트롤 목록은 AWS Security Hub 사용 설명서의 AWS Foundational Security Best Practices 컨트롤을 참조하세요.

  Security Hub 범주에 대한 자세한 내용은 컨트롤 범주를 참조하세요.

- 현재 Security Hub가 AWSFoundational Security Best Practices 보안 표준에 새 컨트롤을 추가하는 경우Trusted Advisor에서 볼 수 있기 전까지 2~4주가 지연될 수 있습니다. 이 기간은 최선의 노력이며 보장되지 않습니다.

주제


- 필수 조건
- Security Hub 결과 보기
- Security Hub 결과 새로 고침
- Trusted Advisor에서 Security Hub 사용 중지
- 문제 해결


## 필수 조건

Security Hub와 Trusted Advisor 통합을 사용하려면 다음 요구 사항을 충족해야 합니다.

- 이 기능을 사용하려면 Business, Enterprise On-Ramp 또는 Enterprise Support 플랜을 이용해야 합니다. 지원 플랜은 AWS Support 센터 또는 지원 플랜 페이지에서 찾을 수 있습니다. 자세한 내용은 AWS Support 플랜 비교를 참조하세요.
- Security Hub 컨트롤에 사용할 AWS 리전에 대해 AWS Config에서 리소스 기록을 사용 설정해야 합니다. 자세한 내용은 AWS Config 설정 및 구성을 참조하세요.
- Security Hub를 사용 설정하고 AWS Foundational Security Best Practices v1.0.0 보안 표준을 선택해야 합니다. 아직 이렇게 하지 않았다면 AWS Security Hub 사용 설명서의 AWS Security Hub 설정을 참조하세요.

> **Note**
>
> 이 사전 조건을 이미 완료한 경우 Security Hub 결과 보기 단계로 건너뛸 수 있습니다.

### AWS Organizations 계정 정보

관리 계정에 대한 사전 조건을 이미 완료한 경우, 조직의 모든 구성원 계정에 대해 이 통합이 자동으로 사용 설정됩니다. 개별 구성원 계정에서 이 기능을 사용 설정하기 위해 AWS Support에 연락할 필요는

없습니다. 그러나 조직의 구성원 계정이 Trusted Advisor에서 결과를 보려면 Security Hub를 사용 설정해야 합니다.

특정 구성원 계정에 대해 이 통합을 사용 중지하려면 AWS Organizations 계정에서 이 기능 사용 중지 섹션을 참조하세요.

## Security Hub 결과 보기

계정에 Security Hub를 사용 설정한 후 결과가 Trusted Advisor 콘솔의 보안 페이지에 표시되기까지 최대 24시간이 걸릴 수 있습니다.

Trusted Advisor에서 Security Hub 결과 보기

1. Trusted Advisor 콘솔로 이동한 다음 보안(Security) 범주를 선택합니다.
2. 키워드로 검색(Search by keyword) 필드에서 컨트롤 이름이나 설명을 필드에 입력합니다.

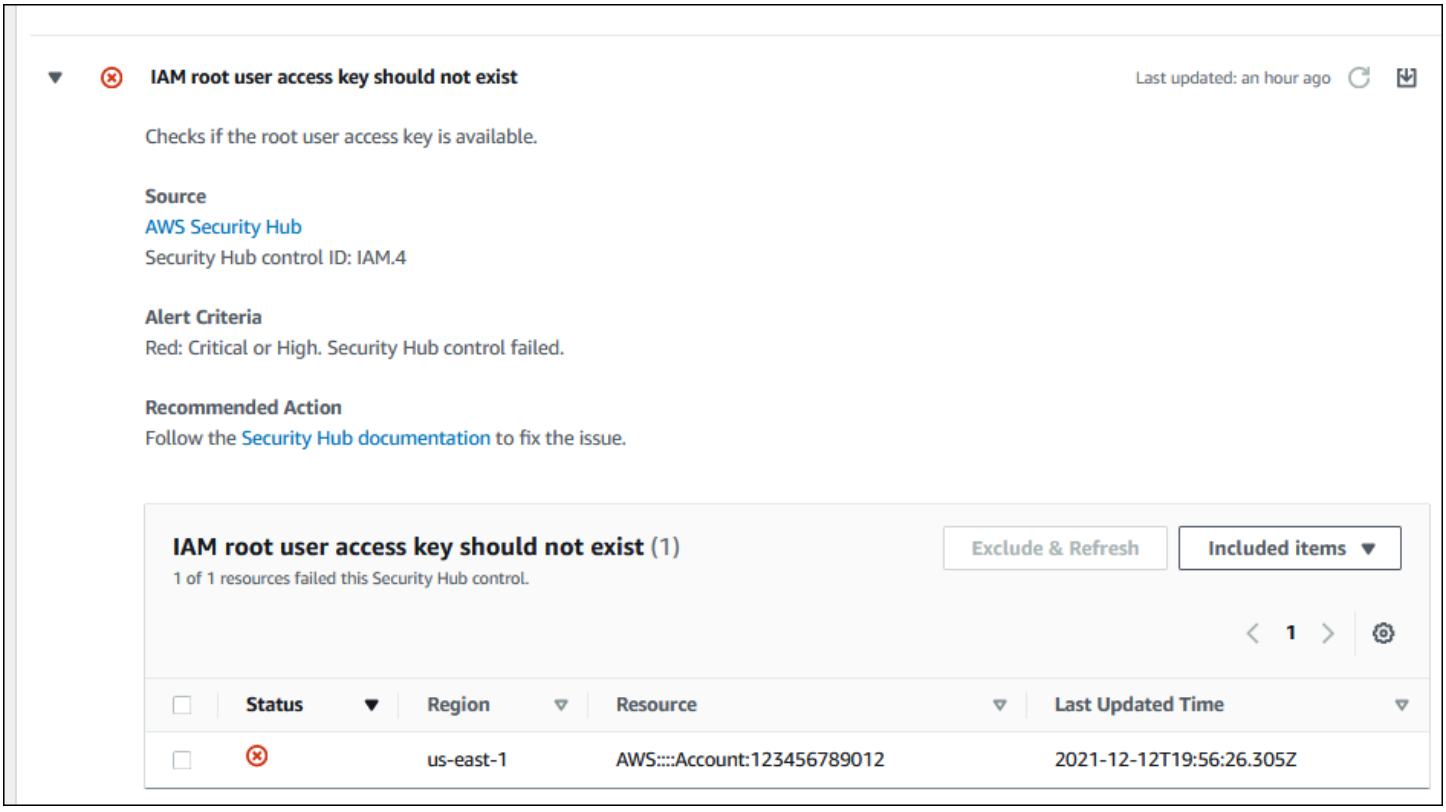
> **Tip**
>
> 소스(Source)에서 AWS Security Hub를 선택하여 Security Hub 컨트롤을 필터링할 수 있습니다.

3. Security Hub 컨트롤 이름을 선택하여 다음 정보를 확인합니다.
   - 설명(Description) - 이 컨트롤이 계정에서 보안 취약성을 검사하는 방법을 설명합니다.
   - 소스(Source) - 검사가 AWS Trusted Advisor 또는 AWS Security Hub 중 어디에서 실행되었는지 확인합니다. Security Hub 컨트롤의 경우 컨트롤 ID를 찾을 수 있습니다.
   - 알림 기준(Alert Criteria) - 컨트롤의 상태입니다. 예를 들어 Security Hub에서 중요한 문제를 감지하면 상태가 빨간색: 심각 또는 높음(Red: Critical or High)으로 표시될 수 있습니다.
   - 권장 조치(Recommended Action) - Security Hub 설명서 링크를 사용하여 문제를 해결하기 위한 권장 단계를 찾을 수 있습니다.
   - Security Hub 리소스(Security Hub resources) - Security Hub가 문제를 감지한 리소스를 계정에서 찾을 수 있습니다.

> **주의**
>
> - 결과에서 리소스를 제외하려면 Security Hub를 사용해야 합니다. 현재는 Trusted Advisor 콘솔을 사용하여 Security Hub 컨트롤에서 항목을 제외할 수 없습니다. 자세한 내용은 결과에 대한 워크플로 상태 설정을 참조하세요.
> - 조직 보기 기능은 이러한 Security Hub와의 통합을 지원합니다. 조직 전체에서 Security Hub 컨트롤에 대한 결과를 확인한 다음 보고서를 생성하고 다운로드할 수 있습니다. 자세한 내용은 AWS Trusted Advisor에 대한 조직 보기 섹션을 참조하세요.

Example 예: IAM 사용자 액세스 키에 대한 Security Hub 컨트롤이 존재하지 않아야 합니다.

다음은 Trusted Advisor 콘솔에서 Security Hub 컨트롤에 대한 보안 취약성 검사 결과의 예입니다.




## Security Hub 결과 새로 고침

보안 표준을 사용 설정한 후 Security Hub가 리소스에 대한 결과를 가져오는 데 최대 2시간이 걸릴 수 있습니다. 그 후 해당 데이터가 Trusted Advisor 콘솔에 표시되는 데 최대 24시간이 걸릴 수 있습니다. 최근에 AWS Foundational Security Best Practices v1.0.0 보안 표준을 사용 설정했다면, Trusted Advisor 콘솔을 나중에 다시 확인하세요.

> **Note**
>
> - 각 Security Hub 컨트롤의 갱신 일정은 주기적이거나 변경에 의해 트리거됩니다. 현재는 Trusted Advisor 콘솔 또는 AWS Support API를 사용하여 Security Hub 컨트롤을 새로 고침할 수 없습니다. 자세한 내용은 보안 검사 실행 일정을 참조하세요.
> - 결과에서 리소스를 제외하려면 Security Hub를 사용해야 합니다. 현재는 Trusted Advisor 콘솔을 사용하여 Security Hub 컨트롤에서 항목을 제외할 수 없습니다. 자세한 내용은 결과에 대한 워크플로 상태 설정을 참조하세요.

## Trusted Advisor에서 Security Hub 사용 중지

Security Hub 정보가 Trusted Advisor 콘솔에 표시되지 않도록 하려면 이 절차를 따르세요. 이 절차는 Security Hub와 Trusted Advisor 통합만 사용 중지합니다. Security Hub의 구성에는 영향을 미치지 않습니다. Security Hub 콘솔을 계속 사용하여 보안 컨트롤, 리소스 및 권장 사항을 볼 수 있습니다.

Security Hub 통합 사용 중지

1. AWS Support에 연락하여 Security Hub와 Trusted Advisor 통합 사용 중지를 요청합니다.

   AWS Support가 이 기능을 비활성화하고 나면 Security Hub가 더 이상 Trusted Advisor로 데이터를 전송하지 않습니다. Security Hub 데이터가 Trusted Advisor에서 제거됩니다.
2. 이 통합을 다시 사용 설정하려면 AWS Support에 연락하세요.

### AWS Organizations 계정에서 이 기능 사용 중지

관리 계정에 대한 이전 절차를 이미 완료한 경우 조직의 모든 구성원 계정에서 Security Hub 통합이 자동으로 제거됩니다. 조직의 개별 구성원 계정에서 별도로 AWS Support에 연락할 필요가 없습니다.

조직 내 구성원 계정의 사용자인 경우 AWS Support에 연락하여 본인의 계정에서만 이 기능을 제거할 수 있습니다.

## 문제 해결

이 통합에 문제가 있는 경우 다음 문제 해결 정보를 참조하세요.

목차

- Trusted Advisor 콘솔에서 Security Hub 결과가 표시되지 않음

- Security Hub와 AWS Config를 올바르게 구성했지만 여전히 결과를 확인할 수 없음
- 특정 Security Hub 제어를 비활성화하고 싶습니다.
- 제외된 Security Hub 리소스를 찾으려는 경우
- AWS 조직에 속한 구성원 계정에 대해 이 기능 사용 설정 또는 사용 중지
- Security Hub 검사로 같은 영향을 받는 리소스에 여러 AWS 리전이 표시됩니다
- 리전에서 Security Hub 또는 AWS Config를 비활성화했습니다.
- 내 컨트롤은 Security Hub에 아카이빙되어 있지만 Trusted Advisor에서 결과는 여전히 볼 수 있습니다.
- 여전히 Security Hub 결과를 볼 수 없음

## Trusted Advisor 콘솔에서 Security Hub 결과가 표시되지 않음

다음 단계를 완료했는지 확인하세요.

- Business, Enterprise On-Ramp 또는 Enterprise Support 플랜을 이용 중입니다.
- Security Hub와 같은 리전 내에서 AWS Config의 리소스 기록을 사용 설정했습니다.
- Security Hub를 사용 설정하고 AWS Foundational Security Best Practices v1.0.0 보안 표준을 선택했습니다.
- Security Hub의 새 컨트롤은 2~4주 내에 검사로 Trusted Advisor에 추가됩니다. 참고를 참조하세요.

자세한 내용은 필수 조건 부분을 참조하세요.

## Security Hub와 AWS Config를 올바르게 구성했지만 여전히 결과를 확인할 수 없음

Security Hub가 리소스에 대한 결과를 가져오는 데 최대 2시간이 걸릴 수 있습니다. 그 후 해당 데이터가 Trusted Advisor 콘솔에 표시되는 데 최대 24시간이 걸릴 수 있습니다. Trusted Advisor 콘솔을 나중에 다시 확인하세요.

> 주의
>
> - AWS Foundational Security Best Practices 보안 표준의 컨트롤에 대한 결과만 Trusted Advisor에 표시됩니다. 단, 범주: 복구 > 복원성(Category: Recover > Resilience)이 있는 컨트롤은 예외입니다.

- Security Hub에 서비스 문제가 있거나 Security Hub가 사용 불가능한 경우, 결과가 Trusted Advisor에 표시되는 데 최대 24시간이 걸릴 수 있습니다. Trusted Advisor 콘솔을 나중에 다시 확인하세요.

## 특정 Security Hub 제어를 비활성화하고 싶습니다.

Security Hub는 데이터를 자동으로 Trusted Advisor에 전송합니다. Security Hub 컨트롤을 사용 중지하거나 해당 컨트롤에 대한 리소스가 더 이상 없는 경우 결과가 Trusted Advisor에 표시되지 않습니다.

Security Hub 콘솔에 로그인하여 컨트롤이 사용 설정되어 있는지 여부를 확인할 수 있습니다.

Security Hub 컨트롤을 비활성화하거나 AWS Foundational Security Best Practices 보안 표준에 대한 모든 제어를 비활성화하면 결과가 향후 5일 내에 아카이브됩니다. 이 5일간의 아카이빙 기간은 근사치이며 항상 보장되지는 않습니다. 아카이빙된 검사 결과는 Trusted Advisor에서 제거됩니다.

자세한 정보는 다음 주제를 참조하세요.

- 개별 제어 비활성화 및 활성화
- 보안 표준 비활성화 또는 활성화

## 제외된 Security Hub 리소스를 찾으려는 경우

Trusted Advisor 콘솔에서 Security Hub 컨트롤 이름을 선택한 다음, 제외된 항목(Excluded items) 옵션을 선택할 수 있습니다. 이 옵션은 Security Hub에서 숨겨진 모든 리소스를 표시합니다.

리소스에 대한 워크플로 상태가 SUPPRESSED로 설정된 경우, 해당 리소스는 Trusted Advisor에서 제외된 항목입니다. Trusted Advisor 콘솔에서는 Security Hub 리소스를 숨길 수 없습니다. 리소스를 숨기려면 Security Hub 콘솔을 사용하세요. 자세한 내용은 결과에 대한 워크플로 상태 설정을 참조하세요.

## AWS 조직에 속한 구성원 계정에 대해 이 기능 사용 설정 또는 사용 중지

기본적으로 구성원 계정은 AWS Organizations 관리 계정으로부터 기능을 상속합니다. 관리 계정에서 이 기능을 사용 설정한 경우 조직의 모든 계정도 해당 기능을 사용할 수 있게 됩니다. 구성원 계정이 있고 해당 계정에 대해 특정 설정을 변경하려면 AWS Support에 연락해야 합니다.

### Security Hub 검사로 같은 영향을 받는 리소스에 여러 AWS 리전이 표시됩니다

IAM 및 Amazon CloudFront CloudFront와 같은 일부 AWS 서비스는 글로벌로 제공되며 특정 리전에 국한되지 않습니다. 기본적으로 Amazon S3 버킷과 같은 글로벌 리소스는 미국 동부(버지니아 북부) 리전에 나타납니다.

글로벌 서비스에 대한 리소스를 평가하는 Security Hub 검사의 경우 영향을 받는 리소스 항목이 두 개 이상 표시될 수 있습니다. 예를 들어 `Hardware MFA should be enabled for the root user` 검사로 계정에서 이 기능을 활성화하지 않았다고 파악되면 동일한 리소스에 대한 여러 리전이 테이블에 표시됩니다.

Security Hub 및 AWS Config 구성으로 동일한 리소스에 대해 여러 리전을 표시하지 않을 수 있습니다. 자세한 내용은 비활성화할 수 있는 AWS 기초 모범 사례 컨트롤 단원을 참조하세요.

### 리전에서 Security Hub 또는 AWS Config를 비활성화했습니다.

AWS 리전에서 AWS Config를 사용하여 리소스 기록을 중지하거나 Security Hub를 비활성화하면 Trusted Advisor는 해당 리전의 모든 컨트롤에 대한 데이터를 더 이상 수신하지 않습니다. Trusted Advisor는 7~9일 이내에 Security Hub 결과를 제거합니다. 이 기간은 최선의 노력이며 보장되지 않습니다. 자세한 내용은 Security Hub 비활성화를 참조하세요.

계정에서 이 기능을 비활성화하려면 Trusted Advisor에서 Security Hub 사용 중지 섹션을 참조하세요.

### 내 컨트롤은 Security Hub에 아카이빙되어 있지만 Trusted Advisor에서 결과는 여전히 볼 수 있습니다.

결과에 대한 `RecordState` 상태가 `ARCHIVED`으로 변경되면 Trusted Advisor가 계정에서 Security Hub 컨트롤에 대한 결과를 삭제합니다. 삭제되기 전에 최대 7~9일 동안 Trusted Advisor에 결과가 계속 표시될 수 있습니다. 이 기간은 최선의 노력이며 보장되지 않습니다.

### 여전히 Security Hub 결과를 볼 수 없음

이 기능을 사용하는 데 여전히 문제가 있는 경우, AWS Support 센터에서 기술 지원 사례를 생성할 수 있습니다.

## Trusted Advisor 수표 AWS Compute Optimizer 신청

Compute Optimizer는 AWS 리소스의 구성 및 사용률 지표를 분석하는 서비스입니다. 이 서비스는 리소스가 효율성과 신뢰성을 위해 올바르게 구성되었는지 여부를 보고합니다. 또한 워크로드 성능을 향

상시키기 위해 구현할 수 있는 개선 사항도 제안합니다. Compute Optimizer를 사용하면 검사에서 동일한 권장 사항을 확인할 수 Trusted Advisor 있습니다.

조직에 속한 사용자 AWS 계정 계정만 옵트인하거나 모든 멤버 계정을 옵트인할 수 있습니다. AWS Organizations자세한 내용은 AWS Compute Optimizer 사용 설명서에서 시작하기를 참조하세요.

Compute Optimizer를 옵트인하면 다음 검사는 Lambda 함수 및 Amazon EBS 볼륨에서 데이터를 받습니다. 결과 및 최적화 권장 사항을 생성하는 데 최대 12시간이 걸릴 수 있습니다. 그러면 다음 검사의 결과를 확인하는 데 최대 48시간이 걸릴 수 있습니다. Trusted Advisor

### 비용 최적화

- Amazon EBS 과다 프로비저닝된 볼륨
- AWS Lambda 메모리 크기 때문에 오버프로비저닝된 함수

### 성능

- Amazon EBS 과소 프로비저닝된 볼륨
- AWS Lambda 메모리 크기에 비해 부족하게 프로비저닝된 함수

> **참고**
>
> - 이러한 검사에 대한 결과는 매일 여러 번 자동으로 새로 고침됩니다. 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이러한 검사에서 리소스를 제외할 수 없습니다.
> - Trusted Advisor 이미 사용률이 낮은 Amazon EBS 볼륨과 과다 사용 Amazon EBS 마그네틱 볼륨 검사를 받았습니다.
>
>  Compute Optimizer를 사용하여 옵트인한 후에는 새로운 Amazon EBS 과다 프로비저닝된 볼륨 및 Amazon EBS 과소 프로비저닝된 볼륨 검사를 대신 사용하는 것이 좋습니다.

## 관련 정보

자세한 정보는 다음 주제를 참조하세요.

- AWS Compute Optimizer 사용 설명서의 Amazon EBS 볼륨 권장 사항 보기
- AWS Compute Optimizer 사용 설명서의 Lambda 함수 권장 사항 보기

- AWS Lambda 개발자 안내서의 Lambda 함수 메모리 구성
- Amazon EC2 사용 설명서에서 Amazon EBS 볼륨에 대한 수정을 요청하십시오.

# AWS Trusted Advisor Priority 시작하기

Trusted Advisor Priority는 AWS 계정을 보호 및 최적화하고 AWS 모범 사례를 따르는 데 도움이 됩니다. AWS 계정 팀은 Trusted Advisor Priority를 사용하여 계정을 사전에 모니터링하고 기회가 식별될 경우 우선 순위가 지정된 권장 사항을 생성할 수 있습니다.

예를 들어 계정 팀은 AWS 계정 루트 사용자에 다중 인증(MFA)이 없는지 확인할 수 있습니다. 계정 팀은 수표 상에 `MFA on Root Account`와(과) 같은 즉각적인 조치를 취할 수 있도록 권장 사항을 생성할 수 있습니다. 권장 사항은 Trusted Advisor 콘솔의 Trusted Advisor Priority 페이지에 활성 우선 순위 지정 권장 사항으로 표시됩니다. 그런 다음 권장 사항에 따라 문제를 해결합니다.

Trusted Advisor Priority 권장 사항은 다음 두 가지 소스 중에서 얻습니다.

- AWS 서비스 - Trusted Advisor, AWS Security Hub 및AWS Well-Architected와 같은 서비스에서는 권장 사항을 자동으로 생성합니다. 이러한 권장 사항이 Trusted Advisor 우선순위에 표시되도록 계정 팀은 해당 권장 사항을 사용자와 공유합니다.
- 계정 팀 - 계정 팀은 수동 권장 사항을 생성할 수 있습니다.

Trusted Advisor Priority는 가장 중요한 권장 사항에 집중할 수 있도록 도와줍니다. 사용자와 계정 팀은 계정 팀이 권장 사항을 공유한 시점부터 사용자가 권장 사항을 승인, 해결 또는 취소할 때까지의 권장 사항 수명 주기를 모니터링할 수 있습니다. Trusted Advisor Priority를 사용하여 조직의 모든 멤버 계정에 대한 권장 사항을 확인할 수 있습니다.

주제

- 사전 조건
- Trusted Advisor Priority 사용
- 우선 순위 지정 권장 사항 보기
- 권장 사항 승인
- 권장 사항 취소
- 권장 사항 해결
- 권장 사항 다시 열기
- 권장 사항 세부 정보 다운로드

- 위임된 관리자 등록
- 위임된 관리자 등록 취소
- Trusted Advisor Priority 알림 관리
- Trusted Advisor Priority 사용 중지

## 사전 조건

Trusted Advisor 우선순위를 사용하려면 다음 요구 사항을 충족해야 합니다.

- Enterprise Support 계획이 있어야 합니다.
- 계정은 AWS Organizations의 모든 기능을 활성화해야 합니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하세요.
- 조직에서 Trusted Advisor에 대한 신뢰할 수 있는 액세스를 활성화해야 합니다. 신뢰할 수 있는 액세스를 사용하려면 관리 계정으로 로그인합니다. Trusted Advisor 콘솔에서 내 조직 페이지를 엽니다.
- 계정의 Trusted Advisor 우선 순위 권장 사항을 보려면 AWS 계정에 로그인해야 합니다.
- 조직 전체에서 집계된 권장 사항을 보려면 조직의 관리 계정이나 위임된 관리자 계정에 로그인해야 합니다. 위임된 관리자 계정을 등록하는 방법에 대한 지침은 위임된 관리자 등록을(를) 참조하세요.
- Trusted Advisor Priority에 액세스하려면 AWS Identity and Access Management(IAM) 권한이 있어야 합니다. Trusted Advisor Priority 액세스를 제어하는 방법에 대한 자세한 내용은 액세스 관리: AWS Trusted Advisor 및 AWS 관리형 정책: AWS Trusted Advisor 단원을 참조하세요.

## Trusted Advisor Priority 사용

계정 팀에 연락하여 이 기능을 활성화하도록 요청합니다. Enterprise Support 플랜이 있어야 하며 조직의 관리 계정 소유자여야 합니다. 콘솔의 Trusted Advisor Priority 페이지에 AWS Organizations를 포함한 신뢰할 수 있는 액세스가 필요하다고 표시되면 AWS Organizations를 포함한 신뢰할 수 있는 액세스 활성화를 선택합니다. 자세한 내용은 사전 조건(을)를 참조하세요.

## 우선 순위 지정 권장 사항 보기

계정 팀에서 Trusted Advisor Priority를 활성화하면 AWS 계정에 대한 최신 권장 사항을 볼 수 있습니다.

우선 순위 지정 권장 사항 보기

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.

2. Trusted Advisor 우선순위 페이지에서 다음 사항을 확인할 수 있습니다.

   AWS Organizations 관리 또는 위임 관리자 계정을 사용하는 경우 내 계정 탭으로 전환하십시오.

   - 필요한 작업 - 응답을 보류 중이거나 진행 중인 권장 사항의 수입니다.
   - Overview(개요) – 다음 정보:
     - 지난 90일 동안 거부된 권장 사항
     - 지난 90일 동안 해결된 권장 사항
     - 30일 이상 업데이트가 없는 권장 사항
     - 권장 사항을 해결하는 데 걸리는 평균 시간
3. 활성 탭의 활성 우선 순위 지정 권장 사항에는 계정 팀이 우선 순위를 지정한 권장 사항이 표시됩니다. 마무리 탭에는 해결되거나 거부된 권장 사항이 표시됩니다.

   - 결과를 필터링하려면 다음 옵션을 사용하세요.
     - Recommendation(권장 사항) - 키워드를 입력하고 이름으로 검색합니다. 검사 이름 또는 계정 팀이 생성한 사용자 정의 이름일 수 있습니다.
     - 상태 - 권장 사항이 응답 보류 중, 진행 중, 취소 또는 해결 상태 여부를 보여줍니다.
     - 소스 - 우선 순위가 지정된 권장 사항의 출처입니다. 권장 사항은 AWS 서비스, AWS 계정 팀 또는 계획된 서비스 이벤트에서 제공될 수 있습니다.
     - 카테고리 - 보안 또는 비용 최적화와 같은 권장 사항 카테고리입니다.
     - Age(기간) - 계정 팀이 권장 사항을 공유한 시점입니다.
4. 권장 사항을 선택하여 세부 정보, 영향을 받는 리소스 및 권장 조치에 대해 자세히 알아봅니다. 그런 다음 권장 사항을 승인하거나 취소할 수 있습니다.

AWS 조직 내 모든 계정에서 우선순위가 지정된 권장 사항을 보는 방법

관리 계정과 Trusted Advisor Priority 위임 관리자 모두 조직 전체에서 집계된 권장 사항을 볼 수 있습니다.

> **Note**
>
> 회원 계정에는 집계된 권장 사항에 액세스할 수 없음.

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.

2. Trusted Advisor 우선순위 페이지에서 내 조직 탭에 있는지 확인하세요.
3. 한 계정에 대한 권장 사항을 보려면 조직에서 계정 선택 드롭다운 목록에서 계정을 선택하세요. 또는 모든 계정의 권장 사항을 볼 수 있습니다.

   내 조직 탭에서는 다음 항목을 볼 수 있습니다.

   - 필요한 작업: 조직 전체에서 응답을 보류 중이거나 진행 중인 권장 사항의 수입니다.
   - 개요: 다음 항목을 보여줍니다.

     - 지난 90일 동안 거부된 권장 사항.

     - 지난 90일 동안 해결된 권장 사항.

     - 30일 이상 업데이트가 없는 권장 사항.

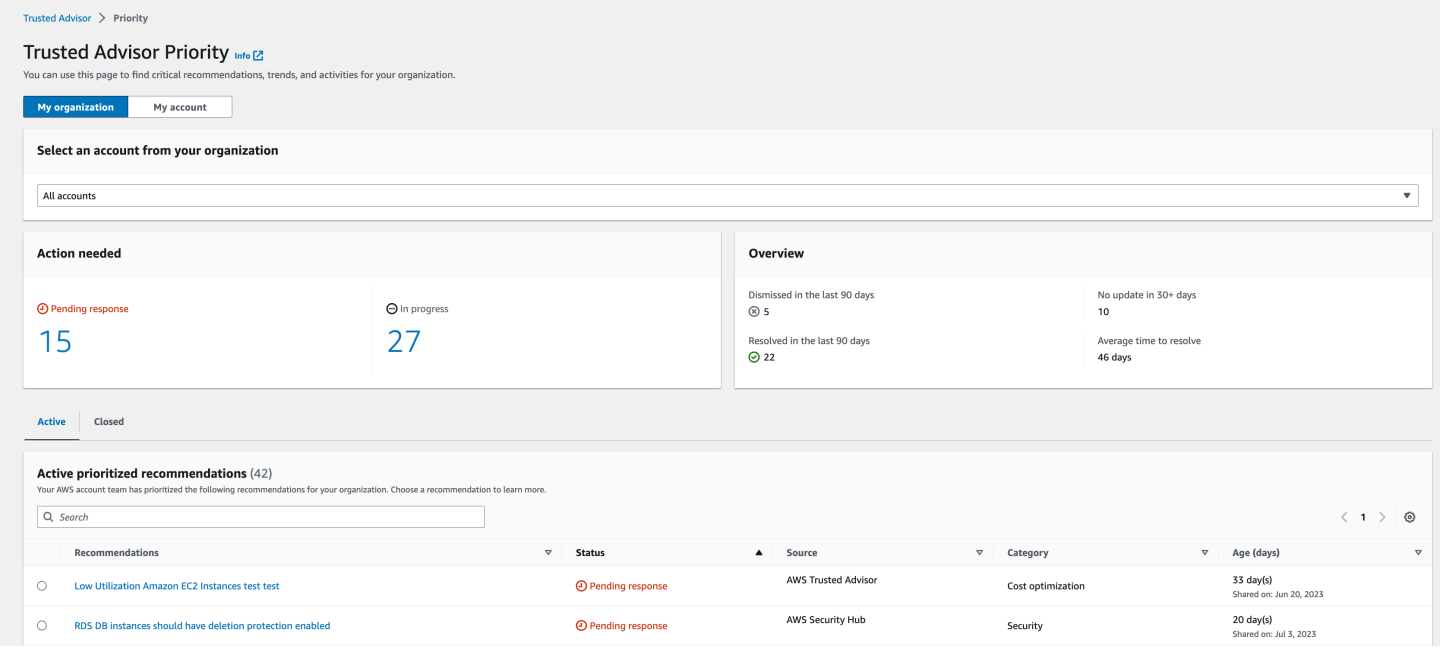
     - 권장 사항을 해결하는 데 걸리는 평균 시간.
4. 활성 탭의 활성 우선 순위 지정 권장 사항 섹션에는 계정 팀이 우선 순위를 지정한 권장 사항이 표시됩니다. 마무리 탭에는 해결되거나 거부된 권장 사항이 표시됩니다.

   결과를 필터링하려면 다음 옵션을 사용하세요.

   - Recommendation(권장 사항) - 키워드를 입력하고 이름으로 검색합니다. 검사 이름 또는 계정 팀이 생성한 사용자 정의 이름일 수 있습니다.
   - 상태 - 권장 사항이 응답 보류 중, 진행 중, 취소 또는 해결 상태 여부를 보여줍니다.
   - 소스 - 우선 순위가 지정된 권장 사항의 출처입니다. 권장 사항은 AWS 서비스, AWS 계정 팀 또는 계획된 서비스 이벤트에서 제공될 수 있습니다.
   - 카테고리 - 보안 또는 비용 최적화와 같은 권장 사항 카테고리입니다.
   - Age(기간) - 계정 팀이 권장 사항을 공유한 시점입니다.
5. 권장 사항을 선택하면 추가 세부 정보, 영향을 받는 계정 및 리소스, 권장 조치를 확인합니다. 그런 다음 권장 사항을 승인하거나 취소할 수 있습니다.

Example : Trusted Advisor Priority 권장 사항

다음 예제에서는 응답 대기 중인 27가지 권장 사항과 작업 필요 섹션에서 진행 중인 15가지 가지 권장 사항을 보여줍니다. 다음 이미지는 우선순위가 지정된 활성 권장 사항 탭에서 응답 보류 중인 두 가지 권장 사항을 보여줍니다.




# 권장 사항 승인

활성 탭에서 권장 사항에 대해 자세히 알아본 다음 승인할지 여부를 결정할 수 있습니다.

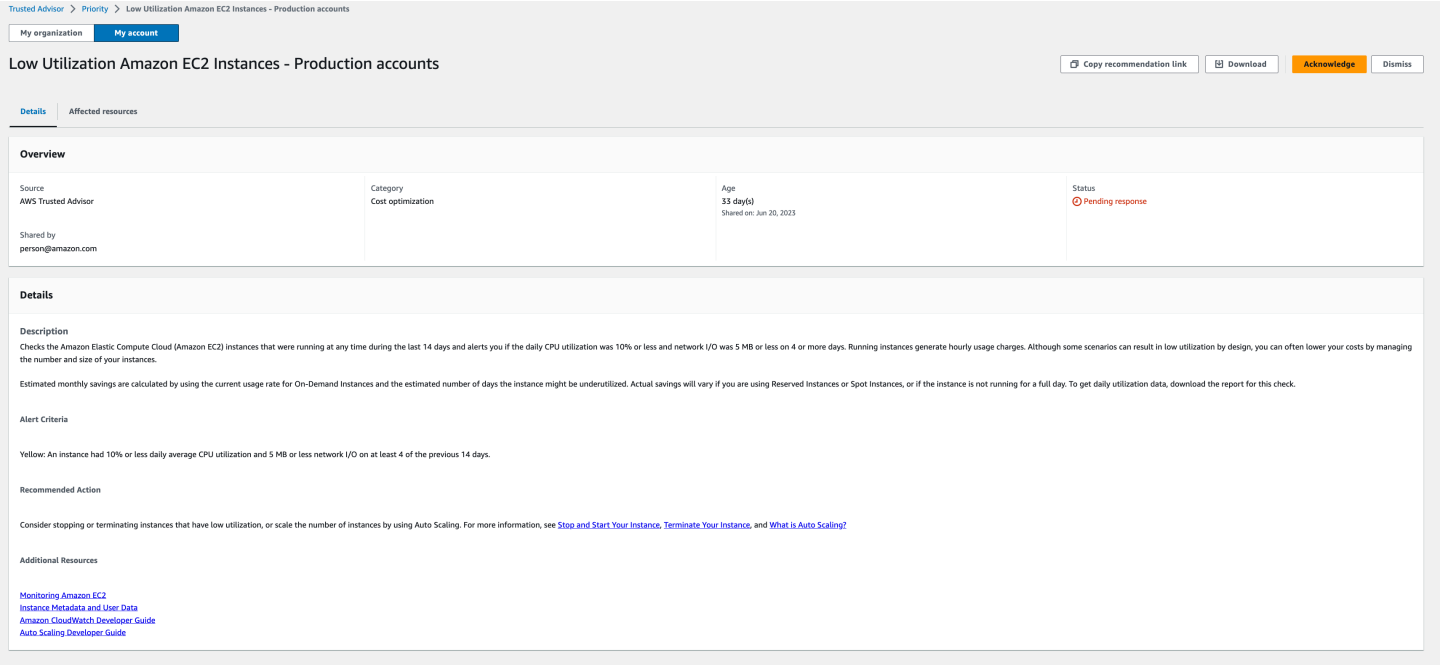
권장 사항을 승인하려면

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. AWS Organizations 관리 또는 위임 관리자 계정을 사용하는 경우 내 계정 탭으로 전환하십시오.
3. Trusted Advisor Priority 페이지의 Active(활성) 탭에서 권장 사항 이름을 선택합니다.
4. 세부 정보 섹션에서는 권장 사항 조치를 검토하여 권장 사항을 해결할 수 있습니다.
5. 영향을 받는 리소스 섹션에서 영향을 받는 리소스를 검토하고 상태별로 필터링할 수 있습니다.
6. 승인을 선택합니다.
7. 권장 사항 승인 대화 상자에서 승인을 선택합니다.

   권장 사항 상태가 진행 중으로 변경됩니다. 진행 중이거나 응답 보류 중인 권장 사항은 Trusted Advisor Priority 페이지의 Active(활성) 탭에 표시됩니다.
8. 권장 사항 조치에 따라 권장 사항을 해결합니다. 자세히 알아보려면 권장 사항 해결의 내용을 참조하세요.

Example : Trusted Advisor Priority의 수동 권장 사항

다음 이미지는 응답 보류 중인 낮은 사용률의 EC2 인스턴스 권장 사항을 보여줍니다.




AWS 조직 내 모든 계정에 대한 권장 사항을 승인하는 방법

관리 계정 또는 Trusted Advisor 위임 관리자는 영향을 받는 모든 계정에 대한 권장 사항을 승인할 수 있습니다.

> **Note**
>
> 회원 계정에는 집계된 권장 사항에 액세스할 수 없음.

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor 우선순위 페이지에서 내 조직 탭에 있는지 확인하세요.
3. 활성 탭에서 추천 이름을 선택합니다.
4. 승인을 선택합니다.
5. 권장 사항 승인 대화 상자에서 승인을 선택합니다.

   권장 사항 상태가 진행 중으로 변경됩니다.
6. 권장 사항 조치에 따라 권장 사항을 해결합니다. 자세히 알아보려면 권장 사항 해결의 내용을 참조하세요.
7. 권장 사항 세부 정보를 보려면 권장 사항 이름을 선택합니다.

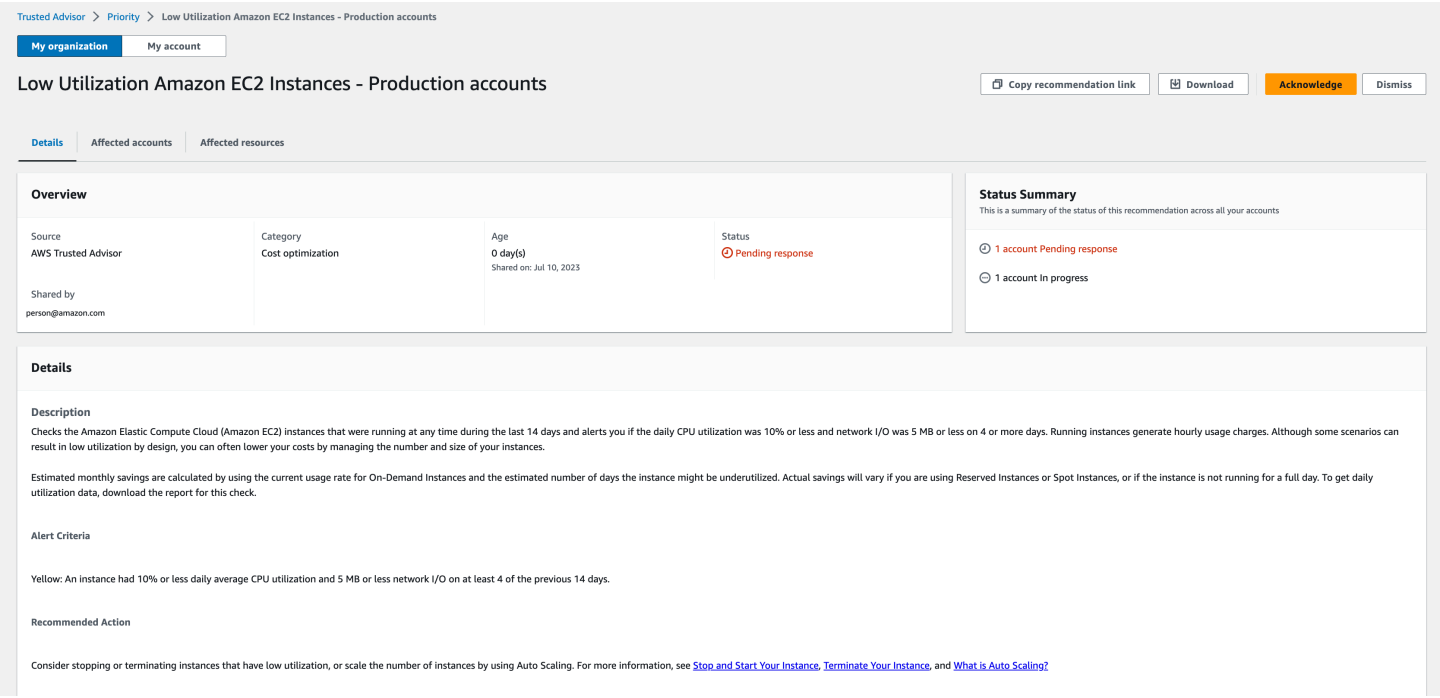
   세부 정보 섹션에서는 권장 사항에 대한 다음 정보를 검토할 수 있습니다.

- 권장 사항 개요 및 완료해야 할 권장 사항 조치를 다루는 세부 정보 섹션.

  영향을 받는 모든 계정의 권장 사항을 보여주는 상태 요약입니다.
- 영향을 받는 계정 섹션에서 모든 계정의 영향을 받는 리소스를 검토할 수 있습니다. 계정 번호 및 상태별로 필터링할 수 있습니다.
- 영향을 받는 리소스 섹션에서 모든 계정의 영향을 받는 리소스를 검토할 수 있습니다. 계정 번호 및 상태별로 필터링할 수 있습니다.

Example : Trusted Advisor Priority의 수동 권장 사항

다음 이미지는 응답 보류 중인 낮은 사용률의 Amazon EC2 인스턴스 권장 사항을 보여줍니다. 영향을 받은 한 계정이 권장 사항을 승인했습니다. 다른 계정이 응답을 보류 중이어서 추천 상태가 응답 보류 상태입니다.




# 권장 사항 취소

권장 사항을 취소할 수도 있습니다. 즉, 권장 사항을 승인하지만 해결하지 못합니다. 계정과 관련되지 않는 경우 권장 사항을 취소할 수 있습니다. 예를 들어 삭제하려는 AWS 계정 테스트가 있는 경우 권장 조치를 따르지 않아도 됩니다.

권장 사항을 취소하는 방법

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. AWS Organizations 관리 또는 위임 관리자 계정을 사용하는 경우 내 계정 탭으로 전환하십시오.
3. Trusted Advisor Priority 페이지의 Active(활성) 탭에서 권장 사항 이름을 선택합니다.
4. 권장 사항 세부 정보 페이지에서 영향을 받는 리소스에 대한 정보를 검토합니다.
5. 이 권장 사항이 계정에 적용되지 않는 경우 취소를 선택합니다.
6. 권장 사항 거부 대화 상자에서 권장 사항을 해결하지 못하는 이유를 선택합니다.
7. (선택 사항) 권장 사항을 취소하는 이유에 대한 세부 사항을 입력합니다. 기타를 선택한 경우 메모 섹션에 설명을 입력해야 합니다.
8. 취소를 선택합니다. 권장 사항 상태가 취소됨으로 변경되고 Trusted Advisor Priority 페이지의 마감 탭에 표시됩니다.

AWS 조직 내 모든 계정에 대한 추천을 취소하는 방법

관리 계정 또는 Trusted Advisor 우선순위의 위임된 관리자는 모든 계정에 대한 추천을 거부할 수 있습니다.

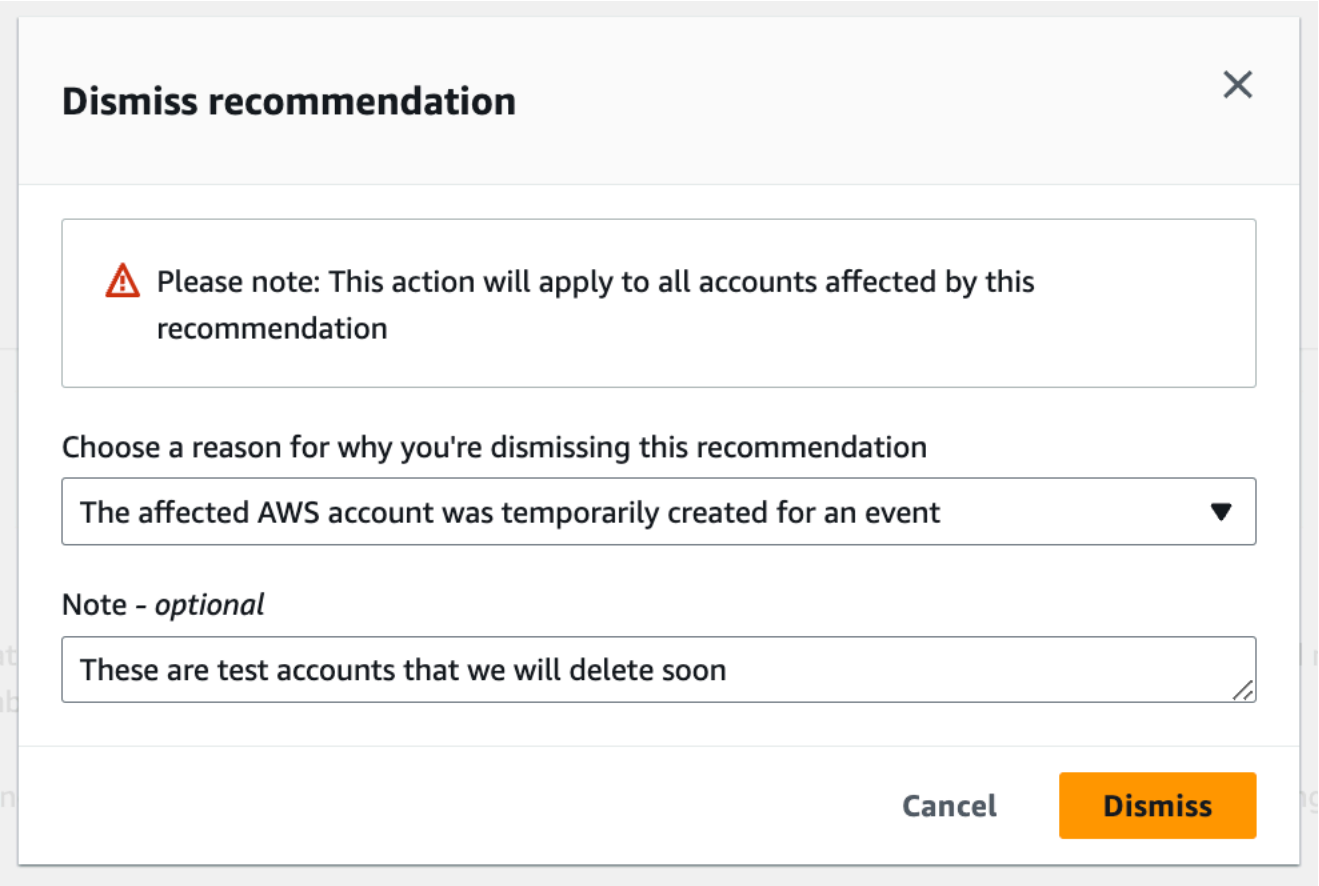
1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor우선순위 페이지에서 내 조직 탭에 있는지 확인하세요.
3. 활성 탭에서 추천 이름을 선택합니다.
4. 이 권장 사항이 계정에 적용되지 않는 경우 취소를 선택합니다.
5. 권장 사항 거부 대화 상자에서 권장 사항을 해결하지 못하는 이유를 선택합니다.
6. (선택 사항) 권장 사항을 취소하는 이유에 대한 세부 사항을 입력합니다. 기타를 선택한 경우 메모 섹션에 설명을 입력해야 합니다.
7. 취소를 선택합니다. 권장 사항 상태가 거부됨으로 변경됩니다. 권장 사항은 Trusted Advisor 우선순위 페이지의 종료됨 탭에 표시됩니다.

> **Note**
>
> 권장 사항 이름을 선택하고 메모 보기를 선택하여 취소 사유를 찾을 수 있습니다. 계정 팀에서 권장 사항을 취소한 경우 해당 이메일 주소가 메모 옆에 표시됩니다.

또한 권장 사항이 취소된 사실을 Trusted Advisor Priority에서 계정 팀에 알립니다.

Example :Trusted Advisor Priority 계정에서 권장 사항 취소

다음 예제에서는 권장 사항을 취소하는 방법을 보여줍니다.




## 권장 사항 해결

권장 사항을 승인하고 권장 조치를 완료한 후 권장 사항을 해결할 수 있습니다.

> **Tip**
> 권장 사항을 해결한 후에는 권장 사항을 다시 열 수 없습니다. 나중에 권장 사항을 다시 보려면 권장 사항 취소 섹션을 참조하세요.

권장 사항 해결

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.

2. Trusted Advisor 우선순위 페이지에서 내 조직 탭에 있는지 확인하세요.
3. Trusted Advisor Priority 페이지에서 권장 사항을 선택한 다음 해결을 선택합니다.
4. 권장 사항 해결 대화 상자에서 해결을 선택합니다. 해결된 권장 사항은 Trusted Advisor Priority 페이지의 Closed(마감) 탭에 표시됩니다. Trusted Advisor 또한 권장 사항이 해결된 사실을 Priority에서 계정 팀에 알립니다.

AWS 조직 내 모든 계정에 대한 권장 사항을 해결하는 방법

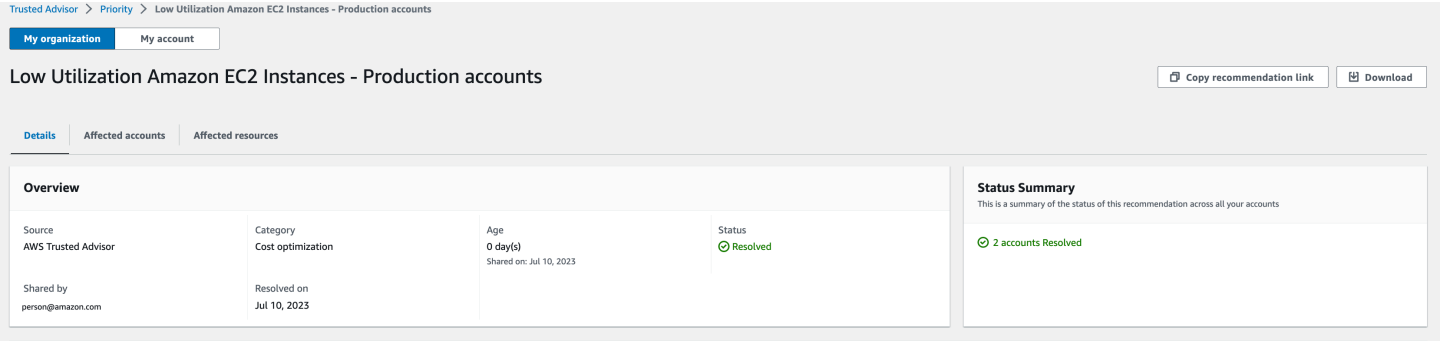
관리 계정 또는 Trusted Advisor 우선순위를 위임받은 관리자는 모든 계정에 대한 권장 사항을 해결할 수 있습니다.

> **Note**
>
> 회원 계정에는 집계된 권장 사항에 액세스할 수 없음.

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. AWS Organizations 관리 또는 위임 관리자 계정을 사용하는 경우 내 계정 탭으로 전환하십시오.
3. 활성 탭에서 추천 이름을 선택합니다.
4. 이 권장 사항이 계정에 적용되지 않는 경우 Resolve를 선택합니다.
5. 권장 사항 해결 대화 상자에서 해결을 선택합니다. 해결된 권장 사항은 Trusted Advisor Priority 페이지의 Closed(마감) 탭에 표시됩니다. Trusted Advisor 또한 권장 사항이 해결된 사실을 Priority에서 계정 팀에 알립니다.

Example : Trusted Advisor Priority의 수동 권장 사항

다음 예제는 낮은 사용률의 Amazon EC2 인스턴스 권장 사항을 보여줍니다.



# 권장 사항 다시 열기

권장 사항을 거부한 후 사용자 또는 계정 팀에서 권장 사항을 다시 열 수 있습니다.

권장 사항을 다시 열려면

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. AWS Organizations 관리 또는 위임 관리자 계정을 사용하는 경우 내 계정 탭으로 전환하십시오.
3. Trusted Advisor Priority 페이지에서 Closed(마감) 탭을 선택합니다.
4. 마감된 권장 사항에서 취소된 권장 사항을 선택한 다음 다시 열기를 선택합니다.
5. 권장 사항 다시 열기 대화 상자에서 권장 사항을 다시 여는 이유를 설명하세요.
6. Reopen(다시 열기)을 선택합니다. 권장 사항 상태가 In progress(진행 중)로 변경되고 Active(활성) 탭에 표시됩니다.

> **Tip**
>
> 권장 사항 이름을 선택한 다음 메모 보기를 선택하여 다시 여는 이유를 찾을 수 있습니다. 계정 팀에서 권장 사항을 다시 연 경우 메모 옆에 해당 팀의 이름이 표시됩니다.

7. 권장 사항 세부 정보의 단계를 따릅니다.

AWS 조직 내 모든 계정에 대한 권장 사항을 다시 여는 방법

관리 계정 또는 Trusted Advisor 우선순위를 위임받은 관리자는 모든 계정에 대한 권장 사항을 다시 열 수 있습니다.

> **Note**
>
> 회원 계정에는 집계된 권장 사항에 액세스할 수 없음.

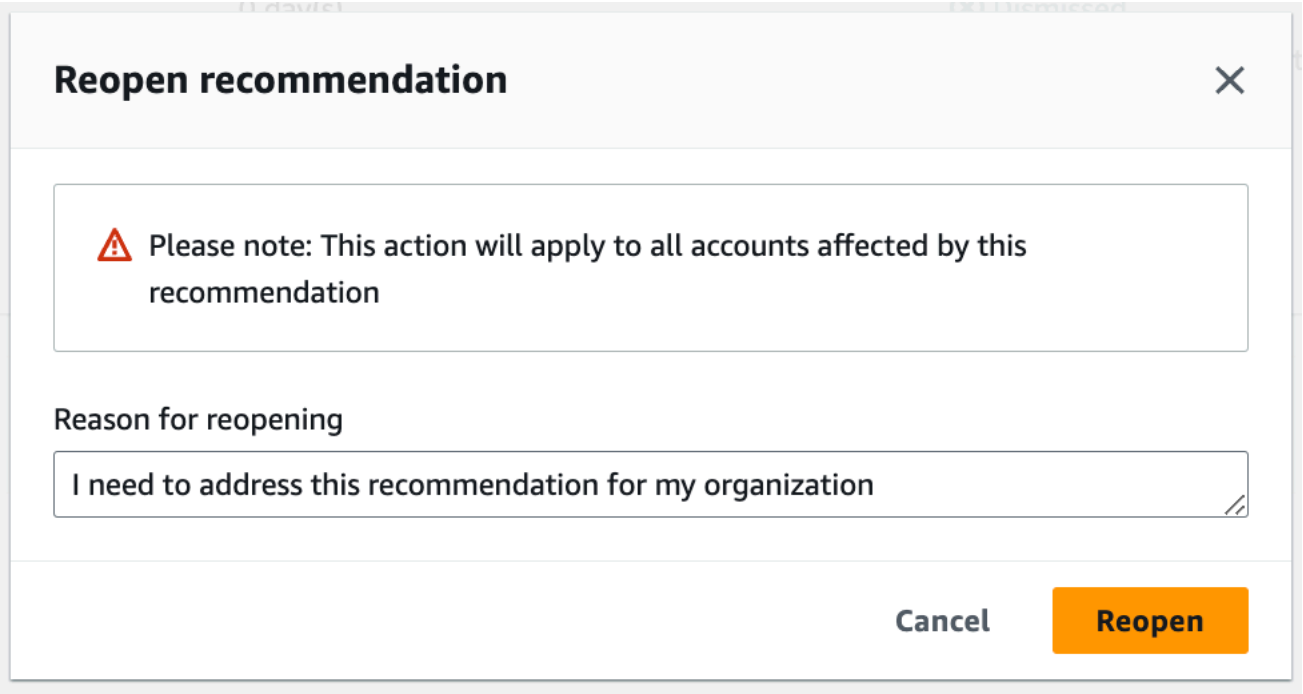
1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor 우선순위 페이지에서 내 조직 탭에 있는지 확인하세요.
3. 마감된 권장 사항에서 취소된 권장 사항을 선택한 다음 다시 열기를 선택합니다.
4. 권장 사항 다시 열기 대화 상자에서 권장 사항을 다시 여는 이유를 설명하세요.
5. Reopen(다시 열기)을 선택합니다. 권장 사항 상태가 In progress(진행 중)로 변경되고 Active(활성) 탭에 표시됩니다.

> **Tip**
>
> 권장 사항 이름을 선택하고 메모 보기를 선택하여 다시 여는 이유를 찾을 수 있습니다. 계정 팀에서 권장 사항을 다시 연 경우 메모 옆에 해당 팀의 이름이 표시됩니다.

6. 권장 사항 세부 정보의 단계를 따릅니다.

Example : Trusted Advisor Priority에서 권장 사항 다시 열기

다음 예는 다시 열려는 권장 사항을 보여줍니다.




## 권장 사항 세부 정보 다운로드

우선 순위 지정 권장 사항의 결과를 Trusted Advisor Priority에서 다운로드할 수 있습니다.

> **Note**
>
> 현재 한 번에 하나의 권장 사항만 다운로드할 수 있습니다.

권장 사항 다운로드

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.

2. Trusted Advisor Priority 페이지에서 권장 사항을 선택한 다음 다운로드를 선택합니다.
3. 파일을 열어 권장 사항 세부 정보를 볼 수 있습니다.

## 위임된 관리자 등록

조직에 속한 멤버 계정을 위임된 관리자로 추가할 수 있습니다. 위임된 관리자 계정은 Trusted Advisor Priority에서 권장 사항을 검토, 승인, 해결, 취소 및 다시 열 수 있습니다.

계정을 등록한 이후에 위임된 관리자에게 Trusted Advisor Priority에 액세스에 하는 데 필요한 AWS Identity and Access Management 권한을 부여해야 합니다. 자세한 내용은 액세스 관리: AWS Trusted Advisor 및 AWS 관리형 정책: AWS Trusted Advisor 단원을 참조하세요.

최대 5개의 멤버 계정을 등록할 수 있습니다. 관리 계정만 조직에 대해 위임된 관리자를 추가할 수 있습니다. 위임된 관리자를 등록하거나 등록 취소하려면 조직의 관리 계정에 로그인해야 합니다.

위임된 관리자를 등록하려면

1. https://console.aws.amazon.com/trustedadvisor/home에서 관리 또는 관리 계정으로 Trusted Advisor 콘솔에 로그인합니다.
2. 탐색 창의 Preferences(기본 설정)에서 Organization(조직)을 선택합니다.
3. Delegated administrator(위임된 관리자)에서 Register new account(새 계정 등록)를 선택합니다.
4. 대화 상자에서 멤버 계정 ID를 입력하고 Register(등록)를 선택합니다.
5. (선택 사항) 계정 등록을 취소하려면 계정을 선택하고 Deregister(등록 취소)를 선택합니다. 대화 상자에서 Deregister(등록 취소)를 다시 선택합니다.

## 위임된 관리자 등록 취소

멤버 계정의 등록을 취소하면 해당 계정은 더 이상 관리 계정과 동일한 권한으로 Trusted Advisor Priority에 액세스할 수 없습니다. 더 이상 위임된 관리자가 아닌 계정은 Trusted Advisor Priority의 이메일 알림을 받지 못합니다.

위임된 관리자를 등록 취소하려면

1. https://console.aws.amazon.com/trustedadvisor/home에서 관리 또는 관리 계정으로 Trusted Advisor 콘솔에 로그인합니다.
2. 탐색 창의 Preferences(기본 설정)에서 Organization(조직)을 선택합니다.
3. 위임된 관리자에서 계정을 선택한 다음 등록 취소를 선택합니다.

4. 대화 상자에서 Deregister(등록 취소)를 선택합니다.

## Trusted Advisor Priority 알림 관리

Trusted Advisor Priority는 이메일을 통해 알림을 제공합니다. 이 이메일 알림에는 계정 팀이 우선 순위를 지정한 권장 사항에 대한 요약이 포함되어 있습니다. Trusted Advisor Priority에서 업데이트를 받는 빈도를 지정할 수 있습니다.

멤버 계정을 위임된 관리자로 등록한 경우 해당 사용자는 Trusted Advisor Priority 이메일 알림을 받도록 계정을 설정할 수도 있습니다.

Trusted Advisor Priority 이메일 알림은 개별 계정에 대한 확인 결과를 포함하지 않으며 Trusted Advisor 권장 사항에 대한 주간 알림과 별개입니다. 자세히 알아보려면 알림 기본 설정 지정의 내용을 참조하세요.

> **Note**
>
> 관리 계정이나 위임된 관리자만 Trusted Advisor 우선 순위 이메일 알림을 설정할 수 있습니다.

Trusted Advisor Priority 알림을 관리하려면 다음과 같이 하십시오.

1. https://console.aws.amazon.com/trustedadvisor/home에서 관리 또는 위임된 관리자 계정으로 Trusted Advisor 콘솔에 로그인합니다.
2. 탐색 창의 Preferences(기본 설정)에서 Notifications(알림)를 선택합니다.
3. Priority에서 다음 옵션을 선택할 수 있습니다.
   a. Daily(일별) - 매일 이메일 알림을 수신합니다.
   b. Weekly(주간) - 주 1회 이메일 알림을 수신합니다.
   c. 수신할 알림 선택:
      - 우선 순위 지정 권장 사항 요약
      - 해결 날짜
4. 수신자의 경우 이메일 알림을 받을 다른 연락처를 선택합니다. AWS Billing and Cost Management 콘솔의 Account Settings(계정 설정) 페이지에서 연락처를 추가하거나 제거할 수 있습니다.
5. Language(언어)에서 이메일 알림에 사용할 언어를 선택합니다.

6. Save your preferences(기본 설정 저장)를 선택합니다.

> **Note**
>
> Trusted Advisor Priority는 noreply@notifications.trustedadvisor.us-west-2.amazonaws.com 주소에서 이메일 알림을 보냅니다. 이메일 클라이언트가 이러한 이메일을 스팸으로 식별하지 않는지 확인해야 할 수 있습니다.

## Trusted Advisor Priority 사용 중지

계정 팀에 연락하여 이 기능을 사용 중지하도록 요청합니다. 이 기능을 비활성화하면 우선 순위가 지정된 권장 사항은 더 이상 Trusted Advisor 콘솔에 표시되지 않습니다.

Trusted Advisor Priority를 사용 중지했다가 나중에 사용하려는 경우 Trusted Advisor Priority를 사용 중지하기 전에 계정 팀이 보낸 권장 사항을 계속해서 볼 수 있습니다.

# AWS Trusted Advisor 참여(미리 보기) 시작하기

> **Note**
>
> AWS Trusted Advisor 참여는 현재 프리뷰 버전이 출시 중이기 때문에 변경될 수도 있습니다. https://aws.amazon.com/service-terms/에서 미리 보기 서비스 약관을 확인할 수 있습니다.

Engage를 사용하면 모든 사전 AWS Trusted Advisor 참여를 쉽게 확인, 요청 및 추적하고 진행 중인 계약에 대해 AWS 계정 팀과 소통할 수 있어 AWS Support 계획을 최대한 활용할 수 있습니다.

예를 들어 AWS Trusted Advisor 콘솔의 참여 페이지로 이동하여 AWS 계정 팀에 대한 “관리 비즈니스 검토”를 요청할 수 있습니다. 그러면 AWS 전문가가 요청에 배정되어 전체 참여 과정을 검토하게 됩니다.

주제

- 사전 조건
- 참여 대시보드 보기
- 참여 유형 카탈로그 보기
- 참여 요청

- 참여 편집
- 첨부 파일 및 메모 제출
- 참여 상태 변경
- 권장 참여와 요청 참여를 구분합니다.
- 참여 검색

## 사전 조건

Trusted Advisor 참여를 사용하려면 다음 요구 사항을 충족하는 데 필요한 조치를 취해야 합니다.

- Enterprise On-Ramp Support 계획이 있어야 합니다.
- 계정이 AWS Organizations의 모든 기능을 활성화해야 합니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하세요.
- 조직에서 Trusted Advisor에 대한 신뢰할 수 있는 액세스를 활성화해야 합니다. 관리 계정으로 로그인하고 Trusted Advisor 콘솔의 내 조직 페이지로 이동하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.
- Trusted Advisor 참여에 액세스하려면 AWS Identity and Access Management (IAM) 권한이 있어야 합니다. Trusted Advisor 참여 액세스를 제어하는 방법에 대한 자세한 내용은 액세스 관리: AWS Trusted Advisor을(를) 참조하세요.

> **Note**
>
> AWS 조직 내 모든 계정에서 참여 요청을 생성할 수 있습니다. 인게이지먼트 소유 계정이 다른 AWS 조직으로 이전되는 경우 해당 계정으로만 인게이지먼트에 액세스할 수 있습니다. 제어를 제한하려면 AWS Trusted Advisor에 대한 예제 서비스 제어 정책을(를) 참조하세요.

## 참여 대시보드 보기

액세스 권한을 획득한 후에는 Trusted Advisor 콘솔의 Trusted Advisor 참여 페이지에 액세스하여 AWS 계정 팀과의 참여를 관리할 수 있는 대시보드를 볼 수 있습니다.

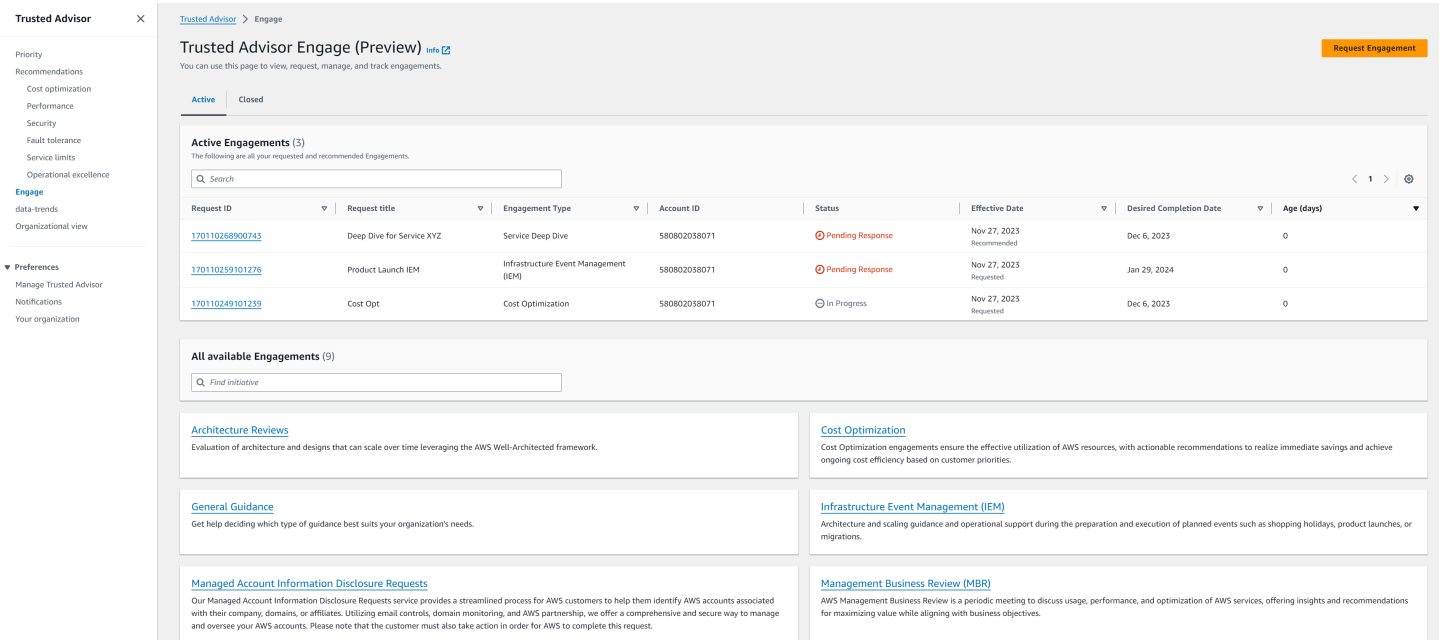
참여를 관리하는 방법:

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.

2. Trusted Advisor 참여 페이지에서 다음 사항을 확인할 수 있습니다.

   - 참여 요청 버튼
   - 액티브 참여 테이블
   - 종료된 참여 테이블
   - 사용 가능한 모든 계약 카탈로그

Example : 참여 대시보드



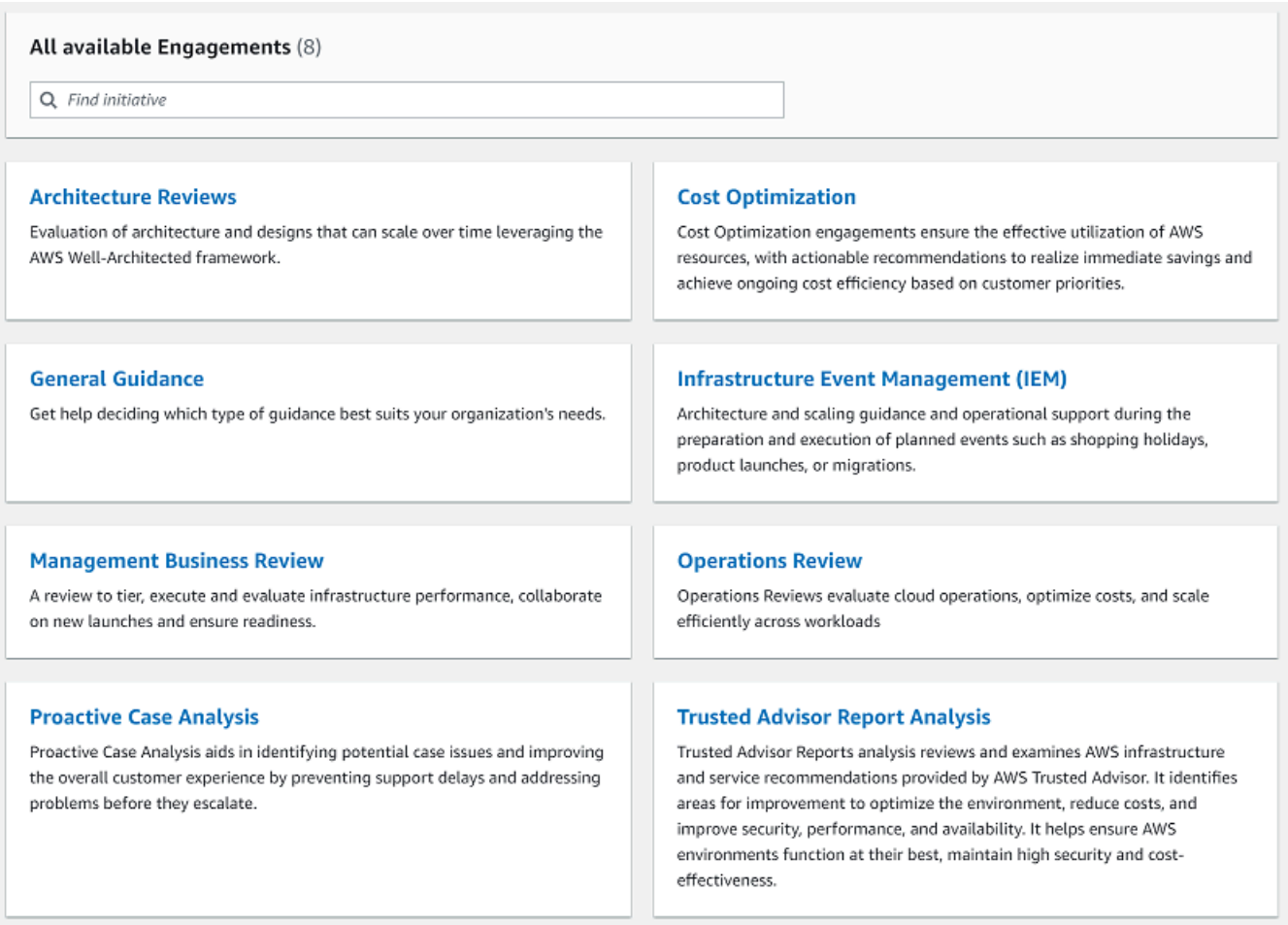

# 참여 유형 카탈로그 보기

참여 유형 카탈로그에서 AWS 계정 팀에 요청할 수 있는 최신 참여 유형을 찾을 수 있습니다.

참여 유형 카탈로그를 보는 방법:

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor 참여 페이지에서 참여 유형 카탈로그를 찾을 수 있습니다.

Example : 참여 유형 카탈로그




# 참여 요청

AWS 지원 계획에 포함된 참여 유형에 따라 AWS 계정 팀에 참여를 요청할 수 있습니다.

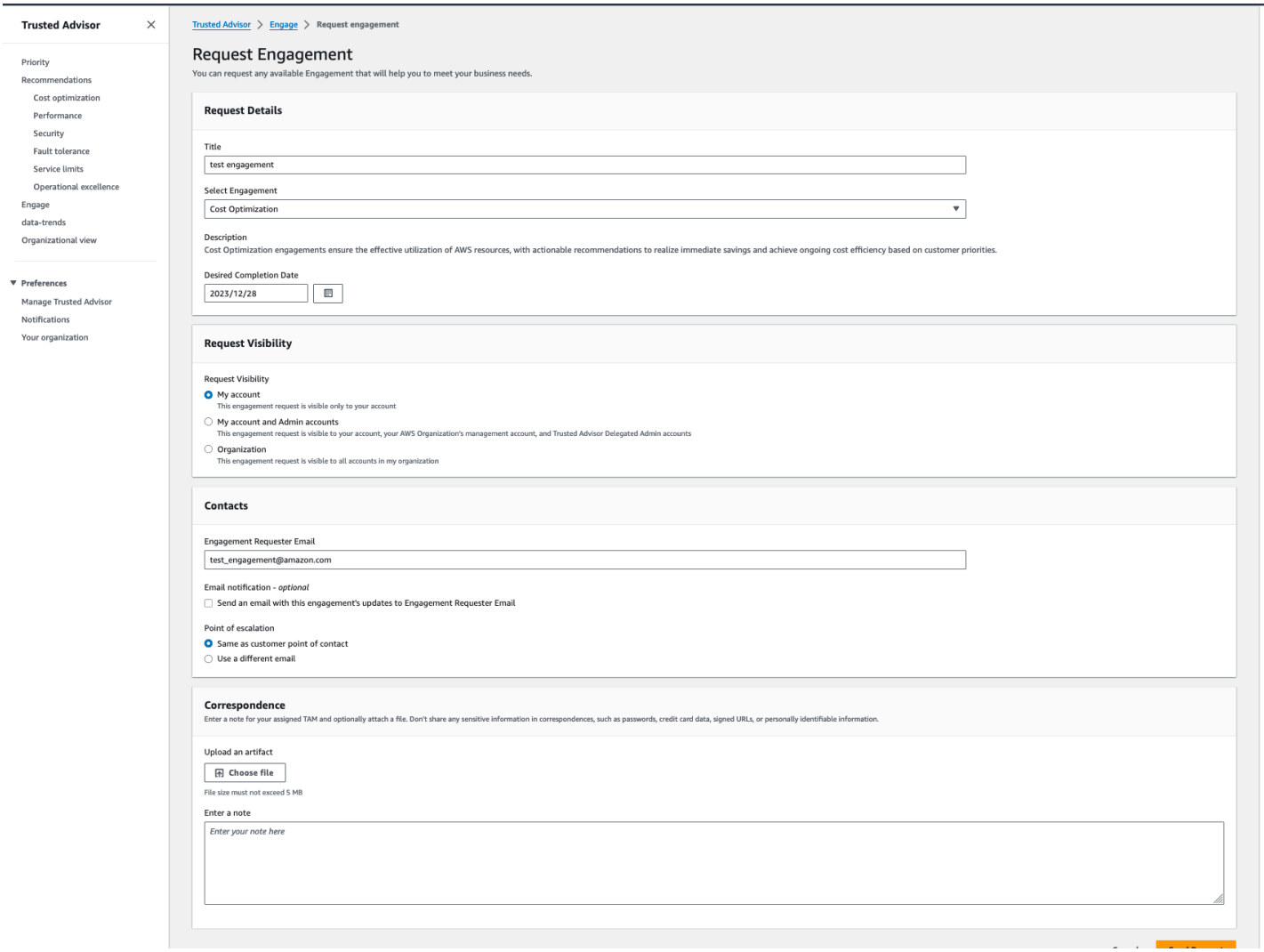
참여를 요청하는 방법:

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor 참여 페이지에서 참여 요청을 선택합니다.
3. 다음 사항을 작성합니다.
   - 제목
   - 참여 선택: 요청하려는 참여 유형입니다.
   - 희망 완료 날짜: 원하는 계약 완료 날짜. 각 계약 유형에는 최소 희망 완료일을 기준으로 계산되는 리드 타임이 다릅니다.

- 요청 가시성:
  - 내 계정: 이 참여 요청은 사용자 계정에서만 볼 수 있습니다.
  - 내 계정 및 관리자 계정: 이 참여 요청은 사용자 계정, 관리 계정 및 AWS 조직의 모든 위임된 관리자 계정에서 볼 수 있습니다.
  - 조직: 이 참여 요청은 AWS 조직의 모든 계정에서 볼 수 있습니다.
- 참여 요청자 이메일: 본 계약의 AWS 기본 연락처로 사용할 이메일 주소입니다.
- 이메일 알림 설정: 참여 요청자 이메일에서 참여에 대한 이메일 알림을 수신할지 여부를 선택합니다.
- 에스컬레이션 지점: 본 계약에 대한 에스컬레이션이 필요할 때 AWS이(가) 사용할 이메일 주소입니다.
- 서신: 본 계약과 관련된 세부 정보를 제공할 수 있는 메모 및 선택적 파일 첨부.

4. 요청 보내기를 선택합니다.

Example : 참여 요청




# 참여 편집

참여 요청의 세부 정보를 편집할 수 있습니다.

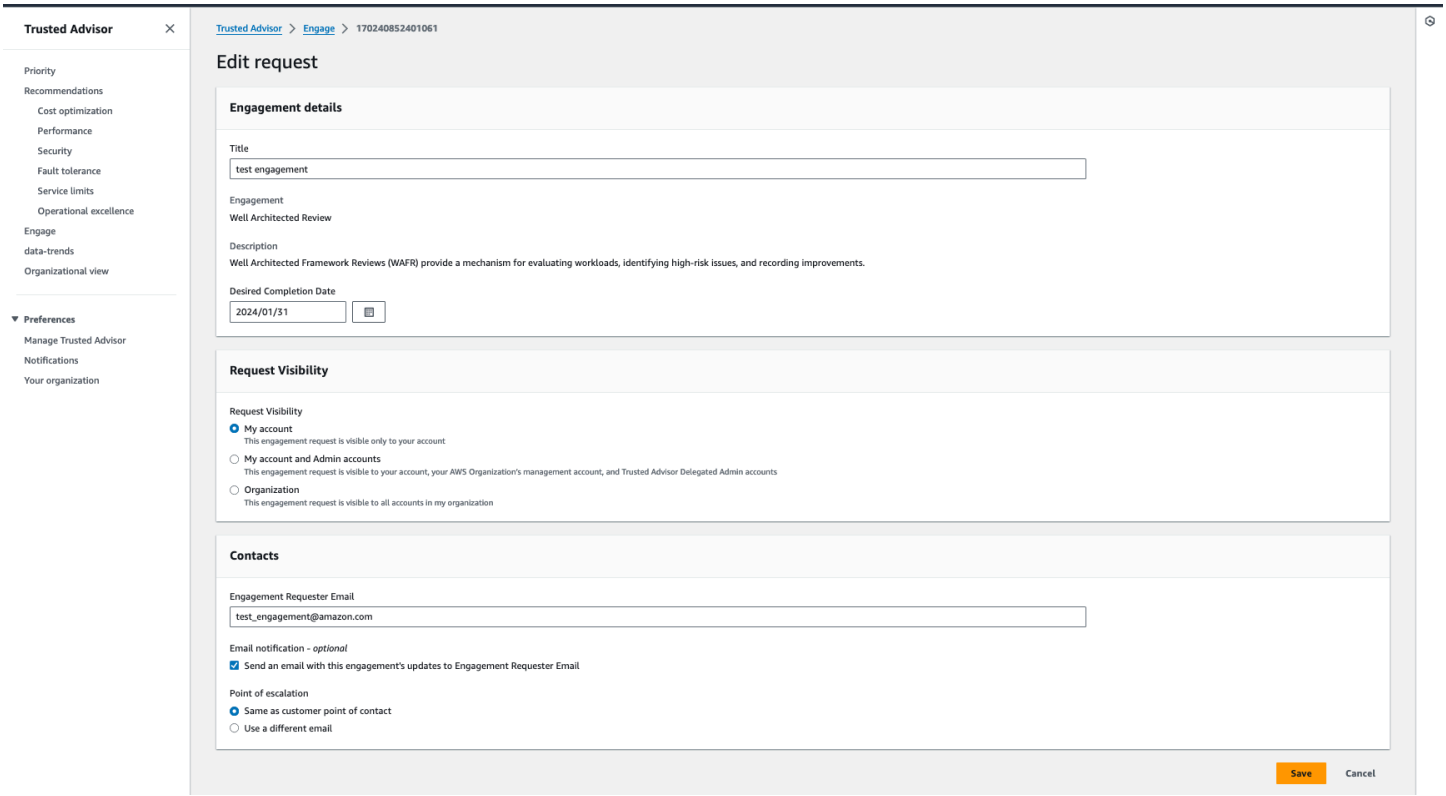
참여를 편집하는 방법:

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor 참여 페이지에서 기존 참여를 선택합니다.
3. [편집(Edit)]을 선택합니다.
4. 다음 사항을 편집할 수 있습니다.
    - 제목

- 희망 완료 날짜: 원하는 계약 완료 날짜. 각 계약 유형에는 최소 희망 완료일을 기준으로 계산되는 리드 타임이 다릅니다.
- 요청 가시성:
  - 내 계정: 이 참여 요청은 사용자 계정에서만 볼 수 있습니다.
  - 내 계정 및 관리자 계정: 이 참여 요청은 사용자 계정, 관리 계정 및 AWS 조직의 모든 위임된 관리자 계정에서 볼 수 있습니다.
  - 조직: 이 참여 요청은 AWS 조직의 모든 계정에서 볼 수 있습니다.
- 참여 요청자 이메일: 본 계약의 기본 연락처로 사용할 이메일 주소입니다. AWS
- 이메일 알림 설정: 참여 요청자 이메일에서 참여에 대한 이메일 알림을 수신할지 여부를 선택합니다.
- 에스컬레이션 지점: 본 계약에 대한 에스컬레이션이 필요할 때 AWS이(가) 사용할 이메일 주소입니다.

5. 저장을 선택합니다.

Example : 참여 편집



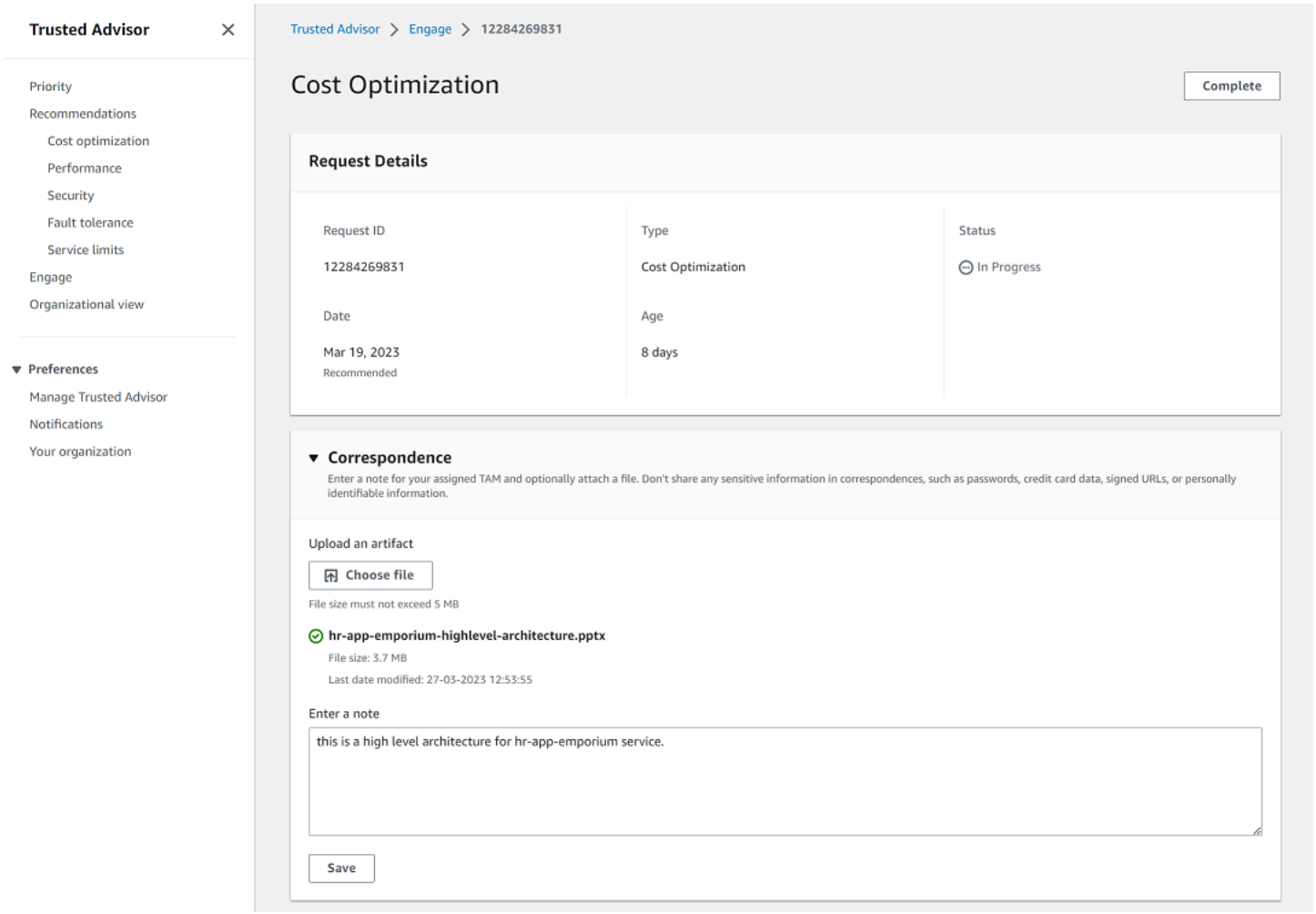
# 첨부 파일 및 메모 제출

참여 요청을 뒷받침하는 메모와 첨부 파일을 보내 개별 업무에 대해 AWS 계정 팀과 소통할 수 있습니다. 커뮤니케이션당 하나의 첨부 파일과 메모를 포함할 수 있고, 참여를 요청한 사람과 동일한 AWS 계정을 사용한 파일만 참여에 첨부할 수 있으며, 커뮤니케이션이 전송된 후에는 첨부 파일이나 메모를 삭제할 수 없습니다.

활성 참여 요청에 파일을 첨부하거나 메모를 추가하는 방법:

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor 참여 페이지에서 파일을 연결하거나 메모를 추가하려는 활성 참여의 ID를 선택합니다.
3. 서신을 선택하여 양식을 확장합니다.
4. 지정된 TAM에 대한 메모를 입력하고 선택적으로 파일을 첨부합니다. 암호, 신용 카드 데이터, 서명된 URL 또는 개인 식별 정보와 같은 민감한 정보는 서신에 공유하지 마십시오.
5. 저장을 선택합니다.

Example : 계약서에 메모 및 첨부 파일 추가




# 참여 상태 변경

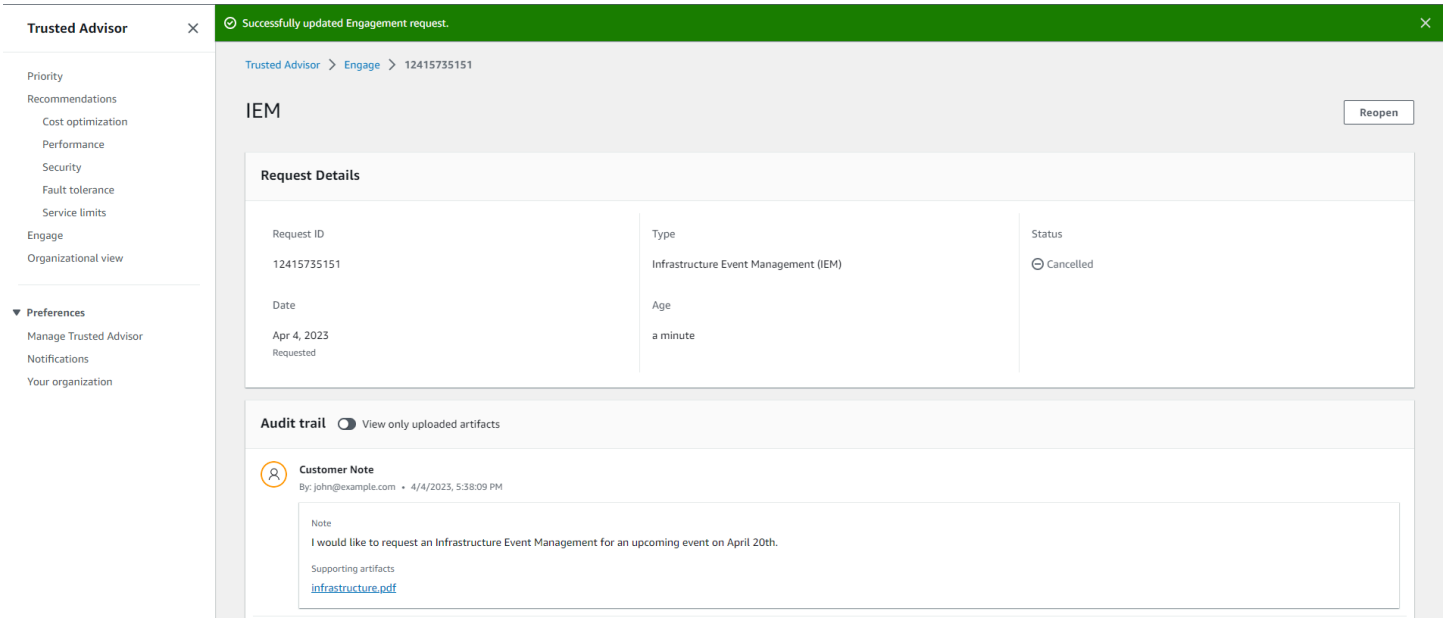
해당 참여 상태를 변경하여 응답 보류 중인 계약을 취소하고, 진행 중인 참여를 완료하고, 취소됨 또는 종료된 것으로 표시된 계약을 다시 열 수 있습니다.

참여 상태를 변경하는 방법:

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor 참여 페이지에서 상태를 변경하려는 활성 참여의 ID를 선택합니다.
3. 참여 세부 정보 페이지에서 상태를 취소됨 또는 완료로 변경할 수 있습니다.
   - 참여 상태가 응답 보류인 경우 취소를 선택할 수 있습니다.
   - 참여 상태가 진행 중인 경우 완료를 선택할 수 있습니다.

- 종료된 계약의 경우 재개를 선택할 수 있습니다. 취소된 참여는 응답 보류로 이동하고, 참여 완료는 진행 중으로 이동합니다.

Example : 참여 상태 변경




# 권장 참여와 요청 참여를 구분합니다.

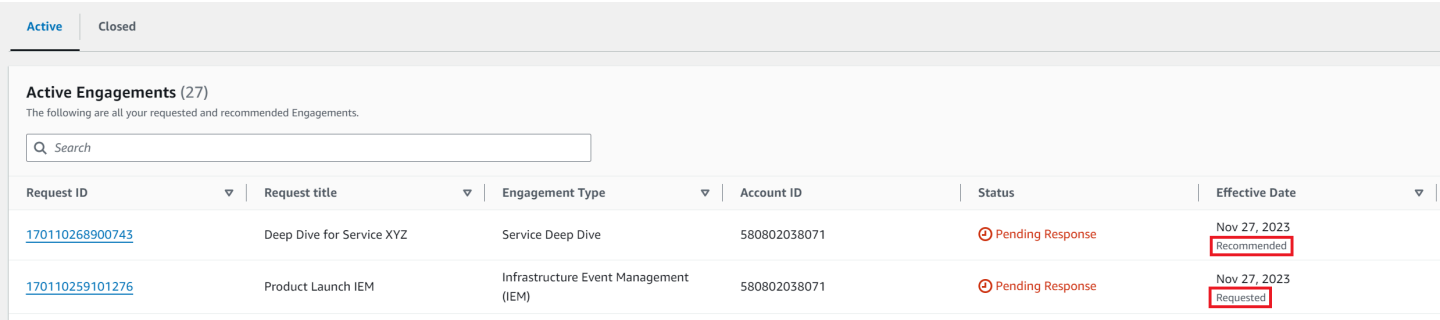
참여의 출처를 식별하여 참여가 본인이 요청했는지 아니면 AWS 계정 팀에서 추천했는지 알 수 있습니다.

활성 참여의 다양한 출처를 보는 방법:

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor참여 페이지에서 유효 날짜 열을 확인하여 권장 계약과 요청된 참여를 구분하십시오.

   - 권장 사항: AWS 계정 팀에서 생성한 참여 요청.
   - 요청: 사용자가 생성한 참여 요청.

Example : 권장 참여 및 요청 참여 구분



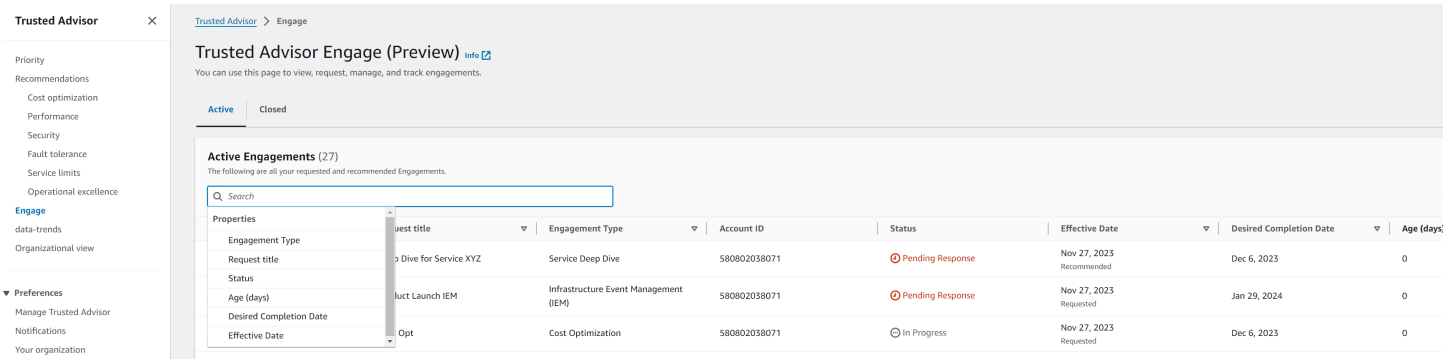

# 참여 검색

필터를 사용하여 기존 활성 및 마감된 계약을 검색할 수 있습니다.

참여를 검색하는 방법:

1. https://console.aws.amazon.com/trustedadvisor/home의 Trusted Advisor 콘솔에 로그인합니다.
2. Trusted Advisor 참여 페이지에서 다음 필터 중에서 선택할 수 있습니다.
   - 연령(일)
   - 인게이지먼트 유형
   - 요청 제목
   - 상태
   - 원하는 완료 날짜
   - 효력 발생일

Example : 검색 참여



# AWS Trusted Advisor 참조 확인

다음 참조에서 모든 Trusted Advisor 검사 이름, 설명 및 ID를 볼 수 있습니다. 또한 Trusted Advisor콘솔에 로그인하여 검사, 권장 작업 및 상태에 대한 자세한 정보를 검토할 수 있습니다.

Business, Enterprise On-Ramp 또는 Enterprise Support 플랜을 보유한 경우 AWS Trusted Advisor API와 AWS Command Line Interface (AWS CLI)를 사용하여 검사에 액세스할 수도 있습니다. 자세한 정보는 다음 주제를 참조하세요.

- Trusted Advisor API로 시작하기
- AWS Trusted Advisor API Reference

> **Note**
>
> 기본 Support 및 개발자 Support 플랜을 보유한 경우 Trusted Advisor 콘솔에서 모든 검사와 서비스 한도 범주와 보안 범주에서 수행할 수 있는 다음 검사에 액세스할 수 있습니다.
>
> - Amazon EBS 퍼블릭 스냅샷
> - Amazon RDS 퍼블릭 스냅샷
> - Amazon S3 버킷 권한
> - 루트 계정의 MFA
> - 보안 그룹 — 제한 없는 특정 포트

검사 범주

- 비용 최적화
- 성능
- 보안
- 내결함성
- 서비스 한도
- 운영 우수성

## 비용 최적화

비용 최적화 범주에 대해 다음과 같은 검사 항목을 사용할 수 있습니다.

검사명

- AWS 계정은 AWS Organizations에 속하지 않음
- Amazon Comprehend 사용률이 낮은 엔드포인트
- Amazon EBS 과다 프로비저닝된 볼륨
- Microsoft SQL Server용 Amazon EC2 인스턴스 통합
- Microsoft SQL Server에 대해 과다 프로비저닝된 Amazon EC2 인스턴스
- Amazon EC2 인스턴스 중지됨
- Amazon EC2 Reserved Instance Lease Expiration
- Amazon EC2 예약 인스턴스 최적화
- 수명 주기 정책이 구성되지 않은 Amazon ECR 리포지토리
- Amazon ElastiCache 예약 노드 최적화
- Amazon OpenSearch 서비스 예약 인스턴스 최적화
- Amazon RDS 유휴 DB 인스턴스
- Amazon Redshift 예약 노드 최적화
- Amazon Relational Database Service(RDS) 예약 인스턴스 최적화
- Amazon Route 53 대기 시간 리소스 레코드 세트
- Amazon S3 버킷 수명 주기 정책 구성
- Amazon S3 미완료 멀티파트 업로드 중단 구성
- 수명 주기 정책이 구성되지 않은 Amazon S3 버전 지원 버킷
- 과도한 시간 초과가 있는 AWS Lambda 함수
- 오류율이 높은 AWS Lambda 함수
- 메모리 크기에 대해 과다 프로비저닝된 AWS Lambda함수
- 비용 최적화에 대한 AWS Well-Architected 위험도 높음 문제
- 유휴 로드 밸런서
- 낮은 사용률의 Amazon EC2 인스턴스
- Savings Plan
- 연결되지 않은 탄력적 IP 주소
- 사용률이 낮은 Amazon EBS 볼륨
- Underutilized Amazon Redshift Clusters

# AWS 계정은 AWS Organizations에 속하지 않음

설명

AWS 계정이 적절한 관리 계정의 AWS Organizations의 일부인지 확인합니다.

AWS Organizations은(는) 여러 AWS 계정을 중앙에서 관리되는 조직으로 통합하기 위한 계정 관리 서비스입니다. 이를 통해 청구 통합을 위한 계정을 중앙에서 구성하고 AWS에 대한 워크로드 확장에 따라 소유권 및 보안 정책을 구현할 수 있습니다.

AWS Config규칙의 MasterAccountId매개변수를 사용하여 관리 계정 ID를 지정할 수 있습니다.

자세한 내용은AWS Organizations란 무엇입니까?를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz127
```

소스(Source)

```
AWS Config Managed Rule: account-part-of-organizations
```

알림 기준

노란색: 이 AWS 계정은 AWS Organizations에 속하지 않습니다.

권장 조치

이 AWS 계정을 AWS Organizations의 일부로 추가합니다.

자세한 내용은 튜토리얼: 조직 생성 및 구성을 참조하세요.

보고서 열

- 상태 표시기
- 리전

- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon Comprehend 사용률이 낮은 엔드포인트

설명

엔드포인트의 처리량 구성을 확인합니다. 이 검사는 엔드포인트가 실시간 추론 요청에 대해 활성 상태로 사용되지 않을 때 경고합니다. 연속 15일 이상 사용되지 않은 엔드포인트는 사용률이 낮은 것으로 간주됩니다. 모든 엔드포인트는 처리량 세트, 및 엔드포인트가 활성 상태인 기간 모두를 기준으로 요금이 발생합니다.

> **Note**
>
> 이 검사는 1일 1회 자동으로 새로 고침됩니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`Cm24dfsM12`

알림 기준

노란색: 엔드포인트가 활성 상태지만, 지난 15일 동안 실시간 추론 요청에 사용되지 않았습니다.

권장 조치

엔드포인트가 지난 15일 동안 사용되지 않은 경우, Application Autoscaling을 사용하여 리소스에 대한 조정 정책을 정의하는 것이 좋습니다.

엔드포인트에 조정 정책이 정의되어 있는데 엔드포인트가 지난 30일 동안 사용되지 않은 경우, 엔드포인트를 삭제하고 비동기 추론을 사용하는 것이 좋습니다. 자세한 내용은 Amazon Comprehend로 엔드포인트 삭제를 참조하세요.

보고서 열

- 상태 표시기

- 리전
- 엔드포인트 ARN
- 프로비저닝된 추론 유닛
- AutoScaling 상태
- 이유
- 최종 업데이트 시간

## Amazon EBS 과다 프로비저닝된 볼륨

### 설명

조회 기간 동안 실행 중이었던 Amazon Elastic Block Store (Amazon EBS) 볼륨을 검사합니다. 이 검사는 워크로드에 대해 EBS 볼륨이 과다 프로비저닝되었는지 여부를 알려줍니다. 과다 프로비저닝된 볼륨이 있는 경우 사용하지 않은 리소스에 대한 비용을 지불하게 됩니다. 일부 시나리오에서는 설계상 최적화가 낮아질 수 있지만 EBS 볼륨의 구성을 변경하여 비용을 절감할 수 있습니다. 예상 월별 절감액은 EBS 볼륨의 현재 사용률을 사용하여 계산됩니다. 실제 절감액은 한 달 동안 볼륨이 없을 경우 달라질 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

### 검사 ID

`C0r6dfpM03`

### 알림 기준

노란색: 조회 기간 동안 과다 프로비저닝된 EBS 볼륨입니다. 볼륨이 오버 프로비저닝되었는지 확인하기 위해 모든 기본 CloudWatch 지표 (IOPS 및 처리량 포함) 를 고려합니다. 과다 프로비저닝된 EBS 볼륨을 식별하는 데 사용되는 알고리즘은 AWS 모범 사례를 따릅니다. 새 패턴이 식별되면 알고리즘이 업데이트됩니다.

### 권장 조치

사용률이 낮은 볼륨의 크기를 줄이는 것이 좋습니다.

자세한 설명은 Trusted Advisor 수표 AWS Compute Optimizer 신청 섹션을 참조하세요.

보고서 열

- 상태 표시기
- 리전
- 볼륨 ID
- 볼륨 유형
- 볼륨 크기(GB)
- 볼륨 기준 IOPS
- 볼륨 버스트 IOPS
- 볼륨 버스트 처리량(throughput)
- 권장 볼륨 유형
- 권장 볼륨 크기(GB)
- 권장 볼륨 기준 IOPS
- 권장 볼륨 버스트 IOPS
- 권장 볼륨 기준 처리량(throughput)
- 권장 볼륨 버스트 처리량(throughput)
- 조회 기간(일)
- 절감 기회(%)
- 예상 월별 절감액
- 예상 월별 절감액 통화
- 최종 업데이트 시간

## Microsoft SQL Server용 Amazon EC2 인스턴스 통합

설명

지난 24시간 동안 SQL Server를 실행한 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스를 확인합니다. 이 검사에서는 인스턴스의 SQL Server 라이선스 수가 최소 수보다 적은 경우 알림을 제공합니다. Microsoft SQL Server 라이선스 가이드에 따르면 인스턴스에 vCPU가 1~2개만 있는 경우에도 4개의 vCPU 라이선스를 지불합니다. 작은 SQL Server 인스턴스를 통합하면 비용을 절감할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`Qsdfp3A4L2`

알림 기준

노란색: SQL Server를 포함하는 인스턴스에 vCPU가 4개 미만입니다.

권장 조치

여러 소규모 SQL Server 워크로드를 vCPU가 4개 이상인 인스턴스로 통합하는 것이 좋습니다.

추가 리소스

- AWS의 Microsoft SQL Server
- AWS의 Microsoft 라이선싱
- Microsoft SQL Server 라이선싱 가이드

보고서 열

- 상태 표시기
- 리전
- 인스턴스 ID
- 인스턴스 유형
- vCPU
- 최소 vCPU
- SQL Server Edition
- 최종 업데이트 시간

## Microsoft SQL Server에 대해 과다 프로비저닝된 Amazon EC2 인스턴스

### 설명

지난 24시간 동안 SQL Server를 실행한 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스를 확인합니다. SQL Server 데이터베이스에서는 각 인스턴스의 컴퓨팅 용량이 제한됩니다. SQL Server Standard Edition을 포함하는 인스턴스는 최대 48개의 vCPU를 사용할 수 있습니다. SQL Server Web을 포함하는 인스턴스는 최대 32개의 vCPU를 사용할 수 있습니다. 이 검사는 인스턴스가 이 vCPU 제한을 초과할 경우 알림을 제공합니다.

인스턴스가 과다 프로비저닝된 경우 전체 가격을 지불해도 성능 향상이 실현되지 않습니다. 인스턴스 수와 크기를 관리하여 비용을 낮출 수 있습니다.

예상 월별 절감액은 SQL Server 인스턴스에서 사용할 수 있는 최대 vCPU 수를 포함하는 동일한 인스턴스 패밀리와 온디맨드 요금을 사용하여 계산됩니다. 예약 인스턴스(RI)를 사용하거나 인스턴스가 하루 종일 실행되지 않는 경우 실제 절감액이 달라집니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

### 검사 ID

`Qsdfp3A4L1`

### 알림 기준

- 빨간색: SQL Server Standard Edition을 포함하는 인스턴스에 48개 넘는 vCPU가 있습니다.
- 빨간색: SQL Server Web Edition을 포함하는 인스턴스에 32개 넘는 vCPU가 있습니다.

### 권장 조치

SQL Server Standard Edition의 경우, 동일한 인스턴스 패밀리에서 vCPU가 48개인 인스턴스로 변경하는 것이 좋습니다. SQL Server Web Edition의 경우, 동일한 인스턴스 패밀리에서 vCPU가 32개인 인스턴스로 변경하는 것이 좋습니다. 메모리를 많이 사용하는 경우, 메모리 최적화 R5 인스턴스로 변경하는 것이 좋습니다. 자세한 내용은 Amazon EC2 Microsoft SQL Server 배포의 모범 사례를 참조하세요.

추가 리소스

- AWS의 Microsoft SQL Server
- Launch Wizard를 사용하여 EC2에서의 SQL 서버 배포를 간소화할 수 있습니다.

보고서 열

- 상태 표시기
- 리전
- 인스턴스 ID
- 인스턴스 유형
- vCPU
- SQL Server Edition
- 최대 vCPU
- 권장 인스턴스 유형
- 예상 월별 절감액
- 최종 업데이트 시간

## Amazon EC2 인스턴스 중지됨

설명

30일 이상 중지된 경우 Amazon EC2 인스턴스가 있는지 확인합니다.

of 파라미터에 허용 일수 값을 지정할 수 있습니다. AllowedDaysAWS Config

자세한 내용은 모든 인스턴스가 종료되었는데 Amazon EC2 요금이 부과되는 이유는 무엇입니까?를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz150
```

소스(Source)

```
AWS Config Managed Rule: ec2-stopped-instance
```

알림 기준

- 노란색: 허용된 일수를 초과하여 중지된 Amazon EC2 인스턴스가 있습니다.

권장 조치

30일 이상 중지된 Amazon EC2 인스턴스를 검토하십시오. 불필요한 비용이 발생하지 않도록 하려면 더 이상 필요하지 않은 모든 인스턴스를 종료하십시오.

자세한 내용은 인스턴스 종료를 참조하세요.

추가 리소스

- Amazon EC2 온디맨드 요금

보고서 열

- 상태 표시기
- 리전
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon EC2 Reserved Instance Lease Expiration

설명

향후 30일 이내에 만료될 예정이거나 이전 30일 이내에 만료된 Amazon EC2 예약 인스턴스를 확인합니다.

예약 인스턴스는 자동으로 갱신되지 않습니다. 중단 없이 예약이 적용되는 Amazon EC2 인스턴스를 계속 사용할 수 있지만 온디맨드 요금이 부과됩니다. 새 예약 인스턴스는 만료된 예약 인스턴스와 같은 파라미터를 사용할 수 있으며, 다른 파라미터가 있는 예약 인스턴스를 구매할 수도 있습니다.

월별 예상 절감액은 동일한 인스턴스 유형에 대한 온디맨드 요금과 예약 인스턴스 요금의 차액입니다.

검사 ID

1e93e4c0b5

알림 기준

- 노란색: 예약 인스턴스 임대가 30일 이내에 만료됩니다.
- 노란색: 예약 인스턴스 임대가 이전 30일 중에 만료되었습니다.

권장 조치

새 예약 인스턴스를 구매하여 사용 기간이 거의 끝난 인스턴스를 교체하는 것이 좋습니다. 자세한 내용은 예약 인스턴스 구매 방법 및 예약 인스턴스 구입을 참조하세요.

추가 리소스

- 예약 인스턴스
- 인스턴스 유형

보고서 열

- 상태 표시기
- 영역
- 인스턴스 유형
- 플랫폼
- 인스턴스 수
- 현재 월별 비용
- 예상 월별 절감액
- 만료 날짜
- Reserved Instance ID
- 이유

## Amazon EC2 예약 인스턴스 최적화

설명

AWS 사용의 중요한 부분으로 예약 인스턴스(RI) 구매와 온디맨드 인스턴스 사용량의 밸런싱입니다. 이 검사는 온디맨드 인스턴스 사용으로 인해 발생하는 비용을 줄이는 데 도움이 되는 RI에 대한 권장 사항을 제공합니다.

지난 30일 동안의 온디맨드 사용량을 분석하여 해당 권장 사항을 생성합니다. 그런 다음 사용을 예약에 적합한 범주로 분류합니다. 생성된 사용 범주의 모든 예약 조합을 시뮬레이션하여 각 RI 유형의 구매 권장 개수를 식별합니다. 이러한 시뮬레이션 및 최적화 프로세스를 통해 비용 절감을 극대화할 수 있습니다. 이 검사에서는 부분 선불 지급 옵션을 사용하는 스탠더드 예약 인스턴스를 기반으로 하는 권장 사항을 다룹니다.

통합 결제에 연결된 계정에서는 이 검사를 사용할 수 없습니다. 이 검사에 대한 권장 사항은 지급 계정에서만 사용할 수 있습니다.

검사 ID

cX3c2R1chu

알림 기준

노란색: 부분 선결제 RI의 사용을 최적화하면 비용을 줄이는 데 도움이 될 수 있습니다.

권장 조치

자세하고 맞춤화된 권장 사항은 Cost Explorer 페이지를 참조하세요. 또한 구매 가이드에서 RI를 구매하는 방법과 제공되는 옵션을 참조하세요.

추가 리소스

- RI에 대한 정보와 RI의 비용 절감 효과에 대한 자세한 내용은 여기에서 확인할 수 있습니다.
- 이 권장 사항에 대한 자세한 내용은 Trusted Advisor FAQ에서 예약 인스턴스 최적화 확인 질문을 참조하세요.

보고서 열

- 리전
- 인스턴스 유형
- 플랫폼
- 권장 구매 RI 수
- 예상 평균 RI 사용률
- 권장 사항을 통한 예상 절감액(월별)
- RI의 선결제 비용
- RI의 예상 비용(월별)
- 권장 RI 구매 후 예상 온디맨드 비용(월별)
- 예상 손익분기점(개월)

- 조회 기간(일)
- 기간(년)

## 수명 주기 정책이 구성되지 않은 Amazon ECR 리포지토리

설명

프라이빗 Amazon ECR 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. 수명 주기 정책을 사용하면 오래된 컨테이너 이미지 또는 사용하지 않은 컨테이너 이미지를 자동으로 정리하는 규칙 세트를 정의할 수 있습니다. 이를 통해 이미지의 수명 주기 관리를 제어할 수 있고, Amazon ECR 리포지토리를 더 잘 구성하고, 전체 스토리지 비용을 절감할 수 있습니다.

자세한 내용은 수명 주기 정책을 참조하세요.

검사 ID

```
c18d2gz128
```

소스(Source)

```
AWS Config Managed Rule: ecr-private-lifecycle-policy-configured
```

알림 기준

노란색: Amazon ECR 프라이빗 리포지토리에는 수명 주기 정책이 구성되어 있지 않습니다.

권장 조치

프라이빗 Amazon ECR 리포지토리에 대해 하나 이상의 수명 주기 정책을 생성하는 것을 고려해 보십시오.

자세한 내용은 수명 주기 정책 생성을 참조하세요.

추가 리소스

- 수명 주기 정책.
- 수명 주기 정책 생성.
- 수명 주기 정책의 예제.

보고서 열

- 상태 표시기
- 리전

- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon ElastiCache 예약 노드 최적화

설명

예약 노드 사용량을 ElastiCache 확인하고 예약 노드 구매에 대한 권장 사항을 제공합니다. 이러한 권장 사항은 온디맨드 사용으로 ElastiCache 발생하는 비용을 줄이기 위해 제공됩니다. 지난 30일 동안의 온디맨드 사용량을 분석하여 이러한 권장 사항을 생성합니다.

이 분석을 사용하여 생성된 사용 범주의 모든 예약 조합을 시뮬레이션합니다. 이를 통해 절감을 극대화하기 위해 구매할 예약 노드의 각 유형 수를 추천할 수 있습니다. 이 수표는 1년 또는 3년 약정과 함께 부분 선불 지급 옵션에 따른 권장 사항을 다룹니다.

통합 결제에 연결된 계정에서는 이 검사를 사용할 수 없습니다. 이 검사에 대한 권장 사항은 지급 계정에서만 사용할 수 있습니다.

검사 ID

`h3L1otH3re`

알림 기준

노란색: ElastiCache 예약 노드 구매를 최적화하면 비용을 절감하는 데 도움이 될 수 있습니다.

권장 조치

자세한 권장 사항, 사용자 지정 옵션 (예: 룩백 기간, 결제 옵션 등) 및 예약 노드 ElastiCache 구매에 대한 자세한 내용은 Cost Explorer 페이지를 참조하십시오.

추가 리소스

- ElastiCache 예약 노드에 대한 정보와 비용을 절감하는 방법은 여기에서 확인할 수 있습니다.
- 이 권장 사항에 대한 자세한 내용은 Trusted Advisor FAQ에서 예약 인스턴스 최적화 확인 질문을 참조하세요.
- 필드에 대한 자세한 설명은 Cost Explorer 설명서를 참조하세요.

보고서 열

- 리전

- Family
- 노드 유형(Node Type)
- 제품 설명
- 권장 구매 예약 노드 수
- 예상 평균 예약 노드 사용률
- 권장 사항을 통한 예상 절감액(월별)
- 예약 노드의 선결제 비용
- 예약 노드의 예상 비용(월별)
- 권장 예약 노드 구매 후 예상 온디맨드 비용(월별)
- 예상 손익분기점(개월)
- 조회 기간(일)
- 기간(년)

## Amazon OpenSearch 서비스 예약 인스턴스 최적화

설명

Amazon OpenSearch 서비스 사용량을 확인하고 예약 인스턴스 구매에 대한 권장 사항을 제공합니다. 이러한 권장 사항은 온디맨드 사용으로 OpenSearch 발생하는 비용을 줄이기 위해 제공됩니다. 지난 30일 동안의 온디맨드 사용량을 분석하여 이러한 권장 사항을 생성합니다.

이 분석을 사용하여 생성된 사용 범주의 모든 예약 조합을 시뮬레이션합니다. 이를 통해 최대한 절감할 수 있도록 구매할 각 예약 인스턴스 유형 수를 추천할 수 있습니다. 이 검사는 1년 또는 3년 약정과 함께 부분 선결제 옵션에 따른 권장 사항을 다룹니다.

통합 결제에 연결된 계정에서는 이 검사를 사용할 수 없습니다. 이 검사에 대한 권장 사항은 지급 계정에서만 사용할 수 있습니다.

검사 ID

```
7ujm6yhn5t
```

알림 기준

노란색: Amazon OpenSearch 서비스 예약 인스턴스 구매를 최적화하면 비용을 절감하는 데 도움이 될 수 있습니다.

권장 조치

자세한 권장 사항, 사용자 지정 옵션 (예: 룩백 기간, 결제 옵션 등) 및 Amazon OpenSearch Service 예약 인스턴스 구매에 대한 자세한 내용은 Cost Explorer 페이지를 참조하십시오.

추가 리소스

- Amazon OpenSearch Service 예약 인스턴스에 대한 정보와 이를 통해 비용을 절감할 수 있는 방법은 여기에서 확인할 수 있습니다.
- 이 권장 사항에 대한 자세한 내용은 Trusted Advisor FAQ에서 예약 인스턴스 최적화 확인 질문을 참조하세요.
- 필드에 대한 자세한 설명은 Cost Explorer 설명서를 참조하세요.

보고서 열

- 리전
- 인스턴스 클래스
- 인스턴스 크기
- 권장 구매 예약 인스턴스 수
- 예상 평균 예약 인스턴스 사용률
- 권장 사항을 통한 예상 절감액(월별)
- 예약 인스턴스의 선결제 비용
- 예약 인스턴스의 예상 비용(월별)
- 권장 예약 인스턴스 구매 후 예상 온디맨드 비용(월별)
- 예상 손익분기점(개월)
- 조회 기간(일)
- 기간(년)

## Amazon RDS 유휴 DB 인스턴스

설명

Amazon Relational Database Service(Amazon RDS) 구성에 유휴 상태인 데이터베이스(DB) 인스턴스가 있는지 확인합니다.

DB 인스턴스가 장시간 연결되지 않은 경우 인스턴스를 삭제하여 비용을 절감할 수 있습니다. DB 인스턴스는 과거 7일 동안 연결되지 않은 경우 유휴 상태로 간주됩니다. 인스턴스의 데이터에 영구

스토리지가 필요한 경우 DB 스냅샷 생성 및 보존과 같이 비용이 저렴한 옵션을 사용할 수 있습니다. 수동으로 생성된 DB 스냅샷은 사용자가 삭제할 때까지 보존됩니다.

검사 ID

`Ti39halfu8`

알림 기준

노란색: 활성 DB 인스턴스가 지난 7일 동안 연결되지 않았습니다.

권장 조치

유휴 DB 인스턴스의 스냅샷을 생성한 다음, 해당 인스턴스를 중지하거나 삭제하는 것이 좋습니다. DB 인스턴스를 중지하면 일부 비용이 배제되지만 스토리지 비용은 배제되지 않습니다. 중지된 인스턴스의 모든 자동 백업은 구성된 보존 기간 동안 유지됩니다. DB 인스턴스를 중지할 경우, 인스턴스를 삭제한 다음 최종 스냅샷만 유지하는 경우와 비교할 때 일반적으로 추가 비용이 발생합니다. Amazon RDS 인스턴스의 일시적 중지 및 최종 스냅샷을 캡처하고 DB 인스턴스를 삭제하는 방법을 참조하세요.

추가 리소스

백업 및 복원

보고서 열

- 리전
- DB 인스턴스 이름
- 다중 AZ
- 인스턴스 유형
- 프로비저닝된 스토리지(GB)
- 마지막 연결 이후 경과 일수
- 예상 월별 절감액(온디맨드)

## Amazon Redshift 예약 노드 최적화

설명

Amazon Redshift 사용량을 확인하고 예약 노드 구매 권장 사항을 제공하여 Amazon Redshift 온디맨드 사용 시 발생하는 비용을 절감합니다.

지난 30일 동안의 온디맨드 사용량을 분석하여 해당 권장 사항을 생성합니다. 이 분석을 사용하여 생성된 사용 범주의 모든 예약 조합을 시뮬레이션합니다. 이를 통해 절감을 극대화하기 위해 구매할 최적의 각 예약 노드 유형 수를 파악할 수 있습니다. 이 검사는 1년 또는 3년 약정과 함께 부분 선불 지급 옵션에 따른 권장 사항을 다룹니다.

통합 결제에 연결된 계정에서는 이 검사를 사용할 수 없습니다. 이 검사에 대한 권장 사항은 지급 계정에서만 사용할 수 있습니다.

검사 ID

```
1qw23er45t
```

알림 기준

노란색: Amazon Redshift 예약 노드 구매를 최적화하면 비용을 줄이는 데 도움이 될 수 있습니다.

권장 조치

Cost Explorer페이지에서 자세한 권장 사항, 사용자 지정 옵션(예: 조회 기간, 결제 옵션 등)을 참조하고 Amazon Redshift 예약 노드를 구매합니다.

추가 리소스

- Amazon Redshift 예약 노드에 대한 정보와 RI의 비용 절감 효과에 대한 자세한 내용은 여기에서 확인할 수 있습니다.
- 이 권장 사항에 대한 자세한 내용은 Trusted Advisor FAQ에서 예약 인스턴스 최적화 확인 질문을 참조하세요.
- 필드에 대한 자세한 설명은 Cost Explorer 설명서를 참조하세요.

보고서 열

- 리전
- Family
- 노드 유형(Node Type)
- 권장 구매 예약 노드 수
- 예상 평균 예약 노드 사용률
- 권장 사항을 통한 예상 절감액(월별)
- UpFront 예약 노드 비용
- 예약 노드의 예상 비용(월별)
- 권장 예약 노드 구매 후 예상 온디맨드 비용(월별)
- 예상 손익분기점(개월)

- 조회 기간(일)
- 기간(년)

## Amazon Relational Database Service(RDS) 예약 인스턴스 최적화

설명

RDS 사용량을 확인하고 예약 인스턴스 구매에 대한 권장 사항을 제공하여 RDS 온디맨드 사용 시 발생하는 비용을 절감합니다.

지난 30일 동안의 온디맨드 사용량을 분석하여 해당 권장 사항을 생성합니다. 이 분석을 사용하여 생성된 사용 범주의 모든 예약 조합을 시뮬레이션합니다. 이를 통해 절감 효과를 극대화하기 위해 구매할 최적의 각 예약 인스턴스 유형 수를 확인할 수 있습니다. 이 검사는 1년 또는 3년 약정으로 부분 선불 지급 옵션에 따른 권장 사항을 다룹니다.

통합 결제에 연결된 계정에서는 이 검사를 사용할 수 없습니다. 이 검사에 대한 권장 사항은 지급 계정에서만 사용할 수 있습니다.

검사 ID

```
1qazXsw23e
```

알림 기준

노란색: Amazon RDS 예약 인스턴스의 구매를 최적화하면 비용을 줄이는 데 도움이 될 수 있습니다.

권장 조치

Cost Explorer페이지에서 자세한 권장 사항, 사용자 지정 옵션(예: 조회 기간, 결제 옵션 등)을 참조하고 Amazon RDS 예약 인스턴스를 구매합니다.

추가 리소스

- Amazon RDS 예약 인스턴스에 대한 정보와 이 예약 인스턴스의 비용 절감 효과에 대한 자세한 내용은 여기에서 확인할 수 있습니다.
- 이 권장 사항에 대한 자세한 내용은 Trusted Advisor FAQ에서 예약 인스턴스 최적화 확인 질문을 참조하세요.
- 필드에 대한 자세한 설명은 Cost Explorer 설명서를 참조하세요.

보고서 열

- 리전

- Family
- 인스턴스 유형
- 라이선스 모델
- 데이터베이스 버전
- 데이터베이스 엔진
- 배포 옵션
- 권장 구매 예약 인스턴스 수
- 예상 평균 예약 인스턴스 사용률
- 권장 사항을 통한 예상 절감액(월별)
- 예약 인스턴스의 선결제 비용
- 예약 인스턴스의 예상 비용(월별)
- 권장 예약 인스턴스 구매 후 예상 온디맨드 비용(월별)
- 예상 손익분기점(개월)
- 조회 기간(일)
- 기간(년)

## Amazon Route 53 대기 시간 리소스 레코드 세트

설명

비효율적으로 구성된 Amazon Route 53 대기 시간 레코드 세트를 확인합니다.

Amazon Route 53가 네트워크 대기 시간이 가장 짧은 AWS 리전에 쿼리를 라우팅하려면 다른 리전에서 특정 도메인 이름(예: example.com)에 대한 대기 시간 리소스 레코드 세트를 생성해야 합니다. 도메인 이름에 대해 대기 시간 리소스 레코드 세트를 하나만 생성하면 모든 쿼리는 하나의 리전으로 라우팅되며 이점은 얻지 않고 지연 시간 기반 라우팅에 대한 추가 비용을 지불하게 됩니다.

AWS 서비스에 의해 생성된 호스팅 영역은 검사 결과에 나타나지 않습니다.

검사 ID

```
51fC20e7I2
```

알림 기준

노란색: 특정 도메인 이름에 대해 대기 시간 리소스 레코드 세트가 하나만 구성되어 있습니다.

권장 조치

여러 리전에 리소스가 있는 경우, 각 리전별로 대기 시간 리소스 레코드 세트를 정의해야 합니다. 대기 시간 기반 라우팅을 참조하세요.

하나의 AWS 리전에만 리소스가 있는 경우, 둘 이상의 AWS 리전에 리소스를 생성하고 각 리전별로 대기 시간 리소스 레코드 세트를 정의하는 것이 좋습니다. 대기 시간 기반 라우팅을 참조하세요.

여러 AWS 리전을 사용하지 않으려면, 단순 리소스 레코드 세트를 사용해야 합니다. 리소스 레코드 세트 관련 작업을 참조하세요.

추가 리소스

- Amazon Route 53 개발자 가이드
- Amazon Route 53 요금

보고서 열

- 호스팅 영역 이름
- 호스팅 영역 ID
- 리소스 레코드 세트 이름
- 리소스 레코드 세트 유형

## Amazon S3 버킷 수명 주기 정책 구성

설명

Amazon S3 버킷에 수명 주기 정책이 구성되어 있는지 확인합니다. Amazon S3 수명 주기 정책은 버킷 내의 Amazon S3 객체가 비용 효율적으로 저장되도록 보장합니다. 이는 데이터 보존 및 저장에 대한 규제 요구 사항을 충족하는 데 중요합니다. 정책 구성은 Amazon S3 서비스가 객체 그룹에 적용하는 작업을 정의하는 규칙 세트입니다. 수명 주기 정책을 사용하면 객체를 저렴한 스토리지 클래스로 전환하거나 노후화됨에 따라 객체를 삭제하는 작업을 자동화할 수 있습니다. 예를 들어 생성 후 30일 후에 Amazon S3 Standard-IA 스토리지로 객체를 이전하거나 1년 후에 Amazon S3 Glacier로 이전할 수 있습니다.

또한 특정 기간이 지나면 Amazon S3가 사용자를 대신하여 객체를 삭제하도록 객체 만료를 정의할 수 있습니다.

AWS Config 규칙의 파라미터를 사용하여 검사 구성을 조정할 수 있습니다.

자세한 내용은 스토리지 수명 주기 관리를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz100`

소스(Source)

`AWS Config Managed Rule: s3-lifecycle-policy-check`

알림 기준

노란색: Amazon S3 버킷에는 수명 주기 정책이 구성되어 있지 않습니다.

권장 조치

Amazon S3 버킷에 수명 주기 정책이 구성되어 있는지 확인하세요.

조직에 보존 정책이 마련되어 있지 않은 경우 Amazon S3 Intelligent-Tiering을 사용하여 비용을 최적화하는 것을 고려해 보세요.

Amazon S3 수명 주기 정책을 정의하는 방법에 대한 자세한 내용은 버킷의 수명 주기 구성 설정을 참조하세요.

Amazon S3 Intelligent-Tiering에 대한 자세한 내용은 Amazon S3 Intelligent-Tiering 스토리지 클래스를 참조하세요.

추가 리소스

버킷에서 수명 주기 구성 설정

S3 수명 주기 구성의 예제

보고서 열

- 상태 표시기
- 리전
- Resource
- AWS Config 규칙

- 입력 파라미터

## Amazon S3 미완료 멀티파트 업로드 중단 구성

설명

각 Amazon S3 버킷에 7일 후에도 완료되지 않은 멀티파트 업로드를 중단하는 수명 주기 규칙이 구성되어 있는지 확인합니다. 수명 주기 규칙을 사용하여 이러한 미완료 업로드를 중단하고 관련 스토리지를 삭제하는 것이 좋습니다.

> **Note**
>
> 이 검사의 결과는 매일 한 번 이상 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1cj39rr6v`

알림 기준

노란색: 수명 주기 구성 버킷에는 7일 후에도 완료되지 않은 모든 멀티파트 업로드를 중단하는 수명 주기 규칙이 포함되어 있지 않습니다.

권장 조치

불완전한 멀티파트 업로드를 모두 정리하는 수명 주기 규칙이 없는 버킷의 수명 주기 구성을 검토하세요. 24시간이 지난 후에도 업로드가 완료되지 않으면 업로드가 완료될 가능성이 낮습니다. 여기를 클릭하여 지침에 따라 라이프사이클 규칙을 생성하세요. 이를 버킷의 모든 객체에 적용하는 것이 좋습니다. 버킷의 선택된 객체에 다른 수명 주기 작업을 적용해야 하는 경우 필터가 다른 규칙을 여러 개 사용할 수 있습니다. 자세한 내용은 스토리지 렌즈 대시보드를 확인하거나 ListMultipartUpload API를 호출하세요.

추가 리소스

라이프사이클 구성 생성

Amazon S3 비용 절감을 위한 불완전한 멀티파트 업로드 발견 및 삭제

멀티파트 업로드를 사용한 객체 업로드 및 복사

라이프사이클 구성 요소

라이프사이클 작업을 설명하는 요소

멀티파트 업로드를 중단하기 위한 라이프사이클 구성

보고서 열

- 상태 표시기
- 리전
- 버킷 이름
- 버킷 ARN
- 불완전한 MPU 삭제를 위한 라이프사이클 규칙
- 시작 후 일수
- 최종 업데이트 시간

## 수명 주기 정책이 구성되지 않은 Amazon S3 버전 지원 버킷

설명

Amazon S3 버전 지원 버킷에 수명 주기 정책이 구성되어 있는지 확인합니다.

자세한 내용은 스토리지 수명 주기 관리를 참조하세요.

AWS Config 규칙의 bucketNames 파라미터를 사용하여 확인하려는 버킷 이름을 지정할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz171
```

소스(Source)

```
AWS Config Managed Rule: s3-version-lifecycle-policy-check
```

알림 기준

노란색: 수명 주기 정책이 구성되어 있지 않은 Amazon S3 버전 지원 버킷.

권장 조치

Amazon S3 버킷에 대한 수명 주기 정책을 구성하여 객체가 수명 주기 전반에 걸쳐 비용 효율적으로 저장되도록 객체를 관리합니다.

자세한 내용은 버킷에 대한 수명 주기 구성 설정을 참조하세요.

추가 리소스

스토리지 수명 주기 관리

버킷에서 수명 주기 구성 설정

보고서 열

- 상태 표시기
- 리전
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## 과도한 시간 초과가 있는 AWS Lambda 함수

설명

시간 초과 비율이 높아서 비용이 늘어날 수 있는 Lambda 함수를 확인합니다.

Lambda 요금은 런타임 및 함수에 대한 요청 수를 기준으로 합니다. 함수 시간 초과로 인해 오류가 발생하여 재시도를 초래합니다. 함수를 다시 시도하면 추가 요청 및 런타임 요금이 발생합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

L4dfs2Q3C3

알림 기준

노란색: 지난 7일 중에 특정 일에 발생한 시간 초과로 인해 호출의 10% 이상이 오류로 끝나는 함수입니다.

권장 조치

함수 로깅 및 X-Ray 트레이스를 검사하여 함수 지속 시간이 길어지는 원인을 확인합니다. API 호출 또는 데이터베이스 연결 전후와 같은 코드의 관련 부분에 로깅을 구현합니다. 기본적으로 AWS SDK 클라이언트 시간 초과는 구성된 함수 지속 시간보다 길어질 수 있습니다. 함수 제한 시간 내에 재시도 또는 실패하도록 API 및 SDK 연결 클라이언트를 조정합니다. 예상 지속 시간이 구성된 제한 시간보다 긴 경우 함수의 시간 초과 설정을 늘릴 수 있습니다. 자세한 내용은 Lambda 애플리케이션 모니터링 및 문제 해결을 참조하세요.

추가 리소스

- Lambda 애플리케이션 모니터링 및 문제 해결
- Lambda 함수 재시도 시간 초과 SDK
- AWS X-Ray과 함께 AWS Lambda 사용
- 다음에 대한 Amazon CloudWatch 로그에 액세스 AWS Lambda
- AWS Lambda용 오류 처리자 샘플 애플리케이션

보고서 열

- 상태 표시기
- 리전
- 함수 ARN
- 최대 일일 시간 초과 비율
- 최대 일일 시간 초과 비율 날짜
- 평균 일일 시간 초과 비율
- 함수 시간 초과 설정(밀리초)
- 일일 컴퓨팅 비용 손실
- 평균 일일 호출 건수
- 오늘 호출 건수
- 오늘 시간 초과 비율
- 최종 업데이트 시간

# 오류율이 높은 AWS Lambda 함수

## 설명

오류 비율이 높아 비용이 많이 들 수 있는 Lambda 함수를 검사합니다.

Lambda 요금은 함수에 대한 요청 수와 함수의 집계 런타임을 기준으로 합니다. 함수 오류로 인해 재시도가 발생하여 추가 비용이 발생할 수 있습니다.

> **Note**
>
> 해당 검사의 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

## 검사 ID

`L4dfs2Q3C2`

## 알림 기준

노란색: 지난 7일 중에 특정 일에 발생한 호출의 10% 이상이 오류로 끝나는 함수입니다.

## 권장 조치

오류를 줄이려면 다음 지침을 고려하세요. 함수 오류에는 함수의 코드가 반환하는 오류와 함수의 런타임에서 반환하는 오류가 포함되어 있습니다.

Lambda 오류를 해결하는 데 도움이 되도록 Lambda는 Amazon 및 같은 서비스와 통합됩니다. CloudWatch AWS X-Ray 로그, 지표, 경보 및 X-Ray 추적의 조합을 사용해 애플리케이션을 지원하는 함수 코드, API 또는 기타 리소스에서 문제를 신속하게 감지하고 식별할 수 있습니다. 자세한 내용은 Lambda 애플리케이션 모니터링 및 문제 해결을 참조하세요.

특정 런타임의 오류 처리에 대한 자세한 내용은 AWS Lambda의 오류 처리 및 자동 재시도를 참조하세요.

추가적인 문제 해결 정보는 Lambda 문제 해결을 참조하세요.

또한 AWS Lambda 파트너가 제공하는 모니터링 및 관측 도구의 생태계에서 도구를 선택할 수도 있습니다. 자세한 내용은 AWS Lambda 파트너를 참조하세요.

## 추가 리소스

- AWS Lambda의 오류 처리 및 자동 재시도

- Lambda 애플리케이션 모니터링 및 문제 해결
- Lambda 함수 재시도 시간 초과 SDK
- Lambda 문제 해결
- API 호출 오류
- AWS Lambda용 오류 처리자 샘플 애플리케이션

보고서 열

- 상태 표시기
- 리전
- 함수 ARN
- 최대 일일 오류 발생률
- 최대 오류 발생률 날짜
- 평균 일일 오류 발생률
- 일일 컴퓨팅 비용 손실
- 평균 일일 호출 건수
- 오늘 호출 건수

  오늘 오류 발생률
- 최종 업데이트 시간

## 메모리 크기에 대해 과다 프로비저닝된 AWS Lambda함수

설명

조회 기간 동안 한 번 이상 호출된 AWS Lambda함수를 검사합니다. 이 검사는 Lambda 함수가 메모리 크기에 대해 과다 프로비저닝되었는지 여부를 알려줍니다. 메모리 크기에 대해 과다 프로비저닝된 Lambda 함수가 있는 경우 사용하지 않은 리소스에 대한 비용을 지불하게 됩니다. 일부 시나리오에서는 설계상 사용률이 낮아질 수 있지만 흔히 Lambda 함수의 메모리 구성을 변경하여 비용을 절감할 수 있습니다. 예상 월별 절감액은 EBS 볼륨의 현재 사용률을 사용하여 계산됩니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`C0r6dfpM05`

알림 기준

노란색: 조회 기간 동안 메모리 크기가 과다 프로비저닝된 Lambda 함수가 있습니다. Lambda 함수가 오버 프로비저닝되었는지 확인하기 위해 해당 함수에 대한 모든 기본 메트릭을 고려합니다. CloudWatch 메모리 크기가 과다 프로비저닝된 Lambda 함수를 식별하는 데 사용되는 알고리즘은 AWS 모범 사례를 따릅니다. 새 패턴이 식별되면 알고리즘이 업데이트됩니다.

권장 조치

Lambda 함수의 메모리 크기를 줄이는 것이 좋습니다.

자세한 설명은 Trusted Advisor 수표 AWS Compute Optimizer 신청 섹션을 참조하세요.

보고서 열

- 상태 표시기
- 리전
- 함수 이름
- Function Version
- 메모리 크기(MB)
- 권장 메모리 크기(MB)
- 조회 기간(일)
- 절감 기회(%)
- 예상 월별 절감액
- 예상 월별 절감액 통화
- 최종 업데이트 시간

## 비용 최적화에 대한 AWS Well-Architected 위험도 높음 문제

설명

비용 최적화 기반에서 워크로드의 위험도 높음 문제(HRI)를 확인합니다. 이 검사는 사용자 AWS-Well Architected 리뷰를 기반으로 합니다. AWS Well-Architected에서 워크로드 평가를 완료했는지 여부에 따라 검사 결과가 달라집니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`Wxdfp4B1L1`

알림 기준

- 빨간색: AWS Well-Architected의 비용 최적화 원칙에서 하나 이상의 활성 고위험 문제가 확인되었습니다.
- 녹색: AWS Well-Architected의 비용 최적화 원칙에서 활성 고위험 문제가 탐지되지 않았습니다.

권장 조치

AWS Well-Architected가 워크로드 평가 중에 고위험 문제를 탐지했습니다. 이러한 문제는 위험을 줄이고 비용을 절감할 수 있는 기회를 나타냅니다. AWS Well-Architected 도구에 로그인하여 답변을 검토하고 활성 문제를 해결하기 위한 조치를 취하세요.

보고서 열

- 상태 표시기
- 리전
- 워크로드 ARN
- 워크로드 이름
- 검토자 이름
- 워크로드 유형
- 워크로드 시작 날짜
- 워크로드 마지막 수정 날짜
- 비용 최적화에 대해 식별된 HRI 수
- 비용 최적화에 대해 해결된 HRI 수
- 비용 최적화에 대해 답변한 질문 수
- 비용 최적화 원칙의 총 질문 수
- 최종 업데이트 시간

## 유휴 로드 밸런서

설명

유휴 상태인 로드 밸런서에 대한 Elastic Load Balancing 구성을 검사합니다.

구성된 모든 로드 밸런서에서 요금이 발생합니다. 로드 밸런서에 연결된 백엔드 인스턴스가 없거나 네트워크 트래픽이 심하게 제한된 경우 로드 밸런서가 효과적으로 사용되지 않는 것입니다. 이 검사는 현재 ELB 서비스 내의 Classic Load Balancer 유형만 확인합니다. 다른 ELB 유형(Application Load Balancer, Network Load Balancer)은 포함되지 않습니다.

검사 ID

`hjLMh88uM8`

알림 기준

- 노란색: 로드 밸런서에 활성 상태의 백엔드 인스턴스가 없습니다.
- 노란색: 로드 밸런서에 정상 상태의 백엔드 인스턴스가 없습니다.
- 노란색: 지난 7일 동안 로드 밸런서의 요청이 하루에 100개 미만이었습니다.

권장 조치

로드 밸런서에 활성 상태의 백엔드 인스턴스가 없는 경우, 인스턴스를 등록하거나 로드 밸런서를 삭제하는 것이 좋습니다. 로드 밸런서에 Amazon EC2 인스턴스 등록 또는 로드 밸런서 삭제를 참조하세요.

로드 밸런서에 정상 상태의 백엔드 인스턴스가 없는 경우 Elastic Load Balancing 문제 해결: 상태 확인 구성을 참조하세요.

로드 밸런서의 요청 수가 적은 경우, 로드 밸런서를 삭제하는 것이 좋습니다. 로드 밸런서 삭제를 참조하세요.

추가 리소스

- 로드 밸런서 관리
- Elastic Load Balancing 문제 해결

보고서 열

- 리전
- load-balancer-name
- 이유
- 예상 월별 절감액

## 낮은 사용률의 Amazon EC2 인스턴스

설명

지난 14일 동안 실행 중이었던 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 모든 시점에서 확인합니다. 이 검사는 일일 CPU 사용률이 10% 이하이고 네트워크 I/O가 4일 이상 5MB 이하인 경우 알립니다.

실행 인스턴스에는 시간당 사용 요금을 부과합니다. 일부 시나리오에서는 설계상 사용률이 낮아질 수 있지만 인스턴스의 수와 크기를 관리하여 비용을 절감할 수 있습니다.

예상 월별 절감액은 온디맨드 인스턴스의 현재 사용률과 인스턴스의 사용률이 낮아질 수 있는 예상 일수를 사용하여 계산됩니다. 예약 인스턴스 또는 스팟 인스턴스를 사용하거나 인스턴스가 하루 종일 실행되지 않는 경우 실제 절감액이 달라집니다. 일일 사용률 데이터를 가져오려면 이 검사에 대한 보고서를 다운로드하십시오.

검사 ID

`Qch7DwouX1`

알림 기준

노란색: 지난 14일 중 4일 이상 인스턴스의 일일 평균 CPU 사용률이 10% 이하이고 네트워크 I/O가 5MB 이하였습니다.

권장 조치

사용률이 낮은 인스턴스를 중지 또는 종료하거나 오토 스케일링을 사용하여 인스턴스 수를 조정하는 것이 좋습니다. 자세한 내용은 인스턴스 중지 및 시작,인스턴스 종료 및 Auto Scaling이란 무엇입니까?를 참조하세요.

추가 리소스

- Amazon EC2 모니터링
- 인스턴스 메타데이터 및 사용자 데이터
- 아마존 CloudWatch 사용 설명서
- 오토 스케일링 개발자 가이드

보고서 열

- 리전/AZ
- 인스턴스 ID
- 인스턴스 이름

- 인스턴스 유형
- 예상 월별 절감액
- CPU 사용률 14일 평균
- 네트워크 I/O 14일 평균
- 사용률이 낮은 일수

## Savings Plan

설명

지난 30일 동안 Amazon EC2, Fargate 및 Lambda 사용량을 확인하여 Savings Plan 구매 권장 사항을 제공합니다. 이러한 권장 사항을 통해 할인된 요금에 대한 대가로 1년 또는 3년 기간 동안 시간당 달러로 측정한 일관된 사용량을 약정할 수 있습니다.

이것은 AWS Cost Explorer에서 소싱되며 여기서 자세한 권장 사항 정보를 얻을 수 있습니다. Cost Explorer를 통해 비용 절감형 플랜을 구매할 수도 있습니다. 이러한 권장 사항은 RI 권장 사항에 대한 대안으로 간주되어야 합니다. 한 세트의 권장 사항에 대해서만 행동하는 것이 좋습니다. 두 세트 모두에 대해 행동하면 과도한 약정이 발생할 수 있습니다.

통합 결제에 연결된 계정에서는 이 검사를 사용할 수 없습니다. 이 검사에 대한 권장 사항은 지급 계정에서만 사용할 수 있습니다.

검사 ID

`vZ2c2W1srf`

알림 기준

노란색: 절감형 플랜 구매를 최적화하면 비용 절감에 도움이 될 수 있습니다.

권장 조치

자세하고 맞춤화된 권장 사항을 참조하고 절감형 플랜을 구매하려면 Cost Explorer 페이지를 참조하세요.

추가 리소스

- 절감형 플랜 사용 설명서
- 절감형 플랜 FAQ

보고서 열

- 절감형 플랜 유형

- 결제 옵션
- 선불 비용
- 시간당 구매 약정
- 예상 평균 사용률
- 예상 월별 절감액
- 예상 절감률
- 기간(년)
- 조회 기간(일)

## 연결되지 않은 탄력적 IP 주소

설명

실행 중인 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 연결되지 않은 Elastic IP 주소(EIP)를 확인합니다.

EIP는 동적 클라우드 컴퓨팅용으로 설계된 고정 IP 주소입니다. 기존의 고정 IP 주소와 달리 EIP는 퍼블릭 IP 주소를 계정의 다른 인스턴스에 다시 매핑하여 인스턴스나 가용 영역의 오류를 마스킹합니다. 실행 중인 인스턴스와 연결되지 않은 EIP에는 명목상의 요금이 부과됩니다.

검사 ID

`Z4AUBRNSmz`

알림 기준

노란색: 할당된 탄력적 IP 주소(EIP)가 실행 중인 Amazon EC2 인스턴스와 연결되어 있지 않습니다.

권장 조치

실행 중인 활성 인스턴스에 EIP를 연결하거나, 연결되지 않은 EIP를 해제합니다. 자세한 내용은 실행 중인 다른 인스턴스와 탄력적 IP 주소 연결 및 탄력적 IP 주소 해제를 참조하세요.

추가 리소스

탄력적 IP 주소

보고서 열

- 리전

- IP 주소

## 사용률이 낮은 Amazon EBS 볼륨

설명

Amazon Elastic Block Store(Amazon EBS) 볼륨 구성을 확인하고 볼륨의 활용도가 낮은 것으로 나타날 경우 경고합니다.

요금은 볼륨이 생성될 때 부과되기 시작합니다. 볼륨이 연결되지 않은 상태로 유지되거나 일정 기간 동안 쓰기 작업이 매우 낮은 경우(부팅 볼륨 제외) 볼륨의 활용도가 낮은 것입니다. 비용을 줄이려면 활용도가 낮은 볼륨을 제거하는 것이 좋습니다.

검사 ID

DAvU99Dc4C

알림 기준

노란색: 볼륨이 연결되지 않았거나, 지난 7일 동안 입출력 양이 하루에 1 IOPS 미만이었습니다.

권장 조치

비용 절감을 위해 스냅샷을 생성하고 볼륨을 삭제하는 것이 좋습니다. 자세한 내용은 Amazon EBS 스냅샷 생성 및 Amazon EBS 볼륨 삭제를 참조하세요.

추가 리소스

- Amazon Elastic Block Store(Amazon EBS)
- 볼륨 상태 모니터링

보고서 열

- 리전
- 볼륨 ID
- 볼륨 이름
- 볼륨 유형
- 볼륨 크기
- 월별 스토리지 비용
- 스냅샷 ID
- 스냅샷 이름

- 스냅샷 경과 시간

> **Note**
>
> AWS Compute Optimizer에 계정을 옵트인한 경우 대신 Amazon EBS 과다 프로비저닝된 볼륨 검사를 사용하는 것이 좋습니다. 자세한 설명은 Trusted Advisor 수표 AWS Compute Optimizer 신청 섹션을 참조하세요.

## Underutilized Amazon Redshift Clusters

설명

Amazon Redshift 구성에서 사용률이 낮은 것으로 보이는 클러스터를 확인합니다.

Amazon Redshift 클러스터가 장기간 연결되지 않았거나 CPU를 적게 사용하는 경우, 클러스터 다운사이징이나 클러스터 종료 및 최종 스냅샷 생성과 같이 비용이 저렴한 옵션을 사용할 수 있습니다. 클러스터를 삭제한 후에도 최종 스냅샷은 보존됩니다.

검사 ID

`G31sQ1E9U`

알림 기준

- 노란색: 실행 중인 클러스터가 지난 7일 동안 연결되지 않았습니다.
- 노란색: 실행 중인 클러스터의 클러스터 전체 평균 CPU 사용률이 지난 7일 중 99%의 시간 동안 5% 미만이었습니다.

권장 조치

클러스터를 종료하고 최종 스냅샷을 생성하거나 클러스터를 축소하는 것이 좋습니다. 클러스터 종료 및 삭제 및 클러스터 크기 조정을 참조하세요.

추가 리소스

아마존 CloudWatch 사용 설명서

보고서 열

- 상태 표시기
- 리전
- 클러스터

- 인스턴스 유형
- 이유
- 예상 월별 절감액

## 성능

서비스 할당량(이전에는 제한이라고 함)을 확인하여 서비스 성능을 향상시키면 프로비저닝된 처리량을 활용하고, 과도하게 사용된 인스턴스를 모니터링하며, 사용되지 않는 리소스를 감지할 수 있습니다.

성능 범주에 대해 다음과 같은 검사를 사용할 수 있습니다.

검사명

- Amazon Aurora DB 클러스터가 읽기 워크로드를 위해 충분히 프로비저닝되지 않음
- Amazon DynamoDB Auto Scaling이 활성화되지 않음
- Amazon EBS 최적화가 활성화되지 않음
- Amazon EBS로 프로비저닝된 IOPS(SSD) 볼륨 첨부 구성
- Amazon EBS 과소 프로비저닝된 볼륨
- Amazon EC2 Auto Scaling 그룹은 시작 템플릿과 연결되어 있지 않음
- Amazon EC2에서 EBS로 처리량 최적화
- EC2 가상화 유형은 반가상입니다
- Amazon ECS 메모리 하드 제한
- Amazon EFS 처리량 모드 최적화
- Amazon RDS 자동 진공 파라미터가 꺼져 있습니다.
- Amazon RDS DB 클러스터는 최대 64TiB 볼륨만 지원합니다.
- 이기종 인스턴스 클래스가 있는 클러스터의 Amazon RDS DB 인스턴스
- 이기종 인스턴스 크기를 사용하는 클러스터의 Amazon RDS DB 인스턴스
- Amazon RDS DB 메모리 파라미터가 기본값과 다릅니다.
- Amazon RDS enable_index 전용 스캔 파라미터가 꺼져 있습니다.
- Amazon RDS enable_indexscan 파라미터가 꺼져 있습니다
- Amazon RDS general_logging 파라미터가 켜져 있습니다.
- 최적 값보다 작은 값을 사용하는 Amazon RDS InnoDB_change_버퍼링 파라미터
- Amazon RDS innodb_open_files 파라미터가 낮음

- Amazon RDS innodb_stats_persistent 파라미터가 비활성화되었습니다
- 시스템 용량에 비해 Amazon RDS 인스턴스가 충분히 프로비저닝되지 않음
- Amazon RDS 마그네틱 볼륨 사용 중
- 대용량 페이지를 사용하지 않는 Amazon RDS 파라미터 그룹
- Amazon RDS 쿼리 캐시 파라미터가 켜져 있습니다.
- Amazon RDS 리소스 인스턴스 클래스 업데이트가 필요합니다.
- Amazon RDS 리소스 메이저 버전 업데이트가 필요합니다.
- 라이선스 포함 시 지원 종료 엔진 에디션을 사용하는 Amazon RDS 리소스
- Amazon Route 53 별칭 리소스 레코드 세트
- 메모리 크기에 대해 과소 프로비저닝된AWS Lambda 함수
- AWS Lambda 동시성 제한이 없는 함수 (구성)
- 성능에 대한 AWS Well-Architected 위험도 높음 문제
- CloudFront 대체 도메인 이름
- CloudFront 콘텐츠 전송 최적화
- CloudFront 헤더 포워딩 및 캐시 적중률
- 높은 사용률의 Amazon EC2 인스턴스

## Amazon Aurora DB 클러스터가 읽기 워크로드를 위해 충분히 프로비저닝되지 않음

설명

Amazon Aurora DB 클러스터에 읽기 워크로드를 지원하는 리소스가 있는지 확인합니다.

검사 ID

`c1qf5bt038`

알림 기준

노란색:

데이터베이스 읽기 증가: 데이터베이스 부하가 높았고 데이터베이스에서 행을 쓰거나 업데이트하는 것보다 읽는 행이 더 많았습니다.

권장 조치

쿼리를 조정하여 데이터베이스 부하를 줄이거나 클러스터의 Writer DB 인스턴스와 동일한 인스턴스 클래스 및 크기의 Reader DB 인스턴스를 DB 클러스터에 추가하는 것이 좋습니다. 현재 구성에

는 주로 읽기 작업으로 인한 데이터베이스 부하가 지속적으로 높은 DB 인스턴스가 하나 이상 있습니다. 클러스터에 다른 DB 인스턴스를 추가하고 읽기 워크로드를 DB 클러스터 읽기 전용 엔드포인트로 전달하여 이러한 작업을 분산하세요.

추가 리소스

Aurora DB 클러스터에는 읽기 전용 연결을 위한 리더 엔드포인트가 하나 있습니다. 이 엔드포인트는 로드 밸런싱을 사용하여 DB 클러스터의 데이터베이스 부하에 가장 많이 기여하는 쿼리를 관리합니다. 리더 엔드포인트는 이러한 명령문을 Aurora 읽기 전용 복제본으로 전달하여 기본 인스턴스의 부하를 줄입니다. 또한 리더 엔드포인트는 클러스터의 Aurora 읽기 전용 복제본 수에 따라 동시 SELECT 쿼리를 처리할 수 있는 용량을 확장합니다.

자세한 내용은 DB 클러스터에 Aurora 복제본 추가 및 Aurora DB 클러스터의 성능 및 조정 관리를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 데이터베이스 읽기 증가 (개수)
- 마지막 탐지 기간
- 최종 업데이트 시간

## Amazon DynamoDB Auto Scaling이 활성화되지 않음

설명

Amazon DynamoDB 테이블 및 글로벌 보조 인덱스에 Auto Scaling 또는 온디맨드 기능이 활성화되어 있는지 확인합니다.

Amazon DynamoDB Auto Scaling은 Application Auto Scaling 서비스를 사용하여 프로비저닝된 처리 능력을 실제 트래픽 패턴에 따라 사용자 대신 동적으로 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기 및 쓰기 용량을 늘려 병목 현상 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다. 워크로드가 감소할 경우 Application Auto Scaling은 사용하지 않는 프로비저닝된 용량에 대한 요금을 지불하지 않도록 처리량을 줄일 수 있습니다.

AWS Config 규칙의 매개변수를 사용하여 검사 구성을 조정할 수 있습니다.

자세한 내용은 DynamoDB Auto Scaling을 사용하여 자동으로 처리량 용량 관리를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c18d2gz136

소스

AWS Config 관리형 규칙: dynamodb-autoscaling-enabled

알림 기준

노란색: DynamoDB 테이블 및/또는 글로벌 보조 인덱스에는 Auto Scaling이 활성화되어 있지 않습니다.

권장 조치

워크로드 요구 사항에 따라 DynamoDB 테이블 및/또는 글로벌 보조 인덱스의 프로비저닝된 처리량을 자동으로 조정하는 메커니즘이 이미 없는 한, Amazon DynamoDB 테이블에 대해 Auto Scaling을 활성화하는 것을 고려해 보십시오.

자세한 내용은 DynamoDB 자동 scalingp과 함께 AWS Management Console 사용을 참조하세요.

추가 리소스

DynamoDB Auto Scaling을 사용하여 자동으로 처리량 용량 관리

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

# Amazon EBS 최적화가 활성화되지 않음

설명

Amazon EC2 인스턴스에 Amazon EBS 최적화가 활성화되어 있는지 확인합니다.

Amazon EBS 최적화 인스턴스는 최적화된 구성 스택을 사용하며 Amazon EBS I/O를 위한 전용 용량을 추가로 제공합니다. 이 최적화는 Amazon EBS I/O와 인스턴스의 다른 트래픽 간의 경합을 최소화하여 Amazon EBS 볼륨에 최상의 성능을 제공합니다.

자세한 내용은 Amazon EBS 최적화 인스턴스를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz142`

소스

AWS Config 관리형 규칙: ebs-optimized-instance

알림 기준

노란색: 지원되는 Amazon EC2 인스턴스에서는 Amazon EBS 최적화가 활성화되어 있지 않습니다.

권장 조치

지원되는 인스턴스에서 Amazon EBS 최적화를 활성화합니다.

자세한 내용은 시작 시 EBS 최적화 활성화를 참조하세요.

추가 리소스

Amazon EBS 최적화 인스턴스

보고서 열

- 상태 표시기
- 지역

- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon EBS로 프로비저닝된 IOPS(SSD) 볼륨 첨부 구성

설명

Amazon EBS로는 최적화되고 EBS로는 최적화되지 않는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결되어 있는 프로비저닝된 IOPS(SSD) 볼륨이 있는지 확인합니다.

Amazon Elastic Block Store(Amazon EBS)의 프로비저닝된 IOPS(SSD) 볼륨은 EBS 최적화 인스턴스에 연결된 경우에만 예상 성능을 제공하도록 설계되었습니다.

검사 ID

`PPkZrjsH2q`

알림 기준

노란색: EBS에 최적화할 수 있는 Amazon EC2 인스턴스에 프로비저닝된 IOPS SSD) 볼륨이 연결되어 있지만, 인스턴스가 EBS에 최적화되어 있지 않습니다.

권장 조치

EBS에 최적화된 새 인스턴스를 생성하고 볼륨을 분리한 다음 볼륨을 새 인스턴스에 다시 연결합니다. 자세한 내용은 Amazon EBS 최적화 인스턴스와 인스턴스에 Amazon EBS 볼륨 연결을 참조하세요.

추가 리소스

- Amazon EBS 볼륨 유형
- Amazon EBS 볼륨 성능

보고서 열

- 상태 표시기
- 리전/AZ
- 볼륨 ID
- 볼륨 이름
- 볼륨 연결

- 인스턴스 ID
- 인스턴스 유형
- EBS 최적

## Amazon EBS 과소 프로비저닝된 볼륨

설명

조회 기간 동안 실행 중이었던 Amazon Elastic Block Store (Amazon EBS) 볼륨을 검사합니다. 이 검사는 워크로드에 대해 EBS 볼륨이 과소 프로비저닝되었는지 알려줍니다. 일관되게 높은 사용률은 최적화된 안정적인 성능을 나타낼 수 있지만 응용 프로그램에 충분한 리소스가 없음을 나타낼 수도 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`COr6dfpM04`

알림 기준

노란색: 조회 기간 동안 과소 프로비저닝된 EBS 볼륨입니다. 볼륨이 제대로 프로비저닝되지 않았는지 확인하기 위해 모든 기본 CloudWatch 지표 (IOPS 및 처리량 포함) 를 고려합니다. 프로비저닝이 부족한 EBS 볼륨을 식별하는 데 사용되는 알고리즘은 모범 사례를 따릅니다. AWS 새 패턴이 식별되면 알고리즘이 업데이트됩니다.

권장 조치

사용률이 높은 볼륨은 크기를 늘리는 것이 좋습니다.

자세한 정보는 Trusted Advisor 수표 AWS Compute Optimizer 신청을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- 볼륨 ID

- 볼륨 유형
- 볼륨 크기(GB)
- 볼륨 기준 IOPS
- 볼륨 버스트 IOPS
- 볼륨 버스트 처리량(throughput)
- 권장 볼륨 유형
- 권장 볼륨 크기(GB)
- 권장 볼륨 기준 IOPS
- 권장 볼륨 버스트 IOPS
- 권장 볼륨 기준 처리량(throughput)
- 권장 볼륨 버스트 처리량(throughput)
- 조회 기간(일)
- 성능 리스크
- 최종 업데이트 시간

## Amazon EC2 Auto Scaling 그룹은 시작 템플릿과 연결되어 있지 않음

설명

Amazon EC2 Auto Scaling 그룹이 Amazon EC2 시작 템플릿으로 생성되었는지 확인합니다.

시작 템플릿을 사용하여 Amazon EC2 Auto Scaling 그룹을 생성하여 최신 Auto Scaling 그룹 기능 및 개선 사항에 액세스할 수 있습니다. 버전 관리 및 여러 인스턴스 유형을 예로 들 수 있습니다.

자세한 내용은 시작 템플릿을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz102`

소스

AWS Config 관리형 규칙: autoscaling-launch-template

알림 기준

노란색: Amazon EC2 Auto Scaling 그룹이 유효한 시작 템플릿과 연결되어 있지 않습니다.

권장 조치

Amazon EC2 시작 템플릿을 사용하여 Amazon EC2 Auto Scaling 그룹을 생성합니다.

자세한 내용은 Auto Scaling 그룹을 위한 시작 템플릿 생성을 참조하세요.

추가 리소스

- 시작 템플릿
- 시작 템플릿 생성

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon EC2에서 EBS로 처리량 최적화

설명

연결된 Amazon EC2 인스턴스의 최대 처리량 성능에 영향을 줄 수 있는 Amazon EBS 볼륨을 확인합니다.

성능을 최적화하려면 Amazon EC2 인스턴스의 최대 처리량이 연결된 EBS 볼륨의 총 최대 처리량보다 큰지 확인해야 합니다. 이 검사는 각 EBS 최적화 인스턴스에 대해 전날(UTC(협정 세계시) 기준)의 각 5분 동안 총 EBS 볼륨 처리량을 계산하고 해당 기간 중 절반 이상의 사용량이 EC2 인스턴스의 최대 처리량의 95%를 초과하는 경우 경고합니다.

검사 ID

Bh2xRR2FGH

알림 기준

노란색: 전날(UTC)에 50%를 넘는 시간 동안, EC2 인스턴스에 연결된 EBS 볼륨의 총 처리량(throughput)(메가바이트/초)이 인스턴스와 EBS 볼륨 간에 게시된 처리량(throughput)의 95%를 초과했습니다.

권장 조치

Amazon EBS 볼륨(Amazon EBS 볼륨 유형 참조)의 최대 처리량(throughput)을 연결된 Amazon EC2 인스턴스의 최대 처리량(throughput)과 비교합니다. EBS 최적화를 지원하는 인스턴스 유형을 참조하세요.

최적의 성능을 얻으려면, Amazon EBS에 더 높은 처리량(throughput)을 지원하는 인스턴스에 볼륨을 연결하는 것이 좋습니다.

추가 리소스

- Amazon EBS 볼륨 유형
- Amazon EBS 최적화 인스턴스
- 볼륨 상태 모니터링
- 인스턴스에 Amazon EBS 볼륨 연결
- 인스턴스에서 Amazon EBS 볼륨 분리
- Amazon EBS 볼륨 삭제

보고서 열

- 상태 표시기
- 지역
- 인스턴스 ID
- 인스턴스 유형
- 최대값에 가까운 시간

## EC2 가상화 유형은 반가상입니다

설명

Amazon EC2 인스턴스의 가상화 유형이 반가상인지 확인합니다.

가능하면 반가상 인스턴스 대신 하드웨어 가상 머신(HVM) 인스턴스를 사용하는 것이 가장 좋습니다. 이는 HVM 가상화 기능이 향상되고 HVM AMI용 PV 드라이버가 제공되는 현재는 이전에는 PV

게스트와 HVM 게스트 간에 존재했던 성능 격차가 줄어들었기 때문입니다. 최신 세대 인스턴스 유형은 PV AMI를 지원하지 않는다는 점에 유의해야 합니다. 따라서 HVM 인스턴스 유형을 선택하면 최상의 성능과 최신 하드웨어와의 호환성을 제공합니다.

자세한 내용은 Linux AMI 가상화 유형을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c18d2gz148

소스

AWS Config 관리형 규칙: ec2-반가상 인스턴스 검사

알림 기준

노란색: Amazon EC2 인스턴스의 가상화 유형은 반가상입니다.

권장 조치

Amazon EC2 인스턴스에 HVM 가상화를 사용하고 호환되는 인스턴스 유형을 사용하십시오.

적절한 가상화 유형을 선택하는 방법에 대한 자세한 내용은 인스턴스 유형 변경을 위한 호환성을 참조하세요.

추가 리소스

인스턴스 유형 변경을 위한 호환성

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon ECS 메모리 하드 제한

설명

Amazon ECS 작업 정의에 컨테이너 정의를 위해 설정된 메모리 제한이 있는지 확인합니다. 작업 내 모든 컨테이너에 대해 예약된 총 메모리 양은 작업 메모리 값보다 작아야 합니다.

자세한 내용은 컨테이너 정의를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c18d2gz176

소스

AWS Config 관리형 규칙: ecs-task-definition-memory -하드 리밋

알림 기준

노란색: Amazon ECS 메모리 하드 제한이 설정되지 않았습니다.

권장 조치

Amazon ECS 작업에 메모리를 할당하여 메모리 부족을 방지합니다. 컨테이너가 지정된 메모리를 초과하려고 시도하면 컨테이너가 종료됩니다.

자세한 내용은 Amazon ECS의 작업에 메모리를 할당하려면 어떻게 해야 합니까?를 참조하세요.

추가 리소스

클러스터 예약

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙

- 입력 파라미터
- 최종 업데이트 시간

## Amazon EFS 처리량 모드 최적화

설명

고객의 Amazon EFS 파일 시스템이 현재 버스팅 처리량 모드를 사용하도록 구성되어 있는지 확인합니다.

EFS의 버스팅 처리량 모드 [1]의 파일 시스템은 일관된 기준 처리량 수준(EFS 표준 스토리지의 데이터 GiB당 50KiB/s)을 제공하며, “버스트 크레딧”을 사용할 수 있는 경우 크레딧 모델을 사용하여 더 높은 수준의 “버스트 처리량” 성능을 제공합니다. 버스트 크레딧을 모두 사용하면 파일 시스템 성능이 이 보다 낮은 기준 수준으로 조절되어 최종 사용자나 애플리케이션에 속도 저하, 시간 초과 또는 기타 형태의 성능 저하를 초래할 수 있습니다.

검사 ID

`c1dfprch02`

알림 기준

- 노란색: 파일 시스템이 버스팅 처리량 모드를 사용하고 있습니다.

권장 조치

사용자와 애플리케이션이 원하는 처리량을 달성할 수 있도록 파일 시스템 구성을 탄력적 처리량 모드 [2]로 업데이트하는 것이 좋습니다. 탄력적 처리량 모드에서 파일 시스템은 AWS 리전 [3]에 따라 최대 10GiB/s의 읽기 처리량 또는 3GiB/s의 쓰기 처리량을 달성할 수 있으며, 사용한 처리량에 대해서만 비용을 지불하면 됩니다. 필요에 따라 탄력적 처리량 모드와 버스팅 처리량 모드 사이를 전환하도록 파일 시스템 구성을 업데이트할 수 있으며, 탄력적 처리량 모드의 파일 시스템은 데이터 전송 [4]에 대해 추가 요금이 발생한다는 점에 유의하세요.

추가 리소스

- [1] Amazon EFS 성능 처리량 모드
- [2] Amazon EFS 성능 Elastic 처리량 모드
- [3] Amazon EFS 할당량 및 한도
- [4] Amazon EFS 요금 책정

보고서 열

- 상태 표시기
- 지역

- EFS 파일 시스템 ID
- 처리량 모드
- 최종 업데이트 시간

## Amazon RDS 자동 진공 파라미터가 꺼져 있습니다.

설명

DB 인스턴스의 autovacuum 파라미터가 비활성화되어 있습니다. autovacuum 기능을 비활성화하면 표 및 인덱스 팽창이 증가하고 성능에 영향을 미칩니다.

DB 파라미터 그룹에서 autovacuum을 켜는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt025`

알림 기준

노란색: DB 파라미터 그룹의 autovacuum 기능이 꺼져 있습니다.

권장 조치

DB 파라미터 그룹에서 autovacuum 파라미터를 활성화하세요.

추가 리소스

PostgreSQL 데이터베이스에는 주기적인 유지 관리가 필요하며 이를 진공 청소라고 합니다. PostgreSQL의 Autovacuum은 VACUUM 및 ANALYZE 명령 실행을 자동화합니다. 이 프로세스는 테이블 통계를 수집하고 데드 행을 삭제합니다. autovacuum을 끄면 테이블 증가, 인덱스 팽창, 부실 통계 등이 데이터베이스 성능에 영향을 미칩니다.

자세한 내용은 PostgreSQL 환경을 위한 Amazon RDS의 자동 진공 관리에 대한 이해를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 가치입니다.
- 최종 업데이트 시간

## Amazon RDS DB 클러스터는 최대 64TiB 볼륨만 지원합니다.

설명

DB 클러스터가 최대 64TiB의 볼륨을 지원합니다. 최신 엔진 버전은 최대 128TiB의 볼륨을 지원합니다. DB 클러스터의 엔진 버전을 최신 버전으로 업그레이드하여 최대 128TiB의 볼륨을 지원하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.

DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt017`

알림 기준

노란색: DB 클러스터는 최대 64TiB의 볼륨만 지원합니다.

권장 조치

DB 클러스터의 엔진 버전을 업그레이드하여 최대 128TiB의 볼륨을 지원하세요.

추가 리소스

단일 Amazon Aurora DB 클러스터에서 애플리케이션을 확장할 때 스토리지 한도가 128TiB인 경우 한도에 도달하지 못할 수 있습니다. 늘어난 스토리지 한도는 데이터를 삭제하거나 데이터베이스를 여러 인스턴스로 분할하는 것을 방지하는 데 도움이 됩니다.

자세한 내용은 Amazon Aurora 크기 제한을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 엔진 이름
- 엔진 버전: 현재
- 권장 값
- 최종 업데이트 시간

## 이기종 인스턴스 클래스가 있는 클러스터의 Amazon RDS DB 인스턴스

설명

DB 클러스터의 모든 DB 인스턴스에 대해 동일한 DB 인스턴스 클래스와 크기를 사용하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt009`

알림 기준

빨간색: DB 클러스터에는 이기종 인스턴스 클래스가 있는 DB 인스턴스가 있습니다.

권장 조치

DB 클러스터의 모든 DB 인스턴스에 대해 동일한 인스턴스 클래스와 크기를 사용하세요.

추가 리소스

DB 클러스터의 DB 인스턴스가 서로 다른 DB 인스턴스 클래스 또는 크기를 사용하는 경우 DB 인스턴스의 워크로드에 불균형이 발생할 수 있습니다. 장애 조치 중에 리더 DB 인스턴스 중 하나가 작성자 DB 인스턴스로 변경됩니다. DB 인스턴스가 동일한 DB 인스턴스 클래스와 크기를 사용하는 경우 DB 클러스터의 DB 인스턴스에 맞게 워크로드를 밸런싱할 수 있습니다.

자세한 내용은 Aurora 복제본을 참조하십시오.

보고서 열

- 상태 표시기
- 지역

- Resource
- 권장 값
- 엔진 이름
- 최종 업데이트 시간

## 이기종 인스턴스 크기를 사용하는 클러스터의 Amazon RDS DB 인스턴스

### 설명

DB 클러스터의 모든 DB 인스턴스에 대해 동일한 DB 인스턴스 클래스와 크기를 사용하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

### 검사 ID

`c1qf5bt008`

### 알림 기준

빨간색: DB 클러스터에는 인스턴스 크기가 서로 다른 DB 인스턴스가 있습니다.

### 권장 조치

DB 클러스터의 모든 DB 인스턴스에 대해 동일한 인스턴스 클래스와 크기를 사용하세요.

추가 리소스

DB 클러스터의 DB 인스턴스가 서로 다른 DB 인스턴스 클래스 또는 크기를 사용하는 경우 DB 인스턴스의 워크로드에 불균형이 발생할 수 있습니다. 장애 조치 중에 리더 DB 인스턴스 중 하나가 작성자 DB 인스턴스로 변경됩니다. DB 인스턴스가 동일한 DB 인스턴스 클래스와 크기를 사용하는 경우 DB 클러스터의 DB 인스턴스에 맞게 워크로드를 밸런싱할 수 있습니다.

자세한 내용은 Aurora 복제본을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 권장 값
- 엔진 이름
- 최종 업데이트 시간

## Amazon RDS DB 메모리 파라미터가 기본값과 다릅니다.

설명

DB 인스턴스의 메모리 파라미터가 기본값과 크게 다릅니다. 이러한 설정은 성능에 영향을 미치고 오류를 일으킬 수 있습니다.

DB 인스턴스에 대한 사용자 지정 메모리 파라미터를 DB 파라미터 그룹의 기본값으로 재설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt020`

알림 기준

노란색: DB 파라미터 그룹에는 메모리 파라미터가 기본값과 상당히 다릅니다.

권장 조치

메모리 파라미터를 기본값으로 재설정하세요.

추가 리소스

자세한 내용은 Amazon RDS for MySQL의 파라미터 구성 모범 사례, 1부: 성능과 관련된 파라미터를 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## Amazon RDS enable_index 전용 스캔 파라미터가 꺼져 있습니다.

설명

인덱스 전용 스캔 계획 유형이 비활성화되어 있으면 쿼리 플래너 또는 옵티마이저가 인덱스 전용 스캔 계획 유형을 사용할 수 없습니다.

enable_indexonlyscan 파라미터 값을 1로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt028`

알림 기준

노란색: DB 파라미터 그룹에는 enable_indexonlyscan 파라미터가 꺼져 있습니다.

권장 조치

enable_indexonlyscan 파라미터를 1로 설정합니다.

추가 리소스

enable_indexonlyscan 매개 변수를 끄면 쿼리 플래너가 최적의 실행 계획을 선택할 수 없습니다. 쿼리 플래너는 인덱스 스캔과 같은 다른 계획 유형을 사용하므로 쿼리 비용과 실행 시간이 늘어날 수 있습니다. 인덱스 전용 스캔 계획 유형은 테이블 데이터에 액세스하지 않고 데이터를 검색합니다.

자세한 내용은 PostgreSQL 설명서 웹 사이트의 enable_indexonlyscan (boolean) 을 참조하십시오.

보고서 열

- 상태 표시기
- 지역

- Resource
- 파라미터 이름
- 권장 값입니다.
- 최종 업데이트 시간

## Amazon RDS enable_indexscan 파라미터가 꺼져 있습니다

설명

인덱스 스캔 계획 유형이 비활성화되어 있으면 쿼리 플래너 또는 옵티마이저가 인덱스 스캔 계획 유형을 사용할 수 없습니다.

enable_indexscan 파라미터 값을 1로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

```
c1qf5bt029
```

알림 기준

노란색: DB 파라미터 그룹에는 enable_indexscan 파라미터가 꺼져 있습니다.

권장 조치

파라미터 enable_indexscan을 1로 설정합니다.

추가 리소스

enable_indexscan 매개 변수를 끄면 쿼리 플래너가 최적의 실행 계획을 선택할 수 없습니다. 쿼리 플래너는 인덱스 스캔과 같은 다른 계획 유형을 사용하므로 쿼리 비용과 실행 시간이 늘어날 수 있습니다.

자세한 내용은 PostgreSQL 설명서 웹 사이트의 enable_indexscan (boolean) 을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값입니다.
- 최종 업데이트 시간

## Amazon RDS general_logging 파라미터가 켜져 있습니다.

설명

DB 인스턴스에 대해 일반 로깅이 설정됩니다. 이 설정은 데이터베이스 문제를 해결하는 데 유용합니다. 그러나 일반 로깅을 활성화하면 I/O 작업량과 할당된 스토리지 공간이 늘어나 경합이 발생하고 성능이 저하될 수 있습니다.

일반 로깅 사용에 대한 요구 사항을 확인하세요. general_logging 파라미터 값을 0으로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt037`

알림 기준

노란색: DB 파라미터 그룹에는 general_loging이 켜져 있습니다.

권장 조치

일반 로깅 사용에 대한 요구 사항을 확인하세요. 필수가 아닌 경우 general_logging 파라미터 값을 0으로 설정하는 것이 좋습니다.

추가 리소스

general_logging 매개변수 값이 1이면 일반 쿼리 로그가 켜집니다. 일반 쿼리 로그에는 데이터베이스 서버 작업 기록이 포함됩니다. 서버는 클라이언트가 연결되거나 연결이 끊길 때 이 로그에 정보를 기록하며, 로그에는 클라이언트로부터 받은 각 SQL 문이 포함됩니다. 일반 쿼리 로그는 클라이언트에 오류가 있다고 의심되어 클라이언트가 데이터베이스 서버로 보낼 정보를 찾으려는 경우에 유용합니다.

자세한 내용은 MySQL용 RDS 데이터베이스 로그 개요를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

# 최적 값보다 작은 값을 사용하는 Amazon RDS InnoDB_change_버퍼링 파라미터

## 설명

변경 버퍼링을 사용하면 MySQL DB 인스턴스가 보조 인덱스를 유지하는 데 필요한 몇 가지 쓰기를 연기할 수 있습니다. 이 기능은 디스크 속도가 느린 환경에서 유용했습니다. 변경 버퍼링 구성으로 인해 DB 성능이 약간 향상되었지만, 충돌 복구가 지연되고 업그레이드 중 종료 시간이 길어졌습니다.

innodb_change_buffering 파라미터의 값을 없음으로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

## 검사 ID

`c1qf5bt021`

## 알림 기준

노란색: DB 파라미터 그룹에는 innodb_change_buffering 파라미터가 낮은 최적값으로 설정되어 있습니다.

## 권장 조치

DB 파라미터 그룹에서 innodb_change_buffering 파라미터 값을 없음으로 설정하십시오.

추가 리소스

자세한 내용은 Amazon RDS for MySQL의 파라미터 구성 모범 사례, 1부: 성능과 관련된 파라미터를 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## Amazon RDS innodb_open_files 파라미터가 낮음

설명

innodb_open_files 매개변수는 InnoDB가 한 번에 열 수 있는 파일 수를 제어합니다. InnoDB는 mysqld가 실행될 때 모든 로그 및 시스템 테이블스페이스 파일을 엽니다.

InnoDB가 한 번에 열 수 있는 최대 파일 수에 대한 DB 인스턴스 값이 낮습니다. innodb_open_files 파라미터를 최소값인 65로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.

DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt033`

알림 기준

노란색: DB 파라미터 그룹의 InnoDB 열린 파일 설정이 잘못 구성되어 있습니다.

권장 조치

innodb_open_files 파라미터를 최소값인 65로 설정합니다.

추가 리소스

innodb_open_files 매개변수는 InnoDB가 한 번에 열 수 있는 파일 수를 제어합니다. InnoDB는 mysqld가 실행될 때 모든 로그 파일과 시스템 테이블스페이스 파일을 열린 상태로 유지합니다. file-per-table 스토리지 모델을 사용하는 경우 InnoDB는 몇 개의.ibd 파일도 열어야 합니다. innodb_open_files 설정이 낮으면 데이터베이스 성능에 영향을 미치고 서버가 시작되지 않을 수 있습니다.

자세한 내용은 설명서 웹 사이트의 InnoDB 시작 옵션 및 시스템 변수 - innodb_open_files를 참조하십시오. MySql

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## Amazon RDS innodb_stats_persistent 파라미터가 비활성화되었습니다

### 설명

DB 인스턴스가 InnoDB 통계를 디스크에 유지하도록 구성되지 않았습니다. 통계가 저장되지 않으면 인스턴스가 다시 시작되고 표에 액세스할 때마다 통계가 다시 계산됩니다. 이로 인해 쿼리 실행 계획이 달라질 수 있습니다. 테이블 수준에서 이 글로벌 파라미터의 값을 수정할 수 있습니다.

innodb_stats_persistent 파라미터 값을 ON으로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

### 검사 ID

`c1qf5bt032`

### 알림 기준

노란색: DB 파라미터 그룹에는 디스크에 저장되지 않는 옵티마이저 통계가 있습니다.

### 권장 조치

innodb_stats_persistent 파라미터 값을 ON으로 설정합니다.

### 추가 리소스

innodb_stats_persistent 파라미터가 ON으로 설정된 경우 인스턴스가 재시작될 때 옵티마이저 통계가 유지됩니다. 이렇게 하면 실행 계획의 안정성과 일관된 쿼리 성능이 향상됩니다. 테이블을 만들

거나 변경할 때 STATS_PERSISTANT 절을 사용하여 테이블 수준에서 글로벌 통계 지속성을 수정할 수 있습니다.

자세한 내용은 Amazon RDS for MySQL의 파라미터 구성 모범 사례, 1부: 성능과 관련된 파라미터를 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## 시스템 용량에 비해 Amazon RDS 인스턴스가 충분히 프로비저닝되지 않음

설명

Amazon RDS 인스턴스 또는 Amazon Aurora DB 인스턴스가 작동하는 데 필요한 시스템 용량이 있는지 확인합니다.

검사 ID

`c1qf5bt039`

알림 기준

노란색:

메모리 부족 종료: OS 수준의 메모리 감소로 인해 데이터베이스 호스트의 프로세스가 중지되면 OOM (Out Of Memory) 킬 카운터가 증가합니다.

과도한 스와핑: os.memory.swap.in과 os.memory.swap.out 메트릭 값이 높았습니다.

권장 조치

메모리를 적게 사용하거나 할당된 메모리가 더 많은 DB 인스턴스 유형을 사용하도록 쿼리를 조정하는 것이 좋습니다. 인스턴스의 메모리가 부족하면 데이터베이스 성능이 영향을 받습니다.

추가 리소스

O ut-of-memory 킬이 감지됨: 호스트에서 실행되는 프로세스에 운영 체제에서 물리적으로 사용할 수 있는 메모리보다 많은 메모리가 필요한 경우 Linux 커널은 OOM (Out of Memory) 킬러를 호출합

니다. 이 경우 OOM Killer는 실행 중인 모든 프로세스를 검토하고 시스템 메모리를 비우고 시스템을 계속 실행하기 위해 하나 이상의 프로세스를 중지합니다.

스와핑이 감지됨: 데이터베이스 호스트의 메모리가 충분하지 않으면 운영 체제가 최소 사용 페이지 몇 개를 스왑 공간의 디스크로 보냅니다. 이 오프로드 프로세스는 데이터베이스 성능에 영향을 줍니다.

자세한 내용은 Amazon RDS 인스턴스 유형 및 Amazon RDS 인스턴스 확장을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- O 킬 (카운트) ut-of-memory
- 과도한 스와핑 (개수)
- 마지막 탐지 기간
- 최종 업데이트 시간

## Amazon RDS 마그네틱 볼륨 사용 중

설명

DB 인스턴스에서 마그네틱 스토리지를 사용 중입니다. 대부분 DB 인스턴스에 대해 마그네틱 스토리지는 권장되지 않습니다. 범용(SSD) 또는 프로비저닝된 IOPS 등 다른 스토리지 유형을 선택하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.

DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt000`

알림 기준

노란색: Amazon RDS 리소스는 마그네틱 스토리지를 사용하고 있습니다.

권장 조치

범용(SSD) 또는 프로비저닝된 IOPS 등 다른 스토리지 유형을 선택하세요.

추가 리소스

마그네틱 스토리지는 이전 세대의 스토리지 유형입니다. 새로운 스토리지 요구 사항에는 범용(SSD) 또는 프로비저닝된 IOPS가 권장되는 스토리지 유형입니다. 이러한 스토리지 유형은 더 우수하고 일관된 성능과 향상된 스토리지 크기 옵션을 제공합니다.

자세한 내용은 이전 세대 볼륨을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 권장 값
- 엔진 이름
- 최종 업데이트 시간

## 대용량 페이지를 사용하지 않는 Amazon RDS 파라미터 그룹

설명

대용량 페이지는 데이터베이스 확장성을 높일 수 있는데, DB 인스턴스가 대용량 페이지를 사용하지 않습니다. DB 인스턴스의 DB 파라미터 그룹에서 use_large_pages 파라미터 값을 ONLY로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt024`

알림 기준

노란색: DB 파라미터 그룹은 큰 페이지를 사용하지 않습니다.

권장 조치

use_large_pages 파라미터 값을 DB 파라미터 그룹에서만 사용하도록 설정합니다.

추가 리소스

자세한 내용은 Oracle용 RDS 인스턴스 HugePages 켜기를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## Amazon RDS 쿼리 캐시 파라미터가 켜져 있습니다.

### 설명

변경으로 인해 쿼리 캐시를 제거해야 하는 경우 DB 인스턴스가 정지된 것처럼 보입니다. 쿼리 캐시는 대부분의 워크로드에 이점이 되지 못합니다. 쿼리 캐시는 MySQL 버전 8.0에서 제거되었습니다. query_cache_type 파라미터를 0으로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

### 검사 ID

`c1qf5bt022`

### 알림 기준

노란색: DB 파라미터 그룹에는 쿼리 캐시가 켜져 있습니다.

### 권장 조치

DB 파라미터 그룹에서 query_cache_type 파라미터 값을 0으로 설정합니다.

### 추가 리소스

자세한 내용은 Amazon RDS for MySQL의 파라미터 구성 모범 사례, 1부: 성능과 관련된 파라미터를 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## Amazon RDS 리소스 인스턴스 클래스 업데이트가 필요합니다.

설명

데이터베이스가 이전 세대 DB 인스턴스 클래스를 실행하고 있습니다. 이전 세대의 DB 인스턴스 클래스를 비용, 성능 또는 둘 다 더 나은 DB 인스턴스 클래스로 교체했습니다. 최신 세대의 DB 인스턴스 클래스로 DB 인스턴스를 실행하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

```
c1qf5bt015
```

알림 기준

빨간색: DB 인스턴스는 지원이 종료된 DB 인스턴스 클래스를 사용하고 있습니다.

권장 조치

최신 DB 인스턴스 클래스로 업그레이드.

추가 리소스

자세한 내용은 DB 인스턴스 클래스에 대해 지원되는 DB 엔진 섹션을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- DB 인스턴스 클래스
- 권장 값
- 엔진 이름
- 최종 업데이트 시간

## Amazon RDS 리소스 메이저 버전 업데이트가 필요합니다.

설명

현재 DB 엔진용 메이저 버전이 설치된 데이터베이스는 지원되지 않습니다. 새 기능과 개선 사항이 포함된 최신 메이저 버전으로 업그레이드하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.

DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt014`

알림 기준

빨간색: RDS 리소스는 지원이 종료된 메이저 버전을 사용하고 있습니다.

권장 조치

DB 엔진의 최신 메이저 버전으로 업그레이드하세요.

추가 리소스

Amazon RDS는 데이터베이스를 최신 버전으로 유지하기 위해 지원되는 데이터베이스 엔진에 대한 새 버전을 출시합니다. 새로 출시된 버전에는 버그 수정, 보안 개선 사항 및 데이터베이스 엔진의 기타 개선 사항이 포함될 수 있습니다. 블루/그린 배포를 사용하여 DB 인스턴스 업그레이드에 필요한 다운타임을 최소화할 수 있습니다.

자세한 정보는 다음 자료를 참조하십시오.

- DB 인스턴스 엔진 버전 업그레이드
- 아마존 Aurora 업데이트
- 데이터베이스 업데이트에 Amazon RDS 블루/그린 배포 사용

보고서 열

- 상태 표시기
- 지역
- Resource
- 엔진 이름
- 엔진 현재 버전
- 권장 값
- 최종 업데이트 시간

## 라이선스 포함 시 지원 종료 엔진 에디션을 사용하는 Amazon RDS 리소스

설명

현재 라이선스를 계속 지원받으려면 메이저 버전을 Amazon RDS에서 지원하는 최신 엔진 버전으로 업그레이드하는 것이 좋습니다. 데이터베이스의 엔진 버전이 현재 라이선스에서 지원되지 않습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt016`

알림 기준

빨간색: Amazon RDS 리소스가 라이선스 포함 모델의 지원 종료 엔진 에디션을 사용하고 있습니다.

권장 조치

라이선스 모델을 계속 사용하려면 데이터베이스를 Amazon RDS에서 지원되는 최신 버전으로 업그레이드하는 것이 좋습니다.

추가 리소스

자세한 내용은 Oracle 메이저 버전 업그레이드를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 엔진 이름
- 엔진 버전: 현재
- 권장 값
- 엔진 이름
- 최종 업데이트 시간

## Amazon Route 53 별칭 리소스 레코드 세트

설명

성능을 향상시키고 비용을 절약하기 위해 별칭 리소스 레코드 세트로 변경할 수 있는 리소스 레코드 세트를 확인합니다.

별칭 리소스 레코드 세트는 DNS 쿼리를 AWS 리소스 (예: Elastic Load Balancing 로드 밸런서 또는 Amazon S3 버킷) 또는 다른 Route 53 리소스 레코드 세트로 라우팅합니다. 별칭 리소스 레코드 세트를 사용하면 Route 53은 무료로 DNS 쿼리를 AWS 리소스로 라우팅합니다.

AWS 서비스에서 생성한 호스팅 영역은 확인 결과에 표시되지 않습니다.

검사 ID

`B913Ef6fb4`

알림 기준

- 노란색: 리소스 레코드 세트가 Amazon S3 웹 사이트에 대한 CNAME입니다.
- 노란색: 리소스 레코드 세트는 Amazon CloudFront 배포에 대한 CNAME입니다.
- 노란색: 리소스 레코드 세트가 Elastic Load Balancing 로드 밸런서에 대한 CNAME입니다.

권장 조치

나열된 CNAME 리소스 레코드 세트를 별칭 리소스 레코드 세트로 바꿉니다. 별칭 및 비별칭 리소스 레코드 세트 간의 선택을 참조하세요.

또한 리소스에 따라 레코드 유형을 CNAME에서 A 또는 AAAA로 변경해야 합니다. AWS Amazon Route 53 레코드를 생성 또는 편집할 때 지정하는 값을 참조하세요.

추가 리소스

쿼리를 리소스로 라우팅 AWS

보고서 열

- 상태 표시기
- 호스팅 영역 이름
- 호스팅 영역 ID
- 리소스 레코드 세트 이름
- 리소스 레코드 세트 유형
- 리소스 레코드 세트 식별자
- 별칭 대상

## 메모리 크기에 대해 과소 프로비저닝된AWS Lambda 함수

설명

룩백 기간 동안 한 번 이상 호출된 AWS Lambda 함수를 확인합니다. 이 검사는 Lambda 함수가 메모리 크기에 대해 과소 프로비저닝되었는지 알려줍니다. 메모리 크기에 대해 과소 프로비저닝된 Lambda 함수가 있는 경우 이러한 함수를 완료하는 데 더 오랜 시간이 걸립니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`COr6dfpM06`

알림 기준

노란색: 조회 기간 동안 메모리 크기가 과소 프로비저닝된 Lambda 함수가 있습니다. Lambda 함수가 제대로 프로비저닝되지 않았는지 확인하기 위해 해당 함수의 모든 기본 메트릭을 고려합니다. CloudWatch 메모리 크기에 대해 프로비저닝이 부족한 Lambda 함수를 식별하는 데 사용되는 알고리즘은 모범 사례를 따릅니다. AWS 새 패턴이 식별되면 알고리즘이 업데이트됩니다.

권장 조치

Lambda 함수의 메모리 크기를 늘리는 것이 좋습니다.

자세한 정보는 Trusted Advisor 수표 AWS Compute Optimizer 신청을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- 함수 이름
- Function Version
- 메모리 크기(MB)
- 권장 메모리 크기(MB)
- 조회 기간(일)
- 성능 리스크
- 최종 업데이트 시간

## AWS Lambda 동시성 제한이 없는 함수 (구성)

설명

AWS Lambda 함수가 함수 수준의 동시 실행 한도로 구성되어 있는지 확인합니다.

동시성은 AWS Lambda 함수가 동시에 처리하는 전송 중인 요청의 수입니다. 각 동시 요청마다 Lambda는 실행 환경의 개별 인스턴스를 프로비저닝합니다.

규칙의 동시성 및 상한 매개변수를 사용하여 최소 및 최대 동시성 LimitLow 한도를 지정할 수 있습니다. ConcurrencyLimit AWS Config

자세한 내용은 Lambda 함수 크기 조정을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c18d2gz181

소스

AWS Config 관리형 규칙: lambda-concurrency-check

알림 기준

노란색: Lambda 함수에는 동시성 제한이 구성되어 있지 않습니다.

권장 조치

Lambda 함수에 동시성이 구성되어 있는지 확인하세요. Lambda 함수의 동시성 한도는 함수가 요청을 안정적이고 예측 가능하게 처리하도록 하는 데 도움이 됩니다. 동시성 한도는 갑작스러운 트래픽 급증으로 인해 함수가 과부하될 위험을 줄여줍니다.

자세한 내용은 예약된 동시성 구성을 참조하세요.

추가 리소스

- Lambda 함수 크기 조정
- 예약된 동시성 구성

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## 성능에 대한 AWS Well-Architected 위험도 높음 문제

설명

성능 기반에서 워크로드의 위험도 높음 문제(HRI)를 확인합니다. 이 검사는 사용자 AWS-Well Architected 리뷰를 기반으로 합니다. AWS Well-Architected에서 워크로드 평가를 완료했는지 여부에 따라 검사 결과가 달라집니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`Wxdfp4B1L2`

알림 기준

- 빨간색: AWS Well-Architected의 성능 기둥에서 하나 이상의 활성 고위험 문제가 확인되었습니다.
- 녹색: AWS Well-Architected의 성능 측면에서 활성 고위험 문제는 발견되지 않았습니다.

권장 조치

AWS Well-Architected는 워크로드 평가 중에 고위험 문제를 감지했습니다. 이러한 문제는 위험을 줄이고 비용을 절감할 수 있는 기회를 나타냅니다. AWS Well-Architected 도구에 로그인하여 답변을 검토하고 활성 문제를 해결하기 위한 조치를 취하세요.

보고서 열

- 상태 표시기
- 지역
- 워크로드 ARN
- 워크로드 이름
- 검토자 이름
- 워크로드 유형
- 워크로드 시작 날짜
- 워크로드 마지막 수정 날짜
- 성과에 대해 식별된 HRI 수
- 성과에 대해 해결된 HRI 수
- 성과 관련 질문에 대한 답변 수
- 성과 원칙의 총 질문 수
- 최종 업데이트 시간

# CloudFront 대체 도메인 이름

## 설명

Amazon CloudFront 배포에서 DNS 설정이 잘못 구성된 대체 도메인 이름 (CNAME) 이 있는지 확인합니다.

CloudFront 배포에 대체 도메인 이름이 포함된 경우 도메인의 DNS 구성에서 DNS 쿼리를 해당 배포로 라우팅해야 합니다.

> **Note**
>
> 이 검사에서는 Amazon Route 53 DNS와 Amazon CloudFront 배포가 동일하게 AWS 계정 구성되어 있다고 가정합니다. 따라서 경고 목록에는 이 AWS 계정의 외부 DNS 설정이 없었더라면 예상대로 작동했을 리소스가 포함될 수 있습니다..

## 검사 ID

`N420c450f2`

## 알림 기준

- 노란색: CloudFront 배포에 대체 도메인 이름이 포함되지만 CNAME 레코드 또는 Amazon Route 53 별칭 리소스 레코드로 DNS 구성이 올바르게 설정되지 않았습니다.
- 노란색: CloudFront 배포에는 대체 도메인 이름이 포함되지만 리디렉션이 너무 많아서 DNS 구성을 평가할 Trusted Advisor 수 없습니다.
- 노란색: CloudFront 배포에는 대체 도메인 이름이 포함되지만 다른 이유로 DNS 구성을 평가할 Trusted Advisor 수 없었습니다. 대부분 시간 초과로 인한 것일 수 있습니다.

## 권장 조치

DNS 구성을 업데이트하여 DNS 쿼리를 CloudFront 배포로 라우팅합니다. 대체 도메인 이름 (CNAME) 사용을 참조하십시오.

Amazon Route 53을 DNS 서비스로 사용하는 경우 도메인 이름을 사용하여 Amazon CloudFront 웹 배포로 트래픽 라우팅을 참조하십시오. 검사 시간이 초과된 경우 검사를 새로 고쳐 봅니다.

## 추가 리소스

Amazon CloudFront 개발자 가이드

보고서 열

- 상태 표시기
- 배포 ID
- 배포 도메인 이름
- 대체 도메인 이름
- 이유

## CloudFront 콘텐츠 전송 최적화

설명

글로벌 콘텐츠 전송 서비스인 Amazon을 사용하여 Amazon Simple Storage Service (Amazon S3) 버킷에서 데이터를 AWS 더 빠르게 전송할 수 있는 경우를 확인합니다. CloudFront

콘텐츠를 CloudFront 전송하도록 구성하면 콘텐츠에 대한 요청이 콘텐츠가 캐시되는 가장 가까운 엣지 로케이션으로 자동 라우팅됩니다. 이 라우팅을 사용하면 최고의 성능으로 사용자에게 콘텐츠를 전달할 수 있습니다. 버킷에 저장된 데이터에 비해 전송된 데이터의 비율이 높으면 Amazon을 사용하여 데이터를 전송하는 CloudFront 것이 유용할 수 있습니다.

검사 ID

`796d6f3D83`

알림 기준

- 노란색: 검사 전 30일 동안 GET 요청에 의해 버킷에서 사용자에게 전송된 데이터의 양이 버킷에 저장된 평균 데이터 양보다 25배 이상 큽니다.
- 빨간색: 검사 전 30일 동안 GET 요청에 의해 버킷에서 사용자에게 전송된 데이터의 양이 10TB 이상이고 버킷에 저장된 평균 데이터 양보다 25배 이상 큽니다.

권장 조치

성능 향상을 CloudFront 위해 사용을 고려해 보십시오. Amazon CloudFront 제품 세부 정보를 참조하십시오.

전송된 데이터가 매월 10TB 이상인 경우 Amazon CloudFront Pricing을 참조하여 가능한 비용 절감 가능성에 대해 알아보십시오.

추가 리소스

- Amazon CloudFront 개발자 가이드
- AWS 사례 연구: PBS

보고서 열

- 상태 표시기
- 지역
- 버킷 이름
- S3 스토리지(GB)
- 데이터 전송(GB)
- 스토리지에 대한 전송 비율

## CloudFront 헤더 포워딩 및 캐시 적중률

설명

CloudFront 현재 클라이언트로부터 수신하여 오리진 서버로 전달하는 HTTP 요청 헤더를 확인합니다.

날짜 또는 사용자 에이전트와 같은 일부 헤더는 캐시 적중률 (에지 캐시에서 제공되는 요청의 비율)을 CloudFront 크게 줄입니다. 그러면 오리진에 더 많은 요청을 CloudFront 전달해야 하므로 오리진의 부하가 증가하고 성능이 저하됩니다.

검사 ID

`N415c450f2`

알림 기준

노란색: 오리진에 CloudFront 전달되는 하나 이상의 요청 헤더는 캐시 적중률을 크게 낮출 수 있습니다.

권장 조치

요청 헤더가 캐시 적중률에 미치는 부정적인 영향을 상쇄할 만큼 충분한 이점을 제공하는지 여부를 고려합니다. 오리진이 주어진 헤더의 값에 관계없이 동일한 객체를 반환하는 경우 해당 헤더를 오리진에 CloudFront 전달하도록 구성하지 않는 것이 좋습니다. 자세한 내용은 요청 헤더를 기반으로 객체를 CloudFront 캐시하도록 구성을 참조하십시오.

추가 리소스

- CloudFront에지 캐시에서 제공되는 요청의 비율 높이기
- CloudFront 캐시 통계 보고서
- HTTP 요청 헤더 및 동작 CloudFront

보고서 열

- 배포 ID
- 배포 도메인 이름
- 캐시 동작 경로 패턴
- 헤더

## 높은 사용률의 Amazon EC2 인스턴스

설명

지난 14일 동안 실행 중이었던 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 모든 시점에서 확인합니다. 일일 CPU 사용률이 4일 이상 90%를 초과하면 알림이 전송됩니다.

사용률이 일관되게 높으면 성능이 최적화되고 안정적임을 의미할 수 있습니다. 그러나 응용 프로그램에 리소스가 충분히 없음을 나타낼 수도 있습니다. 일일 CPU 사용률 데이터를 가져오려면 이 검사에 대한 보고서를 다운로드하십시오.

검사 ID

`ZRxQlPsb6c`

알림 기준

노란색: 이전 14일 중 4일 이상 인스턴스의 일일 평균 CPU 사용률이 90%를 넘었습니다.

권장 조치

인스턴스를 더 추가하는 것이 좋습니다. 수요에 따라 인스턴스 수를 조정하는 방법에 대한 자세한 내용은 Auto Scaling이란 무엇입니까?를 참조하세요.

추가 리소스

- Amazon EC2 모니터링
- 인스턴스 메타데이터 및 사용자 데이터
- 아마존 CloudWatch 사용 설명서
- Amazon EC2 Auto Scaling 사용 설명서

보고서 열

- 리전/AZ
- 인스턴스 ID
- 인스턴스 유형

- 인스턴스 이름
- 14일 평균 CPU 사용률
- 90%의 CPU 사용률을 초과하는 일수

## 보안

보안 범주에 대해 다음 검사를 사용할 수 있습니다.

> **Note**
>
> 에서 Security Hub를 AWS 계정활성화한 경우 Trusted Advisor 콘솔에서 결과를 볼 수 있습니다. 자세한 내용은 AWS Trusted Advisor에서 AWS Security Hub 컨트롤 보기을 참조하세요. AWS 기본 보안 모범 사례 보안 표준에서 모든 컨트롤을 볼 수 있습니다. 단, 범주가 복구 > 복원인 컨트롤은 예외입니다. 지원되는 컨트롤 목록은 AWS Security Hub 사용 설명서의 AWS Foundational Security Best Practices 컨트롤을 참조하세요.

검사명

- Amazon CloudWatch 로그 그룹 보존 기간
- Microsoft SQL Server를 사용하는 Amazon EC2 인스턴스 지원 종료
- Microsoft Windows Server를 사용하는 Amazon EC2 인스턴스 지원 종료
- 우분투 LTS를 사용하는 Amazon EC2 인스턴스 표준 지원 종료
- data-in-transit 암호화를 사용하지 않는 Amazon EFS 클라이언트
- Amazon EBS 퍼블릭 스냅샷
- Amazon RDS Aurora 스토리지 암호화가 해제되었습니다
- Amazon RDS 엔진 마이너 버전 업그레이드가 필요합니다.
- Amazon RDS 퍼블릭 스냅샷
- Amazon RDS 보안 그룹 액세스 위험
- Amazon RDS 스토리지 암호화가 꺼져 있습니다
- S3 버킷을 직접 가리키는 Amazon Route 53 불일치 CNAME 레코드
- Amazon Route 53 MX 리소스 레코드 세트 및 발신자 정책 프레임워크
- Amazon S3 버킷 권한
- Amazon S3 서버 액세스 로그가 활성화되었습니다

- DNS 확인이 비활성화된 Amazon VPC 피어링 연결
- AWS Backup 복구 지점 삭제를 방지하기 위한 리소스 기반 정책을 사용하지 않는 Vault입니다.
- AWS CloudTrail 로깅
- AWS Lambda 더 이상 사용되지 않는 런타임을 사용하는 함수
- 보안에 대한 AWS Well-Architected 위험도 높음 문제
- CloudFrontIAM 인증서 스토어의 사용자 지정 SSL 인증서
- CloudFront 오리진 서버의 SSL 인증서
- ELB 리스너 보안
- ELB 보안 그룹
- 노출된 액세스 키
- IAM 액세스 키 교체
- IAM 암호 정책
- 루트 계정의 MFA
- 보안 그룹 — 제한 없는 특정 포트
- 보안 그룹 — 무제한 액세스

## Amazon CloudWatch 로그 그룹 보존 기간

설명

Amazon CloudWatch 로그 그룹 보존 기간이 365일로 설정되어 있는지 또는 기타 지정된 숫자로 설정되어 있는지 확인합니다.

기본적으로 로그는 무기한으로 저장되고 만료 기간이 없습니다. 하지만 특정 기간의 업계 규정 또는 법적 요구 사항을 준수하도록 각 로그 그룹의 보존 정책을 조정할 수 있습니다.

AWS Config 규칙의 Names 및 MinRetentionTime 매개 변수를 사용하여 최소 보존 시간 및 로그 그룹 LogGroup이름을 지정할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c18d2gz186

소스

AWS Config Managed Rule: cw-loggroup-retention-period-check

알림 기준

노란색: Amazon CloudWatch 로그 그룹의 보존 기간이 원하는 최소 일수보다 짧습니다.

권장 조치

규정 준수 요구 사항을 충족하려면 Amazon CloudWatch Logs에 저장된 로그 데이터의 보존 기간을 365일 이상으로 구성하십시오.

자세한 내용은 Logs의 로그 데이터 보존 변경을 참조하십시오. CloudWatch

추가 리소스

CloudWatch 로그 보존 변경

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Microsoft SQL Server를 사용하는 Amazon EC2 인스턴스 지원 종료

설명

지난 24시간 동안 실행된 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스의 SQL Server 버전을 확인합니다. 이 검사는 해당 버전이 지원 종료일에 가깝거나 도달한 경우 알림을 제공합니다. 각 SQL Server 버전은 5년간의 일반 지원과 5년간의 추가 지원을 포함하여 10년간의 지원을 제공합니다. 지원이 종료되면 SQL Server 버전은 정기 보안 업데이트를 받지 못합니다. 지원되지 않는 SQL Server 버전으로 애플리케이션을 실행하면 보안 또는 규정 준수 위험이 발생할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`Qsdfp3A4L3`

알림 기준

- 빨간색: EC2 인스턴스에 지원이 종료된 SQL Server 버전이 있습니다.
- 노란색: EC2 인스턴스에 12개월 이내에 지원이 종료되는 SQL Server 버전이 있습니다.

권장 조치

SQL Server 워크로드를 현대화하려면 Amazon Aurora 같은 AWS 클라우드 네이티브 데이터베이스로 리팩토링하는 것이 좋습니다. 자세한 내용은 다음을 사용하여 Windows 워크로드 현대화를 참조하십시오. AWS

완전관리형 데이터베이스로 전환하려면 Amazon Relational Database Service(RDS)로 리플랫포밍하는 것이 좋습니다. 자세한 내용은 Amazon RDS for SQL Server를 참조하세요.

Amazon EC2 SQL Server를 업그레이드하려면 Automation 런북을 사용하여 업그레이드를 간소화하는 것이 좋습니다. 자세한 내용은 AWS Systems Manager 설명서를 참조하십시오.

Amazon EC2에서 SQL Server를 업그레이드할 수 없는 경우 Windows Server의 지원 종료 마이그레이션 프로그램(EMP)을 이용할 수 있습니다. 자세한 내용은 EMP 웹 사이트를 참조하세요.

추가 리소스

- 다음과 같은 SQL Server 지원 종료에 대비하세요. AWS
- AWS의 Microsoft SQL Server

보고서 열

- 상태 표시기
- 지역
- 인스턴스 ID
- SQL Server 버전
- 지원 주기

- 지원 종료
- 최종 업데이트 시간

## Microsoft Windows Server를 사용하는 Amazon EC2 인스턴스 지원 종료

설명

이 검사는 해당 버전이 지원 종료일에 가깝거나 도달한 경우 알림을 제공합니다. 각 Windows Server 버전은 10년간 지원을 제공합니다. 여기에는 5년간의 일반 지원과 5년간의 추가 지원이 포함됩니다. 지원이 종료되면 Windows Server 버전은 정기 보안 업데이트를 받지 못합니다. 지원되지 않는 Windows Server 버전으로 애플리케이션을 실행하면 애플리케이션의 보안 또는 규정 준수 위험이 발생합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`Qsdfp3A4L4`

알림 기준

- 빨간색: EC2 인스턴스에는 지원이 종료된 Windows Server 버전(Windows Server 2003, 2003 R2, 2008 및 2008 R2)이 있습니다.
- 노란색: EC2 인스턴스에는 18개월 이내에 지원이 종료되는 Windows Server 버전이 있습니다 (Windows Server 2012 및 2012 R2).

권장 조치

Windows Server 워크로드를 현대화하려면 다음을 사용하여 Windows 워크로드 현대화에서 사용할 수 있는 다양한 옵션을 고려해 보십시오. AWS

Windows Server 워크로드를 최신 버전의 Windows Server에서 실행되도록 업그레이드하려면 자동화 런북을 사용할 수 있습니다. 자세한 내용은 AWS Systems Manager 설명서를 참조하세요.

아래 일련의 단계를 따르세요.

- 윈도우 서버 버전을 업그레이드하세요.

- 업그레이드 시 하드 중지 및 시작
- EC2Config를 사용하는 경우 EC2Launch로 마이그레이션하십시오.

보고서 열

- 상태 표시기
- 지역
- 인스턴스 ID
- Windows Server 버전
- 지원 주기
- 지원 종료
- 최종 업데이트 시간

## 우분투 LTS를 사용하는 Amazon EC2 인스턴스 표준 지원 종료

설명

이 검사를 통해 버전이 표준 지원이 거의 끝나거나 지원 종료 단계에 이르렀는지 알려줍니다. 다음 LTS로 마이그레이션하거나 Ubuntu Pro로 업그레이드하여 조치를 취하는 것이 중요합니다. 지원이 종료되면 18.04 LTS 컴퓨터는 보안 업데이트를 받을 수 없습니다. 우분투 프로 구독을 통해 우분투 18.04 LTS 배포는 2028년까지 확장 보안 유지 관리 (ESM) 를 받을 수 있습니다. 패치가 적용되지 않은 상태로 남아 있는 보안 취약성은 시스템을 해커에 노출시키고 중대한 침해 가능성을 야기할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1dfprch15`

알림 기준

빨간색: Amazon EC2 인스턴스의 우분투 버전이 표준 지원 (우분투 18.04 LTS, 18.04.1 LTS, 18.04.2 LTS, 18.04.3 LTS, 18.04.4 LTS, 18.04.5 LTS, 18.04.6 LTS) 에 도달했습니다.

노란색: Amazon EC2 인스턴스가 6개월 이내에 표준 지원이 종료되는 우분투 버전을 사용하고 있습니다 (우분투 20.04 LTS, 20.04.1 LTS, 20.04.2 LTS, 20.04.3 LTS, 20.04.4 LTS, 20.04.5 LTS, 20.04.6 LTS).

녹색: 모든 Amazon EC2 인스턴스는 규정을 준수합니다.

권장 조치

Ubuntu 18.04 LTS 인스턴스를 지원되는 LTS 버전으로 업그레이드하려면 이 문서에 언급된 단계를 따르십시오. Ubuntu 18.04 LTS 인스턴스를 Ubuntu Pro로 업그레이드하려면 콘솔로 이동하여 사용 설명서에 나와 있는 단계를 따르십시오. AWS License ManagerAWS License Manager Ubuntu 인스턴스를 Ubuntu Pro로 업그레이드하는 단계별 데모를 보여주는 Ubuntu 블로그를 참조할 수도 있습니다.

추가 리소스

요금에 대한 자세한 내용은 에 문의하세요. AWS Support

보고서 열

- 상태 표시기
- 지역
- 우분투 Lts 버전
- 예상 지원 종료 날짜
- 인스턴스 ID
- 지원 주기
- 최종 업데이트 시간

## data-in-transit 암호화를 사용하지 않는 Amazon EFS 클라이언트

설명

Amazon EFS 파일 시스템이 data-in-transit 암호화를 사용하여 마운트되었는지 확인합니다. AWS 데이터가 우발적으로 노출되거나 무단으로 액세스되지 않도록 보호하기 위해 모든 데이터 흐름에 data-in-transit 암호화를 사용할 것을 고객에게 권장합니다. Amazon EFS는 클라이언트가 Amazon EFS 탑재 도우미를 사용하는 '-o tls' 탑재 설정을 사용하여 TLS v1.2를 사용하여 전송 중인 데이터를 암호화할 것을 권장합니다.

검사 ID

```
c1dfpnchv1
```

알림 기준

노란색: Amazon EFS 파일 시스템용 하나 이상의 NFS 클라이언트가 data-in-transit 암호화를 제공하는 권장 마운트 설정을 사용하지 않습니다.

녹색: Amazon EFS 파일 시스템의 모든 NFS 클라이언트는 data-in-transit 암호화를 제공하는 권장 마운트 설정을 사용하고 있습니다.

권장 조치

Amazon EFS의 data-in-transit 암호화 기능을 활용하려면 Amazon EFS 마운트 도우미와 권장 마운트 설정을 사용하여 파일 시스템을 다시 마운트하는 것이 좋습니다.

> **Note**
>
> 일부 Linux 배포판에는 기본적으로 TLS 기능을 지원하는 stunnel 버전이 포함되어 있지 않습니다. 지원되지 않는 Linux 배포판을 사용하는 경우 (여기에서 지원되는 배포판 참조), 다시 마운트하기 전에 권장 마운트 설정으로 업그레이드하는 것이 좋습니다.

추가 리소스

- 전송 중인 데이터 암호화

보고서 열

- 상태 표시기
- 지역
- EFS 파일 시스템 ID
- 암호화되지 않은 연결을 사용하는 AZ
- 최종 업데이트 시간

## Amazon EBS 퍼블릭 스냅샷

설명

Amazon Elastic Block Store (Amazon EBS) 볼륨 스냅샷의 권한 설정을 확인하고 공개적으로 액세스할 수 있는 스냅샷이 있으면 알려줍니다.

스냅샷을 퍼블릭으로 설정하면 모든 AWS 계정 사용자와 사용자에게 스냅샷의 모든 데이터에 대한 액세스 권한이 부여됩니다. 특정 사용자 또는 계정과만 스냅샷을 공유하려면 스냅샷을 비공개로 표

시하세요. 그런 다음 스냅샷 데이터를 공유하려는 사용자 또는 계정을 지정합니다. 참고로 '모든 공유 차단' 모드에서 퍼블릭 액세스 차단을 활성화한 경우 퍼블릭 스냅샷은 공개적으로 액세스할 수 없으며 이 확인 결과에도 표시되지 않습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다.

검사 ID

`ePs02jT06w`

알림 기준

빨간색: EBS 볼륨 스냅샷은 공개적으로 액세스할 수 있습니다.

권장 조치

스냅샷의 모든 데이터를 모든 사용자 AWS 계정 및 사용자와 공유하려는 것이 확실하지 않으면 권한을 수정하십시오. 즉, 스냅샷을 비공개로 표시한 다음 권한을 부여할 계정을 지정하십시오. 자세한 내용은 Amazon EBS 스냅샷 공유를 참조하세요. EBS 스냅샷용 퍼블릭 액세스 차단을 사용하여 데이터에 대한 퍼블릭 액세스를 허용하는 설정을 제어하십시오. 콘솔의 보기에서 이 검사를 제외할 수 없습니다. Trusted Advisor

스냅샷에 대한 권한을 직접 수정하려면 콘솔의 Runbook을 사용하십시오. AWS Systems Manager 자세한 정보는 `AWSSupport-ModifyEBSSnapshotPermission`을 참조하세요.

추가 리소스

Amazon EBS 스냅샷

보고서 열

- 상태 표시기
- 지역
- 볼륨 ID
- 스냅샷 ID
- 설명

# Amazon RDS Aurora 스토리지 암호화가 해제되었습니다

## 설명

Amazon RDS는 사용자가 관리하는 키를 사용하여 모든 데이터베이스 엔진에 대해 저장 중 암호화를 지원합니다. AWS Key Management Service Amazon RDS 암호화를 사용하는 활성 DB 인스턴스에서는 스토리지에 저장된 데이터가 자동 백업, 읽기 전용 복제본 및 스냅샷과 마찬가지로 암호화됩니다.

Aurora DB 클러스터를 생성할 때 암호화를 켜지 않은 경우 암호화된 스냅샷을 암호화된 DB 클러스터로 복원해야 합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

## 검사 ID

`c1qf5bt005`

## 알림 기준

빨간색: Amazon RDS Aurora 리소스에는 암호화가 활성화되어 있지 않습니다.

## 권장 조치

DB 클러스터에 저장된 데이터의 암호화를 활성화하세요.

추가 리소스

DB 인스턴스를 생성할 때 암호화를 활성화하거나, 해결 방법을 사용하여 활성 DB 인스턴스에서 암호화를 활성화할 수 있습니다. 복호화된 DB 클러스터를 암호화된 DB 클러스터로 수정할 수 없습니다. 하지만 해독된 스냅샷을 암호화된 DB 클러스터로 복원할 수 있습니다. 해독된 스냅샷에서 복원할 때는 키를 지정해야 합니다. AWS KMS

자세한 내용은 Amazon Aurora 리소스 암호화 섹션을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- 리소스
- 엔진 이름
- 최종 업데이트 시간

## Amazon RDS 엔진 마이너 버전 업그레이드가 필요합니다.

설명

데이터베이스 리소스가 최신 마이너 DB 엔진 버전을 실행하지 않습니다. 최신 마이너 버전에는 최신 보안 수정 및 기타 개선 사항이 포함되어 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.

DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt003`

알림 기준

빨간색: Amazon RDS 리소스가 최신 마이너 DB 엔진 버전을 실행하고 있지 않습니다.

권장 조치

최신 엔진 버전으로 업그레이드하십시오.

추가 리소스

이 버전에는 최신 보안 및 기능 수정이 포함되어 있으므로 데이터베이스를 최신 DB 엔진 마이너 버전으로 유지 관리하는 것이 좋습니다. DB 엔진 마이너 버전 업그레이드에는 동일한 메이저 버전의 DB 엔진의 이전 마이너 버전과 이전 버전과 호환되는 변경 사항만 포함됩니다.

자세한 내용은 DB 인스턴스 엔진 버전 업그레이드를 참조하세요.

보고서 열

- 상태 표시기
- 지역
- 리소스
- 엔진 이름
- 엔진 버전: 현재
- 권장 값
- 최종 업데이트 시간

## Amazon RDS 퍼블릭 스냅샷

설명

Amazon Relational Database Service(Amazon RDS) DB 스냅샷에 대한 권한 설정을 확인하고 퍼블릭 스냅샷으로 표시된 스냅샷이 있으면 알려줍니다.

스냅샷을 퍼블릭으로 설정하면 모든 AWS 계정 사용자와 사용자에게 스냅샷의 모든 데이터에 대한 액세스 권한을 부여합니다. 특정 사용자 또는 계정에만 스냅샷을 공유하려면 스냅샷을 프라이빗으로 표시합니다. 그런 다음 스냅숏 데이터를 공유할 사용자 또는 계정을 지정합니다.

> **Note**
>
> 해당 검사의 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다.

검사 ID

`rSs93HQwa1`

알림 기준

빨간색: Amazon RDS 스냅샷이 퍼블릭으로 표시되어 있습니다.

권장 조치

스냅샷의 모든 데이터를 모든 사용자 AWS 계정 및 사용자와 공유하려는 것이 확실하지 않으면 권한을 수정하십시오. 즉, 스냅샷을 비공개로 표시한 다음 권한을 부여할 계정을 지정하십시오. 자세한 내용은 DB 스냅샷 또는 DB 클러스터 스냅샷 공유를 참조하세요. Trusted Advisor 콘솔의 보기에서 이 검사를 제외할 수 없습니다.

스냅샷에 대한 권한을 직접 수정하려면 콘솔의 AWS Systems Manager Runbook을 사용하면 됩니다. 자세한 정보는 `AWSSupport-ModifyRDSSnapshotPermission`을 참조하세요.

추가 리소스

Amazon RDS DB 인스턴스 백업 및 복원

보고서 열

- 상태 표시기
- 지역
- DB 인스턴스 또는 클러스터 ID
- 스냅샷 ID

# Amazon RDS 보안 그룹 액세스 위험

설명

Amazon Relational Database Service(Amazon RDS)에 대한 보안 그룹 구성을 확인하고 보안 그룹 규칙이 데이터베이스에 지나치게 방임적인 액세스 권한을 부여하면 경고합니다. 보안 그룹 규칙의 권장 구성은 특정 Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹 또는 특정 IP 주소의 액세스만 허용하는 것입니다.

검사 ID

`nNauJisYIT`

알림 기준

- 노란색: DB 보안 그룹 규칙이 포트 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432, 5500 중 하나에 대한 글로벌 액세스 권한을 부여하는 Amazon EC2 보안 그룹을 참조합니다.
- 노란색: DB 보안 그룹 규칙이 둘 이상의 IP 주소에 대한 액세스 권한을 부여합니다(CIDR 규칙 접미사가 /0 또는 /32가 아님).
- 빨간색: DB 보안 그룹 규칙이 글로벌 액세스 권한을 부여합니다(CIDR 규칙 접미사가 /0).

권장 조치

보안 그룹 규칙을 검토하고 인증된 IP 주소 또는 IP 범위에 대한 액세스를 제한합니다. 보안 그룹을 편집하려면 AuthorizedB SecurityGroup 인그레스 API 또는 를 사용하십시오. AWS Management Console자세한 내용은 DB 보안 그룹 작업을 참조하세요.

추가 리소스

- Amazon RDS 보안 그룹
- 클래스 없는 도메인 간 라우팅
- TCP 및 UDP 포트 번호 목록

보고서 열

- 상태 표시기
- 지역
- RDS 보안 그룹 이름
- 수신 규칙
- 이유

# Amazon RDS 스토리지 암호화가 꺼져 있습니다

## 설명

Amazon RDS는 사용자가 관리하는 키를 사용하여 모든 데이터베이스 엔진에 대해 저장 중 암호화를 지원합니다. AWS Key Management Service Amazon RDS 암호화를 사용하는 활성 DB 인스턴스에서는 스토리지에 저장된 데이터가 자동 백업, 읽기 전용 복제본 및 스냅샷과 마찬가지로 암호화됩니다.

DB 인스턴스를 생성할 때 암호화가 켜져 있지 않은 경우 암호화를 켜기 전에 해독된 스냅샷의 암호화된 사본을 복원해야 합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

## 검사 ID

`c1qf5bt006`

## 알림 기준

빨간색: Amazon RDS 리소스에는 암호화가 활성화되어 있지 않습니다.

## 권장 조치

DB 인스턴스에 저장된 데이터의 암호화를 활성화하세요.

추가 리소스

DB 인스턴스를 생성할 때만 DB 인스턴스를 암호화할 수 있습니다. 기존 활성 DB 인스턴스를 암호화하려면:

원본 DB 인스턴스의 암호화된 사본 생성

1. DB 인스턴스의 DB 스냅샷을 만듭니다.
2. 1단계에서 만든 스냅샷의 암호화된 사본을 생성합니다.
3. 암호화된 스냅샷에서 DB 인스턴스를 복원합니다.

자세한 정보는 다음 자료를 참조하십시오.

- Amazon RDS 리소스 암호화
- DB 스냅샷 복사

보고서 열

- 상태 표시기
- 지역
- 리소스
- 엔진 이름
- 최종 업데이트 시간

## S3 버킷을 직접 가리키는 Amazon Route 53 불일치 CNAME 레코드

설명

Amazon S3 버킷 호스트 이름을 직접 가리키는 CNAME 레코드가 있는 Amazon Route 53 호스팅 영역을 확인하고 CNAME이 S3 버킷 이름과 일치하지 않는 경우 경고합니다.

검사 ID

`c1ng44jvbm`

알림 기준

빨간색: Amazon Route 53 호스팅 영역에 일치하지 않는 S3 버킷 호스트 이름을 가리키는 CNAME 레코드가 있습니다.

녹색: Amazon Route 53 호스팅 영역에서 일치하지 않는 CNAME 레코드를 찾을 수 없습니다.

권장 조치

CNAME 레코드를 S3 버킷 호스트 이름으로 지정할 때는 구성한 모든 CNAME 또는 별칭 레코드와 일치하는 버킷이 존재하는지 확인해야 합니다. 이렇게 하면 CNAME 레코드가 스푸핑될 위험을 피할 수 있습니다. 또한 인증되지 않은 AWS 사용자가 도메인에 결함이 있거나 악의적인 웹 콘텐츠를 호스팅하는 것을 방지할 수 있습니다.

CNAME 레코드가 S3 버킷 호스트 이름을 직접 가리키지 않도록 하려면 원본 액세스 제어 (OAC)를 사용하여 Amazon을 통해 S3 버킷 웹 자산에 액세스하는 것이 좋습니다. CloudFront

CNAME을 Amazon S3 버킷 호스트 이름과 연결하는 방법에 대한 자세한 내용은 CNAME 레코드로 Amazon S3 URL 사용자 지정을 참조하십시오.

추가 리소스

- 호스트 이름을 Amazon S3 버킷에 연결하는 방법
- 다음을 사용하여 Amazon S3 오리진에 대한 액세스를 제한합니다. CloudFront

보고서 열

- 상태 표시기
- 호스팅 영역 ID
- 호스팅 영역 ARN
- 일치하는 CNAME 레코드
- 일치하지 않는 CNAME 레코드
- 최종 업데이트 시간

## Amazon Route 53 MX 리소스 레코드 세트 및 발신자 정책 프레임워크

설명

각 MX 리소스 레코드 세트에 대해 TXT 또는 SPF 리소스 레코드 세트에 유효한 SPF 레코드가 포함되어 있는지 확인합니다. 레코드는 'v=spf1'로 시작해야합니다. SPF 레코드는 귀하의 도메인에 이메일을 보내고, 이는 이메일 주소 스푸핑을 탐지 및 중지하는 데 도움이 되며, 스팸을 줄이기 위해 승인된 서버를 지정합니다. Route 53은 SPF 레코드 대신 TXT 레코드를 사용할 것을 권장합니다. Trusted Advisor 각 MX 리소스 레코드 세트에 하나 이상의 SPF 또는 TXT 레코드가 있는 경우 이 검사를 녹색으로 보고합니다.

검사 ID

`c9D319e7sG`

알림 기준

노란색: MX 리소스 레코드 세트에 유효한 SPF 값을 포함하는 TXT 또는 SPF 리소스 레코드가 없습니다.

권장 조치

각 MX 리소스 레코드 세트에 대해 유효한 SPF 값이 포함된 TXT 레코드 세트를 생성합니다. 자세한 내용은 Sender Policy Framework: SPF 레코드 구문 및 Amazon Route 53 콘솔을 사용하여 리소스 레코드 세트 생성을 참조하세요.

추가 리소스

- Sender Policy Framework
- MX 레코드

보고서 열

- 호스팅 영역 이름
- 호스팅 영역 ID
- 리소스 레코드 세트 이름
- 상태 표시기

## Amazon S3 버킷 권한

설명

공개 액세스 권한이 있거나 인증된 모든 사용자에게 액세스를 허용하는 Amazon Simple Storage Service (Amazon S3) 의 버킷을 검사합니다. AWS

이 검사는 명시적 버킷 권한과 해당 권한을 재정의할 수 있는 버킷 정책을 검사합니다. Amazon S3 버킷의 모든 사용자에게 목록 액세스 권한을 부여하는 것은 권장하지 않습니다. 이러한 권한을 사용하면 의도하지 않은 사용자가 높은 빈도로 버킷의 객체를 나열할 수 있으며, 이로 인해 예상보다 높은 요금이 발생할 수 있습니다. 모든 사람에게 업로드 및 삭제 액세스 권한을 부여하면 버킷의 보안 취약성을 유발할 수 있습니다.

검사 ID

`Pfx0RwqBli`

알림 기준

- 노란색: 버킷 ACL이 모든 사용자 또는 인증된 모든 AWS 사용자에게 나열 액세스 권한을 허용합니다.

- 노란색: 버킷 정책이 모든 종류의 공개 액세스를 허용합니다.
- 노란색: 버킷 정책에 공개 액세스를 허용하는 문이 있습니다. 퍼블릭 정책이 있는 버킷에 대한 퍼블릭 및 교차 계정 액세스 차단(Block public and cross-account access to buckets that have public policies) 설정이 켜져 있고 퍼블릭 문이 삭제될 때까지 해당 계정의 승인된 사용자만 액세스할 수 있도록 제한되었습니다.
- 노란색: Trusted Advisor 정책을 확인할 권한이 없거나 다른 이유로 정책을 평가할 수 없습니다.
- 빨간색: 버킷 ACL이 모든 사용자 또는 인증된 모든 AWS 사용자에게 업로드 및 삭제 액세스 권한을 허용합니다.

권장 조치

버킷이 공개 액세스를 허용하는 경우, 공개 액세스가 정말로 필요한지 확인합니다. 그렇지 않은 경우, 버킷 권한을 업데이트하여 소유자 또는 특정 사용자에 대한 액세스를 제한합니다. Amazon S3 퍼블릭 액세스 차단 기능을 사용하여 데이터에 대한 퍼블릭 액세스를 허용하는 설정을 제어합니다. 버킷 및 객체 액세스 권한 설정을 참조하세요.

추가 리소스

Amazon S3 리소스에 대한 액세스 권한 관리

보고서 열

- 상태 표시기
- 리전 이름
- 리전 API 파라미터
- 버킷 이름
- ACL이 나열 허용
- ACL이 업로드/삭제 허용
- 정책이 액세스 허용

## Amazon S3 서버 액세스 로그가 활성화되었습니다

설명

Amazon 심플 스토리지 서비스 버킷의 로깅 구성을 확인합니다.

서버 액세스 로깅이 활성화되면 세부 액세스 로그가 선택한 버킷에 매시간 전송됩니다. 액세스 로그 레코드에는 요청 유형, 요청과 관련된 리소스, 요청 처리 시간과 날짜 같은 각 요청에 관한 세부

정보가 포함됩니다. 기본적으로 버킷 로깅은 활성화되지 않습니다. 보안 감사를 수행하거나 사용자 및 사용 패턴에 대해 자세히 알아보려면 로깅을 사용하도록 활성화해야 합니다.

로깅을 처음 활성화하면 구성이 자동으로 검증됩니다. 그러나 나중에 수정하면 로깅 오류가 발생할 수 있습니다. 이 검사는 명시적인 Amazon S3 버킷 권한을 검사합니다. 버킷 정책을 사용하여 버킷 권한을 제어하는 것이 가장 좋지만 ACL도 사용할 수 있습니다.

검사 ID

`c1fd6b96l4`

알림 기준

- 노란색: 버킷에 서버 액세스 로깅이 활성화되어 있지 않습니다.
- 노란색: 대상 버킷 권한에 루트 계정이 포함되어 있지 않아 Trusted Advisor 가 로깅 상태를 확인할 수 없습니다.
- 빨간색: 대상 버킷이 존재하지 않습니다.
- 빨간색: 대상 버킷과 소스 버킷의 소유자가 다릅니다.
- 빨간색: 로그 전달자에 대상 버킷에 대한 쓰기 권한이 없습니다.
- 녹색: 버킷에 서버 액세스 로깅이 활성화되어 있고, 대상이 존재하며, 대상에 쓸 수 있는 권한이 있습니다.

권장 조치

대부분의 버킷에 대해 버킷 로깅을 활성화합니다. 콘솔을 이용하여 로깅 활성화와 프로그래밍 방식으로 로깅 활성화를 참조하세요.

대상 버킷 권한에 루트 계정이 포함되지 않은 경우 Trusted Advisor 가 로깅 상태를 확인하게 하려면 루트 계정을 피부여자로 추가합니다. 버킷 권한 편집을 참조하세요.

대상 버킷이 없는 경우 기존 버킷을 대상으로 선택하거나, 새 버킷을 생성하여 대상으로 선택합니다. 버킷 로깅 관리를 참조하세요.

대상과 소스의 소유자가 서로 다른 경우, 대상 버킷을 소스 버킷과 소유자가 같은 버킷으로 변경합니다. 버킷 로깅 관리를 참조하세요.

로그 전달자에게 대상에 대한 쓰기 권한이 없는 경우 (쓰기 사용 안 함), Log Delivery 그룹에 업로드/삭제 권한을 부여하십시오. ACL보다 버킷 정책을 사용하는 것이 좋습니다. 로그 전송을 위한 버킷 권한 및 권한 편집을 참조하십시오.

추가 리소스

버킷 사용

서버 액세스 로깅

서버 액세스 로그 형식

로그 파일 삭제

보고서 열

- 상태 표시기
- 지역
- 리소스 ARN
- 버킷 이름
- 대상 이름
- 대상 존재 여부
- 소유자가 동일한지 여부
- 쓰기가 활성화되어 있는지 여부
- 이유
- 최종 업데이트 시간

## DNS 확인이 비활성화된 Amazon VPC 피어링 연결

설명

VPC 피어링 연결에 수락자 및 요청자 VPC 모두에 대해 DNS 확인이 켜져 있는지 확인합니다.

VPC 피어링 연결의 DNS 확인은 VPC가 쿼리를 보낼 때 퍼블릭 DNS 호스트 이름을 프라이빗 IPv4 주소로 확인하도록 합니다. 이렇게 하면 피어링된 VPC의 리소스 간 통신에 DNS 이름을 사용할 수 있습니다. VPC 피어링 연결의 DNS 확인은 애플리케이션 개발 및 관리를 단순화하고 오류 발생을 줄이며, 리소스가 항상 VPC 피어링 연결을 통해 비공개로 통신하도록 합니다.

규칙의 vPCID 파라미터를 사용하여 VPC ID를 지정할 수 있습니다. AWS Config

자세한 정보는 VPC 피어링 연결에 대해 DNS 확인 사용 설정을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c18d2gz124

소스

AWS Config Managed Rule: vpc-peering-dns-resolution-check

알림 기준

노란색: VPC 피어링 연결의 수락자 및 요청자 VPC 모두에 대해 DNS 확인이 활성화되지 않았습니다.

권장 조치

VPC 피어링 연결에 대한 DNS 확인을 활성화합니다.

추가 리소스

- VPC 피어링 연결 옵션 수정
- VPC의 DNS 속성

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## AWS Backup 복구 지점 삭제를 방지하기 위한 리소스 기반 정책을 사용하지 않는 Vault입니다.

설명

AWS Backup 저장소에 복구 지점 삭제를 방지하는 리소스 기반 정책이 첨부되어 있는지 확인합니다.

리소스 기반 정책은 복구 지점의 예기치 않은 삭제를 방지하므로 백업 데이터에 대해 최소한의 권한으로 액세스를 제어할 수 있습니다.

규칙의 주요 ArnList 매개변수에서 해당 규칙이 체크인하지 않도록 하려는 AWS Identity and Access Management ARN을 지정할 수 있습니다. AWS Config

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz152`

소스

`AWS Config Managed Rule: backup-recovery-point-manual-deletion-disabled`

알림 기준

노란색: 복구 지점 삭제를 방지하는 리소스 기반 정책이 없는 AWS Backup 저장소도 있습니다.

권장 조치

AWS Backup 저장소에 대한 리소스 기반 정책을 만들어 복구 지점의 예기치 않은 삭제를 방지하십시오.

정책에는 백업 (DeleteRecovery지점, 백업: 권한), 백업: UpdateRecovery PointLifecycle 권한과 함께 “거부” 문구가 포함되어야 합니다. PutBackupVaultAccessPolicy

자세한 내용은 백업 볼트에 대한 액세스 정책 설정을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

# AWS CloudTrail 로깅

설명

사용 현황을 확인합니다 AWS CloudTrail. CloudTrail 계정에서 이루어진 AWS API 호출에 대한 정보를 AWS 계정 기록하여 내 활동에 대한 가시성을 높입니다. 이러한 로그를 사용하여 예를 들어, 특정 사용자가 지정한 기간 동안 수행한 작업 또는 지정된 기간 동안 특정 리소스에 대해 작업을 수행한 사용자를 확인할 수 있습니다.

Amazon Simple Storage Service (Amazon S3) 버킷으로 로그 파일을 전송하기 때문에 CloudTrail CloudTrail 버킷에 대한 쓰기 권한이 있어야 합니다. 모든 리전을 추적하는 경우(새 추적을 생성할 때 기본값) Trusted Advisor 보고서에서 추적이 여러 번 나타납니다.

검사 ID

`vjafUGJ9H0`

알림 기준

- 노란색: 트레일의 로그 전송 오류를 CloudTrail 보고합니다.
- 빨간색: 리전에 대한 트레일이 생성되지 않았거나 트레일에 대한 로깅이 해제되었습니다.

권장 조치

트레일을 생성하고 콘솔에서 로깅을 시작하려면 AWS CloudTrail 콘솔로 이동합니다.

로깅을 시작하려면 추적에 대한 로깅 중단 및 시작을 참조하세요.

로그 전송 오류가 발생할 경우 버킷이 있는지, 그리고 필요한 정책이 버킷에 연결되어 있는지 확인합니다. Amazon S3 버킷 정책을 참조하세요.

추가 리소스

- AWS CloudTrail 사용 설명서
- 지원되는 리전
- 지원되는 서비스

보고서 열

- 상태 표시기
- 지역
- 트레일 이름
- 로깅 상태

- 버킷 이름
- 최종 전송 날짜

## AWS Lambda 더 이상 사용되지 않는 런타임을 사용하는 함수

설명

사용 중단에 가까워지거나 더 이상 사용되지 않는 런타임을 사용하도록 $LATEST 버전이 구성된 Lambda 함수를 확인합니다. 지원 중단된 런타임은 보안 업데이트나 기술 지원을 받을 수 없습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

게시된 Lambda 함수 버전은 변경할 수 없습니다. 즉, 호출할 수는 있지만 업데이트할 수는 없습니다. Lambda 함수의 $LATEST 버전만 업데이트할 수 있습니다. 자세한 내용은 Lambda 함수 버전을 참조하세요.

검사 ID

L4dfs2Q4C5

알림 기준

- 빨간색: 함수의 $LATEST 버전은 이미 지원이 중단된 런타임을 사용하도록 구성되었습니다.
- 노란색: 함수의 $LATEST 버전은 180일 이내에 지원이 중단될 런타임에서 실행 중입니다.

권장 조치

사용 중단된 런타임에서 실행 중인 함수가 있는 경우, 지원되는 런타임으로 마이그레이션할 준비를 해야 합니다. 자세한 내용은 런타임 지원 정책을 참조하세요.

더 이상 사용하지 않는 이전 함수 버전은 삭제하는 것이 좋습니다.

추가 리소스

Lambda 런타임

보고서 열

- 상태 표시기

- 지역
- 함수 ARN
- 런타임
- 사용 중단까지 남은 일수
- 사용 중단 날짜
- 평균 일일 호출 건수
- 최종 업데이트 시간

## 보안에 대한 AWS Well-Architected 위험도 높음 문제

설명

보안 기반에서 워크로드의 위험도 높음 문제(HRI)를 확인합니다. 이 검사는 사용자 AWS-Well Architected 리뷰를 기반으로 합니다. AWS Well-Architected에서 워크로드 평가를 완료했는지 여부에 따라 검사 결과가 달라집니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`Wxdfp4B1L3`

알림 기준

- 빨간색: AWS Well-Architected의 보안 기둥에서 하나 이상의 활성 고위험 문제가 확인되었습니다.
- 녹색: AWS Well-Architected의 보안 원칙에서 활발한 고위험 문제는 발견되지 않았습니다.

권장 조치

AWS Well-Architected는 워크로드 평가 중에 고위험 문제를 감지했습니다. 이러한 문제는 위험을 줄이고 비용을 절감할 수 있는 기회를 나타냅니다. AWS Well-Architected 도구에 로그인하여 답변을 검토하고 활성 문제를 해결하기 위한 조치를 취하세요.

보고서 열

- 상태 표시기
- 지역
- 워크로드 ARN
- 워크로드 이름
- 검토자 이름
- 워크로드 유형
- 워크로드 시작 날짜
- 워크로드 마지막 수정 날짜
- 보안에 대해 식별된 HRI 수
- 보안에 대해 해결된 HRI 수
- 보안에 대한 질문 수
- 보안 원칙의 총 질문 수
- 최종 업데이트 시간

## CloudFrontIAM 인증서 스토어의 사용자 지정 SSL 인증서

설명

IAM 인증서 저장소의 CloudFront 대체 도메인 이름에 대한 SSL 인증서를 확인합니다. 이 검사는 인증서가 만료되었거나, 곧 만료되거나, 오래된 암호화를 사용하거나, 배포에 대해 올바르게 구성되지 않은 경우 알림을 표시합니다.

대체 도메인 이름의 사용자 지정 인증서가 만료되면 CloudFront 콘텐츠를 표시하는 브라우저에 웹 사이트 보안에 대한 경고 메시지가 표시될 수 있습니다. SHA-1 해싱 알고리즘을 사용하여 암호화된 인증서는 Chrome 및 Firefox와 같은 웹 브라우저에서 더는 사용되지 않습니다.

인증서에는 최종 사용자 요청의 호스트 헤더에 있는 Origin Domain Name 또는 도메인 이름과 일치하는 도메인 이름이 포함되어야 합니다. 일치하지 않는 경우 사용자에게 HTTP 상태 코드 502 (잘못된 게이트웨이) 를 CloudFront 반환합니다. 자세한 내용은 대체 도메인 이름 및 HTTPS 사용을 참조하십시오.

검사 ID

N425c450f2

알림 기준

- 빨간색: 사용자 지정 SSL 인증서가 만료되었습니다.
- 노란색: 사용자 지정 SSL 인증서가 앞으로 7일 내에 만료됩니다.
- 노란색: SHA-1 해싱 알고리즘을 사용하여 암호화된 사용자 지정 SSL 인증서가 있습니다.
- 노란색: 배포에 있는 대체 도메인 이름 중 하나 이상이 일반 이름(Common Name) 필드 또는 주체 대체 이름(Subject Alternative Names) 필드에 표시되지 않습니다.

권장 조치

만료된 인증서 또는 곧 만료될 인증서를 갱신합니다.

SHA-1 해싱 알고리즘을 사용하여 암호화된 인증서를 SHA-256 해싱 알고리즘을 사용하여 암호화된 인증서로 교체합니다.

인증서를 일반 이름(Common Name) 필드 또는 주체 대체 이름(Subject Alternative Names) 필드에 해당하는 값이 포함된 인증서로 바꿉니다.

추가 리소스

HTTPS 연결을 사용하여 객체에 액세스

보고서 열

- 상태 표시기
- 배포 ID
- 배포 도메인 이름
- 인증서 이름
- 이유

## CloudFront 오리진 서버의 SSL 인증서

설명

만료되었거나, 곧 만료되거나, 누락되었거나, 오래된 암호화를 사용하는 SSL 인증서가 있는지 원본 서버에서 확인합니다. 인증서에 이러한 문제 중 하나가 있는 경우 HTTP 상태 코드 502, Bad Gateway로 콘텐츠 요청에 CloudFront 응답합니다.

SHA-1 해싱 알고리즘을 사용하여 암호화된 인증서는 Chrome 및 Firefox와 같은 웹 브라우저에서 더는 사용되지 않습니다. CloudFront배포에 연결한 SSL 인증서의 수에 따라 이 확인을 통해 웹 호스팅 공급자의 청구서에 매월 몇 센트가 추가될 수 있습니다. 예를 들어 Amazon EC2 또는 Elastic Load Balancing을 배포의 오리진으로 사용하는 AWS 경우 말입니다. CloudFront 이 검사에서는

오리진 인증서 체인이나 인증 기관의 유효성을 검사하지 않습니다. 구성에서 확인할 수 있습니다. CloudFront

검사 ID

N430c450f2

알림 기준

- 빨간색: 오리진의 SSL 인증서가 만료되었거나 누락되었습니다.
- 노란색: 오리진의 SSL 인증서가 향후 30일 내에 만료됩니다.
- 노란색: 오리진에 SHA-1 해싱 알고리즘을 사용하여 암호화된 SSL 인증서가 있습니다.
- 노란색: 오리진에서 SSL 인증서를 찾을 수 없습니다. 시간 초과 또는 기타 HTTPS 연결 문제로 인해 연결이 실패했을 수 있습니다.

권장 조치

인증서가 만료되었거나 곧 만료되는 경우 오리진의 인증서를 갱신합니다.

인증서가 없는 경우에는 인증서를 추가합니다.

SHA-1 해싱 알고리즘을 사용하여 암호화된 인증서를 SHA-256 해싱 알고리즘을 사용하여 암호화된 인증서로 교체합니다.

추가 리소스

대체 도메인 이름과 HTTPS 사용

보고서 열

- 상태 표시기
- 배포 ID
- 배포 도메인 이름
- 오리진(Origin)
- 이유

## ELB 리스너 보안

설명

암호화된 통신을 위한 권장 보안 구성을 사용하지 않는 리스너가 있는 로드 밸런서가 있는지 확인합니다. AWS 보안 프로토콜 (HTTPS 또는 SSL), up-to-date 보안 정책, 안전한 암호 및 프로토콜을 사용할 것을 권장합니다.

프런트 엔드 연결(클라이언트에서 로드 밸런서)에 보안 프로토콜을 사용하면 클라이언트와 로드 밸런서 간에 요청이 암호화되어 더 안전한 환경을 만듭니다. Elastic Load Balancing은 보안 모범 사례를 준수하는 암호 및 프로토콜과 함께 사전 정의된 AWS 보안 정책을 제공합니다. 새 구성을 사용할 수 있게 되면 미리 정의된 정책의 새 버전이 공개됩니다.

검사 ID

`a2sEc6ILx`

알림 기준

- 노란색: 로드 밸런서에 보안 프로토콜(HTTPS 또는 SSL)을 사용하는 리스너가 없습니다.
- 노란색: 로드 밸런서 리스너가 오래된 사전 정의된 SSL 보안 정책을 사용합니다.
- 노란색: 로드 밸런서 리스너가 권장되지 않는 암호 또는 프로토콜을 사용합니다.
- 빨간색: 로드 밸런서 리스너가 안전하지 않은 암호 또는 프로토콜을 사용합니다.

권장 조치

로드 밸런서에 대한 트래픽의 보안을 보장해야 하는 경우, 프런트엔드 연결에 HTTPS 또는 SSL 프로토콜을 사용합니다.

로드 밸런서를 사전 정의된 SSL 보안 정책의 최신 버전으로 업그레이드합니다.

권장 암호 및 프로토콜만 사용합니다.

자세한 내용은 Elastic Load Balancing의 리스너 구성을 참조하세요.

추가 리소스

- 리스너 구성 빠른 참조
- 로드 밸런서의 SSL 협상 구성 업데이트
- Elastic Load Balancing을 위한 SSL 협상 구성
- SSL 보안 정책 테이블

보고서 열

- 상태 표시기
- 지역
- 로드 밸런서 이름
- 로드 밸런서 포트
- 이유

## ELB 보안 그룹

설명

누락된 보안 그룹으로 구성된 로드 밸런서 또는 로드 밸런서에 대해 구성되지 않은 포트에 액세스하도록 허용하는 보안 그룹을 확인합니다.

로드 밸런서와 연결된 보안 그룹을 삭제하되면 로드 밸런서가 예상대로 작동하지 않습니다. 보안 그룹이 로드 밸런서에 대해 구성되지 않은 포트에 액세스하도록 허용하는 경우 데이터 손실 또는 악의적인 공격의 위험이 증가합니다.

검사 ID

xSqX82fQu

알림 기준

- 노란색: 로드 밸런서와 연결된 Amazon VPC 보안 그룹의 인바운드 규칙이 로드 밸런서의 리스너 구성에 정의되지 않은 포트에 대한 액세스를 허용합니다.
- 빨간색: 로드 밸런서와 연결된 보안 그룹이 존재하지 않습니다.

권장 조치

로드 밸런서 리스너 구성에 정의된 포트 및 프로토콜과 경로 MTU 검색을 지원하는 ICMP 프로토콜만으로 액세스를 제한하도록 보안 그룹 규칙을 구성합니다. Classic Load Balancer의 리스너 및 VPC의 로드 밸런서를 위한 보안 그룹을 참조하세요.

보안 그룹이 존재하지 않는 경우에는 로드 밸런서에 새 보안 그룹을 적용합니다. 로드 밸런서 리스너 구성에 정의된 포트 및 프로토콜만으로 액세스를 제한하는 보안 그룹 규칙을 생성합니다. VPC의 로드 밸런서를 위한 보안 그룹을 참조하세요.

추가 리소스

- Elastic Load Balancing 사용 설명서
- Classic Load Balancer 구성

보고서 열

- 상태 표시기
- 지역
- 로드 밸런서 이름
- 보안 그룹 ID

- 이유

## 노출된 액세스 키

설명

넓리 사용되는 코드 리포지토리에서 공개된 액세스 키와 액세스 키가 손상될 수 있는 불규칙한 Amazon Elastic Compute Cloud(Amazon EC2) 사용을 확인합니다.

액세스 키는 액세스 키 ID와 해당 비밀 액세스 키로 구성됩니다. 유출 액세스 키는 계정 및 다른 사용자에게 보안 위험을 초래할 수 있으며, 무단 활동 또는 남용으로 인해 과도한 요금이 부과될 수 있으며 AWS 고객 계약을 위반할 수 있습니다.

액세스 키가 노출된 경우 즉시 조치를 취하여 계정을 보호하십시오. 계정에 과도한 요금이 부과되지 않도록 일부 리소스를 생성할 수 있는 권한을 AWS 일시적으로 제한하십시오. AWS 이렇게 한다고 해서 계정이 안전하게 보호되는 것은 아닙니다. 요금이 부과될 수 있는 무단 사용량을 부분적으로만 제한합니다.

> **Note**
>
> 이 검사는 유출 액세스 키 또는 손상된 EC2 인스턴스의 식별을 보장하지 않습니다. 액세스 키와 AWS 리소스의 안전과 보안에 대한 궁극적인 책임은 사용자에게 있습니다.
> 해당 검사의 결과는 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

액세스 키 기한이 표시된 경우 해당 날짜까지 무단 사용이 중지되지 AWS 계정 않으면 액세스 키가 일시 AWS 중단될 수 있습니다. 알림이 잘못되었다고 판단되면 AWS Support에 문의하세요.

에 표시된 정보는 계정의 최신 상태를 반영하지 Trusted Advisor 않을 수 있습니다. 노출된 액세스 키는 계정에서 노출된 모든 액세스 키가 해결될 때까지 해결된 것으로 표시되지 않습니다. 이 데이터 동기화에는 최대 1주일이 걸릴 수 있습니다.

검사 ID

```
12Fnkpl8Y5
```

알림 기준

- 빨간색: 보안 침해 가능성 — 인터넷에 노출되어 도용 (사용) AWS 되었을 수 있는 액세스 키 ID와 해당 비밀 액세스 키를 식별했습니다.

- 빨간색: 노출됨 — AWS 인터넷에 노출된 액세스 키 ID와 해당 보안 액세스 키를 식별했습니다.
- 빨간색: 의심됨 - 액세스 키가 손상되었을 가능성이 있지만, 인터넷에서 노출된 것으로 식별되지 않았음을 나타내는 변칙적인 Amazon EC2 사용이 있습니다.

권장 조치

영향을 받는 액세스 키를 최대한 빨리 삭제합니다. 키가 IAM 사용자와 연결되어 잇는 경우에는 IAM 사용자의 액세스 키 관리를 참조하세요.

계정이 무단 사용되지 않았는지 확인합니다. AWS Management Console에 로그인하여 각 서비스 콘솔에서 의심스러운 리소스를 확인합니다. Amazon EC2 인스턴스, 스팟 인스턴스 요청, 액세스 키 및 IAM 사용자를 실행 중인 경우 특히 주의해야 합니다. 과금 정보 및 비용 관리 콘솔에서 전체 사용량을 확인할 수도 있습니다.

추가 리소스

- AWS 액세스 키 관리 모범 사례
- AWS 보안 감사 지침

보고서 열

- 액세스 키 ID
- 사용자 이름(IAM 또는 루트)
- 부정 행위 유형
- 사례 ID
- 업데이트된 시간
- 위치
- 기한
- 사용량(일별 USD)

## IAM 액세스 키 교체

설명

지난 90일 동안 교체되지 않은 활성 IAM 액세스 키를 확인합니다.

액세스 키를 정기적으로 교체하면 리소스에 액세스하기 위해 알지 못한 채 손상된 키를 사용할 가능성이 줄어듭니다. 이 검사에서 마지막 순환 날짜 및 시간은 액세스 키가 생성되었거

나 가장 최근에 활성화된 시간입니다. 액세스 키 번호 및 날짜는 최신 IAM 자격 증명 보고서의 `access_key_1_last_rotated` 및 `access_key_2_last_rotated` 정보를 참조하십시오.

보안 인증 보고서의 재생성 빈도가 제한되므로, 이 검사를 새로 고치면 최근 변경 사항이 반영되지 않을 수 있습니다. 자세한 내용은 AWS 계정의 자격 증명 보고서 가져오기를 참조하세요.

액세스 키를 생성하고 교체하려면 사용자에게 적절한 권한이 있어야 합니다. 자세한 내용은 사용자가 자신의 암호, 액세스 키 및 SSH 키를 관리할 수 있도록 허용을 참조하세요.

검사 ID

`DqdJqYeRm5`

알림 기준

- 녹색: 액세스 키가 활성 상태이며 지난 90일 중에 교체되었습니다.
- 노란색: 액세스 키가 활성 상태이며 지난 2년 중에 교체되었지만 교체된 지 90일이 넘었습니다.
- 빨간색: 액세스 키가 활성 상태이며 지난 2년 동안 교체되지 않았습니다.

권장 조치

액세스 키를 주기적으로 교체합니다. 액세스 키 교체 및 IAM 사용자의 액세스 키 관리를 참조하세요.

추가 리소스

- IAM 모범 사례
- IAM 사용자의 액세스 키 교체 방법.

보고서 열

- 상태 표시기
- IAM 사용자
- 액세스 키
- 키를 마지막으로 교체한 날짜
- 이유

## IAM 암호 정책

설명

계정의 암호 정책을 확인하여 암호 정책이 활성화되지 않았거나 암호 콘텐츠 요구 사항이 활성화되지 않은 경우 경고합니다.

암호 콘텐츠 요구 사항은 AWS 환경에서 강력한 사용자 암호를 생성하게 하여 사용자의 전반적인 보안을 강화합니다. 암호 정책을 생성하거나 변경하면 새 사용자에게 변경 사항이 즉시 적용되지만 기존 사용자는 암호를 변경하지 않아도 됩니다.

검사 ID

Yw2K9puPzl

알림 기준

- 노란색: 암호 정책이 활성화되어 있지만 하나 이상의 콘텐츠 요구 사항이 활성화되어 있지 않습니다.
- 빨간색: 활성화된 암호 정책이 없습니다.

권장 조치

일부 콘텐츠 요구 사항이 활성화되지 않은 경우 활성화하는 것이 좋습니다. 활성화된 암호 정책이 없는 경우 새로 생성하고 구성합니다. IAM 사용자의 계정 암호 정책 설정을 참조하세요.

추가 리소스

암호 관리

보고서 열

- 암호 정책
- 대문자
- 소문자
- 숫자
- 영숫자 이외의 문자

## 루트 계정의 MFA

설명

루트 계정을 확인하여 멀티 팩터 인증(MFA)이 활성화되지 않은 경우 경고를 표시합니다.

보안을 강화하려면 MFA를 사용하여 계정을 보호하는 것이 좋습니다. MFA를 사용하면 사용자가 MFA 하드웨어 또는 가상 디바이스에서 가져온 고유한 인증 코드를 입력해야 하고 관련 웹 사이트와 상호 작용할 수 있습니다. AWS Management Console

검사 ID

7DAFEmoDos

알림 기준

빨간색: 루트 계정에 MFA가 활성화되어 있지 않았습니다.

권장 조치

루트 계정에 로그인하여 MFA 디바이스를 활성화합니다. MFA 상태 확인 및 MFA 디바이스 설정을 참조하세요.

추가 리소스

다음과 함께 멀티 팩터 인증 (MFA) 디바이스 사용 AWS

## 보안 그룹 — 제한 없는 특정 포트

설명

보안 그룹에 특정 포트에 대한 무제한 액세스(0.0.0.0/0)를 허용하는 규칙이 있는지 확인합니다.

무제한 액세스는 악의적인 활동 (해킹, denial-of-service 공격, 데이터 손실) 의 기회를 증가시킵니다. 위험이 가장 높은 포트는 빨간색으로 표시되고 위험이 적은 포트는 노란색으로 표시됩니다. 녹색으로 표시된 포트는 일반적으로 HTTP 및 SMTP와 같이 무제한 액세스가 필요한 애플리케이션에서 사용합니다.

이러한 방식으로 보안 그룹을 의도적으로 구성한 경우 추가 보안 조치를 사용하여 인프라(예: IP 테이블) 를 보호하는 것이 좋습니다.

> **Note**
>
> 이 검사는 사용자가 만든 보안 그룹과 IPv4 주소에 대한 인바운드 규칙만 확인합니다. AWS Directory Service 로 생성한 보안 그룹은 빨간색 또는 노란색으로 플래그가 지정되지만 보안 위험을 초래하지 않으며 안전한 것으로 간과하거나 제외됩니다. 자세한 내용은 Trusted Advisor FAQ를 참조하십시오.

> **Note**
>
> 이 검사에는 고객 관리형 접두사 목록이 0.0.0.0/0에 대한 액세스 권한을 부여하고 보안 그룹에서 소스로 사용되는 사용 사례는 포함되지 않습니다.

검사 ID

HCP4007jGY

알림 기준

- 녹색: 포트 80, 25, 443 또는 465에 대한 액세스가 제한되지 않았습니다.
- 빨간색: 포트 20, 21, 1433, 1434, 3306, 3389, 4333, 5432 또는 5500에 대한 액세스가 제한되지 않았습니다.
- 노란색: 다른 포트에 대한 액세스가 제한되지 않았습니다.

권장 조치

액세스가 필요한 IP 주소만으로 액세스를 제한합니다. 특정 IP 주소에 대한 액세스를 제한하려면 접미사를 /32로 설정합니다(예: 192.0.2.10/32). 보다 제한적인 규칙을 생성한 후에는 지나치게 많은 권한을 부여하는 규칙을 삭제해야 합니다.

추가 리소스

- Amazon EC2 보안 그룹

  TCP 및 UDP 포트 번호 목록
- 클래스 없는 도메인 간 라우팅

보고서 열

- 상태 표시기
- 지역
- 보안 그룹 이름
- 보안 그룹 ID
- 프로토콜
- 시작 포트
- 끝 포트

## 보안 그룹 — 무제한 액세스

설명

리소스에 대한 무제한 액세스를 허용하는 규칙이 있는지 보안 그룹을 검사합니다.

무제한 액세스는 악의적인 활동 (해킹, 공격, denial-of-service 데이터 손실) 의 기회를 증가시킵니다.

> **Note**
>
> 이 검사는 사용자가 만든 보안 그룹과 IPv4 주소에 대한 인바운드 규칙만 확인합니다. AWS Directory Service 로 생성한 보안 그룹은 빨간색 또는 노란색으로 플래그가 지정되지만 보안 위험을 초래하지 않으며 안전한 것으로 간과하거나 제외됩니다. 자세한 내용은 Trusted Advisor FAQ를 참조하십시오.

> **Note**
>
> 이 검사에는 고객 관리형 접두사 목록이 0.0.0.0/0에 대한 액세스 권한을 부여하고 보안 그룹에서 소스로 사용되는 사용 사례는 포함되지 않습니다.

검사 ID

`1iG5NDGVre`

알림 기준

빨간색: 보안 그룹 규칙에 25, 80 또는 443 이외의 포트에 대해 접미사가 /0인 소스 IP 주소가 있습니다.

권장 조치

액세스가 필요한 IP 주소만으로 액세스를 제한합니다. 특정 IP 주소에 대한 액세스를 제한하려면 접미사를 /32로 설정합니다(예: 192.0.2.10/32). 보다 제한적인 규칙을 생성한 후에는 지나치게 많은 권한을 부여하는 규칙을 삭제해야 합니다.

추가 리소스

- Amazon EC2 보안 그룹
- 클래스 없는 도메인 간 라우팅

보고서 열

- 상태 표시기
- 지역
- 보안 그룹 이름
- 보안 그룹 ID
- 프로토콜

- 시작 포트
- 끝 포트
- IP 범위

## 내결함성

내결함성 범주에 대해 다음 검사를 사용할 수 있습니다.

검사명

- ALB 멀티-AZ
- Amazon Aurora MySQL 클러스터 백트래킹이 활성화되지 않음
- Amazon Aurora DB 인스턴스 액세스
- 아마존 CloudFront 오리진 페일오버
- Amazon Comprehend 엔드포인트 액세스 위험
- 아마존 DocumentDB 단일 AZ 클러스터
- 아마존 다이나모DB P 복구 oint-in-time
- Amazon DynamoDB 테이블이 백업 계획에 포함되지 않음
- Amazon EBS는 플랜에 AWS Backup 포함되지 않음
- Amazon EBS 스냅샷
- Amazon EC2 Auto Scaling에는 ELB 상태 확인이 활성화되지 않음
- Amazon EC2 Auto Scaling 그룹은 용량 재조정이 활성화됨
- Amazon EC2 Auto Scaling은 여러 AZ에 배포되지 않았거나 최소 AZ 수를 충족하지 않습니다.
- Amazon EC2 가용 영역 균형
- Amazon EC2 세부 모니터링이 활성화되지 않음
- 차단 모드의 Amazon ECS AWS로그 드라이버
- 단일 AZ를 사용하는 Amazon ECS 서비스
- Amazon ECS 다중 AZ 배치 전략
- Amazon EFS 노 마운트 타겟 이중화
- Amazon EFS가 AWS Backup 계획에 포함되지 않음
- 아마존 ElastiCache 멀티-AZ 클러스터
- Amazon ElastiCache Redis 클러스터 자동 백업

- Amazon MemoryDB 다중 AZ 클러스터
- 너무 많은 파티션을 호스팅하는 Amazon MSK 브로커
- 데이터 노드가 3개 미만인 Amazon OpenSearch 서비스 도메인
- Amazon RDS 백업
- Amazon RDS DB 클러스터에 DB 인스턴스가 하나 있습니다.
- 모든 인스턴스가 동일한 가용 영역에 있는 Amazon RDS DB 클러스터
- 모든 리더 인스턴스가 동일한 가용 영역에 있는 Amazon RDS DB 클러스터
- Amazon RDS DB 인스턴스 고급 모니터링이 활성화되지 않았음
- Amazon RDS DB 인스턴스에는 스토리지 자동 크기 조정 기능이 해제되어 있습니다.
- 다중 AZ 배포를 사용하지 않는 Amazon RDS DB 인스턴스
- 아마존 RDS DiskQueueDepth
- 아마존 RDS FreeStorageSpace
- Amazon RDS log_output 파라미터가 테이블로 설정되었습니다.
- Amazon RDS innodb_default_row_format 파라미터 설정은 안전하지 않습니다
- Amazon RDS innodb_flush_log_at_trx_commit 파라미터는 1이 아닙니다
- Amazon RDS max_user_connections 파라미터가 낮음
- Amazon RDS 다중 AZ
- 아마존 RDS는 계획에 포함되지 AWS Backup 않음
- Amazon RDS 읽기 전용 복제본은 쓰기 가능 모드로 열려 있습니다.
- Amazon RDS 리소스 자동 백업이 꺼져 있습니다.
- Amazon RDS sync_binlog 파라미터가 꺼져 있습니다
- RDS DB 클러스터에는 다중 AZ 복제가 활성화되어 있지 않습니다
- RDS 다중 AZ 대기 인스턴스가 활성화되지 않음
- 아마존 RDS ReplicaLag
- Amazon RDS 동기식_커밋 파라미터가 사용 중지되었습니다
- Amazon Redshift 클러스터 자동 스냅샷
- Amazon Route 53 삭제된 상태 확인
- Amazon Route 53 장애 조치 리소스 레코드 세트
- Amazon Route 53 높은 TTL 리소스 레코드 세트

- Amazon Route 53 네임 서버 위임
- Amazon Route 53 Resolver 엔드포인트 가용 영역 이중화
- Amazon S3 버킷 로깅
- Amazon S3 버킷 복제가 활성화되지 않음
- Amazon S3 Bucket Versioning
- 여러 가용 영역에 걸쳐 있지 않은 Application, Network Balancer 및 Gateway Load Balancer
- 서브넷에서 사용 가능한 IP Auto Scaling
- Auto Scaling 그룹 상태 확인
- Auto Scaling 그룹 리소스
- 단일 AZ에서 HSM 인스턴스를 실행하는AWS CloudHSM 클러스터
- AWS Direct Connect 위치 레질리언스
- AWS Lambda 데드레터 대기열이 구성되지 않은 기능
- AWS Lambda 장애 발생 시: 이벤트 목적지
- 다중 AZ 이중화 기능이 없는AWS Lambda VPC 지원 함수
- AWS Resilience Hub 애플리케이션 구성 요소 검사
- AWS Resilience Hub 정책 위반
- AWS Resilience Hub 레질리언스 점수
- AWS Resilience Hub 평가 연령
- AWS Site-to-Site VPN DOWN 상태의 터널이 하나 이상 있음
- 안정성에 대한 AWS Well-Architected 위험도 높음 문제
- Classic Load Balancer에는 다중 AZ가 구성되어 있지 않습니다
- ELB Connection Draining
- Load Balancer 최적화
- NAT 게이트웨이 AZ 독립성
- Network Load Balancer 교차 로드 밸런싱
- NLB - 프라이빗 서브넷의 인터넷 연결 리소스
- NLB 멀티-AZ
- AWS 리전 인시던트 관리자 복제 세트의 수
- 단일 AZ 애플리케이션 검사
- 여러 AZ의 VPC 인터페이스 엔드포인트 네트워크 인터페이스

- VPN 터널 이중성
- ActiveMQ 가용 영역 이중화
- RabbitMQ 가용 영역 이중화

## ALB 멀티-AZ

설명

애플리케이션 로드 밸런서가 두 개 이상의 가용 영역 (AZ) 을 사용하도록 구성되어 있는지 확인합니다. AZ는 다른 영역의 장애로부터 격리된 별개의 위치입니다. 동일한 지역의 여러 AZ에 로드 밸런서를 구성하면 워크로드 가용성을 개선하는 데 도움이 됩니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1dfprch08`

알림 기준

노란색: ALB는 단일 AZ에 있습니다.

녹색: ALB에는 AZ가 두 개 이상 있습니다.

권장 조치

로드 밸런서가 최소 두 개의 가용 영역으로 구성되어 있는지 확인하세요.

자세한 내용은 Application Load Balancer 가용 영역을 참조하세요.

추가 리소스

자세한 내용은 다음 설명서를 참조하세요.

- Elastic Load Balancing의 작동 방식
- 리전, 가용 영역 및 로컬 영역

보고서 열

- 상태 표시기
- 지역
- ALB 이름
- ALB 규칙
- 실험실 ARN
- 여러 AZ의 수
- 최종 업데이트 시간

## Amazon Aurora MySQL 클러스터 백트래킹이 활성화되지 않음

설명

Amazon Aurora MySQL 클러스터에 백트래킹이 활성화되어 있는지 확인합니다.

Amazon Aurora MySQL 클러스터 백트래킹은 새 클러스터를 생성하지 않고도 Aurora DB 클러스터를 이전 시점으로 복원할 수 있는 기능입니다. 스냅샷에서 복원할 필요 없이 데이터베이스를 보존 기간 내의 특정 시점으로 롤백할 수 있습니다.

규칙의 BacktrackWindowInHours파라미터에서 백트래킹 시간 창 (시간) 을 조정할 수 있습니다. AWS Config

자세한 내용은 Amazon Aurora DB 클러스터 역추적을 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz131
```

소스

```
AWS Config Managed Rule: aurora-mysql-backtracking-enabled
```

알림 기준

노란색: Amazon Aurora MySQL 클러스터 백트래킹이 활성화되지 않았습니다.

권장 조치

Amazon Aurora MySQL 클러스터의 백트래킹을 활성화하십시오.

자세한 내용은 Amazon Aurora DB 클러스터 역추적을 참조하십시오.

추가 리소스

Aurora DB 클러스터 역추적

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon Aurora DB 인스턴스 액세스

설명

Amazon Aurora DB 클러스터에 프라이빗 인스턴스와 퍼블릭 인스턴스가 모두 있는 사례를 확인합니다.

기본 인스턴스에 장애가 발생하면 복제본이 기본 인스턴스로 승격됩니다. 복제본이 프라이빗인 경우 퍼블릭 액세스 권한만 있는 사용자는 장애 조치(failover) 후에 더는 데이터베이스에 연결할 수 없습니다. 클러스터의 모든 DB 인스턴스는 동일한 액세스 가능성을 갖는 것이 좋습니다.

검사 ID

`xuy7H1avtl`

알림 기준

노란색: Aurora DB 클러스터에 있는 인스턴스의 액세스 수준(퍼블릭 및 프라이빗의 조합)이 서로 다릅니다.

권장 조치

모두 퍼블릭 또는 프라이빗으로 설정되도록 DB 클러스터에 있는 인스턴스의 `Publicly Accessible` 설정을 수정합니다. 자세한 내용은 MySQL 데이터베이스 엔진 기반 DB 인스턴스의 변경에서 MySQL 인스턴스에 대한 지침을 참조하세요.

추가 리소스

Aurora DB 클러스터의 내결함성

보고서 열

- 상태 표시기
- 지역
- 클러스터
- 퍼블릭 DB 인스턴스
- 프라이빗 DB 인스턴스
- 이유

## 아마존 CloudFront 오리진 페일오버

설명

Amazon에서 오리진 두 개를 포함하는 배포에 대해 오리진 그룹이 구성되어 있는지 확인합니다. CloudFront

자세한 내용은 오리진 장애 조치를 통한 CloudFront 고가용성 최적화를 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz112`

소스

`AWS Config Managed Rule: cloudfront-origin-failover-enabled`

알림 기준

노란색: Amazon CloudFront 오리진 장애 조치가 활성화되지 않았습니다.

권장 조치

최종 사용자에게 콘텐츠를 고가용성으로 전송할 수 있도록 CloudFront 배포에 대한 원본 장애 조치 기능을 켜야 합니다. 이 기능을 켜면 기본 오리진 서버를 사용할 수 없는 경우 트래픽이 백업 오리진 서버로 자동으로 라우팅됩니다. 이렇게 하면 잠재적인 다운타임이 최소화되고 콘텐츠의 지속적인 가용성이 보장됩니다.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon Comprehend 엔드포인트 액세스 위험

설명

고객 관리 키를 사용하여 기본 모델을 암호화한 엔드포인트의 AWS Key Management Service (AWS KMS) 키 권한을 확인합니다. 고객 관리형 키가 비활성화된 경우, 또는 Amazon Comprehend에 허용된 권한을 변경하기 위해 키 정책이 변경되면 엔드포인트 가용성에 영향이 있을 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`Cm24dfsM13`

알림 기준

빨간색: 고객 관리형 키가 비활성화된 경우, 또는 Amazon Comprehend에 허용된 액세스 권한을 변경하기 위해 키 정책이 변경된 경우입니다.

권장 조치

고객 관리형 키가 비활성화된 경우 활성화하는 것이 좋습니다. 자세한 내용은 키 활성화를 참조하세요. 키 정책이 변경되었는데 엔드포인트를 계속 사용하려는 경우 AWS KMS 키 정책을 업데이트하는 것이 좋습니다. 자세한 내용은 키 정책 변경을 참조하세요.

추가 리소스

AWS KMS 권한

보고서 열

- 상태 표시기
- 지역
- 엔드포인트 ARN
- 모델 ARN
- KMS KeyId
- 최종 업데이트 시간

## 아마존 DocumentDB 단일 AZ 클러스터

설명

단일 AZ로 구성된 Amazon DocumentDB 클러스터가 있는지 확인합니다.

단일 AZ 아키텍처에서 Amazon DocumentDB 워크로드를 실행하는 것만으로는 매우 중요한 워크로드에 충분하지 않으며 구성 요소 장애를 복구하는 데 최대 10분이 걸릴 수 있습니다. 고객은 추가 가용 영역에 복제본 인스턴스를 배포하여 유지 관리, 인스턴스 장애, 구성 요소 장애 또는 가용 영역 장애 중에도 가용성을 보장해야 합니다.

> **Note**
>
> 이 검사의 결과는 매일 한 번 이상 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c15vnddn2x

알림 기준

노란색: Amazon DocumentDB 클러스터의 인스턴스가 3개 미만의 가용 영역에 있습니다.

녹색: Amazon DocumentDB 클러스터에는 세 개의 가용 영역에 인스턴스가 있습니다.

권장 조치

애플리케이션에 고가용성이 필요한 경우 복제 인스턴스를 사용하는 다중 AZ를 활성화하도록 DB 인스턴스를 수정하십시오. Amazon DocumentDB 고가용성 및 복제를 참조하십시오.

추가 리소스

Amazon DocumentDB 클러스터 내결함성에 대한 이해

리전 및 가용 영역

보고서 열

- 상태 표시기
- 지역
- 가용 영역
- DB Cluster Identifier
- DB 클러스터 ARN
- 최종 업데이트 시간

## 아마존 다이나모DB P 복구 oint-in-time

설명

Amazon DynamoDB 테이블에 대해 특정 시점으로 복구가 활성화되어 있는지 확인합니다.

특정 시점으로 복구를 사용하면 우발적인 쓰기 또는 삭제 작업으로부터 DynamoDB 테이블을 보호할 수 있습니다. 특정 시점으로 복구를 설정해 두면 온디맨드 백업의 생성, 유지 관리, 예약을 걱정할 필요가 없습니다. 특정 시점 복구는 지난 35일 동안의 특정 시점으로 테이블을 복구합니다. DynamoDB는 테이블의 증분식 백업을 관리합니다.

자세한 내용은 DynamoDB의 P oint-in-time 복구를 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz138`

소스

`AWS Config Managed Rule: dynamodb-pitr-enabled`

알림 기준

노란색: DynamoDB 테이블에 대해 P oint-in-time 복구가 활성화되어 있지 않습니다.

권장 조치

Amazon DynamoDB에서 point-in-time 복구를 활성화하여 테이블 데이터를 지속적으로 백업하십시오.

자세한 내용은 P oint-in-time 복구: 작동 방식을 참조하십시오.

추가 리소스

DynamoDB를 위한 P oint-in-time 복구

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

# Amazon DynamoDB 테이블이 백업 계획에 포함되지 않음

## 설명

Amazon DynamoDB 테이블이 계획의 일부인지 확인합니다. AWS Backup

AWS Backup 마지막 백업 이후 변경된 사항을 캡처하는 DynamoDB 테이블에 대한 증분 백업을 제공합니다. 요금제에 DynamoDB 테이블을 포함하면 우발적인 데이터 손실 시나리오로부터 데이터를 보호하고 백업 프로세스를 자동화하는 데 도움이 됩니다. AWS Backup 이를 통해 DynamoDB 테이블을 위한 안정적이고 확장 가능한 백업 솔루션이 제공되므로 귀중한 데이터를 보호하고 필요에 따라 복구할 수 있습니다.

자세한 내용은 다음을 사용하여 DynamoDB 테이블 백업 생성을 참조하십시오. AWS Backup

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

## 검사 ID

```
c18d2gz107
```

## 소스

```
AWS Config Managed Rule: dynamodb-in-backup-plan
```

## 알림 기준

노란색: Amazon DynamoDB 테이블은 요금제에 포함되어 있지 않습니다. AWS Backup

## 권장 조치

Amazon DynamoDB 테이블이 계획의 일부인지 확인하십시오. AWS Backup

## 추가 리소스

예약한 백업

무엇입니까? AWS Backup

AWS Backup 콘솔을 사용하여 백업 계획 생성

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon EBS는 플랜에 AWS Backup 포함되지 않음

설명

의 백업 계획에 Amazon EBS 볼륨이 있는지 확인합니다. AWS Backup

해당 볼륨에 저장된 데이터의 정기 백업을 자동화하는 AWS Backup 계획에 Amazon EBS 볼륨을 포함시키십시오. 이렇게 하면 데이터 손실을 방지하고, 데이터 관리를 더 쉽게 하고, 필요할 때 데이터를 복원할 수 있습니다. 백업 계획을 세우면 데이터를 안전하게 유지하고 애플리케이션 및 서비스의 복구 시간 및 시점 목표(RTO/RPO)를 달성할 수 있습니다.

자세한 내용은 백업 계획 생성을 참조하세요

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz106
```

소스

```
AWS Config Managed Rule: ebs-in-backup-plan
```

알림 기준

노란색: Amazon EBS 볼륨은 AWS Backup 요금제에 포함되어 있지 않습니다.

권장 조치

Amazon EBS 볼륨이 AWS Backup 계획의 일부인지 확인하십시오.

추가 리소스

콘솔을 AWS Backup 사용하여 백업 계획 생성

이게 뭐야 AWS Backup?

시작하기 3: 예약 백업 생성

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon EBS 스냅샷

설명

Amazon Elastic Block Store(Amazon EBS) 볼륨에 대한 스냅샷의 기간을 확인합니다(사용 가능 또는 사용 중).

Amazon EBS 볼륨이 복제되더라도 오류가 발생할 수 있습니다. 스냅샷은 안정적인 저장 및 복구를 위해 Amazon Simple S3 (Amazon S3) 에 저장됩니다. point-in-time

검사 ID

`H7IgTzjTYb`

알림 기준

- 노란색: 가장 최근의 볼륨 스냅샷이 7일에서 30일 사이의 스냅샷입니다.
- 빨간색: 가장 최근의 볼륨 스냅샷이 30일 이상 지난 스냅샷입니다.
- 빨간색: 볼륨에 스냅샷이 없습니다.

권장 조치

주 1회 또는 월 1회 볼륨의 스냅샷을 생성합니다. 자세한 내용은 Amazon EBS 스냅샷 생성을 참조하세요.

추가 리소스

Amazon Elastic Block Store(Amazon EBS)

보고서 열

- 상태 표시기
- 지역
- 볼륨 ID
- 볼륨 이름
- 스냅샷 ID
- 스냅샷 이름
- 스냅샷 경과 시간
- 볼륨 연결
- 이유

## Amazon EC2 Auto Scaling에는 ELB 상태 확인이 활성화되지 않음

설명

Clastic Load Balancer와 연결된 Amazon EC2 Auto Scaling 그룹이 Elastic Load Balancing 상태 확인에 사용되고 있는지 확인합니다. Auto Scaling 그룹의 기본 상태 검사는 Amazon EC2 상태 확인만 해당합니다. 인스턴스가 상태 확인을 통과하지 못하면 비정상으로 표시되고 종료됩니다. Amazon EC2 Auto Scaling은 새로운 대체 인스턴스를 시작합니다. Elastic Load Balancing 상태 점검은 Amazon EC2 인스턴스를 주기적으로 모니터링하여 비정상 인스턴스를 탐지 및 종료한 다음 새 인스턴스를 시작합니다.

자세한 내용은 Elastic Load Balancing 상태 확인 추가를 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz104
```

소스

```
AWS Config Managed Rule: autoscaling-group-elb-healthcheck-required
```

알림 기준

노란색: Classic Load Balancer에 연결된 Amazon EC2 Auto Scaling 그룹이 Elastic Load Balancing 상태 확인을 활성화하지 않았습니다.

권장 조치

Classic Load Balancer에 연결된 Auto Scaling 그룹이 Elastic Load Balancing 상태 확인을 사용하는지 확인합니다.

Elastic Load Balancing 상태 점검은 로드 밸런서가 정상이고 요청을 처리할 수 있는지 여부를 보고합니다. 이렇게 하면 애플리케이션의 고가용성이 보장됩니다.

자세한 내용은 Auto Scaling 그룹에 Elastic Load Balancing 상태 확인 추가를 참조하세요

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon EC2 Auto Scaling 그룹은 용량 재조정이 활성화됨

설명

여러 인스턴스 유형을 사용하는 Amazon EC2 Auto Scaling 그룹에 대해 용량 재조정이 활성화되어 있음을 확인합니다.

용량 재조정을 통해 Amazon EC2 Auto Scaling 그룹을 구성하면 인스턴스 유형 및 구매 옵션에 관계없이 Amazon EC2 인스턴스를 가용 영역 전체에 균등하게 분산하는 데 도움이 됩니다. 그룹과 관련된 대상 추적 정책(예: CPU 사용률 또는 네트워크 트래픽)을 사용합니다.

자세한 내용은 여러 인스턴스 유형 및 구매 옵션이 포함된 Auto Scaling 그룹을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`AWS Config c18d2gz103`

소스

AWS Config 관리형 규칙: autoscaling-capacity-rebalancing

알림 기준

노란색: Amazon EC2 Auto Scaling 그룹 용량 재분배가 활성화되지 않았습니다.

권장 조치

여러 인스턴스 유형을 사용하는 Amazon EC2 Auto Scaling 그룹에 대해 용량 재조정이 활성화되어 있는지 확인합니다.

자세한 내용은 용량 재분배 활성화(콘솔)를 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

# Amazon EC2 Auto Scaling은 여러 AZ에 배포되지 않았거나 최소 AZ 수를 충족하지 않습니다.

설명

Amazon EC2 Auto Scaling 그룹이 다중 가용 영역에 배포되었는지, 아니면 지정된 최소 가용 영역 수에 따라 배포되었는지 확인합니다. 여러 가용 영역에 Amazon EC2 인스턴스를 배포하여 고가용성을 보장합니다.

AWS Config 규칙의 최소 AvailibilityZones 파라미터를 사용하여 가용 영역의 최소 수를 조정할 수 있습니다.

자세한 내용은 여러 인스턴스 유형 및 구매 옵션이 포함된 Auto Scaling 그룹을 참조하세요.

검사 ID

```
c18d2gz101
```

소스

```
AWS Config Managed Rule: autoscaling-multiple-az
```

알림 기준

빨간색: Amazon EC2 Auto Scaling 그룹에 여러 AZ가 구성되어 있지 않거나 지정된 최소 AZ 수를 충족하지 않습니다.

권장 조치

Amazon EC2 Auto Scaling 그룹이 여러 AZ로 구성되어 있는지 확인하세요. 여러 가용 영역에 Amazon EC2 인스턴스를 배포하여 고가용성을 보장합니다.

추가 리소스

시작 템플릿을 사용하여 Auto Scaling 그룹 생성

시작 구성을 사용하여 Auto Scaling 그룹 생성

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙

- 입력 파라미터
- 최종 업데이트 시간

## Amazon EC2 가용 영역 균형

설명

리전의 가용 영역에서 전반적인 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 배포를 확인합니다.

가용 영역은 다른 가용 영역에서 발생한 장애가 차단되는 리전 내 별도 위치입니다. 가용 영역은 같은 리전에 있는 다른 가용 영역에 대해 저렴하고 대기 시간이 짧은 네트워크 연결을 제공합니다. 같은 리전에 있는 다수의 가용 영역에서 인스턴스를 시작하면 단일 위치에서 장애가 발생할 경우 애플리케이션을 보호할 수 있습니다.

검사 ID

`wuy7G1zxql`

알림 기준

- 노란색: 리전의 여러 영역에 인스턴스가 있지만, 균일하게 분산되어 있지 않습니다(사용된 가용 영역에서 가장 많은 인스턴스 수와 가장 적은 인스턴스 수의 차이가 20%보다 큼).
- 빨간색: 리전의 단일 가용 영역에만 인스턴스가 있습니다.

권장 조치

Amazon EC2 인스턴스를 여러 가용 영역에 걸쳐 균등하게 밸런싱합니다. 인스턴스를 수동으로 시작하거나 오토 스케일링을 사용하여 자동으로 실행하면 됩니다. 자세한 내용은 인스턴스 시작 및 오토 스케일링 그룹의 로드 밸런싱을 참조하세요.

추가 리소스

Amazon EC2 Auto Scaling 사용 설명서

보고서 열

- 상태 표시기
- 지역
- 영역 a 인스턴스
- 영역 b 인스턴스
- 영역 c 인스턴스

- 영역 e 인스턴스
- 영역 f 인스턴스
- 이유

## Amazon EC2 세부 모니터링이 활성화되지 않음

설명

EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다.

Amazon EC2 세부 모니터링은 Amazon EC2 기본 모니터링에 사용되는 5분 간격 대신 1분 간격으로 게시되는 더 빈번한 지표를 제공합니다. Amazon EC2에 대한 세부 모니터링을 활성화하면 Amazon EC2 리소스를 보다 효율적으로 관리할 수 있으므로 추세를 파악하고 조치를 더 빠르게 수행할 수 있습니다.

자세한 내용은 기본 모니터링 및 세부 모니터링을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`AWS Config c18d2gz144`

소스

AWS Config 관리형 규칙: ec2 인스턴스 세부 모니터링 지원

알림 기준

노란색: Amazon EC2 인스턴스에는 세부 모니터링이 활성화되어 있지 않습니다.

권장 조치

Amazon EC2 인스턴스에 대한 세부 모니터링을 활성화하여 Amazon EC2 지표 데이터가 Amazon 에 게시되는 빈도를 5분에서 CloudWatch 1분 간격으로 늘리십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## 차단 모드의 Amazon ECS AWS로그 드라이버

설명

차단 모드에서 AWS로그 로깅 드라이버로 구성된 Amazon ECS 작업 정의를 확인합니다. 차단 모드로 구성된 드라이버는 시스템 가용성을 위험에 빠뜨립니다.

> **Note**
> 이 검사의 결과는 매일 한 번 이상 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1dvkm4z6b`

알림 기준

노란색: awslogs 드라이버 로깅 구성 파라미터 모드가 차단 또는 누락으로 설정되어 있습니다. 누락된 모드 매개변수는 기본 차단 구성을 나타냅니다.

녹색: Amazon ECS 작업 정의가 awslogs 드라이버를 사용하지 않거나 awslogs 드라이버가 비차단 모드로 구성되어 있습니다.

권장 조치

가용성 위험을 줄이려면 작업 정의 AWS로그 드라이버 구성을 차단에서 비차단으로 변경하는 것이 좋습니다. 비차단 모드에서는 매개 변수 값을 설정해야 합니다. max-buffer-size 구성 매개변수에 대

한 자세한 내용 및 지침은 을 참조하십시오. 로그 컨테이너 로그 드라이버의 비차단 모드를 사용한 AWS로그 손실 방지를 참조하십시오.

추가 리소스

AWS 로그 로그 드라이버 사용

배압 방지를 위한 컨테이너 로깅 옵션 선택

로그 컨테이너 로그 드라이버의 비차단 모드로 AWS로그 손실 방지

보고서 열

- 상태 표시기
- 지역
- 태스크 정의 ARN
- 컨테이너 정의 이름
- 최종 업데이트 시간

## 단일 AZ를 사용하는 Amazon ECS 서비스

설명

서비스 구성에서 단일 가용 영역(AZ)을 사용하는지 확인합니다.

AZ는 다른 영역의 장애로부터 격리된 별개의 위치입니다. 이는 동일한 AWS 리전에 있는 AZ 간의 저렴하고 지연 시간이 짧은 네트워크 연결을 지원합니다. 같은 리전에 있는 다수의 AZ에서 인스턴스를 시작하면 단일 위치에서 장애가 발생할 경우 애플리케이션을 보호할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1z7dfpz01`

알림 기준

- 노란색: Amazon ECS 서비스는 단일 AZ에서 모든 작업을 실행합니다.

- 녹색: Amazon ECS 서비스가 두 개 이상의 서로 다른 AZ에서 작업을 실행하고 있습니다.

권장 조치

다른 AZ에서 서비스에 대해 하나 이상의 작업을 생성합니다.

추가 리소스

Amazon ECS 용량 및 가용성

보고서 열

- 상태 표시기
- 지역
- ECS 클러스터 이름/ECS 서비스 이름
- 가용 영역의 수
- 최종 업데이트 시간

## Amazon ECS 다중 AZ 배치 전략

설명

Amazon ECS 서비스가 가용 영역(AZ)에 기반한 스프레드 배치 전략을 사용하는지 확인합니다. 이 전략은 가용 영역 전체에 작업을 동일하게 AWS 리전 분산하여 단일 장애 지점으로부터 애플리케이션을 보호하는 데 도움이 될 수 있습니다.

Amazon ECS 서비스의 일부로 실행되는 작업의 경우 확산은 기본 작업 배치 전략입니다.

또한 이 검사를 통해 활성화된 배치 전략 목록에서 스프레드가 첫 번째 또는 유일한 전략인지 확인할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c1z7dfpz02
```

알림 기준

- 노란색: 가용 영역별 스프레드가 비활성화되었거나 Amazon ECS 서비스에 대해 활성화된 배치 전략 목록의 첫 번째 전략이 아닙니다.
- 녹색: 가용 영역별 분산은 활성화된 배치 전략 목록의 첫 번째 전략이거나 Amazon ECS 서비스에 사용할 수 있는 유일한 배치 전략입니다.

권장 조치

분산 작업 배치 전략을 사용하여 여러 AZ에 작업을 분산할 수 있습니다. 가용 영역별 분산이 모든 사용 가능한 작업 배치 전략의 첫 번째 전략인지 아니면 사용된 유일한 전략인지 확인하십시오. AZ 배치를 관리하기로 선택한 경우 다른 AZ의 미러링된 서비스를 사용하여 이러한 위험을 완화할 수 있습니다.

추가 리소스

Amazon ECS 작업 배치 전략

보고서 열

- 상태 표시기
- 지역
- ECS 클러스터 이름/ECS 서비스 이름
- 분산 작업 배치 전략이 활성화되고 올바르게 적용됨
- 최종 업데이트 시간

## Amazon EFS 노 마운트 타겟 이중화

설명

Amazon EFS 파일 시스템의 여러 가용 영역에 탑재 대상이 있는지 확인합니다.

가용 영역은 다른 영역으로부터 분리된 개별적인 지점입니다. AWS 리전 내 지리적으로 분리된 여러 가용 영역에 탑재 대상을 생성하면 Amazon EFS 파일 시스템의 가용성과 내구성을 최고 수준으로 높일 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1dfprch01`

알림 기준

- 노란색: 파일 시스템에는 단일 가용 영역에 1개의 탑재 대상이 생성되어 있습니다.

  녹색: 파일 시스템에는 여러 가용 영역에 2개 이상의 탑재 대상이 생성되어 있습니다.

권장 조치

One Zone 스토리지 클래스를 사용하는 EFS 파일 시스템의 경우 백업을 새 파일 시스템에 복원하여 표준 스토리지 클래스를 사용하는 새 파일 시스템을 생성하는 것이 좋습니다. 그런 다음 여러 가용 영역에 탑재 대상을 생성합니다.

표준 스토리지 클래스를 사용하는 EFS 파일 시스템의 경우 여러 가용 영역에 탑재 대상을 생성하는 것이 좋습니다.

추가 리소스

- Amazon EFS 콘솔을 사용하여 탑재 대상 관리
- Amazon EFS 할당량 및 한도

보고서 열

- 상태 표시기
- 지역
- EFS 파일 시스템 ID
- 탑재 대상 수
- 여러 AZ의 수
- 최종 업데이트 시간

## Amazon EFS가 AWS Backup 계획에 포함되지 않음

설명

Amazon EFS 파일 시스템이 백업 계획에 포함되어 있는지 확인합니다 AWS Backup.

AWS Backup 는 백업의 생성, 마이그레이션, 복원 및 삭제를 단순화하는 동시에 향상된 보고 및 감사를 제공하도록 설계된 통합 백업 서비스입니다.

자세한 내용은 Amazon EFS 파일 시스템 백업을 참조하세요.

검사 ID

c18d2gz117

소스

AWS Config Managed Rule: EFS_IN_BACKUP_PLAN

알림 기준

빨간색: Amazon EFS는 AWS Backup 플랜에 포함되어 있지 않습니다.

권장 조치

우발적인 데이터 손실이나 데이터 손상으로부터 보호하려면 Amazon EFS 파일 시스템이 AWS Backup 플랜에 포함되어 있는지 확인하십시오.

추가 리소스

Amazon EFS 파일 시스템 백업

Amazon EFS 백업 및 복원을 사용합니다 AWS Backup.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## 아마존 ElastiCache 멀티-AZ 클러스터

설명

단일 가용 영역 (AZ) 에 배포되는 ElastiCache 클러스터가 있는지 확인합니다. 이 검사는 다중 AZ가 클러스터에서 비활성 상태인 경우 경고합니다.

여러 AZ에 배포하면 다른 AZ의 읽기 전용 복제본에 비동기적으로 복제되므로 ElastiCache 클러스터 가용성이 향상됩니다. 계획된 클러스터 유지 관리가 수행되거나 기본 노드를 사용할 수 없는 경

우 복제본을 기본 노드로 자동 승격합니다. ElastiCache 이 장애 조치를 통해 클러스터 쓰기 작업을 재개할 수 있으며 관리자가 개입할 필요가 없습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`ECHdfsQ402`

알림 기준

- 녹색: 클러스터에서 다중 AZ가 활성화되어 있습니다.
- 노란색: 클러스터에서 다중 AZ가 비활성 상태입니다.

권장 조치

기본 AZ와 다른 AZ에서 샤드당 하나 이상의 복제본을 생성합니다.

추가 리소스

자세한 내용은 다중 AZ를 사용하는 Redis의 ElastiCache 다운타임 최소화를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- 클러스터 이름
- 최종 업데이트 시간

## Amazon ElastiCache Redis 클러스터 자동 백업

설명

Amazon ElastiCache for Redis 클러스터에 자동 백업이 켜져 있는지, 스냅샷 보존 기간이 지정된 기간 또는 15일의 기본 한도를 초과하는지 확인합니다. 자동 백업이 활성화되면 클러스터의 백업을 매일 ElastiCache 생성합니다.

AWS Config 규칙의 스냅샷 RetentionPeriod 매개 변수를 사용하여 원하는 스냅샷 보존 한도를 지정할 수 있습니다.

자세한 내용은 ElastiCache Redis용 백업 및 복원을 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz178`

소스

`AWS Config Managed Rule: elasticache-redis-cluster-automatic-backup-check`

알림 기준

빨간색: Amazon ElastiCache for Redis 클러스터에는 자동 백업이 켜져 있지 않거나 스냅샷 보존 기간이 한도 미만입니다.

권장 조치

Amazon ElastiCache for Redis 클러스터에 자동 백업이 켜져 있고 스냅샷 보존 기간이 지정된 또는 15일의 기본 한도보다 높은지 확인하십시오. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

자세한 내용은 ElastiCache Redis용 백업 및 복원을 참조하십시오.

추가 리소스

자세한 내용은 자동 백업 예약을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- 클러스터 이름

- 최종 업데이트 시간

## Amazon MemoryDB 다중 AZ 클러스터

설명

단일 가용 영역(AZ)에 배포된 MemoryDB 클러스터가 있는지 확인합니다. 이 검사는 다중 AZ가 클러스터에서 비활성 상태인 경우 경고합니다.

여러 AZ에 배포하면 다른 AZ의 읽기 전용 복제본에 비동기적으로 복제하여 MemoryDB 클러스터 가용성이 향상됩니다. 계획된 클러스터 유지 관리가 수행되거나 프라이머리 노드를 사용할 수 없는 경우 MemoryDB는 자동으로 복제본을 프라이머리 노드로 승격합니다. 이 장애 조치를 통해 클러스터 쓰기 작업을 재개할 수 있으며 관리자가 개입할 필요가 없습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`MDBdfsQ401`

알림 기준

- 녹색: 클러스터에서 다중 AZ가 활성화되어 있습니다.
- 노란색: 클러스터에서 다중 AZ가 비활성 상태입니다.

권장 조치

기본 AZ와 다른 AZ에서 샤드당 하나 이상의 복제본을 생성합니다.

추가 리소스

자세한 정보는 다중 AZ로 MemoryDB의 가동 중지 시간 최소화를 참조하세요.

보고서 열

- 상태 표시기
- 지역

- 클러스터 이름
- 최종 업데이트 시간

## 너무 많은 파티션을 호스팅하는 Amazon MSK 브로커

설명

Kafka용 관리형 스트리밍(MSK) 클러스터의 브로커에 할당된 파티션 수가 권장보다 많지 않은지 확인합니다.

검사 ID

`Cmsvnj8vf1`

알림 기준

- 빨간색: MSK 브로커가 권장 최대 파티션 제한의 100% 에 도달했거나 초과했습니다.
- 노란색: MSK가 권장 최대 파티션 제한의 80% 에 도달했습니다.

권장 조치

MSK 권장 모범 사례에 따라 MSK 클러스터를 확장하거나 사용하지 않는 파티션을 삭제하세요.

추가 리소스

- 적정 크기의 클러스터

보고서 열

- 상태 표시기
- 지역
- 클러스터 ARN
- 브로커 ID
- 파티션 수

## 데이터 노드가 3개 미만인 Amazon OpenSearch 서비스 도메인

설명

Amazon OpenSearch Service 도메인이 최소 세 개의 데이터 노드로 구성되어 있고 ZoneAwarenessEnabled true인지 확인합니다. ZoneAwarenessEnabled 활성화하면 Amazon OpenSearch Service는 각 기본 샤드와 해당 복제본이 서로 다른 가용 영역에 할당되도록 합니다.

자세한 내용은 Amazon OpenSearch Service의 다중 AZ 도메인 구성을 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz183`

소스

`AWS Config Managed Rule: opensearch-data-node-fault-tolerance`

알림 기준

노란색: Amazon OpenSearch 서비스 도메인은 3개 미만의 데이터 노드로 구성되어 있습니다.

권장 조치

Amazon OpenSearch 서비스 도메인이 최소 3개의 데이터 노드로 구성되어 있는지 확인하십시오. 다중 AZ 도메인을 구성하여 노드를 할당하고 동일한 지역 내 세 가용 영역에 데이터를 복제하여 Amazon OpenSearch Service 클러스터의 가용성을 향상시키십시오. 이는 데이터 손실을 방지하는 데 도움이 되며 노드 또는 데이터 센터(AZ) 장애가 발생할 경우 가동 중지 시간을 최소화합니다.

자세한 내용은 세 개의 가용 영역에 배포하여 Amazon OpenSearch Service의 가용성 향상을 참조하십시오.

추가 리소스

- 세 개의 가용 영역에 배포하여 Amazon OpenSearch 서비스의 가용성을 높입니다.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터

- 최종 업데이트 시간

## Amazon RDS 백업

설명

Amazon RDS DB 인스턴스의 자동 백업이 있는지 확인합니다.

기본적으로 백업은 보존 기간이 하루인 상태로 활성화됩니다. 백업은 예상치 못한 데이터 손실의 위험을 줄이고 point-in-time 복구가 가능합니다.

검사 ID

opQPADkZvH

알림 기준

빨간색: DB 인스턴스의 백업 보존 기간이 백업 보존 기간이 0으로 설정되어 있습니다.

권장 조치

자동 DB 인스턴스 백업의 보존 기간을 애플리케이션 요구 사항에 맞게 1~35일로 설정합니다. 자동 백업 작업을 참조하세요.

추가 리소스

Amazon RDS 시작하기

보고서 열

- 상태 표시기
- 리전/AZ
- DB 인스턴스
- VPC ID
- 백업 보존 기간

## Amazon RDS DB 클러스터에 DB 인스턴스가 하나 있습니다.

설명

DB 클러스터에 하나 이상의 DB 인스턴스를 추가하여 가용성과 성능을 개선하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt011`

알림 기준

노란색: DB 클러스터에는 DB 인스턴스가 하나만 있습니다.

권장 조치

DB 클러스터에 리더 DB 인스턴스를 추가합니다.

추가 리소스

현재 구성에서는 하나의 DB 인스턴스가 읽기 및 쓰기 작업에 모두 사용됩니다. 다른 DB 인스턴스를 추가하여 읽기 재배포 및 장애 조치 옵션을 허용할 수 있습니다.

자세한 내용은 Amazon Aurora의 고가용성을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 엔진 이름

- DB 인스턴스 클래스
- 최종 업데이트 시간

## 모든 인스턴스가 동일한 가용 영역에 있는 Amazon RDS DB 클러스터

### 설명

DB 클러스터는 현재 단일 가용 영역에 있습니다. 여러 가용 영역을 사용하여 가용성을 개선하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

### 검사 ID

`c1qf5bt007`

### 알림 기준

노란색: DB 클러스터의 모든 인스턴스는 동일한 가용 영역에 있습니다.

### 권장 조치

DB 클러스터의 여러 가용 영역에 DB 인스턴스를 추가합니다.

### 추가 리소스

DB 클러스터의 여러 가용 영역에 DB 인스턴스를 추가하는 것이 좋습니다. 여러 가용 영역에 DB 인스턴스를 추가하면 DB 클러스터의 가용성이 향상됩니다.

자세한 내용은 Amazon Aurora의 고가용성을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 엔진 이름
- 최종 업데이트 시간

## 모든 리더 인스턴스가 동일한 가용 영역에 있는 Amazon RDS DB 클러스터

설명

DB 클러스터의 모든 리더 인스턴스가 동일한 가용 영역에 있습니다. DB 클러스터의 여러 가용 영역에 Reader 인스턴스를 배포하는 것이 좋습니다.

배포는 데이터베이스의 가용성을 높이고 클라이언트와 데이터베이스 간의 네트워크 지연 시간을 줄여 응답 시간을 개선합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt018`

알림 기준

빨간색: DB 클러스터의 리더 인스턴스는 동일한 가용 영역에 있습니다.

권장 조치

리더 인스턴스를 여러 가용 영역에 분산합니다.

추가 리소스

가용 영역 (AZ) 은 각 지역 내에서 정전이 발생할 경우 격리를 제공하기 위해 서로 구분되는 위치입니다. AWS DB 클러스터의 가용성을 개선하려면 여러 AZ에 걸쳐 있는 DB 클러스터에 기본 인스턴스와 리더 인스턴스를 배포하는 것이 좋습니다. 클러스터를 생성할 때 AWS Management Console AWS CLI, 또는 Amazon RDS API를 사용하여 다중 AZ 클러스터를 생성할 수 있습니다. 새 리더 인스턴스를 추가하고 다른 AZ를 지정하여 기존 Aurora 클러스터를 다중 AZ 클러스터로 수정할 수 있습니다.

자세한 내용은 Amazon Aurora의 고가용성을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 엔진 이름
- 최종 업데이트 시간

## Amazon RDS DB 인스턴스 고급 모니터링이 활성화되지 않았음

설명

Amazon RDS DB 인스턴스에 향상된 모니터링이 활성화되어 있는지 확인합니다.

Amazon RDS 확장 모니터링은 DB 인스턴스가 실행되는 운영 체제(OS)에 대한 측정치를 실시간으로 제공합니다. Amazon RDS DB 인스턴스에 대한 모든 시스템 지표 및 프로세스 정보는 Amazon RDS 콘솔에서 볼 수 있습니다. 그리고 대시보드를 사용자 지정할 수 있습니다. 향상된 모니터링을 사용하면 Amazon RDS 인스턴스 운영 상태를 거의 실시간으로 파악할 수 있으므로 운영 문제에 더 빠르게 대응할 수 있습니다.

규칙의 모니터링 간격 매개변수를 사용하여 원하는 모니터링 간격을 지정할 수 있습니다. AWS Config

자세한 내용은 향상된 모니터링 개요 및 향상된 모니터링의 OS 지표를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz158`

소스

`AWS Config Managed Rule: rds-enhanced-monitoring-enabled`

알림 기준

노란색: Amazon RDS DB 인스턴스에 향상된 모니터링이 활성화되어 있지 않거나 원하는 간격으로 구성되어 있지 않습니다.

권장 조치

Amazon RDS DB 인스턴스에 대한 향상된 모니터링을 활성화하여 Amazon RDS 인스턴스 작동 상태를 더 잘 파악할 수 있습니다.

자세한 내용은 Enhanced Monitoring을 사용하여 OS 지표 모니터링을 참조하세요.

추가 리소스

향상된 모니터링의 OS 지표

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙

- 입력 파라미터
- 최종 업데이트 시간

## Amazon RDS DB 인스턴스에는 스토리지 자동 크기 조정 기능이 해제되어 있습니다.

설명

Amazon RDS 스토리지 자동 크기 조정은 DB 인스턴스에 대해 켜져 있지 않습니다. 데이터베이스 워크로드가 증가하면 RDS Storage 자동 크기 조정이 다운타임 없이 스토리지 용량을 자동으로 확장합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt013`

알림 기준

빨간색: DB 인스턴스에는 스토리지 자동 크기 조정 기능이 켜져 있지 않습니다.

권장 조치

지정된 최대 스토리지 임계값으로 Amazon RDS 스토리지 자동 확장을 활성화합니다.

추가 리소스

Amazon RDS 스토리지 자동 크기 조정은 데이터베이스 워크로드가 증가할 때 다운타임 없이 스토리지 용량을 자동으로 확장합니다. 스토리지 자동 크기 조정은 스토리지 사용량을 모니터링하고 사용량이 프로비저닝된 스토리지 용량에 가까워지면 자동으로 용량을 확장합니다. Amazon RDS가 DB 인스턴스에 할당할 수 있는 스토리지의 최대 한도를 지정할 수 있습니다. 스토리지 자동 확장에는 추가 비용이 없습니다. DB 인스턴스에 할당된 Amazon RDS 리소스에 대한 비용만 지불하면 됩니다. Amazon RDS 스토리지 자동 크기 조정을 활성화하는 것이 좋습니다.

자세한 내용은 Amazon RDS 스토리지 Auto Scaling을 사용한 용량 자동 관리 섹션을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- 권장 값
- 엔진 이름
- 최종 업데이트 시간

## 다중 AZ 배포를 사용하지 않는 Amazon RDS DB 인스턴스

설명

다중 AZ 배포를 사용하는 것이 좋습니다. 다중 AZ 배포는 DB 인스턴스의 가용성과 내구성을 향상합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.

DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt019`

알림 기준

노란색: DB 인스턴스는 다중 AZ 배포를 사용하지 않습니다.

권장 조치

영향을 받는 DB 인스턴스에 대해 다중 AZ를 설정합니다.

추가 리소스

Amazon RDS 다중 AZ 배포에서 Amazon RDS는 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역의 인스턴스에 데이터를 복제합니다. 장애가 감지되면 Amazon RDS는 수동 개입 없이 자동으로 예비 인스턴스로 장애 조치합니다.

자세한 내용은 요금을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- 엔진 이름
- 최종 업데이트 시간

## 아마존 RDS DiskQueueDepth

설명

CloudWatch DiskQueueDepth 지표에 RDS 인스턴스 데이터베이스 스토리지에 대한 대기 중인 쓰기 수가 운영 조사가 권장되는 수준까지 증가했는지 확인합니다.

검사 ID

`Cmsvnj8db3`

알림 기준

- 빨간색: DiskQueueDepth CloudWatch 지표가 10을 초과했습니다.
- 노란색: DiskQueueDepth CloudWatch 지표가 5보다 크지만 10보다 작거나 같습니다.
- 녹색: DiskQueueDepth CloudWatch 지표가 5보다 작거나 같습니다.

권장 조치

읽기/쓰기 특성을 지원하는 인스턴스 및 스토리지 볼륨으로 이동하는 것을 고려해 보십시오.

보고서 열

- 상태 표시기
- 지역
- DB 인스턴스 ARN
- DiskQueueDepth 미터법

## 아마존 RDS FreeStorageSpace

설명

RDS 데이터베이스 인스턴스의 FreeStorageSpace CloudWatch 지표가 운영상 합당한 임계값 이상으로 증가했는지 확인합니다.

검사 ID

`Cmsvnj8db2`

알림 기준

- 빨간색: 총 용량의 90% 에 FreeStorageSpace 도달했거나 초과했습니다.
- 노란색: FreeStorageSpace 전체 용량의 80% ~ 90% 사이
- 녹색: FreeStorageSpace 전체 용량의 80% 미만

권장 조치

Amazon RDS 관리 콘솔, Amazon RDS API 또는 AWS 명령줄 인터페이스를 사용하여 사용 가능한 스토리지가 부족한 RDS 데이터베이스 인스턴스의 스토리지 공간을 확장할 수 있습니다.

보고서 열

- 상태 표시기

- 지역
- DB 인스턴스 ARN
- FreeStorageSpace 메트릭 (MB)
- DB 인스턴스 할당 스토리지(MB)
- DB 인스턴스 스토리지 사용률

## Amazon RDS log_output 파라미터가 테이블로 설정되었습니다.

설명

log_output이 TABLE로 설정된 경우 log_output이 FILE로 설정된 경우보다 더 많은 스토리지가 사용됩니다. 스토리지 크기 제한에 도달하지 않으려면 매개변수를 FILE로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt023`

알림 기준

노란색: DB 파라미터 그룹의 log_output 파라미터는 TABLE로 설정되어 있습니다.

권장 조치

DB 파라미터 그룹에서 log_output 파라미터 값을 FILE로 설정합니다.

추가 리소스

자세한 내용은 MySQL 데이터베이스 로그 파일을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## Amazon RDS innodb_default_row_format 파라미터 설정은 안전하지 않습니다

설명

DB 인스턴스에서 알려진 문제가 발생했습니다. row_format이 COMPACT 또는 REDUNDANT로 설정된 8.0.26 미만의 MySQL 버전에서 생성된 테이블은 인덱스가 767바이트를 초과하면 액세스할 수 없고 복구할 수 없습니다.

innodb_default_row_format 파라미터 값을 DYNAMIC으로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.

DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt036`

알림 기준

빨간색: DB 파라미터 그룹의 innodb_default_row_format 파라미터에 대해 안전하지 않은 설정이 있습니다.

권장 조치

innodb_default_row_format 파라미터를 DYNAMIC으로 설정합니다.

추가 리소스

row_format이 COMPACT 또는 REDUNDANT로 설정된 8.0.26 미만의 MySQL 버전으로 테이블을 생성하는 경우 767바이트보다 짧은 키 접두사를 사용하여 인덱스를 생성하는 것은 적용되지 않습니다. 데이터베이스를 다시 시작한 후에는 이러한 테이블에 액세스하거나 복구할 수 없습니다.

자세한 내용은 MySQL 설명서 웹 사이트의 MySQL 8.0.26의 변경 사항 (2021-07-20, 일반 가용성)n을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값입니다.
- 최종 업데이트 시간

## Amazon RDS innodb_flush_log_at_trx_commit 파라미터는 1이 아닙니다

설명

DB 인스턴스의 innodb_flush_log_at_trx_commit 파라미터의 값은 안전한 값이 아닙니다. 이 파라미터는 디스크에 대한 커밋 작업의 지속성을 제어합니다.

innodb_flush_log_at_trx_commit 파라미터를 1로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt030`

알림 기준

노란색: DB 파라미터 그룹에는 innodb_flush_log_at_trx_commit이 1이 아닌 다른 것으로 설정되어 있습니다.

권장 조치

innodb_flush_log_at_trx_commit 파라미터 값을 1로 설정합니다.

추가 리소스

로그 버퍼를 지속 가능한 스토리지에 저장하면 데이터베이스 트랜잭션이 계속 유지됩니다. 하지만 디스크에 저장하면 성능에 영향을 줍니다. innodb_flush_log_at_trx_commit 매개 변수에 설정된 값에 따라 로그가 기록되고 디스크에 저장되는 방식의 동작은 달라질 수 있습니다.

- 매개변수 값이 1이면 트랜잭션이 커밋될 때마다 로그가 디스크에 기록되고 저장됩니다.
- 파라미터 값이 0이면 로그가 1초에 한 번씩 디스크에 기록되고 저장됩니다.
- 파라미터 값이 2인 경우 각 트랜잭션이 커밋된 후 로그가 기록되고 1초에 한 번씩 디스크에 저장됩니다. 데이터는 InnoDB 메모리 버퍼에서 메모리에 있는 운영 체제의 캐시로 이동합니다.

> **Note**
>
> 매개 변수 값이 1이 아닌 경우 InnoDB는 ACID 속성을 보장하지 않습니다. 데이터베이스가 충돌하면 최근 1초 동안의 트랜잭션이 손실될 수 있습니다.

자세한 내용은 Amazon RDS for MySQL의 파라미터 구성 모범 사례, 1부: 성능과 관련된 파라미터를 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## Amazon RDS max_user_connections 파라미터가 낮음

설명

DB 인스턴스의 각 데이터베이스 계정에 대한 최대 동시 연결 수 값이 낮습니다.

max_user_connections 파라미터를 5보다 큰 수로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.

DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt034`

알림 기준

노란색: DB 파라미터 그룹에 max_user_connections가 잘못 구성되어 있습니다.

권장 조치

max_user_connections 파라미터의 값을 5보다 큰 수로 늘리십시오.

추가 리소스

max_user_connections 설정은 MySQL 사용자 계정에 허용되는 최대 동시 연결 수를 제어합니다. 이 연결 한도에 도달하면 백업, 패치, 파라미터 변경과 같은 Amazon RDS 인스턴스 관리 작업에 장애가 발생합니다.

자세한 내용은 MySQL 설명서 웹 사이트의 계정 리소스 제한 설정을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## Amazon RDS 다중 AZ

설명

단일 가용 영역(AZ)에 배포된 DB 인스턴스가 있는지 확인합니다.

다중 AZ 배포는 서로 다른 가용 영역에 있는 대기 인스턴스에 동기식으로 복제하여 데이터베이스 가용성을 향상시킵니다. 계획된 데이터베이스 유지 관리 또는 DB 인스턴스나 가용 영역에 장애가

발생하는 경우 Amazon RDS가 대기 복제본을 사용해 자동으로 장애 조치를 통해 대기 모드로 전환합니다. 이 장애 조치를 통해 관리자의 개입 없이 데이터베이스 작업을 신속하게 재개할 수 있습니다. Amazon RDS는 Microsoft SQL Server용 다중 AZ 배포를 지원하지 않으므로 이 검사에서는 SQL Server 인스턴스를 검사하지 않습니다.

검사 ID

`f2iK5R6Dep`

알림 기준

노란색: DB 인스턴스가 단일 가용 영역에 배포되어 있습니다.

권장 조치

애플리케이션에 고가용성이 필요한 경우 DB 인스턴스를 수정하여 다중 AZ 배포를 활성화합니다. 고가용성(다중 AZ)를 참조하세요.

추가 리소스

리전 및 가용 영역

보고서 열

- 상태 표시기
- 리전/AZ
- DB 인스턴스
- VPC ID
- 다중 AZ

## 아마존 RDS는 계획에 포함되지 AWS Backup 않음

설명

Amazon RDS DB 인스턴스가 AWS Backup의 백업 계획에 포함되어 있는지 확인합니다.

AWS Backup 서비스 전반의 데이터 백업을 쉽게 중앙 집중화하고 자동화할 수 있는 완전 관리형 백업 서비스입니다. AWS

Amazon RDS DB 인스턴스를 백업 계획에 포함시키는 것은 규제 준수 의무, 재해 복구, 데이터 보호를 위한 비즈니스 정책 및 비즈니스 연속성 목표를 위해 중요합니다.

자세한 내용은 AWS Backup란 무엇입니까?를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz159`

소스

`AWS Config Managed Rule: rds-in-backup-plan`

알림 기준

노란색: Amazon RDS DB 인스턴스는 백업 계획에 포함되어 있지 않습니다. AWS Backup

권장 조치

Amazon RDS DB 인스턴스를 의 백업 계획에 포함시키십시오. AWS Backup

자세한 내용은 AWS Backup을 사용한 Amazon RDS 백업 및 복원을 참조하세요.

추가 리소스

백업 계획에 리소스 할당

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon RDS 읽기 전용 복제본은 쓰기 가능 모드로 열려 있습니다.

설명

DB 인스턴스에 쓰기 가능 모드의 읽기 전용 복제본이 있어 클라이언트의 업데이트를 허용합니다.

읽기 전용 복제본이 쓰기 가능 모드가 되지 않도록 read_only 파라미터를 TrueIf복제본으로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt035`

알림 기준

노란색: DB 파라미터 그룹은 읽기 전용 복제본에 대해 쓰기 가능 모드를 활성화합니다.

권장 조치

read_only 파라미터 값을 복제본으로 설정합니다. TrueIf

추가 리소스

read_only 매개변수는 클라이언트의 데이터베이스 인스턴스에 대한 쓰기 권한을 제어합니다. 이 매개변수의 기본값은 복제본입니다TrueIf. 복제본 인스턴스의 경우 TrueIfReplica는 read_only 값을 ON (1) 으로 설정하고 클라이언트의 모든 쓰기 작업을 비활성화합니다. 마스터/라이터 인스턴스의 경우, TrueIf복제본은 값을 OFF (0) 로 설정하고 해당 인스턴스에 대한 클라이언트의 쓰기 작업을 활성화합니다. 읽기 전용 복제본을 쓰기 가능 모드로 열면 이 인스턴스에 저장된 데이터가 기본 인스턴스와 달라져 복제 오류가 발생할 수 있습니다.

자세한 내용은 MySQL 설명서 웹 사이트의 MySQL용 Amazon RDS의 파라미터 구성 모범 사례, 2부: 복제와 관련된 파라미터를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## Amazon RDS 리소스 자동 백업이 꺼져 있습니다.

설명

DB 리소스에서 자동 백업이 비활성화되었습니다. 자동 백업을 통해 DB 인스턴스를 point-in-time 복구할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

```
c1qf5bt001
```

알림 기준

빨간색: Amazon RDS 리소스에 자동 백업이 활성화되어 있지 않음

권장 조치

보존 기간이 최대 14일인 자동 백업을 활성화하세요.

추가 리소스

자동 백업을 통해 DB 인스턴스를 point-in-time 복구할 수 있습니다. 자동 백업을 활성화하는 것이 좋습니다. DB 인스턴스의 자동 백업을 활성화하면 Amazon RDS는 원하는 백업 기간 동안 매일 데이터의 전체 백업을 자동으로 수행합니다. 백업은 DB 인스턴스에 업데이트가 있을 때 트랜잭션 로그를 캡처합니다. 추가 비용 없이 DB 인스턴스의 스토리지 크기까지 백업 스토리지를 확보할 수 있습니다.

자세한 정보는 다음 자료를 참조하십시오.

- 자동 백업 활성화
- Amazon RDS 백업 스토리지 비용에 대한 설명

보고서 열

- 상태 표시기
- 지역
- Resource
- 권장 가치
- 엔진 이름
- 최종 업데이트 시간

## Amazon RDS sync_binlog 파라미터가 꺼져 있습니다

설명

트랜잭션 커밋이 DB 인스턴스에서 확인되기 전에는 이진 로그를 디스크에 동기화하지 않습니다.

sync_binlog 파라미터 값을 1로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt031`

알림 기준

노란색: DB 파라미터 그룹의 동기 바이너리 로깅이 꺼져 있습니다.

권장 조치

sync_binlog 파라미터를 1로 설정합니다.

추가 리소스

sync_binlog 파라미터는 MySQL이 바이너리 로그를 디스크로 푸시하는 방법을 제어합니다. 이 매개 변수의 값을 1로 설정하면 트랜잭션이 커밋되기 전에 바이너리 로그를 디스크로 동기화합니다. 이 매개 변수의 값을 0으로 설정하면 디스크와의 이진 로그 동기화가 해제됩니다. 일반적으로 MySQL 서버는 운영 체제에 의존하여 다른 파일과 마찬가지로 바이너리 로그를 디스크로 정기적으로 푸시합니다. sync_binlog 매개 변수 값을 0으로 설정하면 성능이 향상될 수 있습니다. 하지만 정전이나 운영 체제 충돌 시 서버는 바이너리 로그와 동기화되지 않은 커밋된 트랜잭션을 모두 잃게 됩니다.

자세한 내용은 MySQL용 Amazon RDS의 파라미터 구성 모범 사례, 2부: 복제와 관련된 파라미터를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## RDS DB 클러스터에는 다중 AZ 복제가 활성화되어 있지 않습니다

설명

Amazon RDS DB 클러스터에 다중 AZ 복제가 활성화되어 있는지 확인합니다.

다중 AZ DB 클러스터에는 라이터 DB 인스턴스와 두 개의 리더 DB 인스턴스가 세 개의 개별 가용 영역에 있습니다. 다중 AZ DB 클러스터는 다중 AZ 배포에 비해 고가용성, 높은 읽기 워크로드 용량 및 짧은 대기 시간을 제공합니다.

자세한 내용은 다중 AZ DB 클러스터 생성을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz161
```

소스

```
AWS Config Managed Rule: rds-cluster-multi-az-enabled
```

알림 기준

노란색: Amazon RDS DB 클러스터에는 다중 AZ 복제가 구성되어 있지 않습니다.

권장 조치

Amazon RDS DB 클러스터를 생성할 때는 다중 AZ DB 클러스터 배포를 활성화합니다.

자세한 내용은 다중 AZ DB 클러스터 생성을 참조하세요.

추가 리소스

다중 AZ DB 클러스터 배포

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## RDS 다중 AZ 대기 인스턴스가 활성화되지 않음

설명

Amazon RDS DB 인스턴스에 다중 AZ 예비 복제본이 구성되어 있는지 확인합니다.

Amazon RDS Multi-AZ는 서로 다른 가용 영역에 있는 예비 복제본에 데이터를 복제하여 데이터베이스 인스턴스에 고가용성 및 내구성을 제공합니다. 이는 자동 장애 조치를 제공하고 성능을 개선하며 데이터 내구성을 향상시킵니다. 다중 AZ DB 인스턴스 배포에서 Amazon RDS는 자동으로 서로 다른 가용 영역에 동기식 대기 복제본을 프로비저닝하고 유지합니다. 프라이머리 DB 인스턴스는 전체 가용 영역에서 대기 복제본으로 동기식으로 복제되어 시스템 백업 중에 데이터 이중화를 제공하고 대기 시간 급증을 최소화합니다. DB 인스턴스를 고가용성으로 실행하면 계획된 시스템 유지 관리 중 가용성을 높입니다. 또한, DB 인스턴스 오류 및 가용 영역 중단이 일어나지 않도록 방지할 수 있습니다.

자세한 내용은 다중 AZ DB 인스턴스 배포를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz156`

소스

`AWS Config Managed Rule: rds-multi-az-support`

알림 기준

노란색: Amazon RDS DB 인스턴스에는 다중 AZ 복제본이 구성되어 있지 않습니다.

권장 조치

Amazon RDS DB 인스턴스를 생성할 때 다중 AZ 배포를 활성화합니다.

이 체크를 Trusted Advisor 콘솔의 보기에서 제외할 수 없습니다.

추가 리소스

다중 AZ DB 인스턴스 배포

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

# 아마존 RDS ReplicaLag

설명

지난 주 동안 RDS 데이터베이스 인스턴스의 ReplicaLag CloudWatch 지표가 운영상 합당한 임계값 이상으로 증가했는지 확인합니다.

ReplicaLag 측정치는 읽기 전용 복제본이 기본 인스턴스보다 지연되는 시간 (초) 을 측정합니다. 읽기 전용 복제본에 대한 비동기 업데이트가 기본 데이터베이스 인스턴스에서 발생하는 업데이트를 따라가지 못할 때 복제 지연이 발생합니다. 기본 인스턴스에 장애가 발생할 경우 이 값이 운영상 합당한 임계값을 초과하면 읽기 전용 복제본에서 데이터가 누락될 수 있습니다. ReplicaLag

검사 ID

`Cmsvnj8db1`

알림 기준

- 빨간색: 한 주 동안 ReplicaLag 지표가 60초를 최소 한 번 초과했습니다.
- 노란색: 한 주에 한 번 이상 ReplicaLag 지표가 10초를 초과했습니다.
- 녹색: 10초 ReplicaLag 미만입니다.

권장 조치

운영상 안전한 수준 이상으로 높아지는 ReplicaLag 데에는 여러 가지 원인이 있을 수 있습니다. 이러한 상황은 예를 들어 오래된 백업에서 최근에 교체/실행한 복제본 인스턴스와 이러한 복제본이 기본 데이터베이스 인스턴스와 라이브 트랜잭션을 “따라잡는” 데 상당한 시간이 걸리기 때문에 발생할 수 있습니다. 이는 시간이 지나면서 캐치업이 진행됨에 따라 줄어들 ReplicaLag 수 있습니다. 또 다른 예로 기본 데이터베이스 인스턴스에서 달성할 수 있는 트랜잭션 속도가 복제 프로세스나 복제본 인프라에 비해 빠른 경우를 들 수 있습니다. 복제가 기본 데이터베이스 성능과 보조를 맞추지 못해 시간이 지날수록 이 수치는 증가할 ReplicaLag 수 있습니다. 마지막으로, 하루/월 등의 다양한 기간에 걸쳐 워크로드가 폭주하여 때때로 지연될 수 있습니다. ReplicaLag 팀에서는 어떤 근본 원인이 데이터베이스 성능 저하로 이어졌는지 조사하고, 가능하면 데이터베이스 인스턴스 유형이나 워크로드의 기타 특성을 변경하여 복제본의 데이터 연속성이 요구 사항에 맞는지 확인해야 합니다. ReplicaLag

추가 리소스

- Amazon RDS for PostgreSQL의 읽기 전용 복제본 작업
- Amazon RDS에서 MySQL 복제 작업
- MySQL 읽기 전용 복제본 작업

보고서 열

- 상태 표시기
- 지역
- DB 인스턴스 ARN
- ReplicaLag 지표

## Amazon RDS 동기식_커밋 파라미터가 사용 중지되었습니다

설명

synchronous_commit 파라미터를 끄면 데이터베이스 충돌로 인해 데이터가 손실될 수 있습니다. 데이터베이스의 내구성에 악영향을 미칠 수 있습니다.

synchronous_commit 매개 변수를 켜는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt026`

알림 기준

빨간색: DB 파라미터 그룹에는 synchronous_commit 파라미터가 비활성화되어 있습니다.

권장 조치

DB 파라미터 그룹에서 synchronous_commit 파라미터를 활성화하십시오.

추가 리소스

synchronous_commit 파라미터는 데이터베이스 서버가 클라이언트에 성공적인 알림을 보내기 전에 미리 쓰기 로깅 (WAL) 프로세스 완료를 정의합니다. WAL이 트랜잭션을 디스크에 저장하기 전에 클라이언트가 커밋을 승인하기 때문에 이 커밋을 비동기 커밋이라고 합니다. synchronous_commit 파라미터를 끄면 트랜잭션이 손실되고, DB 인스턴스 내구성이 저하되고, 데이터베이스가 충돌하여 데이터가 손실될 수 있습니다.

자세한 내용은 MySQL 데이터베이스 로그 파일을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 이름
- 권장 값
- 최종 업데이트 시간

## Amazon Redshift 클러스터 자동 스냅샷

설명

Amazon Redshift 클러스터에 대해 자동 스냅샷이 활성화되어 있는지 확인합니다.

Amazon Redshift는 이전 자동 스냅샷 이후 클러스터의 변경 사항을 추적하는 증분 스냅샷을 자동으로 생성합니다. 자동 스냅샷은 클러스터를 복원하는 데 필요한 모든 데이터를 유지합니다. 자동 스냅샷을 비활성화하려면 보존 기간을 0으로 설정합니다. RA3 노드 유형에 대한 자동 스냅샷은 비활성화할 수 없습니다.

AWS Config 규칙의 기간 및 기간 매개변수를 사용하여 원하는 최소 및 최대 보존 MaxRetention기간을 지정할 수 있습니다. MinRetention

Amazon Redshift 스냅샷 및 백업

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz135`

소스

`AWS Config Managed Rule: redshift-backup-enabled`

알림 기준

빨간색: Amazon Redshift에는 원하는 보존 기간 내에 구성된 자동 스냅샷이 없습니다.

권장 조치

Amazon Redshift 클러스터에 자동 스냅샷이 활성화되어 있는지 확인하세요.

자세한 내용은 콘솔을 사용한 클러스터 관리를 참조하십시오.

추가 리소스

Amazon Redshift 스냅샷 및 백업

자세한 내용은 백업 작업을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon Route 53 삭제된 상태 확인

설명

삭제된 상태 확인과 연결된 리소스 레코드 세트를 확인합니다.

Route 53은 사용자가 하나 이상의 리소스 레코드 세트와 연결된 상태 확인을 삭제하는 것을 방지하지 않습니다. 연결된 리소스 레코드 세트를 업데이트하지 않고 상태 확인을 삭제하면 DNS 장애 조치 구성에 대한 DNS 쿼리 라우팅이 의도한 대로 작동하지 않습니다.

AWS 서비스에서 생성한 호스팅 영역은 확인 결과에 표시되지 않습니다.

검사 ID

`Cb877eB72b`

알림 기준

노란색: 리소스 레코드 세트가 삭제된 상태 확인과 연결되어 있습니다.

권장 조치

새 상태 확인을 생성한 후, 리소스 레코드 세트와 연결합니다. 상태 확인의 생성, 업데이트, 및 삭제와 리소스 레코드 세트에 상태 확인 추가를 참조하세요.

추가 리소스

- Amazon Route 53 상태 확인 및 DNS 장애 조치
- 단순 Amazon Route 53 구성에서 상태 확인 작동 방식

보고서 열

- 호스팅 영역 이름
- 호스팅 영역 ID
- 리소스 레코드 세트 이름
- 리소스 레코드 세트 유형
- 리소스 레코드 세트 식별자

## Amazon Route 53 장애 조치 리소스 레코드 세트

설명

구성이 잘못된 Amazon Route 53 장애 조치 리소스 레코드 세트가 있는지 확인합니다.

Amazon Route 53 상태 확인에서 기본 리소스가 비정상이라고 판단하면 Amazon Route 53는 보조 백업 리소스 레코드 세트를 사용하여 쿼리에 응답합니다. 장애 조치가 작동하려면 올바르게 구성된 기본 및 보조 리소스 레코드 세트를 생성해야 합니다.

AWS 서비스에서 생성한 호스팅 영역은 확인 결과에 표시되지 않습니다.

검사 ID

b73EEdD790

알림 기준

- 노란색: 기본 장애 조치 리소스 레코드 세트에 해당하는 보조 리소스 레코드 세트가 없습니다.
- 노란색: 보조 장애 조치 리소스 레코드 세트에 해당하는 기본 리소스 레코드 세트가 없습니다.
- 노란색: 이름이 같은 기본 리소스 레코드 세트와 보조 리소스 레코드 세트가 동일한 상태 확인에 연결되어 있습니다.

권장 조치

장애 조치 리소스 세트가 누락된 경우 해당 리소스 레코드 세트를 생성합니다. 장애 조치 리소스 레코드 세트 생성을 참조하세요.

두 리소스 레코드 세트가 동일한 상태 확인에 연결되어 있는 경우 각각에 대해 별도의 상태 확인을 생성합니다. 상태 확인의 생성, 업데이트, 및 삭제를 참조하세요.

추가 리소스

Amazon Route 53 상태 확인 및 DNS 장애 조치

보고서 열

- 호스팅 영역 이름
- 호스팅 영역 ID
- 리소스 레코드 세트 이름
- 리소스 레코드 세트 유형
- 이유

## Amazon Route 53 높은 TTL 리소스 레코드 세트

설명

더 낮은 값 time-to-live (TTL) 으로 혜택을 받을 수 있는 리소스 레코드 세트가 있는지 확인합니다.

TTL은 리소스 레코드 세트가 DNS 해석기에 의해 캐시되는 초 단위 숫자입니다. 긴 TTL을 지정하면 DNS 리졸버가 업데이트된 DNS 레코드를 요청하는 데 시간이 오래 걸리므로 트래픽 재라우팅에서 불필요한 지연이 발생할 수 있습니다. 예를 들어 긴 TTL은 DNS 장애 조치(Failover)가 엔드포인트 오류를 감지한 시점과 트래픽을 재라우팅하여 응답하는 시점 사이에 지연을 만듭니다.

AWS 서비스에서 생성한 호스팅 영역은 확인 결과에 표시되지 않습니다.

검사 ID

`C056F80cR3`

알림 기준

- 노란색: 라우팅 정책이 장애 조치로 설정된 리소스 레코드 세트의 TTL이 60초보다 깁니다.
- 노란색: 연결된 상태 확인이 있는 리소스 레코드 세트의 TTL이 60초보다 깁니다.

권장 조치

나열된 리소스 레코드 세트에 대해 TTL 값으로 60초를 입력합니다. 자세한 내용은 리소스 레코드 세트 관련 작업을 참조하세요.

추가 리소스

Amazon Route 53 상태 확인 및 DNS 장애 조치

보고서 열

- 상태 표시기
- 호스팅 영역 이름
- 호스팅 영역 ID
- 리소스 레코드 세트 이름
- 리소스 레코드 세트 유형
- 리소스 레코드 세트 ID
- TTL

## Amazon Route 53 네임 서버 위임

설명

도메인 등록 기관 또는 DNS가 올바른 Route 53 네임 서버를 사용하지 않는 Amazon Route 53 호스팅 영역이 있는지 확인합니다.

호스팅 영역을 생성할 때 Route 53은 호스팅 영역에 4개의 네임 서버 세트를 할당합니다. 해당 서버의 이름은 ns-###.awsdns-##.com, .net, .org 및 .co.uk이며, 여기서 ### 및 ##은 일반적으로 서로 다른 숫자를 나타냅니다. Route 53에서 도메인에 대한 DNS 쿼리를 라우팅하려면 등록자의 네임 서버 구성을 업데이트하여 등록 기관이 할당한 네임 서버를 제거해야 합니다. 그런 다음 Route 53 위임 집합에 네 개의 네임 서버를 모두 추가해야 합니다. 가용성을 극대화하려면 Route 53 네임 서버 4개를 모두 추가해야 합니다.

AWS 서비스에서 생성한 호스팅 영역은 확인 결과에 표시되지 않습니다.

검사 ID

cF171Db240

알림 기준

노란색: 도메인의 등록 기관이 위임 세트의 Route 53 이름 서버 4개를 모두 사용하지 않는 호스팅 영역이 있습니다.

권장 조치

등록 기관 또는 도메인의 현재 DNS 서비스로 이름 서버 레코드를 추가하거나 업데이트하여 Route 53 위임 세트의 이름 서버 4개를 모두 포함하게 합니다. 이 값을 찾으려면 호스팅 영역에 대한 이름 서버 가져오기를 참조하세요. 이름 서버 레코드를 추가 또는 업데이트하는 방법에 대한 자세한 내용은 Amazon Route 53에서 도메인 및 하위 도메인 생성 및 마이그레이션을 참조하세요.

추가 리소스

호스팅 영역 작업

보고서 열

- 호스팅 영역 이름
- 호스팅 영역 ID
- 사용된 이름 서버 위임 수

## Amazon Route 53 Resolver 엔드포인트 가용 영역 이중화

설명

서비스 구성에 이중화를 위해 최소 두 개의 가용 영역(AZ)에 지정된 IP 주소가 있는지 확인합니다. AZ는 다른 영역의 장애로부터 격리된 별개의 위치입니다. 같은 리전에 있는 다수의 AZ에서 IP 주소를 세부화하면 단일 위치에서 장애가 발생할 경우 애플리케이션을 보호할 수 있습니다.

검사 ID

Chrv231ch1

알림 기준

- 노란색: IP 주소는 한 AZ에만 지정됩니다.
- 녹색: 최소 두 개의 AZ에 IP 주소가 지정되었음

권장 조치

중복성을 위해 가용 영역 2개 이상에서 IP 주소를 지정합니다.

추가 리소스

- 항상 둘 이상의 탄력적 네트워크 인터페이스 엔드포인트를 사용할 수 있어야 하는 경우 네트워크 인터페이스를 필요한 수보다 하나 더 생성하여 트래픽 급증 가능성에 대비할 수 있는 추가 용량을 확보하는 것이 좋습니다. 또한 추가 네트워크 인터페이스는 유지 관리 또는 업그레이드와 같은 서비스 운영 중에도 가용성을 보장합니다.
- Resolver 엔드포인트의 고가용성

보고서 열

- 상태 표시기
- 지역
- 리소스 ARN
- 여러 AZ의 수

## Amazon S3 버킷 로깅

설명

Amazon Simple Storage Service(Amazon S3) 버킷의 로깅 구성을 확인합니다.

서버 액세스 로깅이 활성화되면 세부 액세스 로그가 선택한 버킷에 매시간 전송됩니다. 액세스 로그 레코드에는 요청 유형, 요청과 관련된 리소스, 요청 처리 시간과 날짜 같은 각 요청에 관한 세부 정보가 포함됩니다. 기본적으로 버킷 로깅은 활성화되지 않습니다. 보안 감사를 수행하거나 사용자 및 사용 패턴에 대해 자세히 알아보려면 로깅을 사용하도록 활성화해야 합니다.

로깅을 처음 활성화하면 구성이 자동으로 검증됩니다. 그러나 나중에 수정하면 로깅 오류가 발생할 수 있습니다. 이 검사는 명시적인 Amazon S3 버킷 권한이 있는지 검사하지만 버킷 권한을 재정의할 수 있는 연결된 버킷 정책은 검사하지 않습니다.

검사 ID

BueAdJ7NrP

알림 기준

- 노란색: 버킷에 서버 액세스 로깅이 활성화되어 있지 않습니다.
- 노란색: 대상 버킷 권한에는 루트 계정이 포함되어 있지 않으므로 확인할 Trusted Advisor 수 없습니다.
- 빨간색: 대상 버킷이 존재하지 않습니다.
- 빨간색: 대상 버킷과 소스 버킷의 소유자가 다릅니다.
- 빨간색: 로그 전달자에 대상 버킷에 대한 쓰기 권한이 없습니다.

권장 조치

대부분의 버킷에 대해 버킷 로깅을 활성화합니다. 콘솔을 이용하여 로깅 활성화와 프로그래밍 방식으로 로깅 활성화를 참조하세요.

대상 버킷 권한에 루트 계정이 포함되지 않은 상태에서 로깅 상태를 Trusted Advisor 확인하려면 루트 계정을 수혜자로 추가하십시오. 버킷 권한 편집을 참조하세요.

대상 버킷이 없는 경우 기존 버킷을 대상으로 선택하거나, 새 버킷을 생성하여 대상으로 선택합니다. 버킷 로깅 관리를 참조하세요.

대상과 소스의 소유자가 서로 다른 경우, 대상 버킷을 소스 버킷과 소유자가 같은 버킷으로 변경합니다. 버킷 로깅 관리를 참조하세요.

대상에 대한 쓰기 권한이 로그 전달자에 없는 경우(쓰기가 활성화되어 있지 않음) 로그 전달 그룹에 업로드/삭제 권한을 부여합니다. 버킷 권한 편집을 참조하세요.

추가 리소스

- 버킷을 사용한 작업
- 서버 액세스 로깅
- 서버 액세스 로그 형식
- 로그 파일 삭제

보고서 열

- 상태 표시기
- 지역
- 버킷 이름

- 대상 이름
- 대상 존재 여부
- 소유자가 동일한지 여부
- 쓰기가 활성화되어 있는지 여부
- 이유

## Amazon S3 버킷 복제가 활성화되지 않음

설명

Amazon S3 버킷에 교차 리전 복제, 동일 리전 복제 또는 둘 다에 대해 활성화된 복제 규칙이 있는지 확인합니다.

복제는 동일하거나 다른 지역의 버킷 간에 객체를 비동기식으로 자동 복사하는 것입니다. AWS 복제는 새로 생성된 객체 및 객체 업데이트를 원본 버킷에서 지정된 대상 버킷으로 복사합니다. Amazon S3 버킷 복제를 사용하면 애플리케이션 및 데이터 스토리지의 복원력과 규정 준수를 개선하는 데 도움이 됩니다.

자세한 내용은 객체 복제를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz119
```

소스

```
AWS Config Managed Rule: s3-bucket-replication-enabled
```

알림 기준

노란색: Amazon S3 버킷 복제 규칙은 교차 리전 복제, 동일 리전 복제 또는 둘 다에 대해 활성화되지 않습니다.

권장 조치

Amazon S3 버킷 복제 규칙을 활성화하여 애플리케이션 및 데이터 스토리지의 복원력과 규정 준수를 개선합니다.

자세한 내용은 백업 작업 및 복구 지점 보기 및 복제 설정을 참조하세요.

추가 리소스

연습: 복제 구성 예제

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon S3 Bucket Versioning

설명

버전 관리가 활성화되지 않았거나 버전 관리가 중지된Amazon Simple Storage Service 버킷에 대한 내결함성을 확인합니다.

버전 관리를 활성화하면 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 쉽게 복구할 수 있습니다. 버전 관리를 사용하면 버킷에 저장된 모든 버전의 객체를 모두 보존, 검색 및 복원할 수 있습니다. 객체를 Glacier 스토리지 클래스에 자동으로 아카이빙하여 수명 주기 규칙을 사용하여 객체의 모든 버전뿐만 아니라 관련 비용을 관리할 수 있습니다. 지정된 기간 후에 객체의 버전을 제거하도록 규칙을 구성할 수도 있습니다. 버킷의 객체 삭제 또는 구성 변경을 위해 멀티 팩터 인증(MFA)을 요구할 수도 있습니다.

버전 관리를 활성화한 후에는 비활성화할 수 없습니다. 그러나 새 버전의 객체가 만들어지지 않도록 일시 중단할 수 있습니다. 버전 관리를 사용하면 여러 버전의 객체 스토리지에 대한 비용을 지급하므로 Amazon S3 대한 비용이 증가할 수 있습니다.

검사 ID

```
R365s2Qddf
```

알림 기준

- 녹색: 버킷에 버전 관리가 활성화되어 있습니다.
- 노란색: 버킷에 버전 관리가 활성화되어 있지 않습니다.
- 노란색: 버킷의 버전 관리가 일시 중지되어 있습니다.

권장 조치

대부분의 버킷에 대해 버킷 버전 관리를 활성화하여 실수로 삭제하거나 덮어쓰지 않도록 합니다. 버전 관리 사용과 프로그래밍 방식으로 버전 관리 활성화를 참조하세요.

버킷 버전 관리가 일시 중지된 경우 버전 관리를 다시 활성화하는 것이 좋습니다. 버전 관리가 일시 중지된 버킷의 객체 작업에 대한 자세한 내용은 버전 관리가 일시 중지된 버킷의 객체 관리를 참조하세요.

버전 관리가 활성화되거나 일시 중지된 경우, 특정 객체 버전을 만료된 것으로 표시하거나 필요 없는 객체 버전을 영구적으로 제거하는 수명 주기 구성 규칙을 정의할 수 있습니다. 자세한 내용은 객체 수명 주기 관리를 참조하세요.

버킷의 버전 관리 상태가 변경되거나 객체의 버전이 삭제된 경우 MFA Delete는 추가 인증을 요구합니다. 사용자가 승인된 인증 디바이스의 자격 증명과 코드를 입력하도록 요구합니다. 자세한 내용은 MFA Delete 단원을 참조하십시오.

추가 리소스

버킷을 사용한 작업

보고서 열

- 상태 표시기
- 지역
- 버킷 이름
- 버전 관리
- MFA Delete 활성화됨

## 여러 가용 영역에 걸쳐 있지 않은 Application, Network Balancer 및 Gateway Load Balancer

설명

로드 밸런서(애플리케이션, 네트워크, 게이트웨이 로드 밸런서)가 여러 가용 영역에 걸쳐 서브넷으로 구성되어 있는지 확인합니다.

AWS Config 규칙의 최소 AvailabilityZones 파라미터에 원하는 최소 가용 영역을 지정할 수 있습니다.

자세한 내용은 Application Load Balancer의 가용 영역, 가용 영역 - Network Load Balancer, 게이트웨이 로드 밸런서 생성을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz169`

소스

`AWS Config Managed Rule: elbv2-multiple-az`

알림 기준

노란색: 2개 미만의 가용 영역에 서브넷으로 구성된 애플리케이션, 네트워크 또는 게이트웨이 로드 밸런서.

권장 조치

여러 가용 영역의 서브넷으로 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서를 구성합니다.

추가 리소스

Application Load Balancer 가용 영역

가용 영역(Elastic Load Balancing)

Gateway Load Balancer 생성

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙

- 입력 파라미터
- 최종 업데이트 시간

## 서브넷에서 사용 가능한 IP Auto Scaling

설명

대상 서브넷에 사용 가능한 IP가 충분히 남아 있는지 확인합니다. 사용할 수 있는 충분한 IP가 있으면 Auto Scaling Group이 최대 크기에 도달하여 추가 인스턴스를 시작해야 할 때 도움이 됩니다.

검사 ID

`Cjxm268ch1`

알림 기준

- 빨간색: ASG에서 생성할 수 있는 최대 인스턴스 및 IP 주소 수가 구성된 서브넷에 남아 있는 IP 주소 수를 초과합니다.
- 녹색: ASG에서 가능한 나머지 규모에 사용할 수 있는 IP 주소가 충분합니다.

권장 조치

사용 가능한 IP 주소의 수 증가

보고서 열

- 상태 표시기
- 지역
- 리소스 ARN
- 생성할 수 있는 최대 인스턴스 수
- 사용 가능한 인스턴스 수

## Auto Scaling 그룹 상태 확인

설명

Auto Scaling 그룹의 상태 확인 구성을 검사합니다.

Auto Scaling 그룹에 Elastic Load Balancing 사용하는 경우 구성할 때 Elastic Load Balancing 상태 확인을 활성화하는 것이 좋습니다. Elastic Load Balancing 상태 확인을 사용하지 않는 경우 Auto Scaling 은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 상태에 따라서만 작동할 수 있습니다. Auto Scaling은 인스턴스에서 실행되는 애플리케이션에서는 작동하지 않습니다.

검사 ID

CL0G40CD08

알림 기준

- 노란색: 오토 스케일링 그룹에 연결된 로드 밸런서가 있지만 Elastic Load Balancing 상태 확인이 활성화되어 있지 않습니다.
- 노란색: 오토 스케일링 그룹에 연결된 로드 밸런서가 없지만 Elastic Load Balancing 상태 확인이 활성화되어 있습니다.

권장 조치

오토 스케일링 그룹에 연결된 로드 밸런서가 있지만 Elastic Load Balancing 상태 확인이 활성화되어 있지 않은 경우 Auto Scaling 그룹에 Elastic Load Balancing 상태 확인 추가를 참조하세요.

Elastic Load Balancing 상태 확인이 활성화되어 있지만 오토 스케일링 그룹에 연결된 로드 밸런서가 없는 경우 자동 조정 및 로드 밸런싱된 애플리케이션 설정을 참조하세요.

추가 리소스

Amazon EC2 Auto Scaling 사용 설명서

보고서 열

- 상태 표시기
- 지역
- 오토 스케일링 그룹 이름
- 연결된 로드 밸런서
- 상태 확인

## Auto Scaling 그룹 리소스

설명

시작 구성 및 Auto Scaling 그룹과 연결된 리소스의 가용성을 확인합니다.

사용할 수 없는 리소스를 가리키는 Auto Scaling 그룹은 새 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 시작할 수 없습니다. Auto Scaling을 적절히 구성하면 수요가 급증할 때 Amazon EC2 인스턴스 수가 원활하게 증가하고 수요가 감소하면 자동으로 감소합니다. 사용할 수 없는 리소스를 가리키는 Auto Scaling 그룹 및 시작 구성은 의도한 대로 작동하지 않습니다.

검사 ID

8CNsSllI5v

알림 기준

- 빨간색: 오토 스케일링 그룹이 삭제된 로드 밸런서와 연결되어 있습니다.
- 빨간색: 시작 구성이 삭제된 Amazon Machine Image(AMI)와 연결되어 있습니다.

권장 조치

로드 밸런서가 삭제된 경우, 새 로드 밸런서 또는 대상 그룹을 생성한 다음 이를 Auto Scaling 그룹에 연결하거나 로드 밸런서 없이 새 Auto Scaling 그룹을 생성합니다. 새 로드 밸런서를 사용하여 새 오토 스케일링 그룹을 생성하는 방법에 대한 자세한 내용은 자동 조정 및 로드 밸런싱된 애플리케이션 설정을 참조하세요. 로드 밸런서 없이 새 오토 스케일링 그룹을 생성하는 방법에 대한 자세한 내용은 콘솔을 사용하여 오토 스케일링 시작하기에서 오토 스케일링 그룹 생성을 참조하세요.

AMI가 삭제된 경우, 유효한 AMI를 사용하여 새 시작 템플릿 또는 시작 템플릿 버전을 생성하고 이를 Auto Scaling 그룹과 연결합니다. 콘솔을 사용하여 오토 스케일링 시작하기에서 시작 구성 생성을 참조하세요.

추가 리소스

- 오토 스케일링 문제 해결: Amazon EC2 AMI
- 오토 스케일링 문제 해결: 로드 밸런서 구성
- Amazon EC2 Auto Scaling 사용 설명서

보고서 열

- 상태 표시기
- 지역
- 오토 스케일링 그룹 이름
- 시작 유형
- 리소스 유형
- Resource Name

## 단일 AZ에서 HSM 인스턴스를 실행하는AWS CloudHSM 클러스터

설명

단일 가용 영역(AZ)에서 HSM 인스턴스를 실행하는 클러스터를 확인합니다. 이 검사는 클러스터에 최신 백업이 없을 위험이 있는 경우 경고를 표시합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`hc0dfs7601`

알림 기준

- 노란색: CloudHSM 클러스터가 단일 가용 영역의 모든 HSM 인스턴스를 1시간 넘게 실행하고 있습니다.
- 녹색: CloudHSM 클러스터가 서로 다른 두 개 이상의 가용 영역에 있는 모든 HSM 인스턴스를 실행하고 있습니다.

권장 조치

다른 가용 영역에서 클러스터에 대해 하나 이상의 인스턴스를 생성합니다.

추가 리소스

에 대한 모범 사례 AWS CloudHSM

보고서 열

- 상태 표시기
- 지역
- 클러스터 ID
- HSM 인스턴스 개수
- 최종 업데이트 시간

## AWS Direct Connect 위치 레질리언스

설명

온프레미스를 각 Direct Connect 게이트웨이 또는 가상 프라이빗 게이트웨이에 연결하는 AWS Direct Connect 데 사용되는 사용자의 복원력을 확인합니다.

이 검사는 Direct Connect 게이트웨이 또는 가상 프라이빗 게이트웨이가 최소 두 개의 개별 Direct Connect 위치에 걸쳐 가상 인터페이스로 구성되지 않은 경우 경고를 표시합니다. 위치 복원력이 부족하면 유지 관리 중 예상치 못한 가동 중지, 광케이블 절단, 장치 장애 또는 전체 위치 장애가 발생할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다.

> **Note**
>
> 다이렉트 커넥트는 다이렉트 커넥트 게이트웨이를 사용하여 Transit Gateway와 함께 구현됩니다.

검사 ID

`c1dfpnchv2`

알림 기준

빨간색: Direct Connect 게이트웨이 또는 가상 사설 게이트웨이는 단일 Direct Connect 장치에 하나 이상의 가상 인터페이스로 구성되어 있습니다.

노란색: Direct Connect 게이트웨이 또는 가상 사설 게이트웨이는 단일 Direct Connect 위치의 여러 Direct Connect 장치에 걸친 가상 인터페이스로 구성되어 있습니다.

녹색: Direct Connect 게이트웨이 또는 가상 사설 게이트웨이는 두 개 이상의 개별 Direct Connect 위치에 걸친 가상 인터페이스로 구성되어 있습니다.

권장 조치

Direct Connect 위치 복원력을 구축하려면 Direct Connect 게이트웨이 또는 가상 프라이빗 게이트웨이가 최소 두 개의 개별 Direct Connect 위치에 연결하도록 구성할 수 있습니다. 자세한 내용은 AWS Direct Connect 복원력 권장 사항을 참조하십시오.

추가 리소스

AWS Direct Connect 레질리언스 권장 사항

AWS Direct Connect 페일오버 테스트

보고서 열

- 상태 표시기
- 지역
- 최종 업데이트 시간
- 레질리언스 상태
- 위치
- 연결 ID
- 게이트웨이 ID

## AWS Lambda 데드레터 대기열이 구성되지 않은 기능

설명

AWS Lambda 함수가 데드레터 큐로 구성되어 있는지 확인합니다.

데드레터 큐는 실패한 이벤트를 캡처 및 분석하여 AWS Lambda 해당 이벤트를 적절하게 처리할 수 있는 기능을 제공합니다. 코드에서 예외가 발생하거나, 시간 초과가 발생하거나, 메모리가 부족하여 Lambda 함수의 비동기 실행이 실패할 수 있습니다. DLQ(Dead Letter Queue)는 실패한 간접 호출의 메시지를 저장하여 메시지를 처리하고 실패 문제를 해결하는 방법을 제공합니다.

규칙의 DLQarns 파라미터를 사용하여 확인하려는 데드레터 큐 리소스를 지정할 수 있습니다. AWS Config

자세한 내용은 DLQ(Dead Letter Queue)를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz182
```

소스

```
AWS Config Managed Rule: lambda-dlq-check
```

알림 기준

노란색: AWS Lambda 함수에 데드레터 대기열이 구성되어 있지 않습니다.

권장 조치

AWS Lambda 함수에 실패한 모든 비동기 호출에 대한 메시지 처리를 제어하도록 데드레터 대기열이 구성되어 있는지 확인하십시오.

자세한 내용은 DLQ(Dead Letter Queue)를 참조하세요.

추가 리소스

- AWS Lambda DLQ(Dead Letter Queue)를 사용한 강력한 서버리스 애플리케이션 설계

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## AWS Lambda 장애 발생 시: 이벤트 목적지

설명

계정의 Lambda 함수에 On Failure 이벤트 대상 또는 DLQ(Dead Letter Queue)가 비동기 호출을 위해 구성되어 있는지 확인하여 실패한 간접 호출의 레코드가 추가 조사 또는 처리를 위해 대상으로 라우팅될 수 있도록 합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1dfprch05`

알림 기준

- 노란색: 함수에 On Failure 이벤트 대상 또는 DLQ가 구성되어 있지 않습니다.

권장 조치

추가 디버깅 또는 처리를 위해 Lambda 함수가 다른 세부 정보와 함께 실패한 호출을 사용 가능한 대상 AWS 서비스 중 하나로 전송하도록 On Failure 이벤트 목적지 또는 DLQ를 설정하십시오.

추가 리소스

- 비동기 호출
- AWS Lambda 장애 발생 시: 이벤트 목적지

보고서 열

- 상태 표시기
- 지역
- 버전이 플래그가 지정된 함수입니다.
- 현재 날짜의 비동기 요청 감소율
- 현재 날짜의 비동기 요청
- 평균 일일 비동기 요청 감소율
- 평균 일일 비동기 요청
- 최종 업데이트 시간

## 다중 AZ 이중화 기능이 없는AWS Lambda VPC 지원 함수

설명

단일 가용 영역에서 서비스 중단에 취약한 VPC 지원 Lambda 함수의 $LATEST 버전을 확인합니다. 고가용성을 위해 VPC 지원 기능을 여러 가용 영역에 연결하는 것이 가장 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

L4dfs2Q4C6

알림 기준

노란색: VPC 지원 Lambda 함수의 $LATEST 버전은 단일 가용 영역의 서브넷에 연결되어 있습니다.

권장 조치

VPC에 액세스하기 위한 함수를 구성할 때는 여러 가용 영역의 서브넷을 선택하여 고가용성을 보장합니다.

추가 리소스

- VPC에서 리소스에 액세스하도록 Lambda 함수 구성
- 의 레질리언스 AWS Lambda

보고서 열

- 상태 표시기
- 지역
- 함수 ARN
- VPC ID
- 평균 일일 호출 건수
- 최종 업데이트 시간

## AWS Resilience Hub 애플리케이션 구성 요소 검사

설명

애플리케이션의 애플리케이션 구성 요소 (AppComponent) 를 복구할 수 없는지 확인합니다. 장애 발생 시 AppComponent 복구되지 않으면 알 수 없는 데이터 손실과 시스템 다운타임이 발생할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다.

검사 ID

RH23stmM04

알림 기준

빨간색: 복구할 수 AppComponent 없습니다.

권장 조치

복구 가능한지 확인하려면 복원력 권장 사항을 검토 및 구현한 다음 새 평가를 실행하십시오 AppComponent . 복원력 권장 사항 검토에 대한 자세한 내용은 추가 리소스를 참조하십시오.

추가 리소스

복원력 권장 사항 검토

AWS Resilience Hub 개념

AWS Resilience Hub 사용 설명서

보고서 열

- 상태 표시기
- 지역
- 애플리케이션 이름
- AppComponent 이름
- 최종 업데이트 시간

## AWS Resilience Hub 정책 위반

설명

정책이 정의하는 Recovery Time Objective(RTO) 및 Recovery Point Objective(RPO)를 충족하지 않는 애플리케이션에 대해 Resilience Hub를 검사합니다. 애플리케이션이 Resilience Hub에서 애플리케이션에 대해 설정한 RTO 및 RPO 목표를 충족하지 않는 경우 검사에서 경고합니다.

> **Note**
>
> 해당 검사의 결과는 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

RH23stmM02

알림 기준

- 녹색: 애플리케이션에 정책이 있으며 RTO 및 RPO 목표를 충족합니다.
- 노란색: 애플리케이션이 아직 평가되지 않았습니다.
- 빨간색: 애플리케이션에 정책이 있지만 RTO 및 RPO 목표를 충족하지 못합니다.

권장 조치

Resilience Hub 콘솔에 로그인하고 권장 사항을 검토하여 애플리케이션이 RTO 및 RPO 목표를 충족하는지 확인하세요.

추가 리소스

Resilience Hub 개념

보고서 열

- 상태 표시기
- 지역
- 애플리케이션 이름
- 최종 업데이트 시간

## AWS Resilience Hub 레질리언스 점수

설명

Resilience Hub에서 애플리케이션에 대한 평가를 실행했는지 확인합니다. 이 검사는 복원력 점수가 특정 값보다 낮으면 경고합니다.

> **Note**
>
> 해당 검사의 결과는 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

RH23stmM01

알림 기준

- 녹색: 애플리케이션의 복원력 점수가 70 이상입니다.
- 노란색: 애플리케이션의 복원력 점수가 40~69입니다.
- 노란색: 애플리케이션이 아직 평가되지 않았습니다.
- 노란색: 애플리케이션의 복원력 점수가 40 미만입니다.

권장 조치

Resilience Hub 콘솔에 로그인하고 애플리케이션에 대한 평가를 실행합니다. 권장 사항을 검토하여 복원력 점수를 개선하세요.

추가 리소스

Resilience Hub 개념

보고서 열

- 상태 표시기
- 지역
- 애플리케이션 이름
- 애플리케이션 복원력 점수
- 최종 업데이트 시간

## AWS Resilience Hub 평가 연령

설명

애플리케이션 평가를 마지막으로 실행한 지 얼마나 지났는지 확인합니다. 이 검사는 지정된 일수 동안 애플리케이션 평가를 실행하지 않은 경우 알려줍니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`RH23stmM03`

알림 기준

- 녹색: 지난 30일 동안 애플리케이션 평가를 실행했습니다.
- 노란색: 지난 30일 동안 애플리케이션 평가가 실행되지 않았습니다.

권장 조치

Resilience Hub 콘솔에 로그인하고 애플리케이션에 대한 평가를 실행합니다.

추가 리소스

Resilience Hub 개념

보고서 열

- 상태 표시기
- 지역
- 애플리케이션 이름
- 마지막 평가 실행 이후 일수
- 마지막 평가 실행 시간
- 최종 업데이트 시간

## AWS Site-to-Site VPN DOWN 상태의 터널이 하나 이상 있음

설명

각 터널에 대해 활성 상태인 터널의 수를 확인합니다 AWS Site-to-Site VPN.

VPN에는 항상 두 개의 터널이 구성되어 있어야 합니다. 이것은 AWS 엔드포인트에서 장치의 중단 또는 계획된 유지 관리의 경우 이중성을 제공합니다. 일부 하드웨어의 경우 한 번에 하나의 터널만 활성화됩니다. VPN에 활성 터널이 없는 경우 VPN에 대한 요금이 계속 적용될 수 있습니다.

자세한 내용은 AWS Site-to-Site VPN란 무엇입니까?를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz123
```

소스

```
AWS Config Managed Rule: vpc-vpn-2-tunnels-up
```

알림 기준

노란색: Site-to-Site VPN에는 하나 이상의 터널이 다운되어 있습니다.

권장 조치

VPN 연결을 위해 두 개의 터널이 구성되어 있는지 확인하세요. 그리고 하드웨어가 지원하는 경우 두 터널이 모두 활성 상태인지 확인합니다. VPN 연결이 더 이상 필요하지 않으면 요금이 발생하지 않도록 삭제합니다.

자세한 내용은 고객 게이트웨이 디바이스 및 AWS 지식 센터에서 제공되는 콘텐츠를 참조하세요.

추가 리소스

- AWS Site-to-Site VPN 사용 설명서
- VPC에 가상 프라이빗 게이트웨이 추가

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## 안정성에 대한 AWS Well-Architected 위험도 높음 문제

설명

안정성 기반에서 워크로드의 위험도 높음 문제(HRI)를 확인합니다. 이 검사는 사용자 AWS-Well Architected 리뷰를 기반으로 합니다. AWS Well-Architected에서 워크로드 평가를 완료했는지 여부에 따라 검사 결과가 달라집니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`Wxdfp4B1L4`

알림 기준

- 빨간색: AWS Well-Architected의 안정성 항목에서 적어도 하나의 활성 고위험 문제가 확인되었습니다.
- 녹색: AWS Well-Architected의 안정성 원칙에서 활발한 고위험 문제는 발견되지 않았습니다.

권장 조치

AWS Well-Architected는 워크로드 평가 중에 고위험 문제를 감지했습니다. 이러한 문제는 위험을 줄이고 비용을 절감할 수 있는 기회를 나타냅니다. AWS Well-Architected 도구에 로그인하여 답변을 검토하고 활성 문제를 해결하기 위한 조치를 취하세요.

보고서 열

- 상태 표시기
- 지역
- 워크로드 ARN
- 워크로드 이름
- 검토자 이름
- 워크로드 유형
- 워크로드 시작 날짜
- 워크로드 마지막 수정 날짜
- 신뢰성에 대해 식별된 HRI 수
- 신뢰성에 대해 해결된 HRI 수
- 신뢰성에 대해 답변된 질문 수
- 신뢰성 원칙의 총 질문 수
- 최종 업데이트 시간

## Classic Load Balancer에는 다중 AZ가 구성되어 있지 않습니다

### 설명

Classic Load Balancer가 여러 가용 영역(AZ)에 걸쳐 있는지 확인합니다.

로드 밸런서는 여러 가용 영역에서 여러 Amazon EC2 인스턴스에 수신 애플리케이션 트래픽을 분산합니다. 기본적으로 로드 밸런서는 사용자의 로드 밸런서에 대해 활성화된 가용 영역에 트래픽을 고르게 분산합니다. 가용 영역 중 하나에 장애가 발생할 경우 로드 밸런서 노드는 자동으로 하나 이상의 가용 영역에서 정상 상태의 등록 인스턴스로 요청을 전달합니다.

규칙의 최소 AvailabilityZones 파라미터를 사용하여 최소 가용 영역 수를 조정할 수 있습니다. AWS Config

자세한 내용은 Classic Load Balancer란 무엇입니까?를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

### 검사 ID

```
c18d2gz154
```

### 소스

```
AWS Config Managed Rule: clb-multiple-az
```

### 알림 기준

노란색: Classic Load Balancer에 다중 AZ가 구성되어 있지 않거나 지정된 최소 AZ 수를 충족하지 않습니다.

### 권장 조치

클래식 로드 밸런서에 여러 가용 영역이 구성되어 있는지 확인하세요. 로드 밸런서를 여러 AZ로 확장하여 애플리케이션의 가용성이 높은지 확인하십시오.

자세한 내용은 튜토리얼: Classic Load Balancer 생성을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## ELB Connection Draining

설명

Connection Draining이 활성화되지 않은 로드 밸런서를 확인합니다.

Connection Draining이 활성화되지 않고 로드 밸런서에서 Amazon EC2 인스턴스의 등록을 취소하면 로드 밸런서가 해당 인스턴스로 트래픽 라우팅을 중지하고 연결을 닫습니다. Connection Draining이 활성화되면 로드 밸런서는 등록 취소된 인스턴스로 새 요청 전송하기를 중지하지만 활성 요청을 처리하기 위해 연결을 계속 열어 둡니다.

검사 ID

`7qGXsKIUw`

알림 기준

노란색: 로드 밸런서에 대해 Connection Draining이 활성화되지 않았습니다.

권장 조치

로드 밸런서에 대해 Connection Draining을 활성화합니다. 자세한 내용은 Connection Draining과 로드 밸런서에 대한 Connection Draining 활성화 또는 비활성화를 참조하세요.

추가 리소스

Elastic Load Balancing 개념

보고서 열

- 상태 표시기
- 지역
- load-balancer-name

- 이유

## Load Balancer 최적화

설명

로드 밸런서 구성을 확인합니다.

Elastic Load Balancing을 사용할 때 Amazon Elastic Compute Cloud(Amazon EC2)에서 내결함성 수준을 높이려면 한 리전의 여러 가용 영역에서 동일한 수의 인스턴스를 실행하는 것이 좋습니다. 구성된 로드 밸런서는 요금이 발생하므로 비용 최적화 검사도 됩니다.

검사 ID

`iqdCTZKCUp`

알림 기준

- 노란색: 로드 밸런서가 단일 가용 영역에 대해 활성화되어 있습니다.
- 노란색: 활성 인스턴스가 없는 가용 영역에 대해 로드 밸런서가 활성화되어 있습니다.
- 노란색: 로드 밸런서에 등록된 Amazon EC2 인스턴스가 여러 가용 영역 전체에 고르게 분산되어 있지 않습니다. 사용된 가용 영역에서 가장 많은 인스턴스 수와 가장 적은 인스턴스 수의 차이가 1 이상이며, 이 차이는 가장 많은 수의 20% 이상입니다.

권장 조치

로드 밸런서가 최소 2개의 가용 영역에서 활성 상태의 정상 인스턴스를 가리키는지 확인합니다. 자세한 내용은 가용 영역 추가를 참조하세요.

정상 상태의 인스턴스가 없는 가용 영역에 대해 로드 밸런서가 구성되어 있거나, 여러 가용 영역 전체에 걸쳐 인스턴스가 불균형하게 분산되어 있는 경우 모든 가용 영역이 필요한지 확인합니다. 불필요한 가용 영역을 생략하고 나머지 가용 영역에 인스턴스가 균형 있게 분산되도록 해야 합니다. 자세한 내용은 가용 영역 제거를 참조하세요.

추가 리소스

- 가용 영역 및 리전
- 로드 밸런서 관리
- Elastic Load Balancing 평가의 모범 사례

보고서 열

- 상태 표시기
- 지역

- 로드 밸런서 이름
- 영역 수
- 영역 a 인스턴스
- 영역 b 인스턴스
- 영역 c 인스턴스
- 영역 d 인스턴스
- 영역 e 인스턴스
- 영역 f 인스턴스
- 이유

## NAT 게이트웨이 AZ 독립성

### 설명

NAT 게이트웨이가 가용 영역(AZ) 독립성을 갖도록 구성되어 있는지 확인합니다.

NAT 게이트웨이를 사용하면 프라이빗 서브넷의 리소스를 NAT 게이트웨이의 IP 주소를 사용하여 서브넷 외부의 서비스에 안전하게 연결하고 원치 않는 인바운드 트래픽을 차단할 수 있습니다. 각 NAT 게이트웨이는 지정된 가용 영역(AZ) 내에서 작동하며 해당 AZ에서만 이중화를 통해 구축됩니다. 따라서 특정 AZ의 리소스는 동일한 AZ의 NAT 게이트웨이를 사용해야 합니다. 그래야 NAT 게이트웨이 또는 해당 AZ의 잠재적 중단이 다른 AZ의 리소스에 영향을 미치지 않습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

### 검사 ID

`c1dfptbg10`

### 알림 기준

- 빨간색: 한 AZ에 있는 서브넷의 트래픽이 다른 AZ의 NATGW를 통해 라우팅되고 있습니다.
- 녹색: 한 AZ의 서브넷에서 나오는 트래픽이 동일한 AZ의 NATGW를 통해 라우팅되고 있습니다.

권장 조치

서브넷의 AZ를 확인하고 동일한 AZ의 NAT 게이트웨이를 통해 트래픽을 라우팅하십시오.

AZ에 NATGW가 없는 경우 NATGW를 생성한 다음 이를 통해 서브넷 트래픽을 라우팅하십시오.

서로 다른 AZ의 서브넷 간에 동일한 라우팅 테이블이 연결되어 있는 경우 이 라우팅 테이블을 NAT 게이트웨이와 동일한 AZ에 있는 서브넷에 연결하고 다른 AZ의 서브넷에 대해서는 별도의 라우팅 테이블을 이 다른 AZ의 NAT 게이트웨이에 대한 경로와 연결하세요.

Amazon VPC의 아키텍처 변경을 위한 유지 관리 기간을 선택하는 것이 좋습니다.

추가 리소스

- NAT 게이트웨이를 생성하는 방법
- 다양한 NAT 게이트웨이 사용 사례에 맞게 경로를 구성하는 방법

보고서 열

- 상태 표시기
- 지역
- NAT 가용 영역
- NAT ID
- 가용 영역 서브넷
- 서브넷 ID
- 라우팅 테이블 ID
- NAT ARN
- 최종 업데이트 시간

## Network Load Balancer 교차 로드 밸런싱

설명

Network Load Balancer에서 교차 영역 로드 밸런싱의 활성화 여부를 확인합니다.

교차 영역 로드 밸런싱은 여러 가용 영역의 인스턴스 간에 들어오는 트래픽을 균일하게 분산하는 데 도움이 됩니다. 이렇게 하면 로드 밸런서가 모든 트래픽을 동일한 가용 영역의 인스턴스로 라우팅하지 못하여 트래픽이 고르지 않고 과부하가 발생할 수 있습니다. 또한 이 기능은 단일 가용 영역에 장애가 발생하는 경우 다른 가용 영역의 정상 인스턴스로 트래픽을 자동으로 라우팅하여 애플리케이션 안정성을 높여줍니다.

자세한 내용은 교차 영역 로드 밸런싱을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz105`

소스

`AWS Config Managed Rule: nlb-cross-zone-load-balancing-enabled`

알림 기준

- 노란색: Network Load Balancer에는 영역 간 부하 분산이 활성화되어 있지 않습니다.

권장 조치

Network Load Balancer에서 교차 영역 로드 밸런싱이 활성화되어 있는지 확인합니다.

추가 리소스

교차 영역 로드 밸런싱(Network Load Balancer)

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## NLB - 프라이빗 서브넷의 인터넷 연결 리소스

설명

인터넷 연결 NLB (Network Load Balancer) 가 프라이빗 서브넷으로 구성되어 있는지 확인합니다. 트래픽을 수신하려면 퍼블릭 서브넷에 인터넷 연결 NLB (Network Load Balancer) 를 구성해야 합

니다. 퍼블릭 서브넷은 인터넷 게이트웨이로 직접 연결되는 서브넷으로 정의됩니다. 서브넷이 사설로 구성된 경우 가용 영역 (AZ) 에 트래픽이 수신되지 않아 가용성 문제가 발생할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c1dfpnchv4

알림 기준

빨간색: NLB는 하나 이상의 프라이빗 서브넷으로 구성되어 있습니다.

녹색: 인터넷 연결 NLB에 대해 구성된 프라이빗 서브넷이 없습니다.

권장 조치

인터넷 연결 로드 밸런서에 구성된 서브넷이 공용인지 확인하십시오. 퍼블릭 서브넷은 인터넷 게이트웨이로 직접 연결되는 서브넷으로 정의됩니다. 다음 옵션 중 하나를 사용하십시오.

- 새 로드 밸런서를 만들고 인터넷 게이트웨이로 직접 연결되는 다른 서브넷을 선택합니다.
- 현재 로드 밸런서에 연결되어 있는 서브넷을 사설에서 공용으로 변경합니다. 이렇게 하려면 라우팅 테이블을 변경하고 인터넷 게이트웨이를 연결하세요.

추가 리소스

- 로드 밸런서와 리스너를 구성합니다.
- VPC용 서브넷
- 게이트웨이를 라우팅 테이블에 연결

보고서 열

- 상태 표시기
- 지역
- NLB Arn
- NLB 이름
- 서브넷 ID
- NLB 제도

- 서브넷 유형
- 최종 업데이트 시간

## NLB 멀티-AZ

설명

네트워크 로드 밸런서가 두 개 이상의 가용 영역 (AZ) 을 사용하도록 구성되어 있는지 확인합니다. AZ는 다른 영역의 장애로부터 격리된 별개의 위치입니다. 동일한 지역의 여러 AZ에 로드 밸런서를 구성하면 워크로드 가용성을 개선하는 데 도움이 됩니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1dfprch09`

알림 기준

노란색: NLB는 단일 AZ에 있습니다.

녹색: NLB에는 AZ가 두 개 이상 있습니다.

권장 조치

로드 밸런서가 최소 두 개의 가용 영역으로 구성되어 있는지 확인하세요.

추가 리소스

자세한 내용은 다음 설명서를 참조하세요.

- 가용 영역
- AWS Well-Architected - 워크로드를 여러 위치에 배포
- 리전 및 가용 영역

보고서 열

- 상태 표시기

- 지역
- 여러 AZ의 수
- NLB ARN
- NLB 이름
- 최종 업데이트 시간

## AWS 리전 인시던트 관리자 복제 세트의 수

설명

인시던트 관리자 복제 세트의 구성이 지역별 장애 조치 및 대응을 지원하는 AWS 리전 데 둘 이상을 사용하는지 확인합니다. CloudWatch 경보나 EventBridge 이벤트로 인해 발생한 인시던트의 경우 Incident Manager는 경보 또는 이벤트 AWS 리전 규칙과 동일한 방식으로 인시던트를 생성합니다. 해당 리전에서 Incident Manager를 일시적으로 사용할 수 없는 경우 시스템은 복제 세트의 다른 리전에 인시던트를 생성하려고 시도합니다. 복제 세트에 한 지역만 포함된 경우 인시던트 관리자를 사용할 수 없는 동안에는 시스템이 인시던트 레코드를 만들지 못합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`cIdfp1js9r`

알림 기준

- 녹색: 복제 세트에 두 개 이상의 지역이 포함되어 있습니다.
- 노란색: 복제 세트에 한 개의 지역이 포함되어 있습니다.

권장 조치

복제 세트에 하나 이상의 지역을 추가합니다.

추가 리소스

자세한 내용은 교차 리전 인시던트 관리를 참조하세요.

보고서 열

- 상태 표시기
- 다중 지역
- 복제 세트
- 최종 업데이트 시간

## 단일 AZ 애플리케이션 검사

설명

송신 네트워크 트래픽이 단일 가용 영역(AZ)을 통해 라우팅되고 있는지 네트워크 패턴을 확인합니다.

AZ는 다른 영역에 미치는 영향으로부터 격리된 별개의 위치입니다. 서비스를 여러 AZ에 분산하면 AZ 고장의 폭발 반경을 제한할 수 있습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1dfptbg11`

알림 기준

- 노란색: 관찰된 egress 네트워크 패턴을 기반으로 애플리케이션을 하나의 AZ에만 배포할 수 있습니다. 이것이 참이고 애플리케이션이 고가용성을 기대한다면 애플리케이션 리소스를 프로비저닝하고 네트워크 흐름을 구현하여 여러 가용 영역을 활용하는 것이 좋습니다.

권장 조치

애플리케이션에 고가용성이 필요한 경우 고가용성을 위한 다중 AZ 아키텍처를 구현해 보십시오.

보고서 열

- 상태 표시기
- 지역

- VPC ID
- 최종 업데이트 시간

## 여러 AZ의 VPC 인터페이스 엔드포인트 네트워크 인터페이스

설명

AWS PrivateLink VPC 인터페이스 엔드포인트가 두 개 이상의 가용 영역 (AZ) 을 사용하도록 구성되어 있는지 확인합니다. AZ는 다른 영역의 장애로부터 격리된 별개의 위치입니다. 이는 동일 지역의 AZ 간 저렴하고 지연 시간이 짧은 네트워크 연결을 지원합니다. AWS 인터페이스 엔드포인트를 생성할 때 여러 AZ의 서브넷을 선택하면 단일 장애 지점으로부터 애플리케이션을 보호하는 데 도움이 됩니다.

> **Note**
>
> 이 검사에는 현재 인터페이스 엔드포인트만 포함됩니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1dfprch10`

알림 기준

노란색: VPC 엔드포인트가 단일 AZ에 있습니다.

녹색: VPC 엔드포인트가 최소 두 개의 AZ에 있습니다.

권장 조치

VPC 인터페이스 엔드포인트가 최소 두 개의 가용 영역으로 구성되어 있는지 확인하십시오.

추가 리소스

자세한 내용은 다음 설명서를 참조하세요.

- 인터페이스 AWS VPC 엔드포인트를 사용하여 서비스에 액세스
- 엔드포인트 네트워크 인터페이스의 프라이빗 IP 주소
- AWS PrivateLink 개념
- 리전 및 가용 영역

보고서 열

- 상태 표시기
- 지역
- VPC 엔드포인트 ID
- 멀티 AZ인가요?
- 최종 업데이트 시간

## VPN 터널 이중성

설명

각 VPN에 대해 활성 상태인 터널 수를 확인합니다.

VPN에는 항상 두 개의 터널이 구성되어 있어야 합니다. 이것은 AWS 종단점에서 장치의 중단 또는 계획된 유지 관리의 경우 이중성을 제공합니다. 일부 하드웨어의 경우 한 번에 하나의 터널만 활성화됩니다. VPN에 활성 터널이 없는 경우 VPN에 대한 요금이 계속 적용될 수 있습니다. 자세한 내용은 AWS Client VPN 관리자 안내서를 참조하십시오.

검사 ID

`S45wrEXrLz`

알림 기준

- 노란색: VPN에 활성 터널이 하나 있습니다(일부 하드웨어의 경우 정상).
- 노란색: VPN에 활성 터널이 없습니다.

권장 조치

VPN 연결에 2개의 터널이 구성되어 있고, 하드웨어에서 지원하는 경우 두 터널이 모두 활성화되어 있는지 확인합니다. VPN 연결이 더 이상 필요하지 않으면 요금이 발생하지 않도록 삭제할 수 있습니다. 자세한 내용은 고객 게이트웨이 또는 VPN 연결 삭제를 참조하세요.

추가 리소스

- AWS 사이트-투-사이트 VPN 사용자 가이드
- VPC에 하드웨어 가상 프라이빗 게이트웨이 추가

보고서 열

- 상태 표시기
- 지역
- VPN ID
- VPC
- 가상 프라이빗 게이트웨이
- 고객 게이트웨이
- 활성 터널
- 이유

## ActiveMQ 가용 영역 이중화

설명

ActiveMQ용 Amazon MQ 브로커가 여러 가용 영역에 액티브/스탠바이 브로커와 함께 고가용성을 제공하도록 구성되어 있는지 확인합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1t3k8mqv1`

알림 기준

- 노란색: ActiveMQ용 Amazon MQ의 브로커가 단일 가용 영역에 구성되어 있습니다.

  녹색: ActiveMQ용 Amazon MQ 브로커가 최소 2개의 가용 영역에 구성되어 있습니다.

권장 조치

액티브/스탠바이 배포 모드로 새 브로커를 생성합니다.

추가 리소스

- ActiveMQ 브로커 생성

보고서 열

- 상태 표시기
- 지역
- ActiveMQ 브로커 ID
- 브로커 엔진 유형
- 배포 모드
- 최종 업데이트 시간

## RabbitMQ 가용 영역 이중화

설명

RabbitMQ용 Amazon MQ 브로커가 여러 가용 영역의 클러스터 인스턴스와 함께 고가용성을 제공하도록 구성되어 있는지 확인합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c1t3k8mqv2`

알림 기준

- 노란색: RabbitMQ용 Amazon MQ의 브로커가 단일 가용 영역에 구성되어 있습니다.

  녹색: RabbitMQ 브로커용 Amazon MQ가 여러 가용 영역에 구성되어 있습니다.

권장 조치

클러스터 배포 모드로 새 브로커를 생성합니다.

추가 리소스

- RabbitMQ 브로커 생성

보고서 열

- 상태 표시기

- 지역
- RabbitMQ 브로커 ID
- 브로커 엔진 유형
- 배포 모드
- 최종 업데이트 시간

## 서비스 한도

서비스 한도(할당량이라고도 함) 범주는 다음 검사를 참조하십시오.

이 범주의 모든 검사에는 다음과 같은 설명이 있습니다.

알림 기준

- 노란색: 한도의 80%에 도달했습니다.
- 빨간색: 한도의 100%에 도달했습니다.
- 파란색: Trusted Advisor가 하나 이상의 AWS 리전에서 사용률 또는 한도를 검색할 수 없습니다.

권장 조치

서비스 한도를 초과할 것으로 예상되는 경우 Service Quotas 콘솔에서 직접 한도 증가를 요청하세요. 아직 Service Quotas가 지원되지 않는 서비스인 경우 지원 센터에서 지원 사례를 열 수 있습니다.

보고서 열

- 상태 표시기
- Service
- 리전
- 한도 용량
- 현재 사용량

> **Note**
>
> - 값은 스냅샷을 기반으로 하므로 현재 사용량이 다를 수 있습니다. 할당량 및 사용량 데이터에 변경 사항이 반영되려면 최대 24시간이 걸릴 수 있습니다. 최근에 할당량이 증가한 경우 할당량을 초과하는 사용률이 일시적으로 표시될 수 있습니다.

검사명

- Auto Scaling 그룹
- Auto Scaling 시작 구성
- CloudFormation 스택
- DynamoDB 읽기 용량
- DynamoDB 쓰기 용량
- EBS 활성 스냅샷
- EBS 콜드 HDD(sc1) 볼륨 스토리지
- EBS 범용 SSD(gp2) 볼륨 스토리지
- EBS 범용 SSD(gp3) 볼륨 스토리지
- EBS 마그네틱(표준) 볼륨 스토리지
- EBS 프로비저닝된 IOPS(SSD) 볼륨 집계 IOPS
- EBS 프로비저닝된 IOPS SSD(io1) 볼륨 스토리지
- EBS 프로비저닝된 IOPS SSD(IO2) 볼륨 스토리지
- EBS 처리량 최적화 HDD(st1) 볼륨
- EC2 온디맨드 인스턴스
- EC2 예약 인스턴스 임대
- EC2-Classic 탄력적 IP 주소
- EC2-VPC 탄력적 IP 주소
- ELB Application Load Balancers
- ELB Classic Load Balancer
- ELB 네트워크 로드 밸런서
- IAM 그룹
- IAM 인스턴스 프로파일
- IAM 정책
- IAM 역할
- IAM 서버 인증서
- IAM 사용자
- 리전당 Kinesis 샤드

- Lambda 코드 스토리지 사용량
- RDS 클러스터 파라미터 그룹
- RDS 클러스터 역할
- RDS 클러스터
- RDS DB 인스턴스
- RDS DB 수동 스냅샷
- RDS DB 파라미터 그룹
- RDS DB 보안 그룹
- RDS 이벤트 구독
- 보안 그룹당 RDS 최대 인증
- RDS 옵션 그룹
- 마스터당 RDS 읽기 전용 복제본
- RDS 예약 인스턴스
- RDS 서브넷 그룹
- 서브넷 그룹 당 RDS 서브넷 수
- RDS 총 스토리지 할당량
- Route 53 호스팅 영역
- Route 53 최대 상태 확인
- Route 53 재사용 가능한 위임 세트
- Route 53 트래픽 정책
- Route 53 트래픽 정책 인스턴스
- SES 일일 전송 할당량
- VPC
- VPC 인터넷 게이트웨이

## Auto Scaling 그룹

### Description

Auto Scaling 그룹 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

fW7HH0l7J9

추가 리소스

오토 스케일링 할당량

## Auto Scaling 시작 구성

Description

Auto Scaling 시작 구성 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

aW7HH0l7J9

추가 리소스

오토 스케일링 할당량

## CloudFormation 스택

Description

CloudFormation 스택 할당량의 80% 가 넘는 사용량을 확인합니다.

검사 ID

gW7HH0l7J9

추가 리소스

AWS CloudFormation 할당량

## DynamoDB 읽기 용량

Description

AWS 계정 당 DynamoDB로 프로비저닝된 처리량 제한의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`6gtQddfEw6`

추가 리소스

DynamoDB 할당량

## DynamoDB 쓰기 용량

Description

AWS 계정 당 DynamoDB로 프로비저닝된 처리량 제한의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`c5ftjdfkMr`

추가 리소스

DynamoDB 할당량

## EBS 활성 스냅샷

Description

EBS 활성 스냅샷 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`eI7KK0l7J9`

추가 리소스

Amazon EBS 한도

## EBS 콜드 HDD(sc1) 볼륨 스토리지

Description

EBS 콜드 HDD(sc1) 볼륨 스토리지 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

gH5CC0e3J9

추가 리소스

Amazon EBS 한도

## EBS 범용 SSD(gp2) 볼륨 스토리지

Description

EBS 범용 SSD(gp2) 볼륨 스토리지 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

dH7RR0l6J9

추가 리소스

Amazon EBS 한도

## EBS 범용 SSD(gp3) 볼륨 스토리지

Description

EBS 범용 SSD(gp3) 볼륨 스토리지 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

dH7RR0l6J3

추가 리소스

Amazon EBS 한도

## EBS 마그네틱(표준) 볼륨 스토리지

Description

EBS 마그네틱(표준) 볼륨 스토리지 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

cG7HH0l7J9

추가 리소스

Amazon EBS 한도

## EBS 프로비저닝된 IOPS(SSD) 볼륨 집계 IOPS

Description

EBS 프로비저닝된 IOPS(SSD) 볼륨 집계 IOPS 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`tV7YY0l7J9`

추가 리소스

Amazon EBS 한도

## EBS 프로비저닝된 IOPS SSD(io1) 볼륨 스토리지

Description

EBS 프로비저닝된 IOPS SSD(io1) 볼륨 스토리지 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`gI7MM0l7J9`

추가 리소스

Amazon EBS 한도

## EBS 프로비저닝된 IOPS SSD(IO2) 볼륨 스토리지

Description

EBS 프로비저닝된 IOPS SSD(io2) 볼륨 스토리지 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`gI7MM0l7J2`

추가 리소스

Amazon EBS 한도

## EBS 처리량 최적화 HDD(st1) 볼륨

Description

EBS 처리량 최적화 HDD(st1) 볼륨 스토리지 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`wH7DD0l3J9`

추가 리소스

Amazon EBS 한도

## EC2 온디맨드 인스턴스

Description

EC2 온디맨드 인스턴스 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`0Xc6LMYG8P`

추가 리소스

Amazon EC2 할당량

## EC2 예약 인스턴스 임대

Description

EC2 예약 인스턴스 임대 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`iH7PP0l7J9`

추가 리소스

Amazon EC2 할당량

## EC2-Classic 탄력적 IP 주소

Description

EC2-Classic 탄력적 IP 주소 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

aW9HH0l8J6

추가 리소스

Amazon EC2 할당량

## EC2-VPC 탄력적 IP 주소

Description

EC2-VPC 탄력적 IP 주소 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

lN7RR0l7J9

추가 리소스

VPC 탄력적 IP 할당량

## ELB Application Load Balancers

Description

ELB Application Load Balancers 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

EM8b3yLRTr

추가 리소스

Elastic Load Balancing 할당량

## ELB Classic Load Balancer

Description

ELB 클래식 로드 밸런서 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`iK7000l7J9`

추가 리소스

Elastic Load Balancing 할당량

## ELB 네트워크 로드 밸런서

Description

ELB 네트워크 로드 밸런서 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`8wIqYSt25K`

추가 리소스

Elastic Load Balancing 할당량

## IAM 그룹

Description

IAM 그룹 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`sU7XX0l7J9`

추가 리소스

IAM 할당량

## IAM 인스턴스 프로파일

Description

IAM 인스턴스 프로파일 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

n07SS0l7J9

추가 리소스

IAM 할당량

## IAM 정책

Description

IAM 정책 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

pR7UU0l7J9

추가 리소스

IAM 할당량

## IAM 역할

Description

IAM 역할 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

oQ7TT0l7J9

추가 리소스

IAM 할당량

## IAM 서버 인증서

Description

IAM 서버 인증서 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`rT7WW0l7J9`

추가 리소스

IAM 할당량

## IAM 사용자

Description

IAM 사용자 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`qS7VV0l7J9`

추가 리소스

IAM 할당량

## 리전당 Kinesis 샤드

Description

리전 할당량당 Kinesis 샤드의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`bW7HH0l7J9`

추가 리소스

Kinesis 할당량

# Lambda 코드 스토리지 사용량

## Description

계정 한도의 80%를 초과하는 코드 스토리지 사용량을 확인합니다.

> **Note**
>
> 해당 검사의 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

## 검사 ID

`c1dfprch07`

## 알림 기준

- 노란색: 한도의 80%에 도달했습니다.

## 권장 조치

사용하지 않는 Lambda 함수 또는 버전을 식별하고 제거하여 해당 리전의 계정에 사용할 코드 스토리지를 확보하십시오. 추가 스토리지가 필요한 경우 지원 센터에서 지원 사례를 생성하세요. 서비스 한도를 초과할 것으로 예상되는 경우 Service Quotas 콘솔에서 직접 한도 증가를 요청하세요. 아직 Service Quotas가 지원되지 않는 서비스인 경우 지원 센터에서 지원 사례를 열 수 있습니다.

## 추가 리소스

- Lambda 코드 스토리지 사용량

## 보고서 열

- 상태 표시기
- 리전
- 이 리소스의 적격 함수 ARN입니다.
- 함수 코드 저장소 사용량은 소수점 2자리입니다. MegaBytes
- 함수에 포함된 버전의 양
- 최종 업데이트 시간

## RDS 클러스터 파라미터 그룹

Description

RDS 클러스터 매개 변수 그룹 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`jtlIMO3qZM`

추가 리소스

Amazon RDS 할당량

## RDS 클러스터 역할

Description

RDS 클러스터 역할 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`7fuccf1Mx7`

추가 리소스

Amazon RDS 할당량

## RDS 클러스터

Description

RDS 클러스터 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`gjqMBn6pjz`

추가 리소스

Amazon RDS 할당량

## RDS DB 인스턴스

Description

RDS DB 인스턴스 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`XG0aXHpIEt`

추가 리소스

Amazon RDS 할당량

## RDS DB 수동 스냅샷

Description

RDS DB 수동 스냅샷 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`dV84wpqRUs`

추가 리소스

Amazon RDS 할당량

## RDS DB 파라미터 그룹

Description

RDS DB 파라미터 그룹 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`jEECYg2YVU`

추가 리소스

Amazon RDS 할당량

## RDS DB 보안 그룹

Description

RDS DB 보안 그룹 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`gfZAn3W7wl`

추가 리소스

Amazon RDS 할당량

## RDS 이벤트 구독

Description

RDS 이벤트 구독 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`keAhfbH5yb`

추가 리소스

Amazon RDS 할당량

## 보안 그룹당 RDS 최대 인증

Description

보안 그룹 할당량당 RDS 최대 인증의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`dBkuNCvqn5`

추가 리소스

Amazon RDS 할당량

## RDS 옵션 그룹

Description

RDS 옵션 그룹 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

3Njm0DJQO9

추가 리소스

Amazon RDS 할당량

## 마스터당 RDS 읽기 전용 복제본

Description

마스터 할당량당 RDS 읽기 전용 복제본의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

pYW8UkYz2w

추가 리소스

Amazon RDS 할당량

## RDS 예약 인스턴스

Description

RDS 예약 인스턴스 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

UUDv0a5r34

추가 리소스

Amazon RDS 할당량

## RDS 서브넷 그룹

Description

RDS 서브넷 그룹 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`dYWBaXaaMM`

추가 리소스

Amazon RDS 할당량

## 서브넷 그룹 당 RDS 서브넷 수

Description

서브넷 그룹 할당량당 RDS 서브넷의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`jEhCtdJKOY`

추가 리소스

Amazon RDS 할당량

## RDS 총 스토리지 할당량

Description

RDS 총 스토리지 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`P1jhKWEmLa`

추가 리소스

Amazon RDS 할당량

## Route 53 호스팅 영역

Description

계정당 Route 53 호스팅 영역 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`dx3xfcdfMr`

추가 리소스

Route 53 할당량

## Route 53 최대 상태 확인

Description

계정당 Route 53 상태 확인 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`ru4xfcdfMr`

추가 리소스

Route 53 할당량

## Route 53 재사용 가능한 위임 세트

Description

계정당 Route 53 재사용 가능한 위임 집합 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`ty3xfcdfMr`

추가 리소스

Route 53 할당량

## Route 53 트래픽 정책

Description

계정당 Route 53 트래픽 정책 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`dx3xfbjfMr`

추가 리소스

Route 53 할당량

## Route 53 트래픽 정책 인스턴스

Description

계정당 Route 53 트래픽 정책 인스턴스 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`dx8afcdfMr`

추가 리소스

Route 53 할당량

## SES 일일 전송 할당량

Description

Amazon SES 일일 전송 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`hJ7NN0l7J9`

추가 리소스

Amazon SES 할당량

### VPC

Description

VPC 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`jL7PP0l7J9`

추가 리소스

VPC 할당량

### VPC 인터넷 게이트웨이

Description

VPC 인터넷 게이트웨이 할당량의 80%를 초과하는 사용량이 있는지 확인합니다.

검사 ID

`kM7QQ0l7J9`

추가 리소스

VPC 할당량

## 운영 우수성

성능 우수성 범주에 대해 다음과 같은 검사를 사용할 수 있습니다.

검사명

- Amazon API Gateway에서 실행 로그를 기록하지 않음
- X-Ray 추적이 활성화되지 않은 Amazon API Gateway REST API
- Amazon CloudFront 액세스 로그 구성
- Amazon CloudWatch 알람 작업이 비활성화되었습니다.
- 에서 관리하지 않는 Amazon EC2 인스턴스 AWS Systems Manager
- 태그 불변성이 비활성화된 Amazon ECR 리포지토리
- 컨테이너 인사이트가 비활성화된 Amazon ECS 클러스터
- Amazon ECS 작업 로깅이 활성화되지 않음

- Amazon OpenSearch 서비스 로깅이 CloudWatch 구성되지 않음
- 이기종 파라미터 그룹이 있는 클러스터의 Amazon RDS DB 인스턴스
- Amazon RDS 향상된 모니터링 기능이 꺼져 있습니다.
- Amazon RDS Performance Insights가 비활성화되었습니다.
- Amazon RDS 트랙_카운트 파라미터가 비활성화되었습니다
- Amazon Redshift 클러스터 감사 로깅
- Amazon S3에는 이벤트 알림이 활성화되어 있지 않습니다
- Amazon SNS 주제가 메시지 전송 상태를 기록하지 않음
- 흐름 로그가 없는 Amazon VPC
- Application Load Balancer 및 Classic Load Balancer(액세스 로그 사용 안 함)
- AWS CloudFormation 스택 알림
- AWS CloudTrail S3 버킷의 객체에 대한 데이터 이벤트 로깅
- AWS CodeBuild 프로젝트 로깅
- AWS CodeDeploy 자동 롤백 및 모니터링 활성화
- AWS CodeDeploy Lambda는 배포 구성을 사용하고 있습니다. all-at-once
- AWS Elastic Beanstalk Enhanced Health Reporting이 구성되지 않았습니다.
- AWS Elastic Beanstalk 관리형 플랫폼 업데이트가 비활성화된 경우
- AWS Fargate 플랫폼 버전이 최신 버전이 아닙니다.
- AWS Systems Manager 비준수 지위의 주 관리자 협회
- CloudTrail Amazon CloudWatch Logs에는 트레일이 구성되어 있지 않습니다.
- 로드 밸런서에 Elastic Load Balancing 삭제 보호 기능이 활성화되지 않음
- RDS DB 클러스터 삭제 보호 검사
- RDS DB 인스턴스 자동 마이너 버전 업그레이드 확인

## Amazon API Gateway에서 실행 로그를 기록하지 않음

설명

Amazon API Gateway에서 원하는 로깅 수준에서 CloudWatch 로그가 켜져 있는지 확인합니다.

Amazon API Gateway에서 REST WebSocket API 메서드 또는 API 경로에 대한 CloudWatch 로깅을 활성화하여 API에서 수신한 요청에 대한 실행 CloudWatch 로그를 로그에 수집합니다. 실행 로그에 포함된 정보는 API와 관련된 문제를 식별하고 해결하는 데 도움이 됩니다.

규칙의 LoggingLevel 매개 변수에 로깅 수준 (오류, 정보) ID를 지정할 수 있습니다. AWS Config

Amazon API Gateway에 CloudWatch 로그인하는 방법에 대한 자세한 내용은 WebSocket REST API 또는 API 설명서를 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz125
```

소스

```
AWS Config Managed Rule: api-gw-execution-logging-enabled
```

알림 기준

노란색: Amazon API Gateway의 원하는 CloudWatch 로깅 수준에서 실행 로그 수집을 위한 로깅 설정이 활성화되지 않았습니다.

권장 조치

적절한 CloudWatch 로깅 수준 (오류, 정보) 을 가진 Amazon API Gateway REST API 또는 WebSocket API에 대한 실행 로그에 대한 로깅을 활성화하십시오.

자세한 내용은 흐름 로그 생성을 참조하세요.

추가 리소스

- API Gateway에서 REST API에 대한 CloudWatch 로깅 설정
- WebSocket API에 대한 로깅 구성

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터

- 최종 업데이트 시간

## X-Ray 추적이 활성화되지 않은 Amazon API Gateway REST API

설명

Amazon API Gateway REST API에 AWS X-Ray 추적 기능이 켜져 있는지 확인합니다.

REST API에 대한 X-Ray 추적 기능을 켜면 API 게이트웨이에서 추적 정보를 사용하여 API 간접 호출 요청을 샘플링할 수 있습니다. 이를 통해 API Gateway REST API를 통해 다운스트림 서비스로 이동하는 요청을 추적하고 분석할 수 있습니다. AWS X-Ray

자세한 내용은 X-Ray를 사용하여 REST API 사용자 요청 추적을 참조하세요.

> **Note**
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz126
```

소스

```
AWS Config Managed Rule: api-gw-xray-enabled
```

알림 기준

노란색: API Gateway REST API에 대해 X-Ray 추적이 켜져 있지 않습니다.

권장 조치

API 게이트웨이 REST API에 대해 X-Ray 추적을 활성화합니다.

자세한 내용은 API Gateway REST API를 AWS X-Ray 사용한 설정을 참조하십시오.

추가 리소스

- X-Ray를 사용하여 REST API에 대한 사용자 요청 추적
- 무엇입니까 AWS X-Ray?

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon CloudFront 액세스 로그 구성

설명

Amazon S3 서버 액세스 로그에서 정보를 캡처하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. Amazon S3 서버 액세스 로그는 CloudFront 수신하는 모든 사용자 요청에 대한 세부 정보를 포함합니다.

AWS Config 규칙의 S3 BucketName 파라미터를 사용하여 서버 액세스 로그를 저장하기 위한 Amazon S3 버킷의 이름을 조정할 수 있습니다.

자세한 내용은 표준 로그(액세스 로그) 구성 및 사용을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz110
```

소스

```
AWS Config Managed Rule: cloudfront-accesslogs-enabled
```

알림 기준

노란색: Amazon CloudFront 액세스 로깅이 활성화되지 않았습니다.

권장 조치

CloudFront 수신하는 모든 사용자 요청에 대한 세부 정보를 캡처하려면 CloudFront 액세스 로깅을 켜야 합니다.

배포를 만들거나 업데이트할 때 표준 로그를 켤 수 있습니다.

자세한 내용은 배포를 생성하거나 업데이트할 때 지정하는 값을 참조하세요.

추가 리소스

- 배포를 만들거나 업데이트할 때 지정하는 값
- 표준 로그(액세스 로그) 구성 및 사용

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon CloudWatch 알람 작업이 비활성화되었습니다.

설명

Amazon CloudWatch 알람 조치가 비활성화 상태인지 확인합니다.

를 사용하여 알람의 AWS CLI 작업 기능을 활성화하거나 비활성화할 수 있습니다. 또는 AWS SDK를 사용하여 프로그래밍 방식으로 작업 기능을 비활성화하거나 활성화할 수 있습니다. 알람 동작 기능을 끄면 어떤 상태에서도 정의된 동작을 수행하지 CloudWatch 않습니다 (OK, IMPUCIENT_DATA, ALARM).

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz109
```

소스

```
AWS Config Managed Rule: cloudwatch-alarm-action-enabled-check
```

알림 기준

노란색: Amazon CloudWatch 알람 작업이 활성화되지 않았습니다. 어떤 경보 상태에서도 아무 조치도 수행되지 않습니다.

권장 조치

CloudWatch 알람을 비활성화해야 할 타당한 이유 (예: 테스트 목적) 가 없는 한 알람에서 작업을 활성화하십시오.

CloudWatch 알람이 더 이상 필요하지 않은 경우 불필요한 비용이 발생하지 않도록 삭제하십시오.

자세한 내용은 AWS CLI 명령 참조의 알람 액션 활성화 및 Go용 CloudWatchSDK EnableAlarmActions API 참조의 func (*) 를 참조하십시오. AWS

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## 에서 관리하지 않는 Amazon EC2 인스턴스 AWS Systems Manager

설명

계정의 Amazon EC2 인스턴스가 에서 관리되는지 확인합니다. AWS Systems Manager

시스템 관리자를 사용하면 Amazon EC2 인스턴스 및 OS 구성의 현재 상태를 이해하고 제어할 수 있습니다. Systems Manager를 사용하면 설치된 소프트웨어를 포함하여 인스턴스 플릿에 대한 소프트웨어 구성 및 인벤토리 정보를 수집할 수 있습니다. 이를 통해 세부 시스템 구성, OS 패치 수준, 애플리케이션 구성 및 배포에 대한 기타 세부 정보를 추적할 수 있습니다.

자세한 내용은 EC2 인스턴스의 시스템 관리자 설정을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz145`

소스

`AWS Config Managed Rule: ec2-instance-managed-by-systems-manager`

알림 기준

노란색: Amazon EC2 인스턴스는 시스템 관리자가 관리하지 않습니다.

권장 조치

시스템 관리자에서 관리하도록 Amazon EC2 인스턴스를 구성합니다.

Trusted Advisor 콘솔의 보기에서 이 검사를 제외할 수 없습니다.

자세한 내용은 시스템 관리자에서 내 EC2 인스턴스가 관리형 노드로 표시되지 않거나 “연결 끊김” 상태로 표시되는 이유는 무엇입니까?를 참조하세요.

추가 리소스

EC2 인스턴스용 시스템 관리자 설정

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

# 태그 불변성이 비활성화된 Amazon ECR 리포지토리

설명

프라이빗 Amazon ECR 리포지토리에 이미지 태그 불변성이 켜져 있는지 확인합니다.

프라이빗 Amazon ECR 리포지토리에 대해 이미지 태그 변경 불가능이 켜지도록 합니다. 그러면 이미지 태그를 덮어쓰는 걸 방지할 수 있습니다. 따라서 설명 태그를 신뢰할 수 있는 메커니즘으로 사용하여 이미지를 추적하고 고유하게 식별할 수 있습니다. 예를 들어 이미지 태그 불변성이 켜져 있는 경우 사용자는 이미지 태그를 사용하여 배포된 이미지 버전과 해당 이미지를 생성한 빌드의 상관 관계를 파악할 수 있습니다.

자세한 내용은 이미지 태그 가변성.을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz129
```

소스

```
AWS Config Managed Rule: ecr-private-tag-immutability-enabled
```

알림 기준

노란색: Amazon ECR 프라이빗 리포지토리에는 태그 불변성이 켜져 있지 않습니다.

권장 조치

Amazon ECR 프라이빗 리포지토리의 이미지 태그 불변성을 활성화하십시오.

자세한 내용은 이미지 태그 가변성.을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource

- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## 컨테이너 인사이트가 비활성화된 Amazon ECS 클러스터

설명

Amazon ECS 클러스터에 대해 Amazon CloudWatch 컨테이너 인사이트가 켜져 있는지 확인합니다.

CloudWatch Container Insights는 컨테이너식 애플리케이션 및 마이크로서비스에서 지표와 로그를 수집, 집계 및 요약합니다. 이 지표에는 CPU, 메모리, 디스크, 네트워크 같은 리소스 사용률이 포함되어 있습니다.

자세한 내용은 Amazon ECS CloudWatch 컨테이너 인사이트를 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz173
```

소스

```
AWS Config Managed Rule: ecs-container-insights-enabled
```

알림 기준

노란색: Amazon ECS 클러스터에는 컨테이너 인사이트가 활성화되어 있지 않습니다.

권장 조치

Amazon ECS 클러스터에서 CloudWatch 컨테이너 인사이트를 활성화하십시오.

자세한 내용은 컨테이너 인사이트 사용을 참조하세요.

추가 리소스

Amazon ECS CloudWatch 컨테이너 인사이트

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon ECS 작업 로깅이 활성화되지 않음

설명

활성 Amazon ECS 작업 정의에 로그 구성이 설정되어 있는지 확인합니다.

Amazon ECS 작업 정의에서 로그 구성을 확인하면 컨테이너에서 생성된 로그가 제대로 구성되고 저장되었는지 확인할 수 있습니다. 이를 통해 문제를 더 빠르게 식별 및 해결하고, 성능을 최적화하고, 규정 준수 요구 사항을 충족할 수 있습니다.

기본적으로 수집되는 로그는 컨테이너를 로컬에서 실행했을 때 일반적으로 대화식 터미널에 표시되는 명령을 나타냅니다. awslogs 드라이버는 이러한 로그를 Docker에서 Amazon Logs로 전달합니다. CloudWatch

자세한 내용은 awslogs 로그 드라이버 사용을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c18d2gz175

소스

AWS Config Managed Rule: ecs-task-definition-log-configuration

알림 기준

노란색: Amazon ECS 작업 정의에는 로깅 구성이 없습니다.

권장 조치

로그 정보를 CloudWatch Logs 또는 다른 로깅 드라이버로 보내려면 컨테이너 정의에서 로그 드라이버 구성을 지정하는 것을 고려해 보십시오.

자세한 내용은 LogConfiguration를 참조하세요.

추가 리소스

로그 정보를 로그 또는 다른 로깅 드라이버로 보내려면 컨테이너 정의에서 CloudWatch 로그 드라이버 구성을 지정하는 것이 좋습니다.

자세한 내용은 작업 정의 예시를 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon OpenSearch 서비스 로깅이 CloudWatch 구성되지 않음

설명

Amazon OpenSearch 서비스 도메인이 Amazon Logs에 로그를 전송하도록 구성되어 있는지 확인합니다. CloudWatch

로그 모니터링은 OpenSearch 서비스의 안정성, 가용성 및 성능을 유지하는 데 매우 중요합니다.

검색 느린 로그, 인덱싱 느린 로그 및 오류 로그는 워크로도의 성능 및 안정성 문제 해결에 유용합니다. 데이터를 캡처하려면 이러한 로그를 활성화해야 합니다.

AWS Config 규칙의 LogTypes 매개 변수를 사용하여 필터링하려는 로그 유형 (오류, 검색, 인덱스)을 지정할 수 있습니다.

자세한 내용은 Amazon OpenSearch 서비스 도메인 모니터링을 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz184
```

소스

```
AWS Config Managed Rule: opensearch-logs-to-cloudwatch
```

알림 기준

노란색: Amazon OpenSearch 서비스에는 Amazon CloudWatch Logs를 사용한 로깅 구성이 없습니다.

권장 조치

로그를 로그에 게시하도록 OpenSearch 서비스 도메인을 구성합니다. CloudWatch

자세한 내용은 로그 게시 활성화(콘솔)를 참조하세요.

추가 리소스

- Amazon을 통한 OpenSearch 서비스 클러스터 지표 모니터링 CloudWatch

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터

- 최종 업데이트 시간

## 이기종 파라미터 그룹이 있는 클러스터의 Amazon RDS DB 인스턴스

설명

DB 클러스터의 모든 DB 인스턴스가 동일한 DB 파라미터 그룹을 사용하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt010`

알림 기준

노란색: DB 클러스터에는 이기종 파라미터 그룹이 있는 DB 인스턴스가 있습니다.

권장 조치

DB 인스턴스를 DB 클러스터의 라이터 인스턴스와 연결된 DB 파라미터 그룹과 연결하세요.

추가 리소스

DB 클러스터의 DB 인스턴스가 서로 다른 DB 파라미터 그룹을 사용하는 경우 장애 조치 중에 동작이 일관되지 않거나 DB 클러스터의 DB 인스턴스 간에 호환성 문제가 발생할 수 있습니다.

자세한 내용은 파라미터 그룹 작업을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- 권장 값
- 엔진 이름
- 최종 업데이트 시간

## Amazon RDS 향상된 모니터링 기능이 꺼져 있습니다.

설명

데이터베이스 리소스에 향상된 모니터링이 켜져 있지 않습니다. 확장된 모니터링은 모니터링 및 문제 해결을 위해 실시간 운영 체제 지표를 제공합니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

```
c1qf5bt004
```

알림 기준

노란색: Amazon RDS 리소스에는 향상된 모니터링이 켜져 있지 않습니다.

권장 조치

향상된 모니터링을 켜세요.

추가 리소스

Amazon RDS에 대한 향상된 모니터링을 통해 DB 인스턴스의 상태를 추가로 파악할 수 있습니다. 향상된 모니터링을 활성화하는 것이 좋습니다. DB 인스턴스에 대해 향상된 모니터링 옵션을 켜면 중요한 운영 체제 지표와 프로세스 정보가 수집됩니다.

자세한 내용은 Enhanced Monitoring을 사용하여 OS 지표 모니터링을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- 권장 값
- 엔진 이름
- 최종 업데이트 시간

## Amazon RDS Performance Insights가 비활성화되었습니다.

설명

Amazon RDS Performance Insights는 DB 인스턴스 부하를 모니터링하여 데이터베이스 성능 문제를 분석하고 해결하는 데 도움이 됩니다. 성능 개선 도우미를 켜는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔이나 Amazon RDS 관리 콘솔에서 해당 인스턴스 Trusted Advisor 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

검사 ID

`c1qf5bt012`

알림 기준

노란색: Amazon RDS 리소스에는 Performance Insights가 켜져 있지 않습니다.

권장 조치

성능 개선 도우미를 활성화합니다.

추가 리소스

Performance Insights는 애플리케이션의 성능에 영향을 주지 않는 간단한 데이터 수집 방법을 사용합니다. Performance Insights를 사용하면 데이터베이스 부하를 빠르게 평가할 수 있습니다.

자세한 내용은 Amazon RDS의 Performance Insights를 사용한 DB 부하 모니터링을 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 권장 값
- 엔진 이름
- 최종 업데이트 시간

# Amazon RDS 트랙_카운트 파라미터가 비활성화되었습니다

## 설명

track_counts 파라미터를 끄면 데이터베이스는 데이터베이스 활동 통계를 수집하지 않습니다. Autovacuum을 사용하려면 이러한 통계가 제대로 작동해야 합니다.

track_counts 파라미터를 1로 설정하는 것이 좋습니다.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

> **Note**
>
> DB 인스턴스 또는 DB 클러스터가 중지되면 3~5일 동안 Amazon RDS 권장 사항을 확인할 수 있습니다. Trusted Advisor 5일이 지나면 에서 Trusted Advisor권장 사항을 사용할 수 없습니다. 권장 사항을 보려면 Amazon RDS 콘솔을 열고 [권장 사항] 을 선택합니다.
> DB 인스턴스 또는 DB 클러스터를 삭제하면 Amazon RDS 관리 콘솔에서 Trusted Advisor 해당 인스턴스 또는 클러스터와 관련된 권장 사항을 사용할 수 없습니다.

## 검사 ID

`c1qf5bt027`

## 알림 기준

노란색: DB 파라미터 그룹에는 track_counts 파라미터가 꺼져 있습니다.

## 권장 조치

트랙_카운트 파라미터를 1로 설정합니다.

## 추가 리소스

track_counts 매개 변수를 끄면 데이터베이스 활동 통계 수집이 비활성화됩니다. autovacuum 데몬은 자동진공 및 자동분석을 위한 테이블을 식별하기 위해 수집된 통계를 필요로 합니다.

자세한 내용은 PostgreSQL 설명서 웹 사이트에서 PostgreSQL의 런타임 통계를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- 파라미터 값
- 권장 값입니다.
- 최종 업데이트 시간

## Amazon Redshift 클러스터 감사 로깅

설명

Amazon Redshift 클러스터에 데이터베이스 감사 로깅이 켜져 있는지 확인합니다. Amazon Redshift는 연결 및 사용자 작업에 대한 정보를 데이터베이스에 기록합니다.

규칙의 BucketNames 파라미터와 일치하도록 원하는 로깅 Amazon S3 버킷 이름을 지정할 수 있습니다. AWS Config

자세한 내용은 데이터베이스 감사 로깅을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz134
```

소스

```
AWS Config Managed Rule: redshift-audit-logging-enabled
```

알림 기준

노란색: Amazon Redshift 클러스터의 데이터베이스 감사 로깅이 비활성화되어 있습니다.

권장 조치

Amazon Redshift 클러스터에 대한 로깅 및 모니터링을 활성화합니다.

자세한 내용은 콘솔을 사용한 감사 구성을 참조하세요.

추가 리소스

Amazon Redshift의 로깅 및 모니터링

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon S3에는 이벤트 알림이 활성화되어 있지 않습니다

설명

Amazon S3 이벤트 알림이 활성화되었는지 또는 원하는 대상 또는 유형으로 올바르게 구성되었는지 확인합니다.

Amazon S3 이벤트 알림 기능을 사용하면 Amazon S3 버킷에서 특정 이벤트가 발생할 때 알림을 보내드립니다. Amazon S3는 Amazon SQS 대기열, Amazon SNS 주제 및 함수에 알림 메시지를 보낼 수 있습니다. AWS Lambda

규칙의 DestinationARN 및 EventTypes 파라미터를 사용하여 원하는 대상 및 이벤트 유형을 지정할 수 있습니다. AWS Config

자세한 내용은 Amazon S3 이벤트 알림을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c18d2gz163

소스

AWS Config Managed Rule: s3-event-notifications-enabled

알림 기준

노란색: Amazon S3에는 이벤트 알림이 활성화되어 있지 않거나 원하는 대상 또는 유형으로 구성되어 있지 않습니다.

권장 조치

객체 및 버킷 이벤트에 대한 Amazon S3 이벤트 알림을 구성합니다.

자세한 내용은 Amazon S3 콘솔을 사용하여 이벤트 알림 활성화 및 구성을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Amazon SNS 주제가 메시지 전송 상태를 기록하지 않음

설명

Amazon SNS 주제에 메시지 전송 상태 로깅이 켜져 있는지 확인합니다.

더 나은 운영 통찰력을 제공하는 데 도움이 되도록 메시지 전송 상태를 로깅하도록 Amazon SNS 주제를 구성합니다. 예를 들어 메시지 전송 로깅은 메시지가 특정 Amazon SNS 엔드포인트에 전송되었는지 확인합니다. 그리고 엔드포인트에서 전송되는 응답을 식별하는 데도 도움이 됩니다.

자세한 내용은 Amazon SNS 메시지 전달 상태를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz121`

소스

`AWS Config Managed Rule: sns-topic-message-delivery-notification-enabled`

알림 기준

노란색: Amazon SNS 주제에 대한 메시지 전송 상태 로깅이 켜져 있지 않습니다.

권장 조치

SNS 주제에 대한 메시지 전송 상태 로깅을 활성화하십시오.

자세한 내용은 AWS Management Console을 사용한 전송 상태 로깅 구성 을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## 흐름 로그가 없는 Amazon VPC

설명

VPC에 대해 Amazon Virtual Private 클라우드 흐름 로그가 생성되었는지 확인합니다.

규칙의 TrafficType 파라미터를 사용하여 트래픽 유형을 지정할 수 있습니다. AWS Config

자세한 내용은 VPC 흐름 로그를 사용하여 IP 트래픽 로깅을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz122`

소스

`AWS Config Managed Rule: vpc-flow-logs-enabled`

알림 기준

노란색: VPC에는 Amazon VPC 흐름 로그가 없습니다.

권장 조치

각 VPC에 대한 VPC 흐름 로그를 생성합니다.

자세한 내용은 흐름 로그 생성을 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## Application Load Balancer 및 Classic Load Balancer(액세스 로그 사용 안 함)

설명

Application Load Balancer 및 Classic Load Balancer에 액세스 로깅이 활성화되어 있는지 확인합니다.

Elastic Load Balancing은 로드 밸런서에 전송된 요청에 대한 자세한 정보를 캡처하는 액세스 로그를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다. 이러한 액세스 로그를 사용하여 트래픽 패턴을 분석하고 문제를 해결할 수 있습니다.

액세스 로그는 Elastic Load Balancing의 옵션 기능으로, 기본적으로 비활성화되어 있습니다. 로드 밸런서에 대해 액세스 로그를 활성화하면 Elastic Load Balancing에서 로그를 캡처하여 지정한 Amazon S3 버킷에 저장합니다.

AWS Config 규칙의 s3 BucketNames 파라미터를 사용하여 확인하려는 액세스 로그 Amazon S3 버킷을 지정할 수 있습니다.

자세한 내용은 Application Load Balancer의 액세스 로그 또는 Classic Load Balancer의 액세스 로그를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz167
```

소스

```
AWS Config Managed Rule: elb-logging-enabled
```

알림 기준

노란색: Application Load Balancer 또는 Classic Load Balancer에 대해 액세스 로그 기능이 활성화되지 않았습니다.

권장 조치

Application Load Balancer 및 Classic Load Balancer에 대한 액세스 로그를 활성화합니다.

자세한 내용은 Application Load Balancer에 대한 액세스 로그 활성화 또는 Classic Load Balancer에 대한 액세스 로그 활성화를 참조하세요.

보고서 열

- 상태 표시기

- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## AWS CloudFormation 스택 알림

설명

이벤트 발생 시 모든 AWS CloudFormation 스택이 Amazon SNS를 사용하여 알림을 수신하는지 확인합니다.

AWS Config 규칙의 파라미터를 사용하여 특정 Amazon SNS 주제 ARN을 찾도록 이 검사를 구성할 수 있습니다.

자세한 내용은 AWS CloudFormation스택 옵션 설정을 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz111
```

소스

```
AWS Config Managed Rule: cloudformation-stack-notification-check
```

알림 기준

노란색: AWS CloudFormation 스택에 대한 Amazon SNS 이벤트 알림이 켜져 있지 않습니다.

권장 조치

이벤트 발생 시 AWS CloudFormation 스택에서 Amazon SNS를 사용하여 알림을 수신해야 합니다.

스택 이벤트를 모니터링하면 환경을 변경할 수 있는 무단 조치에 신속하게 대응할 수 있습니다 AWS .

추가 리소스

AWS CloudFormation 스택이 ROLLBACK_IN_PROGRESS 상태가 되면 이메일 알림을 받으려면 어떻게 해야 합니까?

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## AWS CloudTrail S3 버킷의 객체에 대한 데이터 이벤트 로깅

설명

하나 이상의 AWS CloudTrail 트레일이 모든 Amazon S3 버킷에 대해 Amazon S3 데이터 이벤트를 기록하는지 확인합니다.

자세한 내용은 AWS CloudTrail을(를) 사용한 Amazon S3 API 호출 로깅을 참조하세요.

> **Note**
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz166
```

소스

```
AWS Config Managed Rule: cloudtrail-s3-dataevents-enabled
```

알림 기준

노란색: Amazon S3 버킷에 대한 AWS CloudTrail 이벤트 로깅이 구성되지 않음

권장 조치

Amazon S3 버킷 및 객체에 대한 CloudTrail 이벤트 로깅을 활성화하여 대상 버킷 액세스 요청을 추적합니다.

자세한 내용은 S3 버킷 및 객체에 대한 CloudTrail 이벤트 로깅 활성화를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## AWS CodeBuild 프로젝트 로깅

설명

AWS CodeBuild 프로젝트 환경에서 로깅을 사용하는지 확인합니다. 로깅 옵션은 Amazon Logs의 로그이거나, 지정된 Amazon S3 버킷에 내장된 CloudWatch 로그이거나, 둘 다일 수 있습니다. CodeBuild 프로젝트 로그인을 활성화하면 디버깅 및 감사와 같은 여러 가지 이점을 제공할 수 있습니다.

AWS Config 규칙의 s3 또는 cloud WatchGroup Names 파라미터를 사용하여 CloudWatch 로그를 저장할 Amazon S3 버킷 BucketNames 또는 Logs 그룹의 이름을 지정할 수 있습니다.

자세한 내용은 모니터링 AWS CodeBuild을 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz113
```

소스

```
AWS Config Managed Rule: codebuild-project-logging-enabled
```

알림 기준

노란색: AWS CodeBuild 프로젝트 로깅이 활성화되지 않았습니다.

권장 조치

AWS CodeBuild 프로젝트에 로깅이 켜져 있는지 확인하세요. AWS Trusted Advisor 콘솔의 보기에서 이 체크를 제외할 수 없습니다.

자세한 내용은 로그인 및 모니터링을 참조하십시오 AWS CodeBuild.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## AWS CodeDeploy 자동 롤백 및 모니터링 활성화

설명

배포 그룹이 자동 배포 롤백 및 경보가 첨부된 배포 모니터링으로 구성되어 있는지 확인합니다. 배포 중에 문제가 발생하면 자동으로 롤백되어 애플리케이션이 안정적인 상태로 유지됩니다.

자세한 내용은 배포 재배포 및 롤백을 참조하십시오. CodeDeploy

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c18d2gz114

소스

AWS Config Managed Rule: codedeploy-auto-rollback-monitor-enabled

알림 기준

노란색: AWS CodeDeploy 자동 배포 롤백 및 배포 모니터링이 활성화되지 않았습니다.

권장 조치

배포에 실패하거나 지정한 모니터링 임계값이 충족될 때 자동으로 롤백하도록 배포 그룹 또는 배포를 구성합니다.

배포 프로세스 중에 CPU 사용량, 메모리 사용량 또는 네트워크 트래픽과 같은 다양한 지표를 모니터링하도록 경보를 구성합니다. 이러한 지표 중 하나라도 특정 임계값을 초과하면 경보가 트리거되고 배포가 중지되거나 롤백됩니다.

배포 그룹의 자동 롤백 설정 및 경보 구성에 대한 자세한 내용은 배포 그룹의 고급 옵션 구성을 참조하세요.

추가 리소스

무엇입니까 CodeDeploy?

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## AWS CodeDeploy Lambda는 배포 구성을 사용하고 있습니다. all-at-once

설명

AWS Lambda 컴퓨팅 플랫폼용 AWS CodeDeploy 배포 그룹이 배포 구성을 사용하고 all-at-once 있는지 확인합니다.

CodeDeploy에서 Lambda 함수의 배포 실패 위험을 줄이려면 모든 트래픽이 원래 Lambda 함수에서 업데이트된 함수로 한 번에 이동하는 기본 옵션 대신 canary 또는 선형 배포 구성을 사용하는 것이 가장 좋습니다.

자세한 내용은 Lambda 함수 버전 및 배포 구성을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz115`

소스

`AWS Config Managed Rule: codedeploy-lambda-allatonce-traffic-shift-disabled`

알림 기준

노란색: AWS CodeDeploy Lambda 배포는 배포 구성을 사용하여 all-at-once 모든 트래픽을 업데이트된 Lambda 함수로 한 번에 이동합니다.

권장 조치

Lambda 컴퓨팅 플랫폼에 대한 CodeDeploy 배포 그룹의 Canary 또는 Linear 배포 구성을 사용하십시오.

추가 리소스

배포 구성

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

# AWS Elastic Beanstalk Enhanced Health Reporting이 구성되지 않았습니다.

설명

AWS Elastic Beanstalk 환경이 향상된 상태 보고를 위해 구성되어 있는지 확인합니다.

Elastic Beanstalk 고급 상태 보고는 CPU 사용량, 메모리 사용량, 네트워크 트래픽, 인프라 상태 정보(예: 인스턴스 수 및 로드 밸런서 상태)와 같은 자세한 성능 지표를 제공합니다.

자세한 내용은 향상된 상태 보고 및 모니터링을 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz108
```

소스

```
AWS Config Managed Rule: beanstalk-enhanced-health-reporting-enabled
```

알림 기준

노란색: Elastic Beanstalk 환경은 향상된 상태 보고를 위해 구성되지 않았습니다.

권장 조치

Elastic Beanstalk 환경이 향상된 상태 보고를 위해 구성되어 있는지 확인하세요.

자세한 내용은 Elastic Beanstalk 콘솔을 사용한 확장 상태 보고 활성화를 참조하세요.

추가 리소스

- Elastic Beanstalk 개선 상태 보고 활성화
- 향상된 상태 보고 및 모니터링

보고서 열

- 상태 표시기
- 지역
- Resource

- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## AWS Elastic Beanstalk 관리형 플랫폼 업데이트가 비활성화된 경우

설명

Elastic Beanstalk 환경 및 구성 템플릿에서 관리형 플랫폼 업데이트가 활성화되었는지 확인합니다.

AWS Elastic Beanstalk 플랫폼 업데이트를 정기적으로 릴리스하여 수정, 소프트웨어 업데이트 및 새 기능을 제공합니다. 관리형 플랫폼 업데이트를 통해 Elastic Beanstalk는 새 패치 및 마이너 플랫폼 버전에 대한 플랫폼 업데이트를 자동으로 수행할 수 있습니다.

AWS Config 규칙의 UpdateLevel매개변수에서 원하는 업데이트 수준을 지정할 수 있습니다.

자세한 내용은 Elastic Beanstalk 환경의 플랫폼 버전 업데이트를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz177`

소스

`AWS Config Managed Rule: elastic-beanstalk-managed-updates-enabled`

알림 기준

노란색: AWS Elastic Beanstalk 관리형 플랫폼 업데이트는 마이너 또는 패치 수준을 포함하여 전혀 구성되지 않았습니다.

권장 조치

Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하거나 마이너 또는 업데이트 수준에서 구성합니다.

자세한 내용은 관리형 플랫폼 업데이트를 참조하세요.

추가 리소스

- Elastic Beanstalk 개선 상태 보고 활성화
- 향상된 상태 보고 및 모니터링

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## AWS Fargate 플랫폼 버전이 최신 버전이 아닙니다.

설명

Amazon ECS에서 AWS Fargate의 최신 플랫폼 버전을 실행하고 있는지 확인합니다. Fargate 플랫폼 버전은 Fargate 태스크 인프라를 위한 특정 실행 시간 환경을 참조하는 데 사용합니다. 이것은 커널 버전과 컨테이너 실행 시간 버전의 조합입니다. 런타임 환경이 발전함에 따라 새 플랫폼 버전이 출시됩니다. 예를 들면 커널 또는 운영 체제 업데이트, 새로운 기능, 버그 수정 또는 보안 업데이트가 있는 경우가 있습니다.

자세한 내용은 Fargate 작업 유지관리를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz174
```

소스

```
AWS Config Managed Rule: ecs-fargate-latest-platform-version
```

알림 기준

노란색: Amazon ECS는 최신 버전의 Fargate 플랫폼에서 실행되지 않습니다.

권장 조치

최신 Fargate 플랫폼 버전으로 업데이트하십시오.

자세한 내용은 Fargate 작업 유지관리를 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## AWS Systems Manager 비준수 지위의 주 관리자 협회

설명

인스턴스에서 AWS Systems Manager 연결을 실행한 후 연결 규정 준수 상태가 COMPLIANT 또는 NON_COMPLIANT인지 확인합니다.

의 AWS Systems Manager기능인 State Manager는 관리형 노드 및 기타 AWS 리소스를 사용자가 정의한 상태로 유지하는 프로세스를 자동화하는 안전하고 확장 가능한 구성 관리 서비스입니다. State Manager 연결은 AWS 리소스에 할당하는 구성입니다. 구성은 리소스에서 유지하려는 상태를 정의하므로 Amazon EC2 인스턴스 전반의 구성 편차 방지와 같은 목표를 달성하는 데 도움이 됩니다.

자세한 내용은 AWS Systems Manager 상태 관리자를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

c18d2gz147

소스

AWS Config Managed Rule: ec2-managedinstance-association-compliance-status-check

알림 기준

노란색: AWS Systems Manager 협회 규정 준수 상태는 NON_COMPLIANT입니다.

권장 조치

State Manager 협회의 상태를 확인한 다음 필요한 조치를 취하여 상태를 COMPLIANT로 되돌립니다.

자세한 내용은 상태 관리자 소개를 참조하세요.

추가 리소스

AWS Systems Manager 스테이트 매니저

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## CloudTrail Amazon CloudWatch Logs에는 트레일이 구성되어 있지 않습니다.

설명

로그로 로그를 전송하도록 AWS CloudTrail 트레일이 구성되어 있는지 확인합니다. CloudWatch

로그와 함께 CloudTrail CloudWatch 로그 파일을 모니터링하여 중요 이벤트가 캡처될 때 자동 응답을 트리거합니다. AWS CloudTrail

자세한 내용은 CloudWatch 로그를 포함한 CloudTrail 로그 파일 모니터링을 참조하십시오.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

`c18d2gz164`

소스

`AWS Config Managed Rule: cloud-trail-cloud-watch-logs-enabled`

알림 기준

노란색: CloudWatch 로그 통합으로 AWS CloudTrail 설정되지 않았습니다.

권장 조치

로그 이벤트를 CloudTrail Logs로 전송하도록 트레일을 구성합니다. CloudWatch

자세한 내용은 CloudTrail 이벤트 CloudWatch 알람 만들기: 예제를 참조하십시오.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

## 로드 밸런서에 Elastic Load Balancing 삭제 보호 기능이 활성화되지 않음

설명

로드 밸런서에 삭제 방지가 켜져 있는지 확인합니다.

Elastic Load Balancing은 Application Load Balancer, Network Load Balancer 및 게이트웨이 로드 밸런서에 대한 삭제 보호를 지원합니다. 로드 밸런서가 실수로 삭제되는 것을 방지하려면 삭제 보

호를 켜세요. 로드 밸런서를 생성할 때 기본적으로 삭제 방지가 해제됩니다. 로드 밸런서가 프로덕션 환경에 속해 있는 경우 삭제 방지 기능을 켜는 것을 고려해 보세요.

액세스 로그는 Elastic Load Balancing의 옵션 기능으로, 기본적으로 비활성화되어 있습니다. 로드 밸런서에 대해 액세스 로그를 활성화하면 Elastic Load Balancing에서 로그를 캡처하여 지정한 Amazon S3 버킷에 저장합니다.

자세한 내용은 Application Load Balancer 삭제 보호, Network Load Balancer 삭제 보호 또는 게이트웨이 로드 밸런서 삭제 보호를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz168
```

소스

```
AWS Config Managed Rule: elb-deletion-protection-enabled
```

알림 기준

노란색: 로드 밸런서에 대해 삭제 방지가 활성화되지 않았습니다.

권장 조치

Application Load Balancer, Network Load Balancer 및 Gateway Load Balancer에 대한 삭제 보호를 활성화합니다.

자세한 내용은 Application Load Balancer 삭제 보호, Network Load Balancer 삭제 보호 또는 게이트웨이 로드 밸런서 삭제 보호를 참조하세요.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터

- 최종 업데이트 시간

## RDS DB 클러스터 삭제 보호 검사

설명

Amazon RDS DB 클러스터에 삭제 방지가 활성화되어 있는지 확인합니다.

클러스터가 삭제 방지 기능으로 구성되면 어떤 사용자도 데이터베이스를 삭제할 수 없습니다.

MySQL용 Amazon Aurora 및 RDS, MariaDB용 RDS, 오라클용 RDS, Oracle용 RDS, PostgreSQL용 RDS, SQL Server 데이터베이스 인스턴스용 RDS에서 모든 지역에서 삭제 보호를 사용할 수 있습니다. AWS

자세한 내용은 Aurora 클러스터의 삭제 방지를 참조하세요.

검사 ID

```
c18d2gz160
```

소스

```
AWS Config Managed Rule: rds-cluster-deletion-protection-enabled
```

알림 기준

노란색: Amazon RDS DB 클러스터에서 삭제 방지가 활성화되지 않았습니다.

권장 조치

Amazon RDS DB 클러스터를 생성할 때 삭제 방지 기능을 활성화하십시오.

삭제 보호가 활성화되지 않은 클러스터는 삭제만 삭제할 수 있습니다. 삭제 보호를 활성화하면 보호 계층이 추가되어 데이터베이스 인스턴스의 우발적 또는 비우발적 삭제로 인한 데이터 손실을 방지할 수 있습니다. 삭제 보호는 규제 준수 요구 사항을 충족하고 비즈니스 연속성을 보장하는 데에도 도움이 됩니다.

자세한 내용은 Aurora 클러스터의 삭제 방지를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

추가 리소스

Aurora 클러스터의 삭제 방지

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙:
- 입력 파라미터
- 최종 업데이트 시간

## RDS DB 인스턴스 자동 마이너 버전 업그레이드 확인

설명

Amazon RDS DB 인스턴스에 자동 마이너 버전 업그레이드가 구성되어 있는지 확인합니다.

Amazon RDS 인스턴스의 자동 마이너 버전 업그레이드를 활성화하여 데이터베이스가 항상 안전하고 안정적인 최신 버전을 실행하도록 하십시오. 마이너 업그레이드는 보안 업데이트, 버그 수정, 성능 개선을 제공하고 기존 애플리케이션과의 호환성을 유지합니다.

자세한 내용은 DB 인스턴스 엔진 버전 업그레이드를 참조하세요.

> **Note**
>
> 이 검사 결과는 매일 여러 번 자동으로 새로 고쳐지며 새로 고침 요청은 허용되지 않습니다. 변경 사항이 표시되는 데 몇 시간이 걸릴 수도 있습니다. 현재 이 검사에서 리소스를 제외할 수 없습니다.

검사 ID

```
c18d2gz155
```

소스

```
AWS Config Managed Rule: rds-automatic-minor-version-upgrade-enabled
```

알림 기준

노란색: RDS DB 인스턴스에는 자동 마이너 버전 업그레이드가 켜져 있지 않습니다.

권장 조치

Amazon RDS DB 인스턴스를 생성할 때 자동 마이너 버전 업그레이드를 활성화하십시오.

마이너 버전 업그레이드를 켜면 데이터베이스 버전이 수동으로 업그레이드된 엔진 버전보다 낮은 DB 엔진의 마이너 버전을 실행하는 경우 데이터베이스 버전이 자동으로 업그레이드됩니다.

보고서 열

- 상태 표시기
- 지역
- Resource
- AWS Config 규칙
- 입력 파라미터
- 최종 업데이트 시간

# 로그 변경 대상 AWS Trusted Advisor

Trusted Advisor 수표의 최근 변경 사항은 다음 주제를 참조하십시오.

> **Note**
>
> Trusted Advisor 콘솔 또는 AWS Support API를 사용하는 경우 제거된 검사는 검사 결과에 표시되지 않습니다. AWS Support API 작업이나 코드에서 검사 ID를 지정하는 등 제거된 검사를 사용하는 경우 API 호출 오류를 방지하려면 이러한 검사를 제거해야 합니다.

사용 가능한 검사에 대한 자세한 내용은 AWS Trusted Advisor 참조 확인 단원을 참조하세요.

## 검사 5개를 제거하고 검사 1개를 추가했습니다.

Trusted Advisor 2024년 5월 15일에 내결함성 검사 3개, 성능 검사 1개, 보안 검사 1개를 지원 중단했습니다.

- IAM 사용
- ELB 교차 영역 로드 밸런싱

- 과다 사용된 Amazon EBS 마그네틱 볼륨
- 인스턴스에 적용된 EC2 보안 그룹 규칙 수가 많음
- EC2 보안 그룹의 수많은 규칙

Trusted Advisor 2024년 5월 15일에 새로운 보안 검사 1개가 추가되었습니다.

- Amazon S3 서버 액세스 로그가 활성화됨

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 내결함성 검사가 제거되었습니다.

Trusted Advisor 2024년 4월 25일에 3 내결함성 검사 지원이 중단되었습니다.

- AWS Direct Connect 연결 리던던시
- AWS Direct Connect 위치 리던던시
- AWS Direct Connect 가상 인터페이스 리던던시

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 새로운 내결함성 검사

Trusted Advisor 2024년 2월 29일에 내결함성 검사 1개가 추가되었습니다.

- NLB - 프라이빗 서브넷의 인터넷 연결 리소스

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 내결함성 및 보안 검사 업데이트

Trusted Advisor 2024년 3월 28일에 새로운 내결함성 검사 1개를 추가하고 기존 내결함성 검사 1개와 보안 검사 1개를 수정했습니다.

- AWS Resilience Hub 애플리케이션 구성 요소 검사 추가
- AWS Lambda 다중 AZ 이중화 없이 업데이트된 VPC 지원 함수
- 더 AWS Lambda 이상 사용되지 않는 런타임을 사용하여 함수를 업데이트했습니다.

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 새로운 내결함성 검사

Trusted Advisor 2024년 1월 31일에 내결함성 검사 1개가 추가되었습니다.

- AWS Direct Connect 위치 복원력

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 내결함성 검사 업데이트

Trusted Advisor 2024년 1월 8일에 1건의 내결함성 검사를 수정했습니다.

- Amazon RDS innodb_flush_log_at_trx_commit 파라미터는 1이 아닙니다

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 보안 검사 업데이트

Trusted Advisor 2023년 12월 21일에 보안 검사 1건을 수정했습니다.

- AWS Lambda 더 이상 사용되지 않는 런타임을 사용하는 함수

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 새로운 보안 및 성능 검사

Trusted Advisor 2023년 12월 20일에 2개의 새로운 보안 검사와 2개의 새로운 성능 검사를 추가했습니다.

- data-in-transit 암호화를 사용하지 않는 Amazon EFS 클라이언트
- Amazon Aurora DB 클러스터가 읽기 워크로드를 위해 충분히 프로비저닝되지 않음
- 시스템 용량에 비해 Amazon RDS 인스턴스가 충분히 프로비저닝되지 않음
- 우분투 LTS를 사용하는 Amazon EC2 인스턴스 표준 지원 종료

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 새 보안 검사

Trusted Advisor 2023년 12월 15일에 새로운 보안 검사 1개가 추가되었습니다.

- S3 버킷을 직접 가리키는 Amazon Route 53 불일치 CNAME 레코드

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 새로운 내결함성 및 비용 최적화 검사

Trusted Advisor 2023년 12월 7일에 2개의 새로운 내결함성 검사와 1개의 새로운 비용 최적화 검사를 추가했습니다.

- 아마존 DocumentDB 단일 AZ 클러스터
- Amazon S3 미완료 멀티파트 업로드 중단 구성
- 차단 모드의 Amazon ECS AWS로그 드라이버

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 새로운 내결함성 검사

Trusted Advisor 2023년 11월 17일에 세 가지 새로운 내결함성 검사를 추가했습니다.

- ALB 멀티-AZ
- NLB 멀티-AZ
- 여러 AZ의 VPC 인터페이스 엔드포인트 네트워크 인터페이스

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## Amazon RDS에 대한 새로운 검사

Trusted Advisor 2023년 11월 15일에 Amazon RDS에 대한 37개의 새로운 검사를 추가했습니다.

자세한 내용은 AWS Trusted Advisor 참조 확인을 참조하세요.

## 새 API AWS Trusted Advisor

AWS Trusted Advisor Trusted Advisor 모범 사례 검사, 권장 사항 및 우선 순위가 지정된 권장 사항에 프로그래밍 방식으로 액세스할 수 있도록 하는 새 API를 소개합니다. Trusted Advisor API를 사용하면

선호하는 운영 도구와 프로그래밍 방식으로 통합하여 워크로드를 Trusted Advisor 대규모로 자동화하고 최적화할 수 있습니다. Business, Enterprise On-Ramp 또는 Enterprise Support 고객이 사용할 수 있는 새 API를 사용하면 사용자 계정 또는 지급인 계정 내의 모든 연결 계정에 대한 Trusted Advisor 권장 사항에 액세스할 수 있습니다. 관리 계정 또는 위임된 관리자 계정에 액세스할 수 있는 Enterprise Support 고객은 조직 전체에서 우선 순위가 지정된 권장 사항을 프로그래밍 방식으로 추가로 검색할 수 있습니다.

새 Trusted Advisor API는 이전에 AWS 지원 API (SAPI) 를 통해 제공되었던 세 가지 기능을 대체합니다. SAPI는 사례 및 기타 지원 정보를 계속 제공할 것입니다.

Trusted Advisor API는 일반적으로 미국 동부 (오하이오), 미국 동부 (버지니아 북부), 미국 서부 (오레곤), 아시아 태평양 (서울), 아시아 태평양 (시드니), 유럽 (아일랜드) 지역에서 사용할 수 있습니다.

자세한 내용은 API 페이지를 참조하십시오.AWS Trusted Advisor

## Trusted Advisor 체크 제거

Trusted Advisor 2023년 11월 9일에 다음 검사를 제거했습니다.

| 검사 이름 | 검사 범주 | 검사 ID |
| --- | --- | --- |
| EBS 볼륨은 EC2 인스턴스에 연결해야 합니다. | 보안 | Hs4Ma3G119 |
| S3 버킷에는 서버 측 암호화가 활성화되어 있어야 합니다. | 보안 | Hs4Ma3G167 |
| CloudFront 배포에는 원본 액세스 ID가 활성화되어 있어야 합니다. | 보안 | Hs4Ma3G195 |

## AWS Config 검사 통합: Trusted Advisor

Trusted Advisor 2023년 10월 AWS Config 30일에 64개의 새로운 검사가 추가되었습니다.

자세한 내용은 AWS Config에 의해 구동되는 AWS Trusted Advisor 검사 보기을 참조하세요.

## 새로운 내결함성 검사

Trusted Advisor 2023년 10월 12일에 다음 체크를 추가했습니다.

- 아마존 RDS ReplicaLag
- 아마존 RDS FreeStorageSpace
- 아마존 RDS DiskQueueDepth
- Amazon Route 53 Resolver 엔드포인트 가용 영역 이중화
- 서브넷에서 사용 가능한 IP Auto Scaling
- 너무 많은 파티션을 호스팅하는 Amazon MSK 브로커

자세한 내용은 내결함성 범주를 참조하세요.

## 새로운 서비스 한도 검사

Trusted Advisor 2023년 8월 17일에 다음 검사를 추가했습니다.

- Lambda 코드 스토리지 사용량

자세한 내용은 서비스 한도 범주를 참조하세요.

## 새로운 내결함성 검사

Trusted Advisor 2023년 8월 3일에 다음 체크를 추가했습니다.

- AWS Lambda 장애 이벤트 목적지 시

자세한 내용은 내결함성 범주를 참조하세요.

## 새로운 내결함성 및 성능 검사

Trusted Advisor 2023년 6월 1일에 다음 검사를 추가했습니다.

- Amazon EFS 노 마운트 타겟 이중화
- Amazon EFS 처리량 모드 최적화
- ActiveMQ 가용 영역 이중화
- RabbitMQ 가용 영역 이중화

자세한 내용은 내결함성 범주 및 성능 범주를 참조하세요.

## 새로운 내결함성 검사

Trusted Advisor 2023년 5월 16일에 다음 체크를 추가했습니다.

- NAT 게이트웨이 AZ 독립성
- 단일 AZ 애플리케이션 검사

자세한 내용은 내결함성 범주를 참조하세요.

## 새로운 내결함성 검사

Trusted Advisor 2023년 4월 27일에 다음 체크를 추가했습니다.

- AWS 리전 인시던트 관리자 복제 세트의 수
- AWS Resilience Hub 평가 연령

자세한 내용은 내결함성 범주를 참조하세요.

## Amazon ECS 내결함성 검사의 지역 확장

Trusted Advisor 2023년 4월 27일에 다음 검사를 추가 지역으로 확대했습니다. Trusted Advisor 이제 Amazon ECS를 일반적으로 사용할 수 있는 모든 지역에서 Amazon ECS 검사를 사용할 수 있습니다.

- 단일 AZ를 사용하는 Amazon ECS 서비스
- Amazon ECS 다중 AZ 배치 전략

리전은 아프리카(케이프타운), 아시아 태평양(홍콩), 아시아 태평양(하이데라바드), 아시아 태평양(자카르타), 아시아 태평양(멜버른), 유럽(밀라노), 유럽(스페인), 유럽(취리히), 중동(바레인), 중동(UAE)으로 확장됩니다.

## 새로운 내결함성 검사

Trusted Advisor 2023년 3월 30일에 다음 검사를 추가했습니다.

- 단일 AZ를 사용하는 Amazon ECS 서비스
- Amazon ECS 다중 AZ 배치 전략

자세한 내용은 내결함성 범주를 참조하세요.

## 새로운 내결함성 검사

Trusted Advisor 2022년 12월 15일에 다음 체크를 추가했습니다.

- AWS CloudHSM 단일 AZ에서 HSM 인스턴스를 실행하는 클러스터
- 아마존 ElastiCache 다중 AZ 클러스터
- Amazon MemoryDB 다중 AZ 클러스터

AWS CloudHSM ElastiCache, 및 MemoryDB 클러스터의 결과를 받으려면 Trusted Advisor 가용 영역에 클러스터가 있어야 합니다. 자세한 내용은 다음 설명서를 참조하세요.

- AWS CloudHSM 사용 설명서
- Amazon MemoryDB for Redis 개발자 안내서
- ElastiCache Redis용 Amazon 사용 설명서

Trusted Advisor 2022년 12월 15일에 다음 점검 정보를 업데이트했습니다.

- AWS Resilience Hub 정책 위반 — 앱 이름이 애플리케이션 이름으로 업데이트되었습니다.
- AWS Resilience Hub 복원력 점수 - 애플리케이션 이름 및 애플리케이션 복구 점수가 애플리케이션 이름 및 애플리케이션 복구 점수로 업데이트되었습니다.

자세한 내용은 내결함성 범주를 참조하세요.

## 와의 통합 업데이트 Trusted AdvisorAWS Security Hub

Trusted Advisor 2022년 11월 17일에 다음과 같은 업데이트를 적용했습니다.

Security AWS Config Hub를 사용하지 않도록 설정하거나 사용하지 않도록 설정하는 경우 Trusted Advisor 이제 7~9일 AWS 리전 내에 해당 제어 결과를 제거합니다. AWS 리전이전에는 Security Hub 데이터를 제거하는 데 90일이 Trusted Advisor 걸렸습니다.

자세한 내용은 문제 해결 주제의 다음 단원을 참조하세요.

- 리전에서 Security Hub 또는 AWS Config를 비활성화했습니다.
- 내 컨트롤은 Security Hub에 아카이빙되어 있지만 Trusted Advisor에서 결과는 여전히 볼 수 있습니다.

## AWS Resilience Hub에 대한 새로운 내결함성 검사

Trusted Advisor 2022년 11월 17일에 다음 검사를 추가했습니다.

- AWS Resilience Hub 정책 위반
- AWS Resilience Hub 레질리언스 점수

애플리케이션의 최신 복원성 정책 상태 및 복원성 점수를 확인하기 위해 이러한 검사를 사용할 수 있습니다. 복원성과 가용성을 정의, 추적 및 관리할 수 있는 중앙 위치를 제공합니다. Resilience Hub는 애플리케이션의 복원성 및 가용성을 정의, 추적 및 관리할 수 있는 중심지를 제공합니다.

Resilience Hub 애플리케이션에 Trusted Advisor 대한 결과를 받으려면 애플리케이션을 배포하고 Resilience Hub를 사용하여 AWS 애플리케이션의 복원력 상태를 추적해야 합니다. 자세한 내용은 AWS Resilience Hub 사용 설명서를 참조하세요.

사용자 ElastiCache 및 MemoryDB 클러스터에 대한 결과를 받으려면 Trusted Advisor 가용 영역에 클러스터가 있어야 합니다. 자세한 내용은 다음 설명서를 참조하세요.

- Amazon MemoryDB for Redis 개발자 안내서
- ElastiCache Redis용 Amazon 사용 설명서

자세한 내용은 내결함성 범주를 참조하세요.

## 콘솔 업데이트 Trusted Advisor

Trusted Advisor 2022년 11월 16일에 다음 변경 사항이 추가되었습니다.

콘솔의 Trusted Advisor 대시보드는 이제 Trusted Advisor 권장 사항입니다. 이 Trusted Advisor 권장 사항 페이지에는 여전히 검사 결과와 AWS 계정의 각 범주에 사용할 수 있는 검사가 표시됩니다.

이 이름 변경은 Trusted Advisor 콘솔만 업데이트합니다. 평소처럼 Trusted Advisor 콘솔과 AWS Support API의 Trusted Advisor 작업을 계속 사용할 수 있습니다.

자세한 정보는 Trusted Advisor 권장 사항 시작하기을 참조하세요.

## Amazon EC2에 대한 새로운 검사

Trusted Advisor 2022년 9월 1일에 다음 검사를 추가했습니다.

- Microsoft Windows Server를 사용하는 Amazon EC2 인스턴스 지원 종료

자세한 내용은 보안 범주를 참조하세요.

## Trusted Advisor에 Security Hub 검사 추가

2022년 6월 23일부터 2022년 4월 7일까지 사용할 수 있는 Security Hub Trusted Advisor 컨트롤만 지원합니다. 이 릴리스는 AWS 기본 보안 모범 사례 보안 표준의 모든 컨트롤을 지원합니다. 단, 복구 > 복구 범주의 컨트롤은 예외입니다. 자세한 정보는 AWS Trusted Advisor에서 AWS Security Hub 컨트롤 보기을 참조하세요.

지원되는 컨트롤 목록은 AWS Security Hub 사용 설명서의 AWS Foundational Security Best Practices 컨트롤을 참조하세요.

## 에서 검사를 추가했습니다. AWS Compute Optimizer

Trusted Advisor 2022년 5월 4일에 다음 체크를 추가했습니다.

| 검사 이름 | 검사 범주 | 검사 ID |
| --- | --- | --- |
| Amazon EBS 과다 프로비저닝된 볼륨 | 비용 최적화 | `COr6dfpM03` |
| Amazon EBS 과소 프로비저닝된 볼륨 | 성능 | `COr6dfpM04` |
| AWS Lambda 메모리 크기를 위해 오버프로비저닝된 함수 | 비용 최적화 | `COr6dfpM05` |
| AWS Lambda 메모리 크기에 비해 부족하게 프로비저닝된 함수 | 성능 | `COr6dfpM06` |

Compute Optimizer를 AWS 계정 선택하여 이러한 검사에서 Lambda 및 Amazon EBS 리소스로부터 데이터를 수신할 수 있도록 해야 합니다. 자세한 정보는 Trusted Advisor 수표 AWS Compute Optimizer 신청을 참조하세요.

## 노출된 액세스 키 검사 업데이트

Trusted Advisor 2022년 4월 25일에 다음 검사를 업데이트했습니다.

| 검사 이름 | 검사 범주 | 검사 ID |
| --- | --- | --- |
| 노출된 액세스 키 | 보안 | 12Fnkpl8Y5 |

Trusted Advisor 이제 이 체크가 자동으로 새로 고쳐집니다. 이 체크는 Trusted Advisor 콘솔 또는 API에서 수동으로 새로 고칠 수 없습니다. AWS Support 애플리케이션 또는 코드에서 이 검사를 새로 고치는 경우 이 검사를 더 이상 새로 고치지 않도록 AWS 계정업데이트하는 것이 좋습니다. 그렇지 않으면 `InvalidParameterValue`오류가 발생할 수 있습니다.

이 업데이트 이전에 제외한 액세스 키는 더 이상 제외되지 않으며 영향을 받은 리소스로 표시됩니다. 검사 결과에서 액세스 키를 제외할 수 없습니다. 자세한 정보는 노출된 액세스 키을 참조하세요.

> **Note**
>
> 2022년 4월 25일 AWS 계정 이후에 생성한 액세스 키의 경우 노출된 액세스 키의 검사 결과에는 노출되지 않은 액세스 키의 경우에도 처음에는 회색 아이콘 ( ) 이 표시됩니다. 이는 Trusted Advisor 가 검사 변경 사항을 확인하지 않았다는 것을 의미합니다.
> 위험에 처한 리소스가 Trusted Advisor 식별되면 상태가 조치 권장 아이콘 ()
>
> 으로 변경됩니다. 리소스를 수정하거나 삭제한 후 검사 결과는 확인 표시 아이콘 ( ) 을 표시합니다.

## AWS Direct Connect검사가 업데이트됨

Trusted Advisor 2022년 3월 29일에 다음 검사를 업데이트했습니다.

| 검사 이름 | 검사 범주 | 검사 ID |
| --- | --- | --- |
| AWS Direct Connect 연결 리던던시 | 내결함성 | 0t121N1Ty3 |

| 검사 이름 | 검사 범주 | 검사 ID |
| --- | --- | --- |
| AWS Direct Connect 위치 리던던시 | 내결함성 | 8M012Ph3U5 |
| AWS Direct Connect 가상 인터페이스 리던던시 | 내결함성 | 4g3Nt5M1Th |

- 리전 열의 값에 이제 전체 이름 대신 AWS 리전 코드가 표시됩니다. 예를 들어 미국 동부(버지니아 북부)의 리소스는 값이 이제 `us-east-1`입니다.
- 타임스탬프 열의 값이 이제 RFC 3339 형식(예: `2022-03-30T01:02:27.000Z`)으로 표시됩니다.
- 발견된 문제가 없는 리소스가 이제 검사 테이블에 나타납니다. 이러한 리소스에는 옆에 확인 표시 아이콘
  (  )
  이 있습니다.

  이전에는 조사를 Trusted Advisor 권장하는 리소스만 표에 표시되었습니다. 이러한 리소스에는 옆에 경고 아이콘
  (  )
  이 있습니다.

## AWS Security HubAWS Trusted Advisor 콘솔에 컨트롤이 추가되었습니다.

AWS Trusted Advisor 2022년 1월 18일에 보안 범주에 111개의 Security Hub 컨트롤을 추가했습니다.

AWS 기본 보안 모범 사례 보안 표준에서 Security Hub 컨트롤에 대한 조사 결과를 확인할 수 있습니다. 이 통합에는 범주: 복구 > 복원성(Category: Recover > Resilience)이 있는 컨트롤은 포함되지 않습니다.

이 기능에 대한 자세한 내용은 AWS Trusted Advisor에서 AWS Security Hub 컨트롤 보기 섹션을 참조하세요.

## Amazon EC2 및 AWS Well-Architected에 대한 새로운 검사

Trusted Advisor 2021년 12월 20일에 다음 검사를 추가했습니다.

- Microsoft SQL Server용 Amazon EC2 인스턴스 통합

- Microsoft SQL Server에 대해 과다 프로비저닝된 Amazon EC2 인스턴스
- Microsoft SQL Server를 사용하는 Amazon EC2 인스턴스 지원 종료
- 비용 최적화에 대한 AWS Well-Architected 위험도 높음 문제
- 성능에 대한 AWS Well-Architected 위험도 높음 문제
- 보안에 대한 AWS Well-Architected 위험도 높음 문제
- 안정성에 대한 AWS Well-Architected 위험도 높음 문제

자세한 내용은 AWS Trusted Advisor 검사 참조를 참조하세요.

## Amazon OpenSearch 서비스의 체크 이름 업데이트

Trusted Advisor 2021년 9월 8일에 Amazon OpenSearch Service Reserved Instance Optimization 수표의 이름을 업데이트했습니다.

검사 권장 사항, 범주 및 ID는 동일합니다.

| 검사 이름 | 검사 범주 | 검사 ID |
| --- | --- | --- |
| Amazon OpenSearch 서비스 예약 인스턴스 최적화 | 비용 최적화 | `7ujm6yhn5t` |

> **Note**
>
> Amazon Trusted Advisor CloudWatch 지표에 사용하는 경우 이 검사의 지표 이름도 업데이트됩니다. 자세한 정보는 AWS Trusted Advisor 지표를 모니터링하여 Amazon CloudWatch 경보 생성을 참조하세요.

## Amazon Elastic Block Store 볼륨 스토리지에 대한 검사가 추가됨

Trusted Advisor 2021년 6월 8일에 다음 검사를 추가했습니다.

| 검사 이름 | 검사 범주 | 검사 ID |
| --- | --- | --- |
| EBS 범용 SSD(gp3) 볼륨 스토리지 | 서비스 한도 | `dH7RR0l6J3` |

| 검사 이름 | 검사 범주 | 검사 ID |
| --- | --- | --- |
| EBS 프로비저닝된 IOPS SSD(io2) 볼륨 스토리지 | 서비스 한도 | gI7MM0l7J2 |

## 에 대한 검사가 추가되었습니다. AWS Lambda

Trusted Advisor 2021년 3월 8일에 다음 체크를 추가했습니다.

| 검사 이름 | 검사 범주 | 검사 ID |
| --- | --- | --- |
| AWS Lambda 타임아웃이 너무 많은 함수 | 비용 최적화 | L4dfs2Q3C3 |
| AWS Lambda 오류율이 높은 함수 | 비용 최적화 | L4dfs2Q3C2 |
| AWS Lambda 더 이상 사용되지 않는 런타임을 사용하는 함수 | 보안 | L4dfs2Q4C5 |
| AWS Lambda 다중 AZ 이중화가 없는 VPC 지원 함수 | 내결함성 | L4dfs2Q4C6 |

Lambda에서AWS Lambda 이러한 검사를 사용하는 방법에 대한 자세한 내용은 개발자 안내서의 권장 사항을 보기 위한 AWS Trusted Advisor 예제 워크플로를 참조하십시오.

## Trusted Advisor 수표 제거

Trusted Advisor 2021년 3월 AWS GovCloud (US) Region 8일에 대한 다음 체크를 삭제했습니다.

| 검사 이름 | 검사 범주 | 검사 ID |
| --- | --- | --- |
| EC2 탄력적 IP 주소 | 서비스 한도 | aW9HH0l8J6 |

# Amazon Elastic Block Store 검사가 업데이트됨

Trusted Advisor 2021년 3월 5일에 다음 검사를 위해 Amazon EBS 볼륨 단위를 기비바이트 (GiB) 에서 테비바이트 (TiB) 로 업데이트했습니다.

> **Note**
>
> Amazon Trusted Advisor CloudWatch 지표에 사용하는 경우 이 다섯 가지 검사에 대한 지표 이름도 업데이트됩니다. 자세한 정보는 AWS Trusted Advisor 지표를 모니터링하여 Amazon CloudWatch 경보 생성을 참조하세요.

| 검사 이름 | 검사 범주 | 검사 ID | 에 대한 CloudWatch 측정치를 업데이트했습니다. ServiceLimit |
|---|---|---|---|
| EBS 콜드 HDD(sc1) 볼륨 스토리지 | 서비스 한도 | gH5CC0e3J9 | 콜드 HDD(sc1) 볼륨 스토리지(TiB) |
| EBS 범용 SSD(gp2) 볼륨 스토리지 | 서비스 한도 | dH7RR0l6J9 | 범용 SSD(gp2) 볼륨 스토리지 (TiB) |
| EBS 마그네틱(표준) 볼륨 스토리지 | 서비스 한도 | cG7HH0l7J9 | 마그네틱(표준) 볼륨 스토리지 (TiB) |
| EBS 프로비저닝된 IOPS SSD(io1) 볼륨 스토리지 | 서비스 한도 | gI7MM0l7J9 | 프로비저닝된 IOPS(SSD) 스토리지 (TiB) |
| EBS 처리량 최적화 HDD(st1) 볼륨 스토리지 | 서비스 한도 | wH7DD0l3J9 | 처리량 최적화 HDD(st1) 볼륨 스토리지(TiB) |

# Trusted Advisor 수표 제거

> **Note**
>
> Trusted Advisor 2020년 11월 18일에 다음 검사 항목이 제거되었습니다.

| 2020년 11월 18일에 검사가 제거됨 | 검사 범주 | 검사 ID |
|---|---|---|
| EC2 Windows 인스턴스용 EC2Config 서비스 | 내결함성 | V77iOLlBqz |
| EC2 Windows 인스턴스용 ENA 드라이버 버전 | 내결함성 | TyfdMXG69d |
| EC2 Windows 인스턴스용 NVMe 드라이버 버전 | 내결함성 | yHAGQJV9K5 |
| EC2 Windows 인스턴스용 PV 드라이버 버전 | 내결함성 | Wnwm9Il5bG |
| EBS 활성 볼륨 | 서비스 한도 | fH7LL0l7J9 |

이제 Amazon Elastic Block Store에서 사용자가 프로비저닝할 수 있는 볼륨 수에는 제한이 없습니다.

다른 서드 파티 도구인 AWS Systems Manager Distributor를 사용하여 Amazon EC2 인스턴스를 모니터링해서 최신 상태 여부를 확인할 수도 있고, Windows Management Instrumentation(WMI)에 대한 드라이버 정보를 반환하도록 자체 스크립트를 작성할 수도 있습니다.

## Trusted Advisor 수표 제거

Trusted Advisor 2020년 2월 18일에 다음 체크를 제거했습니다.

| 검사 이름 | 검사 범주 | 검사 ID |
|---|---|---|
| 서비스 한도 | 성능 | eW7HH0l7J9 |

# AWS Support 슬랙의 앱

AWS Support 앱을 사용하여 Slack에서 AWS 지원 사례를 관리할 수 있습니다. 팀원을 채팅 채널에 초대하고, 사례 업데이트에 응답하고, 지원 담당자와 직접 채팅하세요. AWS Support 앱을 사용하여 Slack에서 지원 사례를 빠르게 관리하세요.

AWS Support 앱을 사용하여 다음을 수행하십시오.

- Slack 채널에서 지원 사례 생성, 업데이트, 검색 및 해결
- 지원 사례에 파일 첨부
- Service Quotas에서 할당량 증가 요청
- Slack 채널을 떠나지 않고 지원 사례 세부 정보를 팀과 공유
- 지원 에이전트와 실시간 채팅 세션 시작

AWS Support 앱에서 지원 사례를 생성, 업데이트 또는 해결하면 사례도 에서 업데이트됩니다 AWS Support Center Console. 지원 사례를 별도로 관리하기 위해 지원 센터 콘솔에 로그인할 필요가 없습니다.

> **참고**
>
> - 사례를 Slack에서 생성했든 지원 센터 콘솔에서 생성했든 상관없이 지원 사례에 대한 응답 시간은 동일합니다.
> - 계정 및 결제 지원, 서비스 할당량 증가, 기술 지원에 대한 지원 사례를 생성할 수 있습니다.

주제


- 필수 조건
- Slack 작업 영역 승인
- Slack 채널 구성
- Slack 채널에서 지원 사례 생성
- Slack의 지원 사례에 회신
- 라이브 채팅 세션에 참여하세요 AWS Support
- Slack에서 지원 사례 검색
- Slack의 지원 사례 해결

- Slack에서 지원 사례 다시 열기
- 서비스 할당량 증가 요청
- AWS Support 앱에서 Slack 채널 구성 삭제
- AWS Support 앱에서 Slack 작업 영역 구성 삭제
- Slack의 AWS Support 앱 명령
- AWS Support Center Console에서 AWS Support 앱 서신 보기
- AWS CloudFormation으로 Slack 리소스에서 AWS Support 앱 생성

# 필수 조건

Slack에서 AWS Support 앱을 사용하려면 다음 요구 사항을 충족해야 합니다.

- Business, Enterprise On-Ramp 또는 Enterprise Support 플랜을 이용 중입니다. 지원 플랜은 AWS Support Center Console 또는 지원 플랜 페이지에서 찾을 수 있습니다. 자세한 내용은 AWS Support 플랜 비교를 참조하세요.
- 조직에 대한 Slack 작업 영역과 채널이 있습니다. Slack 작업 영역 관리자이거나 해당 Slack 작업 영역에 앱을 추가할 권한이 있어야 합니다. 자세한 내용은 Slack 도움말 센터를 참조하세요.
- AWS 계정에 필요한 권한을 가진 AWS Identity and Access Management(IAM) 사용자 또는 역할로 로그인합니다. 자세한 내용은 AWS Support 앱 위젯에 대한 액세스 관리 섹션을 참조하세요.
- 작업을 수행하는 데 필요한 권한을 가진 IAM 역할을 생성해야 합니다. AWS Support 앱에서는 이 역할을 사용하여 다른 서비스에 대한 API를 호출합니다. 자세한 내용은 AWS Support 앱에 대한 액세스 관리 섹션을 참조하세요.

주제

- AWS Support 앱 위젯에 대한 액세스 관리
- AWS Support 앱에 대한 액세스 관리

## AWS Support 앱 위젯에 대한 액세스 관리

AWS Identity and Access Management(IAM) 정책을 연결하여 IAM 사용자에게 AWS Support Center Console에서 AWS Support 앱 위젯을 구성할 수 있는 권한을 부여할 수 있습니다.

정책을 IAM 엔터티에 연결하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 자격 증명 권한 추가(콘솔)를 참조하세요.

> **Note**
>
> AWS 계정에서 루트 사용자로 로그인할 수도 있지만 이렇게 하지 않는 것이 좋습니다. 루트 사용자 액세스에 대한 자세한 내용은 IAM 사용 설명서의 루트 사용자 보안 인증을 보호하고 일상적인 작업에 사용하지 마세요를 참조하세요.

## IAM 정책 예제

IAM 사용자 또는 그룹과 같은 엔터티에 다음 정책을 연결할 수 있습니다. 이 정책을 사용하여 Slack 작업 공간을 승인하고 지원 센터 콘솔에서 Slack 채널을 구성할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportapp:GetSlackOauthParameters",
                "supportapp:RedeemSlackOauthCode",
                "supportapp:DescribeSlackChannels",
                "supportapp:ListSlackWorkspaceConfigurations",
                "supportapp:ListSlackChannelConfigurations",
                "supportapp:CreateSlackChannelConfiguration",
                "supportapp:DeleteSlackChannelConfiguration",
                "supportapp:DeleteSlackWorkspaceConfiguration",
                "supportapp:GetAccountAlias",
                "supportapp:PutAccountAlias",
                "supportapp:DeleteAccountAlias",
                "supportapp:UpdateSlackChannelConfiguration",
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

### Slack에 AWS Support 앱을 연결하는 데 필요한 권한

AWS Support 앱에는 API 작업에 직접 해당하지 않는 권한 전용 작업이 포함되어 있습니다. 이러한 작업은 Service Authorization Reference(서비스 인증 참조)에서 [permission only]([권한 전용])로 표시됩니다.

AWS Support 앱은 다음 API 작업을 사용하여 Slack에 연결한 다음 AWS Support Center Console에 퍼블릭 Slack 채널을 나열합니다.

- `supportapp:GetSlackOauthParameters`
- `supportapp:RedeemSlackOauthCode`
- `supportapp:DescribeSlackChannels`

이러한 API 작업은 코드로 호출되는 것이 아닙니다. 따라서 이러한 API 작업은 AWS CLI 및 AWS SDK에 포함되지 않습니다.

## AWS Support 앱에 대한 액세스 관리

AWS Support 앱 위젯에 대한 권한을 얻은 후 AWS Identity and Access Management(IAM) 역할을 생성해야 합니다. 이 역할은 AWS Support API 및 Service Quotas와 같은 다른 AWS 서비스의 작업을 수행합니다.

그런 다음 해당 역할에 이러한 작업을 완료하는 데 필요한 권한을 부여하는 IAM 정책을 이 역할에 연결합니다. 지원 센터 콘솔에서 Slack 채널 구성을 생성할 때 이 역할을 선택합니다.

Slack 채널의 사용자는 IAM 역할에 부여한 것과 동일한 권한을 가집니다. 예를 들어 지원 사례에 대한 읽기 전용 액세스 권한을 지정할 경우 Slack 채널의 사용자는 지원 사례를 볼 수 있지만 업데이트할 수는 없습니다.

> **Important**
>
> 지원 에이전트와의 실시간 채팅을 요청하고 새 비공개 채널을 실시간 채팅 채널 기본 설정으로 선택하면 AWS Support 앱에서 별도의 Slack 채널을 생성합니다. 이 Slack 채널은 사례를 생성하거나 채팅을 시작한 채널과 동일한 권한을 가집니다.
>
> IAM 역할 또는 IAM 정책을 변경하면 구성된 Slack 채널과 AWS Support 앱에서 생성하는 새로운 실시간 채팅 Slack 채널에 변경 사항이 적용됩니다.

다음 절차에 따라 IAM 역할 및 정책을 생성합니다.

주제


- AWS 관리형 정책 사용 또는 고객 관리형 정책 생성
- IAM 역할 생성
- 문제 해결


## AWS 관리형 정책 사용 또는 고객 관리형 정책 생성

역할 권한을 부여하려면 AWS 관리형 정책이나 고객 관리형 정책을 사용할 수 있습니다.

> **Tip**
>
> 정책을 수동으로 생성하지 않으려면 AWS 관리형 정책을 대신 사용하고 이 절차를 건너뛰는 것이 좋습니다. 관리형 정책은 AWS Support 앱에 필요한 권한을 자동으로 사용합니다. 정책을 수동으로 업데이트할 필요가 없습니다. 자세한 내용은 AWS Slack의 AWS Support 앱에 대한 관리형 정책 섹션을 참조하세요.

다음 절차에 따라 역할에 맞는 고객 관리형 정책을 생성합니다. 이 절차에서는 IAM 콘솔에서 JSON 정책 편집기를 사용합니다.

AWS Support 앱을 위한 고객 관리형 정책을 생성하는 방법

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Policies(정책)을 선택합니다.
3. [정책 생성(Create policy)]을 선택합니다.
4. JSON 탭을 선택합니다.
5. JSON을 입력한 다음 편집기에서 기본 JSON을 교체합니다. 예제 정책을 사용할 수 있습니다.
6. Next: Tags(다음: 태그)를 선택합니다.
7. (선택 사항) 태그를 키 값 페어로 사용하여 메타데이터를 정책에 추가할 수 있습니다.
8. Next: Review(다음: 검토)를 선택합니다.
9. Review Policy(정책 검토) 페이지에서 Name(이름)(예: *AWSSupportAppRolePolicy*) 및 Description(설명)(선택 사항)을 입력합니다(선택 사항).
10. Summary(요약) 페이지를 검토하여 정책에서 허용하는 권한을 확인한 다음 Create policy(정책 생성)를 선택합니다.

이 정책은 이 역할이 수행할 수 있는 작업을 정의합니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

IAM 정책 예제

IAM 역할에 다음 예제 정책을 연결할 수 있습니다. 이 정책은 역할이 AWS Support 앱에 필요한 모든 작업에 대한 전체 권한을 가질 수 있도록 허용합니다. 역할로 Slack 채널을 구성하면 채널의 모든 사용자가 동일한 권한을 가집니다.

> **Note**
>
> AWS 관리형 정책의 목록은 AWS Slack의 AWS Support 앱에 대한 관리형 정책 단원을 참조하세요.

AWS Support 앱에서 권한을 제거하도록 정책을 업데이트할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

각 작업에 대한 설명은 서비스 승인 참조에서 다음 항목을 참조하세요.

- AWS Support에 사용되는 작업, 리소스 및 조건 키
- Service Quotas에 사용되는 작업, 리소스 및 조건 키
- AWS Identity and Access Management에 사용되는 작업, 리소스 및 조건 키

## IAM 역할 생성

정책이 있으면 IAM 역할을 생성한 다음 이 정책을 해당 역할에 연결해야 합니다. 지원 센터 콘솔에서 Slack 채널 구성을 생성할 때 이 역할을 선택합니다.

AWS Support 앱에 대한 역할을 생성하려면

1. AWS Management Console에 로그인하여 https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할(Roles)을 선택한 후 역할 생성(Create role)을 선택합니다.
3. Select trusted entity(신뢰할 수 있는 엔터티 선택)에서 AWS 서비스를 선택합니다.
4. AWS Support 앱을 선택합니다.
5. 다음: 권한을 선택합니다.
6. 정책 이름을 입력합니다. AWS 관리형 정책을 선택하거나 생성한 고객 관리형 정책(예: *AWSSupportAppRolePolicy*)을 선택할 수 있습니다. 그런 다음 정책 옆의 확인란을 선택합니다.
7. Next: Tags(다음: 태그)를 선택합니다.
8. (선택 사항) 태그를 키 값 페어로 사용하여 메타데이터를 역할에 추가할 수 있습니다.
9. Next: Review(다음: 검토)를 선택합니다.
10. Role name(역할 이름)에 이름(예: *AWSSupportAppRole*)을 입력합니다.
11. (선택 사항) Role description(역할 설명)에 역할에 대한 설명을 입력합니다.
12. 역할을 검토한 다음 [Create role]을 선택합니다. 이제 지원 센터 콘솔에서 Slack 채널을 구성할 때 이 역할을 선택할 수 있습니다. Slack 채널 구성 섹션을 참조하세요.

자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 역할 생성을 참조하세요.

## 문제 해결

다음 항목을 참조하여 AWS Support 앱에 대한 액세스를 관리합니다.

목차


- 내 Slack 채널의 특정 사용자가 특정 작업을 하지 못하도록 제한하고 싶습니다.
- Slack 채널을 구성할 때 생성한 IAM 역할이 보이지 않습니다.
- 내 IAM 역할에 권한이 없습니다
- 내 IAM 역할이 유효하지 않다는 Slack 오류가 표시됩니다.
- AWS Support 앱에 Service Quotas에 대한 IAM 역할이 누락되었다는 메시지가 표시됩니다.


### 내 Slack 채널의 특정 사용자가 특정 작업을 하지 못하도록 제한하고 싶습니다.

기본적으로 Slack 채널의 사용자는 생성된 IAM 역할에 연결된 IAM 정책에 지정된 것과 동일한 권한을 가집니다. 즉, 채널의 모든 사용자는 AWS 계정이 있는지 IAM 사용자인지 여부에 상관없이 지원 사례에 대한 읽기 또는 쓰기 권한을 가집니다.

다음 모범 사례를 따르는 것이 좋습니다.

- AWS Support 앱으로 프라이빗 Slack 채널 구성
- 지원 사례에 액세스해야 하는 사용자만 채널에 초대하세요.
- AWS Support 앱에 필요한 최소 권한을 허용하는 IAM 정책을 사용합니다. AWS Slack의 AWS Support 앱에 대한 관리형 정책 섹션을 참조하세요.

### Slack 채널을 구성할 때 생성한 IAM 역할이 보이지 않습니다.

IAM 역할이 AWS Support 앱의 IAM 역할할 목록에 표시되지 않는 경우 해당 역할이 AWS Support 앱을 신뢰할 수 있는 엔터티로 간주하지 않거나 역할이 삭제되었습니다. 기존 추적을 업데이트하거나 다른 역할을 생성할 수 있습니다. IAM 역할 생성 섹션을 참조하세요.

### 내 IAM 역할에 권한이 없습니다

Slack 채널용으로 생성한 IAM 역할은 필요한 작업을 수행할 수 있는 권한이 필요합니다. 예를 들어 Slack의 사용자가 지원 사례를 생성하도록 하려면 역할에 `support:CreateCase` 권한이 있어야 합니다. AWS Support 앱은 이 역할이 이러한 작업을 대신 수행하는 것으로 간주합니다.

AWS Support 앱에서 권한 누락 오류가 발생하면 역할에 연결된 정책에 필요한 권한이 있는지 확인하세요.

이전 IAM 정책 예제을 참조하세요.

내 IAM 역할이 유효하지 않다는 Slack 오류가 표시됩니다.

채널 구성에 올바른 역할을 선택했는지 확인하세요.

역할을 확인하려면

1. https://console.aws.amazon.com/support/앱#/config 페이지에서 AWS Support Center Console에 로그인합니다.
2. AWS Support 앱에서 구성한 채널을 선택합니다.
3. Permissions(권한) 섹션에서 선택한 IAM 역할 이름을 찾습니다.
   - 역할을 변경하려면 Edit(편집)을 선택하고 다른 역할을 선택한 다음 Save(저장)를 선택합니다.
   - 역할 또는 역할에 연결된 정책을 업데이트하려면 IAM 콘솔에 로그인합니다.

AWS Support 앱에 Service Quotas에 대한 IAM 역할이 누락되었다는 메시지가 표시됩니다.

Service Quotas에서 할당량 증가를 요청하려면 계정에 `AWSServiceRoleForServiceQuotas` 역할이 있어야 합니다. 누락된 리소스에 대한 오류가 발생하는 경우 다음 단계 중 하나를 완료하세요.

- 할당량 증가를 요청하려면 Service Quotas 콘솔을 사용합니다. 요청이 성공하면 Service Quotas에서 이 역할을 자동으로 생성합니다. 그러면 AWS Support 앱을 사용하여 Slack에서 할당량 증가를 요청할 수 있습니다. 자세한 내용은 할당량 증가 요청을 참조하세요.
- 역할에 연결된 IAM 정책을 업데이트합니다. 이렇게 함으로써 Service Quotas에 역할 권한을 부여합니다. IAM 정책 예제의 다음 섹션에서는 AWS Support 앱이 Service Quotas 역할을 생성하도록 허용합니다.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
     }
}
```

채널에 대해 구성한 IAM 역할을 삭제할 경우 역할을 수동으로 생성하거나 AWS Support 앱의 역할 생성을 허용하도록 IAM 정책을 업데이트합니다.

## Slack 작업 영역 승인

작업 영역을 승인하고 AWS Support 앱에 작업 영역 액세스 권한을 부여한 후 AWS 계정에 대한 AWS Identity and Access Management(IAM) 역할이 필요합니다. AWS Support 앱은 이 역할을 사용하여 AWS Support 및 Service Quotas에서 API 작업을 호출합니다. 예를 들어 AWS Support 앱은 역할을 사용하여 Slack에서 사용자에 대한 지원 사례를 생성하기 위해 `CreateCase` 작업을 호출합니다.

> 주의
>
> - Slack 채널은 IAM 역할의 권한을 상속합니다. 즉, Slack 채널의 모든 사용자는 역할에 연결된 IAM 정책에 지정된 것과 동일한 권한을 가집니다.
>
>  예를 들어 IAM 정책에서 해당 역할이 지원 사례에 대한 전체 읽기 및 쓰기 권한을 갖도록 허용하는 경우 Slack 채널의 모든 사용자가 지원 사례를 생성하고 업데이트하고 해결할 수 있습니다. IAM 정책에서 역할에 읽기 전용 권한을 허용하는 경우 Slack 채널의 사용자는 지원 사례에 대한 읽기 권한만 가집니다.
> - 지원 작업을 관리하는 데 필요한 Slack 작업 영역 및 채널을 추가하는 것이 좋습니다. 프라이빗 채널을 구성하고 필요한 사용자만 초대하는 것이 좋습니다.

AWS 계정에 사용할 각 Slack 작업 영역을 승인해야 합니다. 여러 AWS 계정를 사용하는 경우 각 계정에 로그인하고 다음 절차를 반복하여 작업 영역을 승인해야 합니다. 계정이 AWS Organizations 내 조직에 속하고 여러 계정을 승인하려면 여러 계정 승인으로 건너뛰세요.

AWS 계정에 대한 Slack 작업 영역을 승인하려면

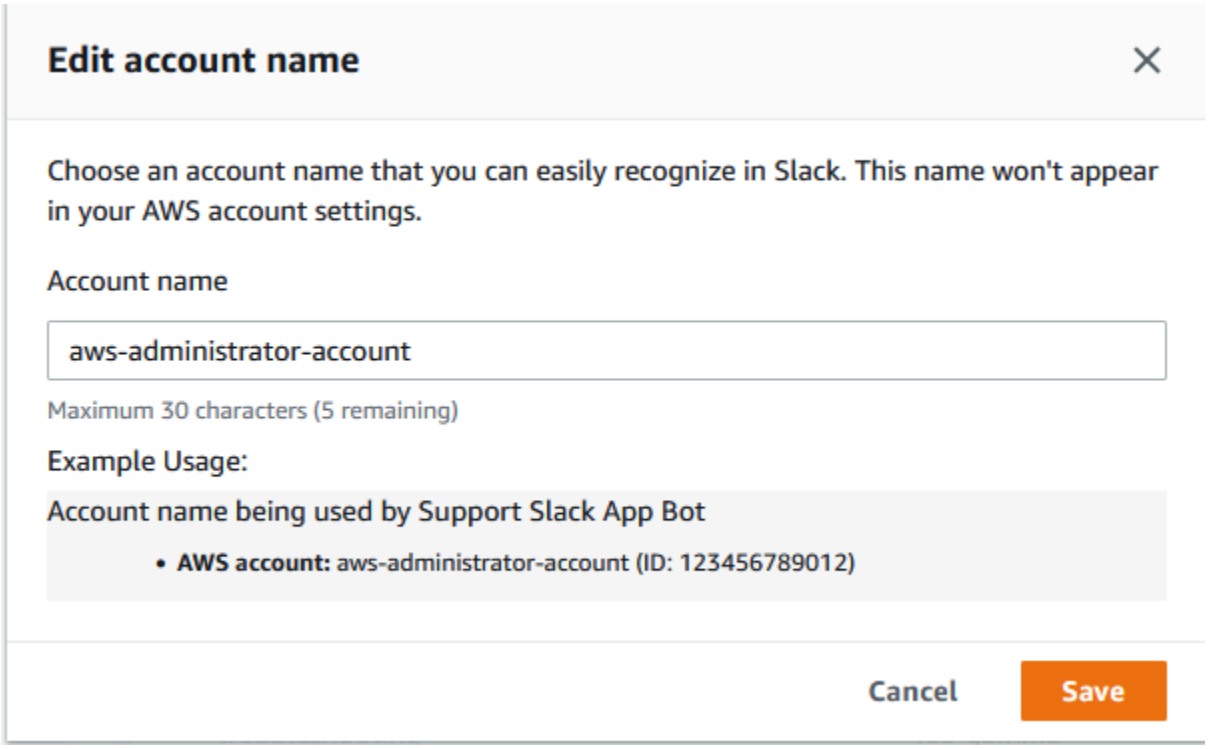
1. AWS Support Center Console에 로그인하고 Slack configuration(Slack 구성)을 선택합니다.
2. Getting started(시작하기) 페이지에서 Authorize workspace(작업 영역 승인)를 선택합니다.
3. 아직 Slack에 로그인하지 않은 경우 Sign in to your workspace(작업 영역에 로그인) 페이지에서 작업 영역 이름을 입력한 다음 Continue(계속)를 선택합니다.
4. AWS Support is requesting permission to access the your-workspace-name Slack 페이지에서 Allow(허용)를 선택합니다.

> **Note**
>
> Slack에 작업 영역에 액세스하도록 허용할 수 없는 경우 Slack 관리자로부터 AWS Support 앱을 작업 영역에 추가할 수 있는 권한이 있는지 확인합니다. 필수 조건 섹션을 참조하세요.

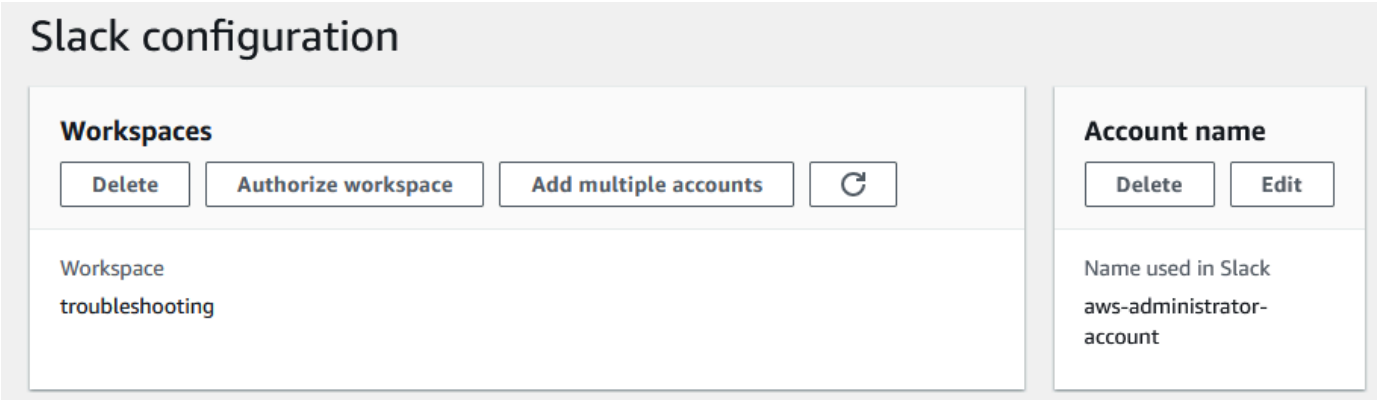
Slack configuration(Slack 구성) 페이지에서 작업 영역 이름이 Workspaces(작업 영역) 아래에 표시됩니다.

5. (선택 사항) 작업 영역을 더 추가하려면 Authorize workspace(작업 영역 승인)를 선택하고 3-4 단계를 반복합니다. 계정에 최대 5개의 작업 영역을 추가할 수 있습니다.
6. (선택 사항) 기본적으로 AWS 계정 ID 번호는 Slack 채널에 계정 이름으로 표시됩니다. 이 값을 변경하려면 Account name(계정 이름)에서 Edit(편집)을 선택하고 계정 이름을 입력한 다음 Save(저장)를 선택합니다.

> **Tip**
>
> 사용자와 팀이 쉽게 알아볼 수 있는 이름을 사용하세요. AWS Support 앱은 이 이름을 사용하여 Slack 채널에서 계정을 식별합니다. 언제든지 이 이름을 업데이트할 수 있습니다.




작업 영역 이름이 Slack configuration(Slack 구성) 페이지에 표시됩니다.




## 여러 계정 승인

Slack 작업 영역을 사용하도록 여러 AWS 계정에 권한을 부여하려면 AWS CloudFormation 또는 Terraform을 사용하여 AWS Support 앱 리소스를 생성할 수 있습니다.

# Slack 채널 구성

Slack 작업 영역을 승인한 후 AWS Support 앱을 사용하도록 Slack 채널을 구성할 수 있습니다.

AWS Support 앱을 초대하고 추가하는 채널에서 사례를 생성 및 검색하고 사례 알림을 받을 수 있습니다. 이 채널에서는 새로 생성되거나 해결된 사례, 추가된 서신, 공유된 사례 세부 정보 등의 사례 업데이트를 보여줍니다.

Slack 채널은 IAM 역할의 권한을 상속합니다. 즉, Slack 채널의 모든 사용자는 역할에 연결된 IAM 정책에 지정된 것과 동일한 권한을 가집니다.

예를 들어 IAM 정책에서 해당 역할이 지원 사례에 대한 전체 읽기 및 쓰기 권한을 갖도록 허용하는 경우 Slack 채널의 모든 사용자가 지원 사례를 생성하고 업데이트하고 해결할 수 있습니다. IAM 정책에서 역할에 읽기 전용 권한을 허용하는 경우 Slack 채널의 사용자는 지원 사례에 대한 읽기 권한만 가집니다.

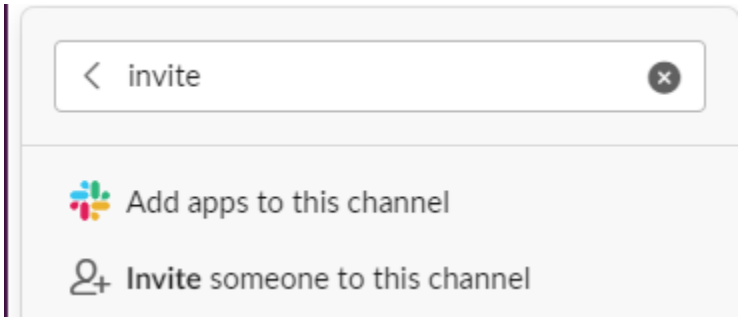
계정 당 최대 20개의 채널을 추가할 수 있습니다. Slack 채널은 최대 100개의 AWS 계정를 가질 수 있습니다. 즉, 100개의 계정만 AWS Support 앱에 동일한 Slack 채널을 추가할 수 있습니다. 조직의 지원 사례를 관리하는 데 필요한 계정만 추가하는 것이 좋습니다. 그러면 채널에서 받는 알림 수를 줄여 사용자와 팀이 방해 받는 일을 줄일 수 있습니다.

각 AWS 계정은 AWS Support 앱에서 Slack 채널을 별도로 구성해야 합니다. 그러면 AWS Support 앱에서 해당 AWS 계정의 지원 사례에 액세스할 수 있습니다. 조직의 다른 AWS 계정가 AWS Support 앱을 해당 Slack 채널에 이미 초대한 경우 3단계로 건너뜁니다.

> **Note**
>
> Slack Connect의 일부에 해당하는 채널 및 수많은 작업 영역과 공유되는 채널을 구성할 수 있습니다. 하지만 AWS Support 앱은 AWS 계정에 대해 공유 채널을 구성한 첫 번째 작업 영역에서만 사용할 수 있습니다. 다른 작업 영역에 동일한 Slack 채널을 구성하려고 시도할 경우, AWS Support 앱에서 오류 메시지가 반환됩니다.

Slack 채널을 구성하려면

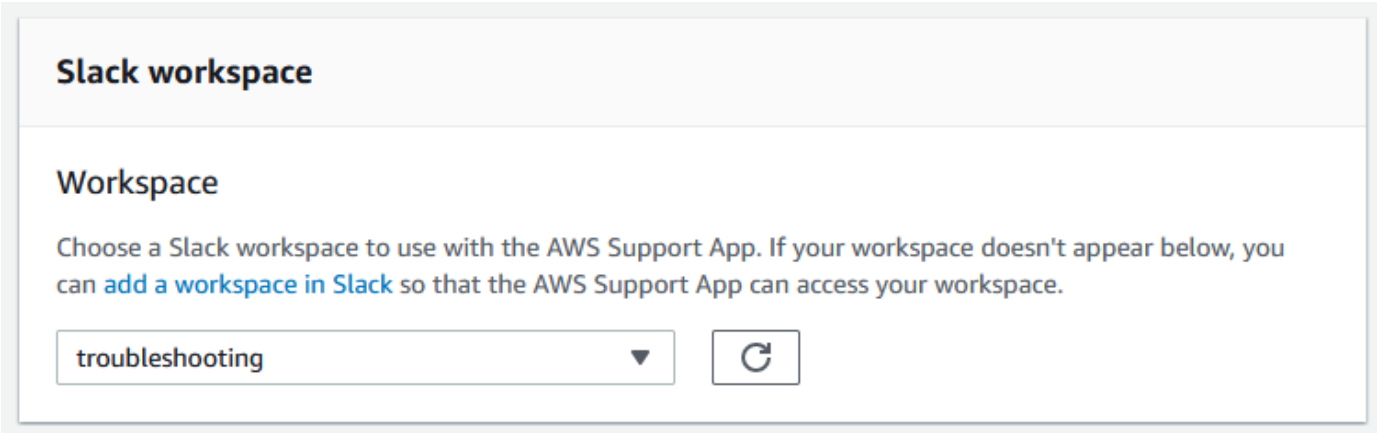
1. Slack 애플리케이션에서 AWS Support 앱에 사용할 Slack 채널을 선택합니다.
2. 다음 단계를 완료하여 AWS Support 앱을 채널에 초대합니다.
   a. + 아이콘을 선택하고 `invite`를 입력한 다음 메시지가 표시되면 Add 앱s to this channel(이 채널에 앱 추가)을 선택합니다.




b. 앱을 검색하려면 Add apps to channelName(channelName에 앱 추가)에 AWS Support App을 입력합니다.

c. AWS Support 앱 옆에 있는 Add(추가)를 선택합니다.


3. Support Center Console(지원 센터 콘솔)에 로그인하고 Slack configuration(Slack 구성)을 선택합니다.
4. Add channel(채널 추가)을 선택합니다.
5. Add channel(채널 추가) 페이지의 Workspace(작업 영역)에서 이전에 승인한 작업 영역 이름을 선택합니다. 작업 영역 이름이 목록에 표시되지 않는 경우 새로 고침 아이콘을 선택할 수 있습니다.



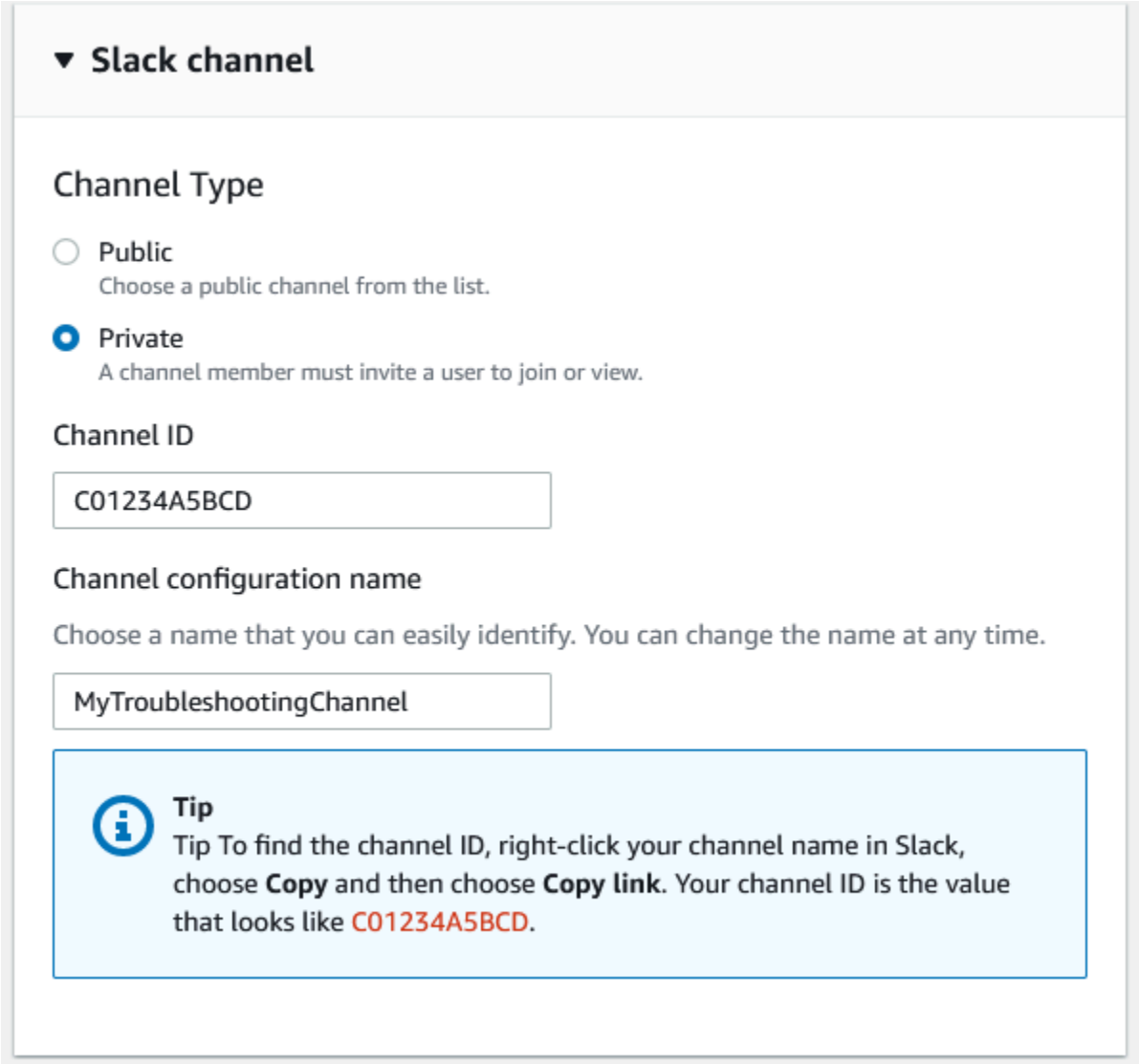

6. Slack channel(Slack 채널)의 Channel type(채널 유형)에서 다음 중 하나를 선택합니다.
   - Public(퍼블릭) - Public channel(퍼블릭 채널)에서 AWS Support 앱을 초대한 Slack 채널을 선택합니다(2단계). 채널이 목록에 표시되지 않으면 새로 고침 아이콘을 선택하고 다시 시도하세요.

- Private(프라이빗) - Channel ID(채널 ID)에서 AWS Support 앱을 초대한 Slack 채널의 ID 또는 URL을 입력합니다.

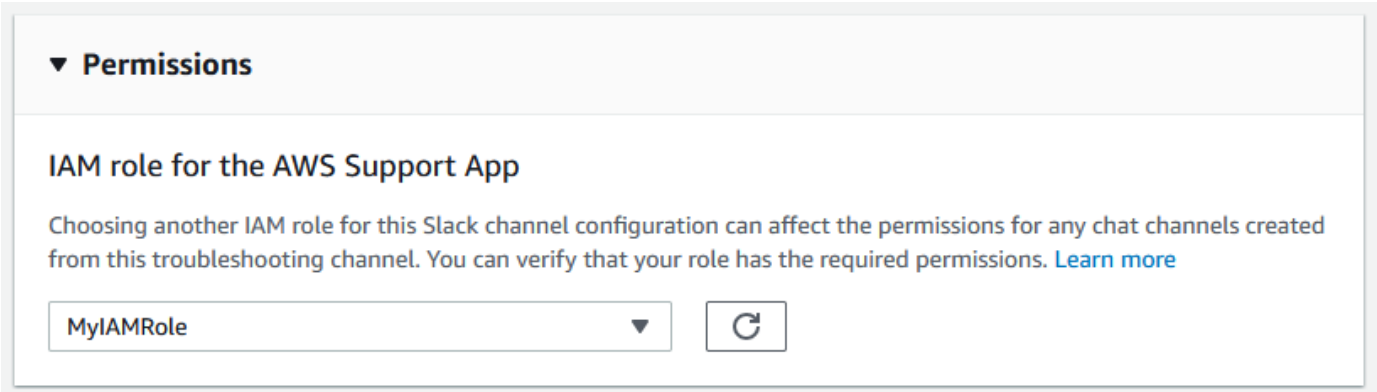
  > **Tip**
  >
  > 채널 ID를 찾으려면 Slack에서 채널 이름에 대한 컨텍스트(오른쪽 클릭) 메뉴를 연 다음 Copy(복사), Copy link(링크 복사)를 차례로 선택합니다. 채널 ID는 *C01234A5BCD*와 같은 값입니다.

7. Channel configuration name(채널 구성 이름)에서 AWS Support 앱에 대한 Slack 채널 구성을 쉽게 식별할 수 있는 이름을 입력합니다. 이 이름은 AWS 계정에만 표시되고 Slack에는 표시되지 않습니다. 나중에 채널 구성 이름을 변경할 수 있습니다.

   Slack 채널 유형은 다음 예시와 비슷합니다.




8. Permissions(권한)의 IAM role for the AWS Support 앱 in Slack(Slack의 AWS Support 앱에 대한 IAM 역할)에서 앱에 대해 생성한 역할을 선택합니다. AWS Support 앱이 있는 역할만 목록에 신뢰할 수 있는 엔터티로 표시됩니다.



> **Note**
>
> 역할을 생성하지 않았거나 역할이 목록에 표시되지 않는 경우 AWS Support 앱에 대한 액세스 관리 단원을 참조하세요.

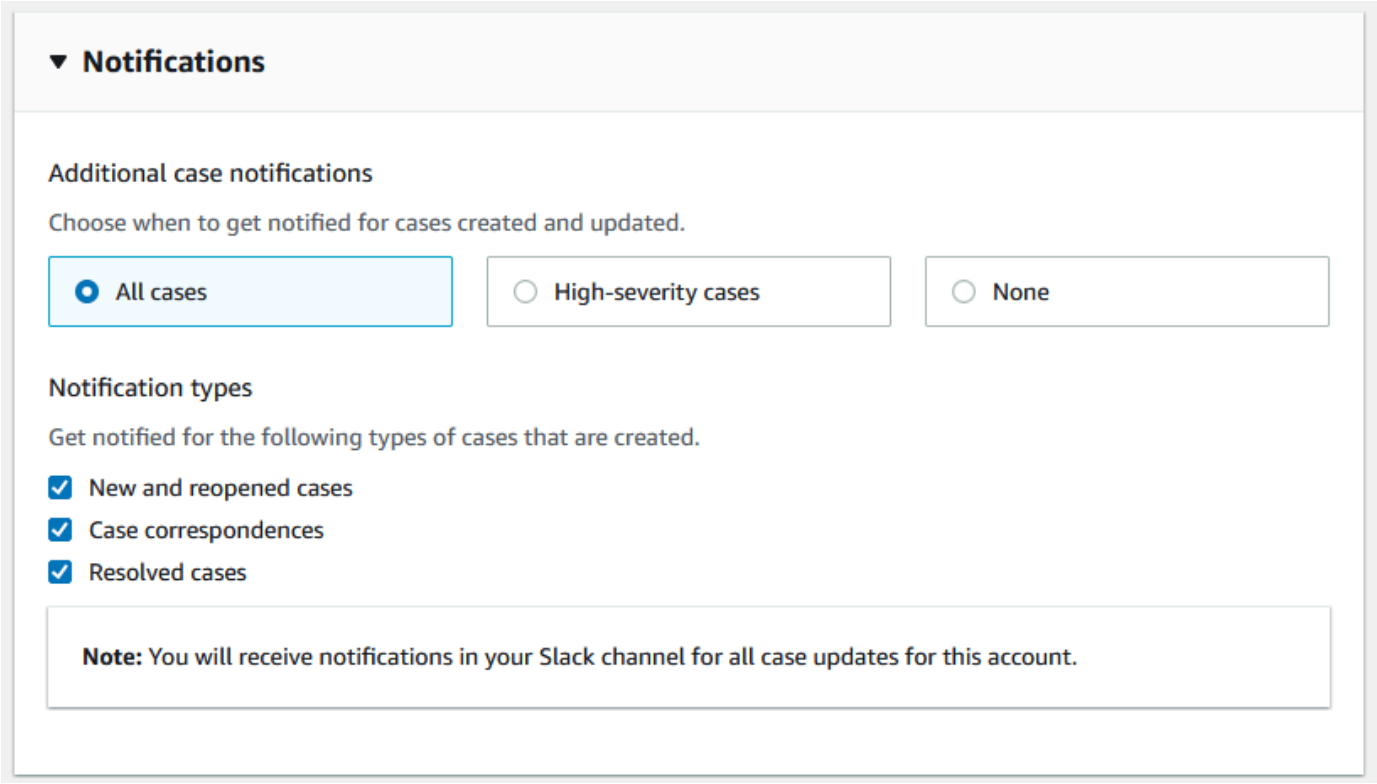
9. Notifications(알림)에서 사례에 대한 알림 수신 방법을 지정합니다.

   - All cases(모든 사례) - 모든 사례 업데이트에 대한 알림을 받습니다.
   - High-severity cases(심각도가 높은 사례) - 운영 시스템 이상에 영향을 미치는 사례에 대해서만 알림을 받습니다. 자세한 내용은 심각도 선택 섹션을 참조하세요.
   - None(없음) - 사례 업데이트에 대한 알림을 받지 않습니다.

10. (선택 사항) All cases(모든 사례) 또는 High-severity cases(심각도가 높은 사례)를 선택한 경우 다음 옵션 중 하나 이상을 선택해야 합니다.

    - New and reopened cases(신규 및 다시 열린 사례)
    - Case correspondences(사례 대응 서신)
    - Resolved cases(해결된 사례)

    다음 채널은 Slack의 모든 사례 업데이트에 대한 사례 알림을 받습니다.




11. 구성을 검토하고 Add channel(채널 추가)을 선택합니다. 채널이 Slack configuration(Slack 구성) 페이지에 표시됩니다.

## Slack 채널 구성 업데이트

Slack 채널을 구성한 후 나중에 업데이트하여 IAM 역할 또는 사례 알림을 변경할 수 있습니다.

Slack 채널 구성을 업데이트하려면

1. Support Center Console(지원 센터 콘솔)에 로그인하고 Slack configuration(Slack 구성)을 선택합니다.
2. Channels(채널)에서 원하는 채널 구성을 선택합니다.
3. ***channelName*** 페이지에서 다음 작업을 수행할 수 있습니다.
   - Rename(이름 변경)을 선택하여 채널 구성 이름을 업데이트합니다. 이 이름은 AWS 계정에만 표시되고 Slack에는 표시되지 않습니다.
   - Delete(삭제)를 선택하여 AWS Support 앱에서 채널 구성을 삭제합니다. AWS Support 앱에서 Slack 채널 구성 삭제 섹션을 참조하세요.
   - Open in Slack(Slack에서 열기)을 선택하여 브라우저에서 Slack 채널을 엽니다.
   - Edit(편집)을 선택하여 IAM 역할 또는 알림을 변경할 수 있습니다.

# Slack 채널에서 지원 사례 생성

Slack 작업 영역을 승인하고 Slack 채널을 추가한 이후에 Slack 채널에서 지원 사례를 생성할 수 있습니다.

Slack에서 지원 사례를 생성하려면

1. Slack 채널에 다음 명령을 입력합니다.

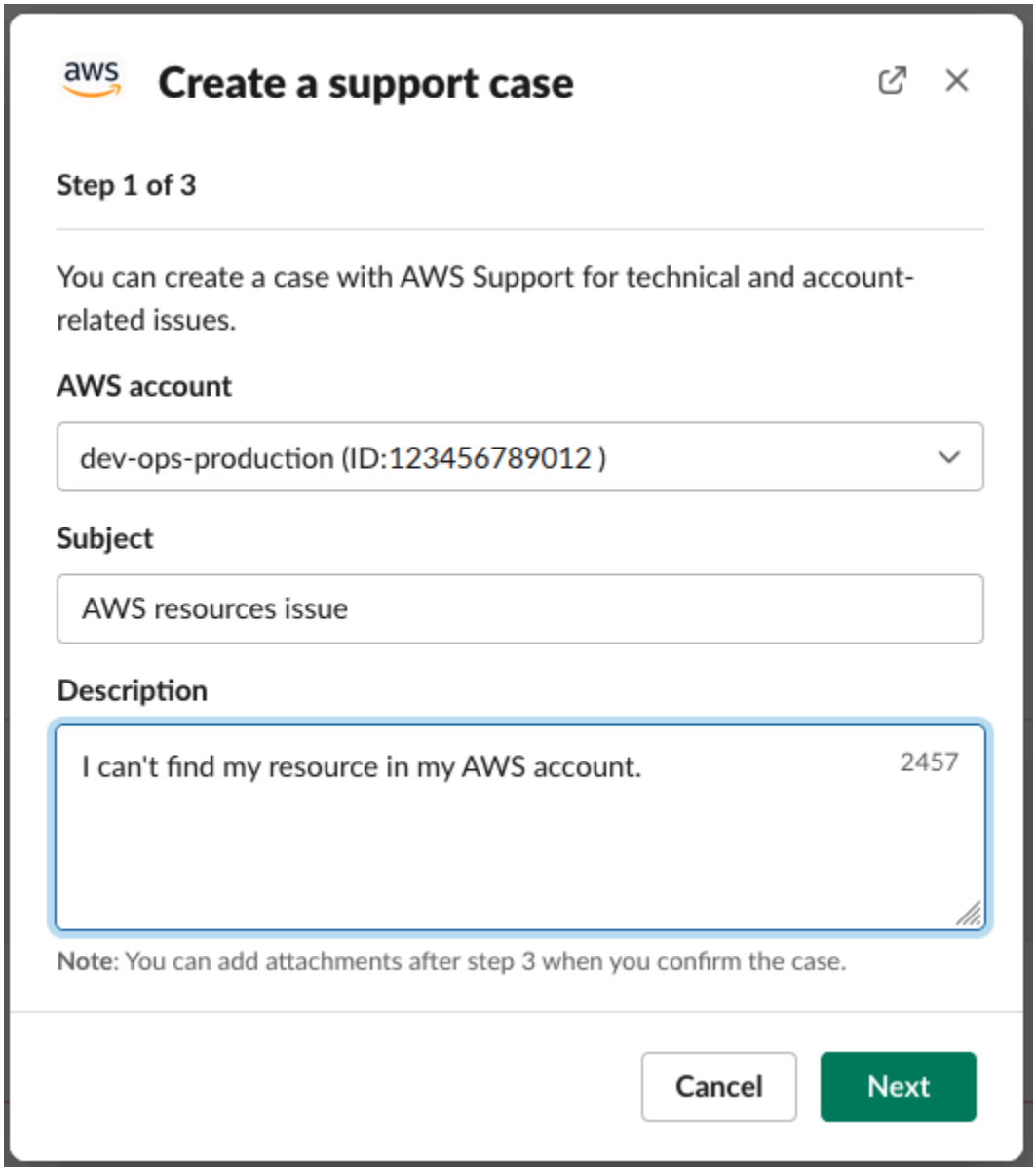
   ```
   /awssupport create
   ```

2. Create a support case(지원 사례 생성) 대화 상자에서 다음 작업을 수행합니다.

   a. 이 Slack 채널에 대해 하나 이상의 계정을 구성한 경우 AWS 계정에서 계정 ID를 선택합니다. 계정 이름을 생성한 경우 이 값이 계정 ID 옆에 표시됩니다. 자세한 내용은 Slack 작업 영역 승인 섹션을 참조하세요.

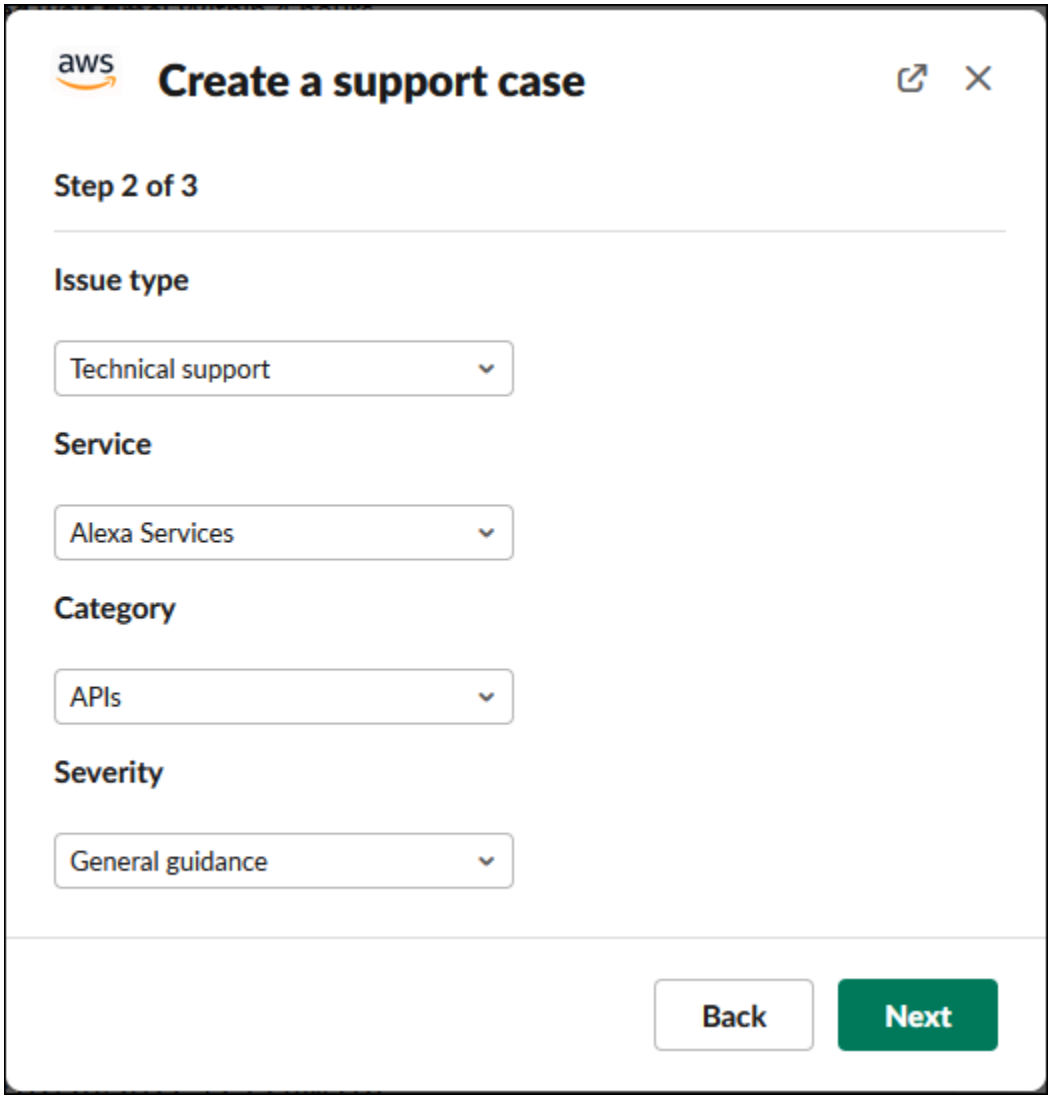
   b. Subject(제목)에 지원 사례 제목을 입력합니다.

   c. Description(설명)에서 지원 사례를 설명합니다. AWS 서비스 사용 방법 및 시도한 문제 해결 단계와 같은 세부 정보를 제공하세요.




3. 다음(Next)을 선택합니다.
4. Create a support case(지원 사례 생성) 대화 상자에서 다음 옵션을 지정합니다.
   a. Issue type(문제 유형)을 선택합니다.
   b. Service(서비스)를 선택합니다.
   c. Category(카테고리)를 선택합니다.
   d. Severity(심각도)를 선택합니다.
   e. 사례 세부 정보를 검토하고 Next(다음)를 선택합니다.

   다음 예는 Alexa 서비스에 대한 기술 지원 사례를 보여줍니다.

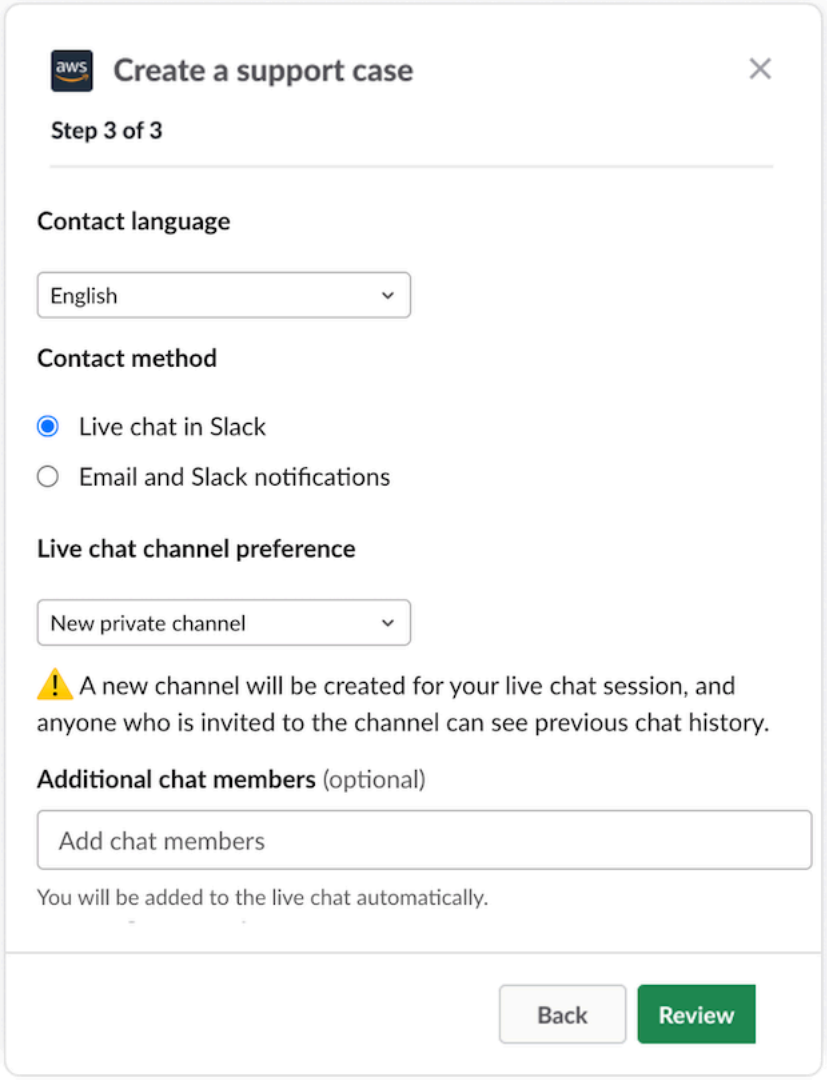



5. Contact language(고객 응대 언어)에서는 지원 사례에 사용할 선호 언어를 선택합니다.

> **Note**
>
> 계정 및 결제 사례의 경우 Slack의 실시간 채팅에는 일본어가 지원되지 않습니다.

6. Contact method(연락 방법)에서 Email and Slack notifications(이메일 및 Slack 알림) 또는 Live chat in Slack(Slack에서 실시간 채팅)을 선택합니다.

   다음 예제는 Slack에서 실시간 채팅을 선택하는 방법을 보여줍니다.




a. Slack에서 라이브 채팅을 선택하는 경우 라이브 채팅 채널 기본 설정으로 새 비공개 채널 또는 현재 채널을 선택하세요. 새 비공개 채널은 AWS Support 상담원과 채팅할 수 있는 별도의 비공개 채널을 만들고, 현재 채널은 현재 채널의 스레드를 사용하여 AWS Support 상담원과 채팅할 수 있습니다.

b. (선택 사항) Live chat in Slack(Slack에서 실시간 채팅)을 선택한 경우 다른 Slack 멤버의 이름을 입력할 수 있습니다. 새 비공개 채널의 경우 AWS Support 앱은 귀하와 선택된 멤버를 새 채널에 자동으로 추가합니다. 현재 채널의 경우 AWS Support 상담원이 참여하면 AWS Support 앱이 채팅 스레드에서 나와 선택된 멤버를 자동으로 태그합니다.

> **Important**
>
> - 지원 사례 세부 정보 및 채팅 기록에 대한 액세스를 허용할 채팅 멤버만 추가하는 것이 좋습니다.
> - 기존 지원 사례에 대해 새 실시간 채팅 세션을 시작하는 경우 AWS Support 앱은 이전 실시간 채팅에서 사용한 것과 동일한 채팅 채널 또는 스레드를 사용합니다. 또한 AWS Support 앱은 이전에 사용했던 것과 동일한 실시간 채팅 채널 환경설정을 사용합니다.
> - 현재 채널 옵션은 비공개 채널에서 채팅을 요청하는 경우에만 사용할 수 있습니다. 지원 사례에 대한 액세스를 허용할 채팅 멤버만 추가하는 것이 좋습니다.

7. (선택 사항) Additional contacts to notify(알림을 받을 추가 연락처)에 이 지원 사례에 대한 업데이트를 받을 이메일 주소를 입력합니다. 최대 10개의 이메일 주소를 추가할 수 있습니다.
8. Review(검토)를 선택합니다.
9. Slack 채널에서 사례 세부 정보를 검토합니다. 다음을 수행할 수 있습니다.
   - 사례 세부 정보를 변경하려면 Edit(편집)을 선택합니다.
   - 케이스에 파일을 추가합니다. 이렇게 하려면 다음 단계를 따르세요.
     a. Attach file(파일 첨부)을 선택하고 Slack에서 + 아이콘을 선택한 다음 Your computer(컴퓨터)를 선택합니다.
     b. 파일로 이동하여 선택합니다.
     c. Upload a file(파일 업로드) 대화 상자에 `@awssupport`를 입력하고 메시지 전송

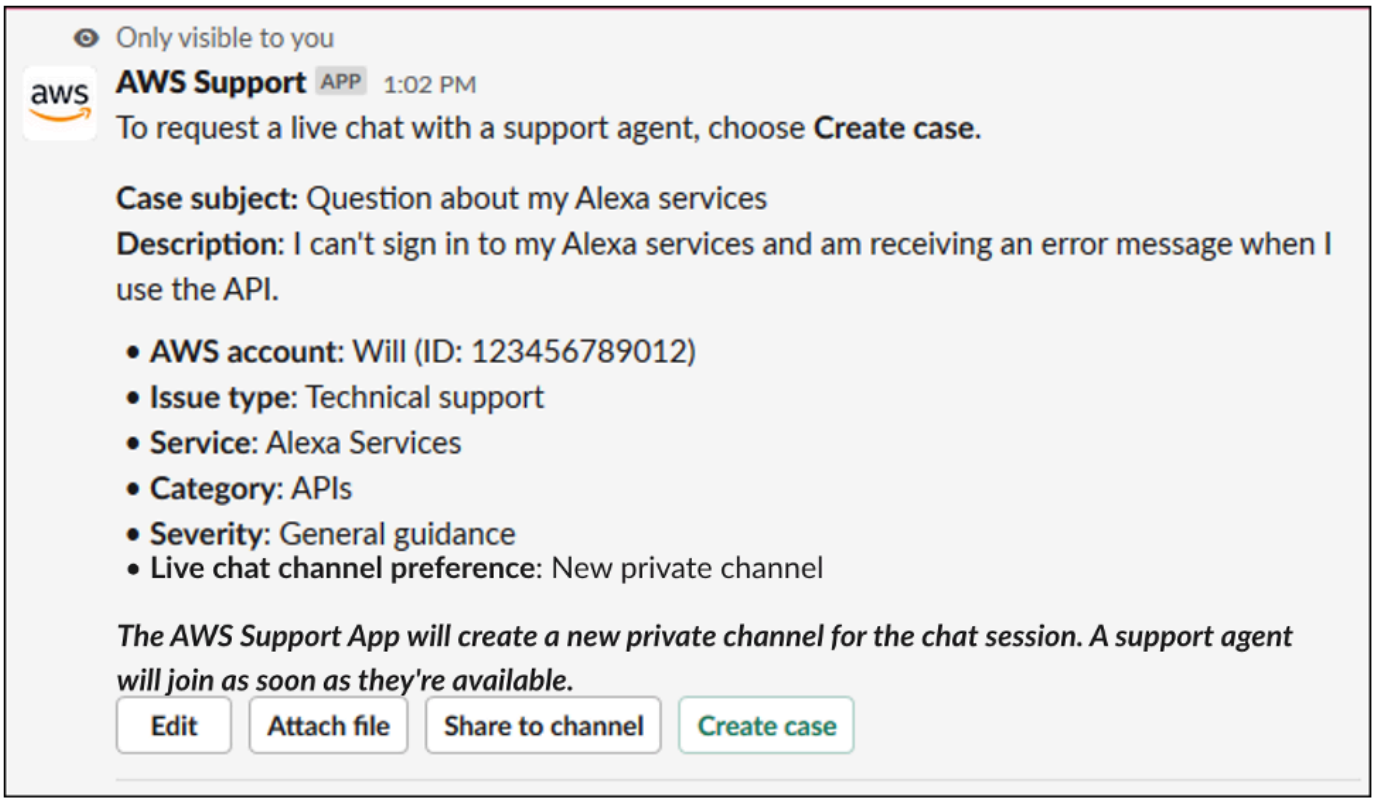
        아이콘을 누릅니다.

> **주의**
>
> - 최대 3개의 파일을 첨부할 수 있습니다. 각 파일의 크기는 최대 5MB까지입니다.
> - 지원 사례에 파일을 첨부하는 경우 1시간 이내에 사례를 제출해야 합니다. 그렇지 않으면 파일을 다시 추가해야 합니다.

- Share to channel(채널에 공유)을 선택하여 Slack 채널에서 다른 사용자와 사례 세부 정보를 공유합니다. 이 옵션을 사용하면 사례를 생성하기 전에 사례 세부 정보를 팀과 공유할 수 있습니다.

10. 사례 세부 정보를 검토한 다음 Create case(사례 생성)를 선택합니다.

    다음 예는 Alexa 서비스에 대한 기술 지원 사례를 보여줍니다.




    지원 사례를 생성한 후 사례 세부 정보가 표시되는 데 몇 분 정도 걸릴 수 있습니다.

11. 지원 사례가 업데이트되면 See details(세부 정보 보기)를 선택하여 사례 정보를 볼 수 있습니다. 그러면 다음 작업을 수행할 수 있습니다.

    - Share to channel(채널에 공유)을 선택하여 Slack 채널에서 다른 사용자와 사례 세부 정보를 공유합니다.
    - Reply(회신)를 선택하여 서신을 추가합니다.
    - Resolve case(사례 해결)를 선택합니다.

> **Note**
>
> Slack에서 자동 사례 업데이트를 수신하도록 선택하지 않은 경우 지원 사례를 검색하여 See details(세부 정보 보기) 옵션을 찾을 수 있습니다.

# Slack의 지원 사례에 회신

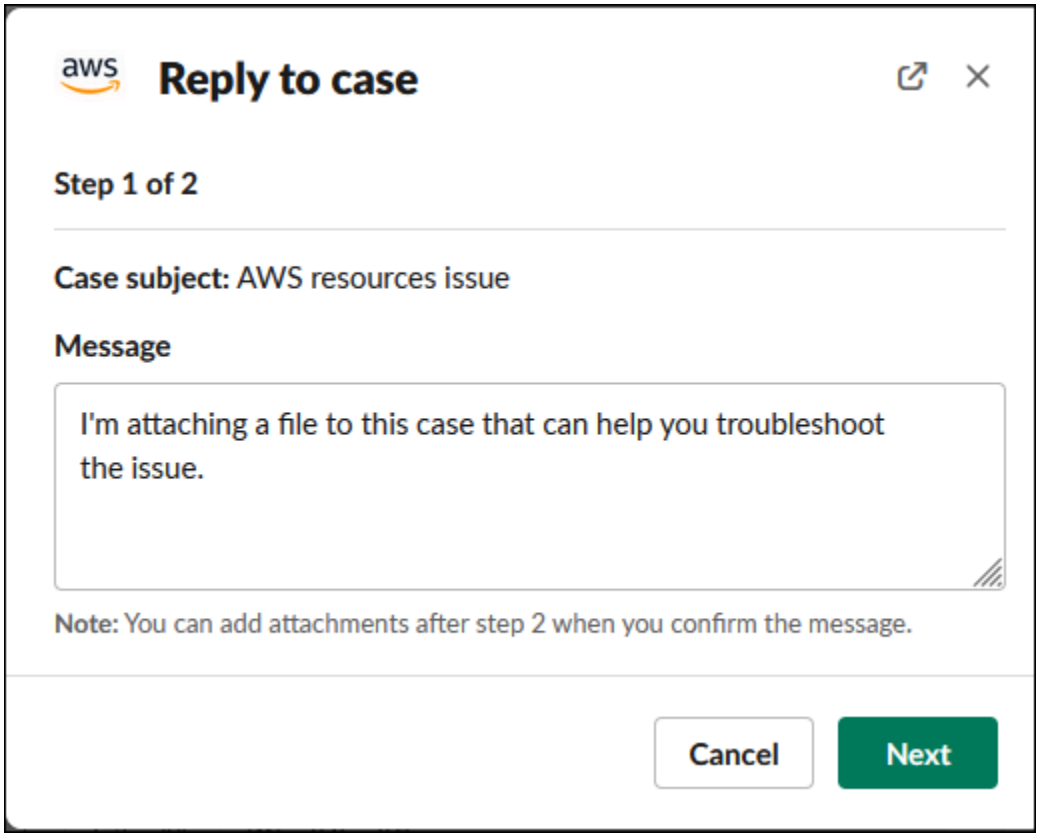
사례에 사례 세부 정보 및 첨부 파일과 같은 업데이트를 추가하고 지원 에이전트의 응답에 회신할 수 있습니다.

> **Note**
>
> - AWS Support Center Console를 사용하여 지원 에이전트에 회신할 수도 있습니다. 자세한 내용은 사례 업데이트, 해결 및 다시 열기 섹션을 참조하세요.
> - AWS Support 앱에서 생성된 채팅 채널의 사례에는 서신을 추가할 수 없습니다. 실시간 채팅 채널은 실시간 채팅 중에만 에이전트에게 메시지를 보냅니다.

Slack의 지원 사례에 회신하려면

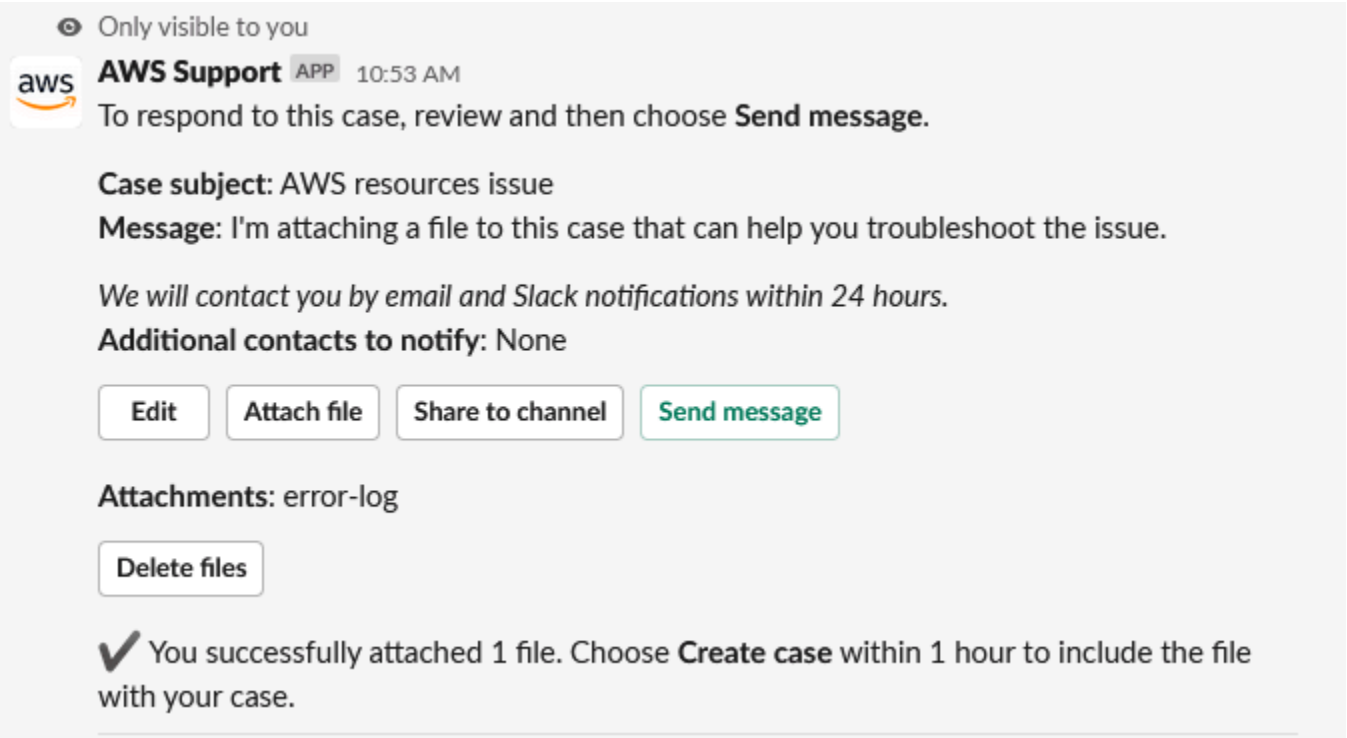
1. Slack 채널에서 응답할 사례를 선택합니다. `/awssupport search`를 입력하여 지원 사례를 찾을 수 있습니다.
2. 원하는 사례 옆에 있는 See details(세부 정보 보기)를 선택합니다.
3. 사례 세부 정보 하단에서 Reply(회신)를 선택합니다.


4. Reply to case(사례에 회신) 대화 상자의 Message(메시지) 필드에 문제에 대한 간략한 설명을 입력합니다. 이후 다음을 선택합니다.




5. 연락 방법을 선택합니다. 사용 가능한 연락 방법은 사례 유형 및 지원 플랜에 따라 달라집니다.
6. (선택 사항) Additional contacts to notify(알림을 받을 추가 연락처)에 이 지원 사례에 대한 업데이트를 받을 추가 이메일 주소를 입력합니다. 최대 10개의 이메일 주소를 추가할 수 있습니다.
7. Review(검토)를 선택합니다. 그런 다음 회신 내용을 편집하거나, 파일을 첨부하거나, 채널에 공유할지를 선택할 수 있습니다.
8. 회신할 준비가 되면 Send message(메시지 전송)를 선택합니다.
9. (선택 사항) 사례에 대한 이전 서신을 보려면 Previous correspondence(이전 서신)를 선택하세요. 단축된 메시지를 보려면 Show full message(전체 메시지 보기)를 선택합니다.

Example : Slack의 사례에 회신




# 라이브 채팅 세션에 참여하세요 AWS Support

케이스에 대한 실시간 채팅을 요청할 때는 새 채팅 채널을 사용하거나 현재 채널의 스레드를 사용하여 AWS Support 상담원과 상담원을 대신할 수 있습니다. 이 채팅 채널 또는 스레드를 사용하여 지원 에이전트 및 실시간 채팅에 초대한 다른 사람들과 통신할 수 있습니다.

> **Important**
>
> 실시간 채팅 채널에 가입한 사람은 누구나 특정 지원 사례에 대한 세부 정보를 볼 수 있습니다. 지원 사례에 액세스해야 하는 사용자만 추가하는 것이 좋습니다. 채팅 채널 또는 스레드의 구성원은 활성 채팅에 참여할 수도 있습니다.

> **Note**
>
> 실시간 채팅 채널 및 스레드는 실시간 채팅 세션 외부에서 사례에 서신이 추가될 때도 알림을 받습니다. 이는 채팅 세션 전, 도중, 후에 발생하므로 채팅 채널이나 스레드를 사용하여 사례에

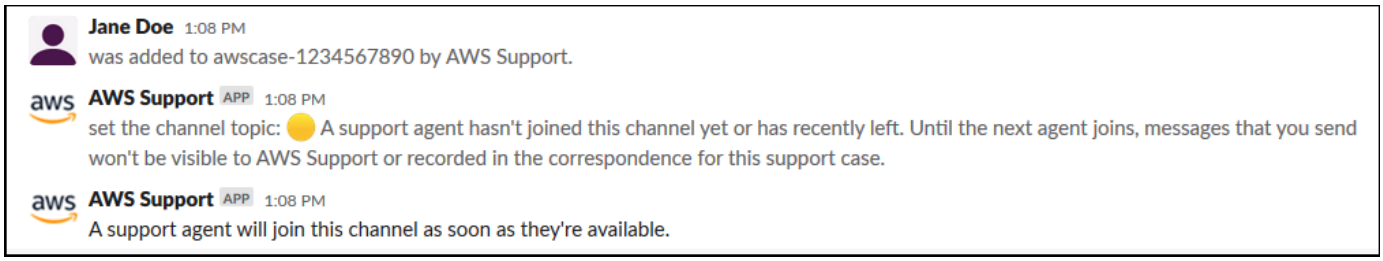
대한 모든 업데이트를 모니터링할 수 있습니다. 새 채팅 채널을 사용하기로 선택한 경우 AWS Support 앱을 초대한 구성 채널을 사용하여 이러한 서신에 회신하십시오.

새 AWS Support 채널에서 실시간 채팅 세션에 참여하려면

1. Slack 애플리케이션에서 AWS Support 앱이 생성한 채널로 이동합니다. 채널 이름에는 지원 사례 ID(예: *awscase-1234567890*)가 포함되어 있습니다.

   > **Note**
   >
   > AWS Support 앱은 지원 사례에 대한 세부 정보가 포함된 고정 메시지를 실시간 채팅 채널에 추가합니다. 고정된 메시지에서 채팅을 종료하거나 사례를 해결할 수 있습니다. 채널 이름에서 이 채널의 모든 고정된 메시지를 찾을 수 있습니다.

2. 지원 에이전트가 채널에 참여하면 지원 사례에 대해 채팅할 수 있습니다. 지원 상담원이 채널에 참여할 때까지 상담원은 해당 채팅의 메시지를 볼 수 없으며 케이스 서신에도 메시지가 표시되지 않습니다.

3. (선택 사항) 다른 멤버를 채팅 채널에 추가합니다. 기본적으로 채팅 채널은 프라이빗입니다.
4. 지원 에이전트가 채팅에 참여하면 채팅 채널이 활성화되고 AWS Support 앱이 채팅을 기록합니다.

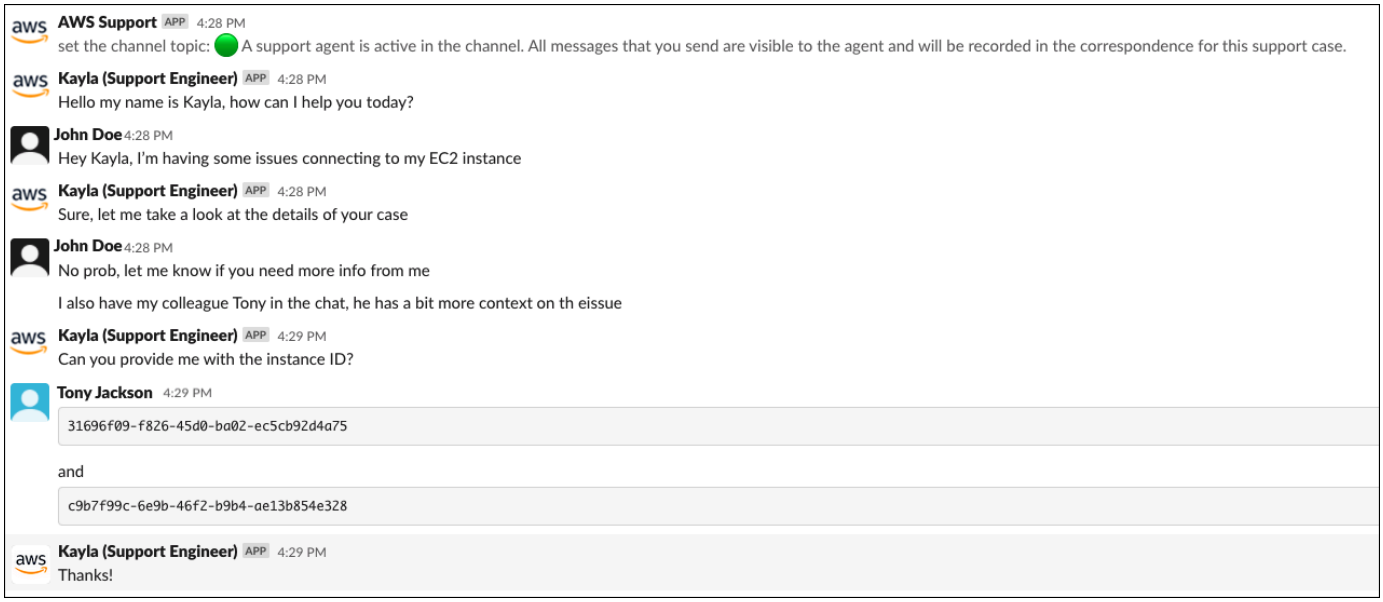
   지원 사례에 대해 에이전트와 채팅하고 첨부 파일을 채널에 업로드할 수 있습니다. AWS Support 앱은 자동으로 파일 및 채팅 로그를 케이스 서신에 저장합니다.

   > **Note**
   >
   > 지원 담당자와 채팅할 때는 앱용 Slack의 다음과 같은 차이점을 참고하세요. AWS Support
   >
   > - 지원 에이전트는 공유된 메시지 또는 스레드를 볼 수 없습니다. 메시지 또는 스레드의 텍스트를 공유하려면 텍스트를 새 메시지로 입력합니다.

- 메시지를 편집하거나 삭제해도 에이전트는 원본 메시지만 볼 수 있습니다. 수정 버전을 표시하려면 새 메시지를 다시 입력해야 합니다.

Example : 실시간 채팅 세션

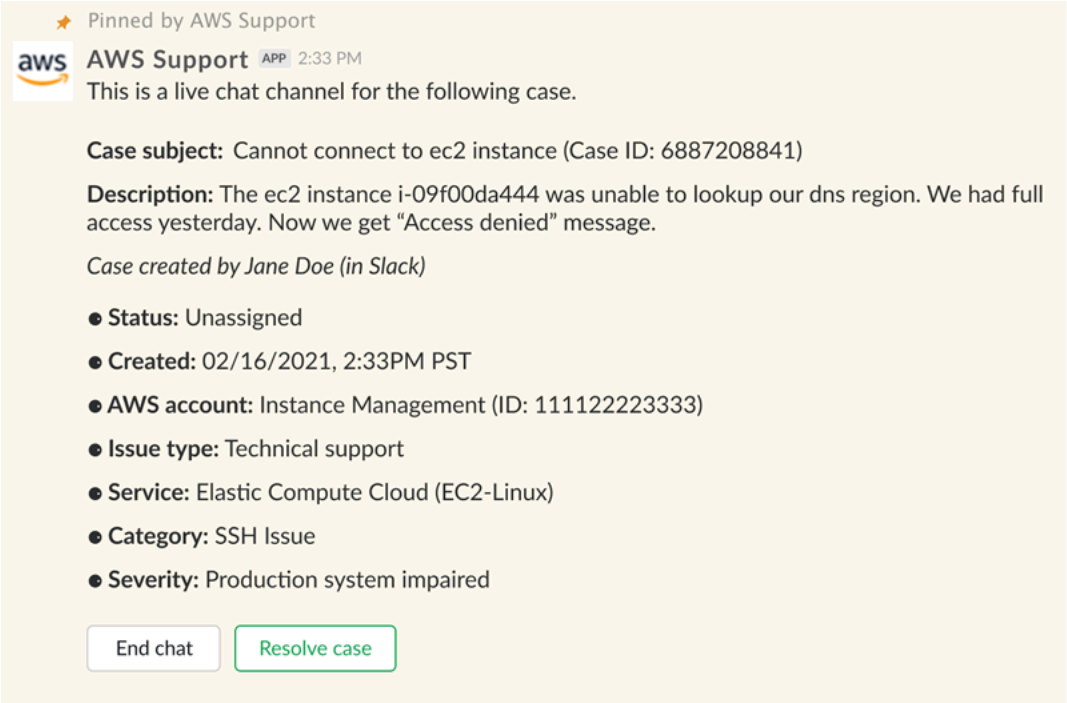
다음은 두 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 대한 연결 문제를 해결하기 위해 수행하는 지원 에이전트와의 실시간 채팅 세션을 보여주는 예입니다.




5. (선택 사항) 실시간 채팅을 중단하려면 End chat(채팅 종료)을 선택합니다. 지원 상담원이 채널을 떠나고 AWS Support 앱은 실시간 채팅 녹화를 중단합니다. 이 지원 사례에 대한 사례 대응 서신에 첨부된 채팅 기록을 찾을 수 있습니다.
6. 문제가 해결된 경우 고정 메시지에서 Resolve case(사례 해결)를 선택하거나 `/awssupport resolve`를 입력할 수 있습니다.

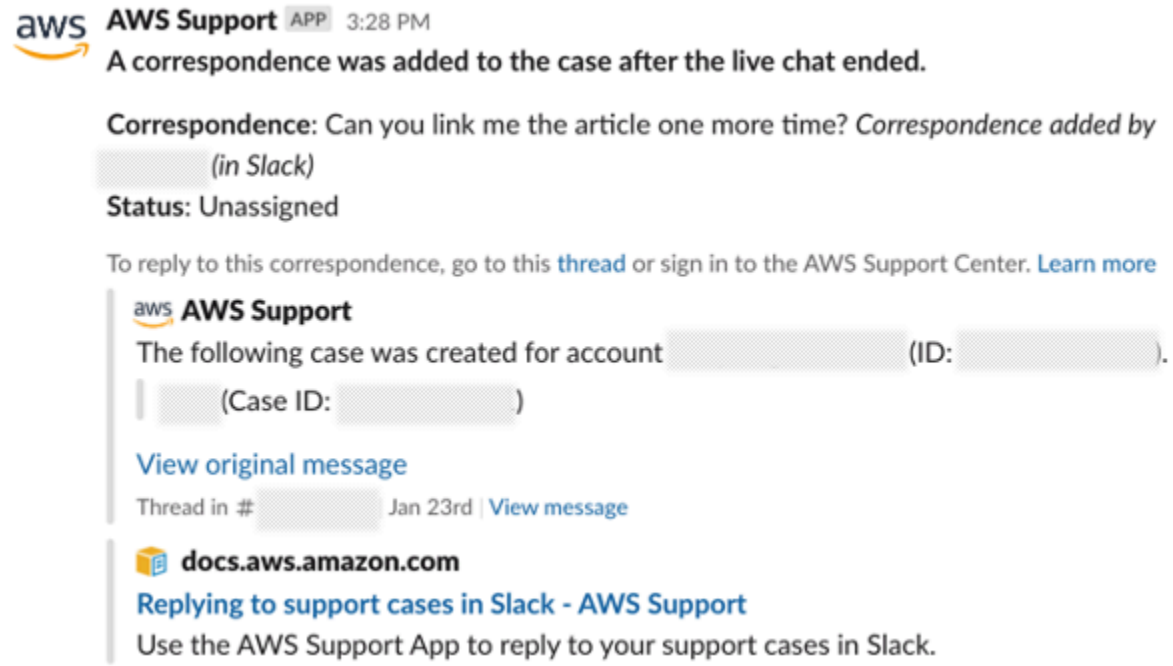
Example : 라이브 채팅 종료

다음 고정 메시지는 Amazon EC2 인스턴스에 대한 사례 세부 정보를 보여줍니다. Slack 채널 이름에서 고정된 메시지를 찾을 수 있습니다.




Example : 채팅 채널의 서신 알림

다음은 채팅이 종료된 후 다른 공동 작업자가 업데이트를 추가할 때 알림을 받는 실시간 채팅 채널의 예제입니다.

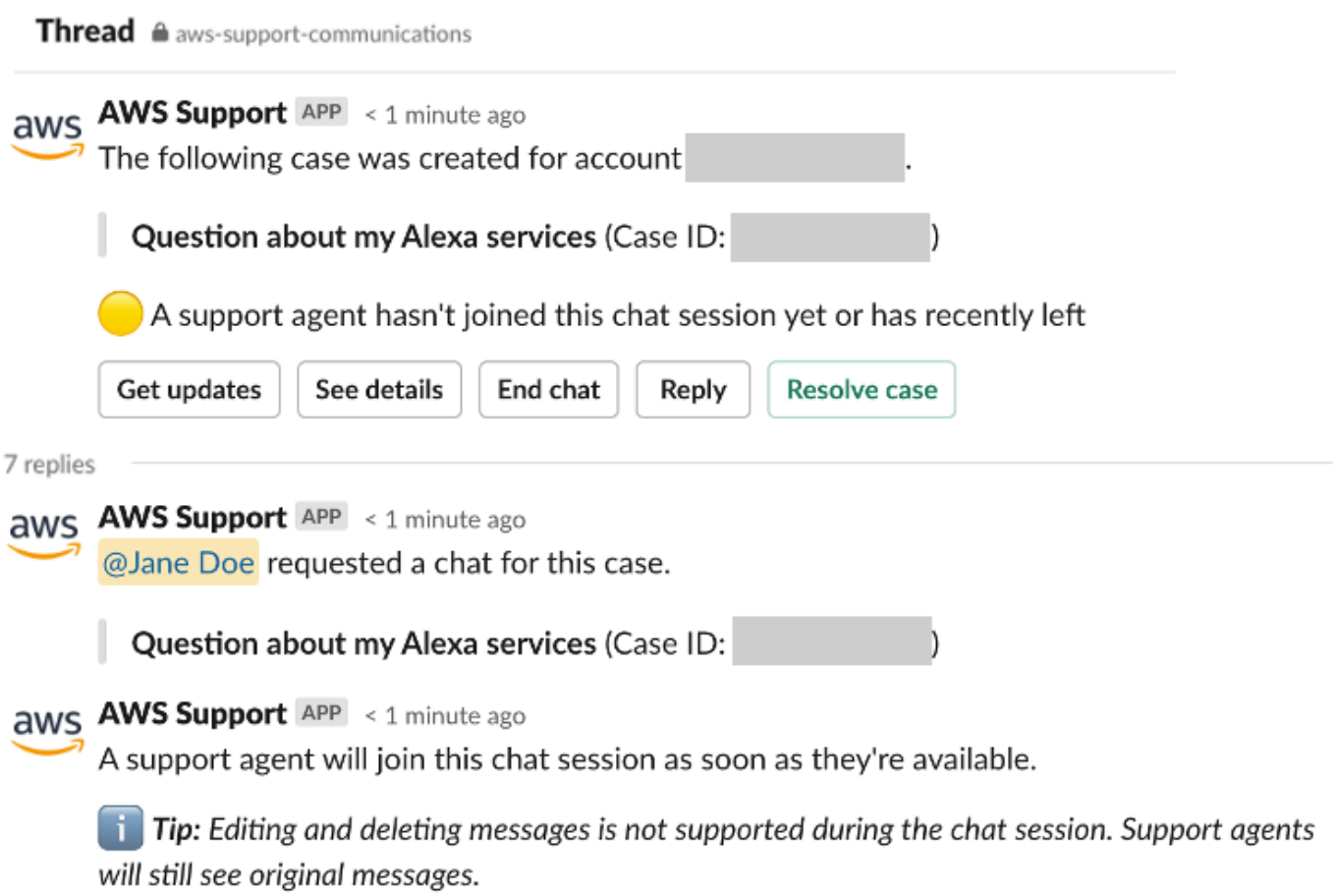


알림에는 채팅 상태(요청, 진행 중 또는 종료됨)와 해당 서신을 에이전트가 추가했는지 아니면 다른 공동 작업자가 추가했는지 여부가 표시됩니다. 또한 지원 앱은 이 채팅이 요청된 원래 Slack 스레드 또는 채널로 다시 연결하려고 시도합니다. 해당 채널 또는 이 사례에 액세스할 수 있는 다른 모든 채널에서 이 사례에 회신할 수 있습니다.

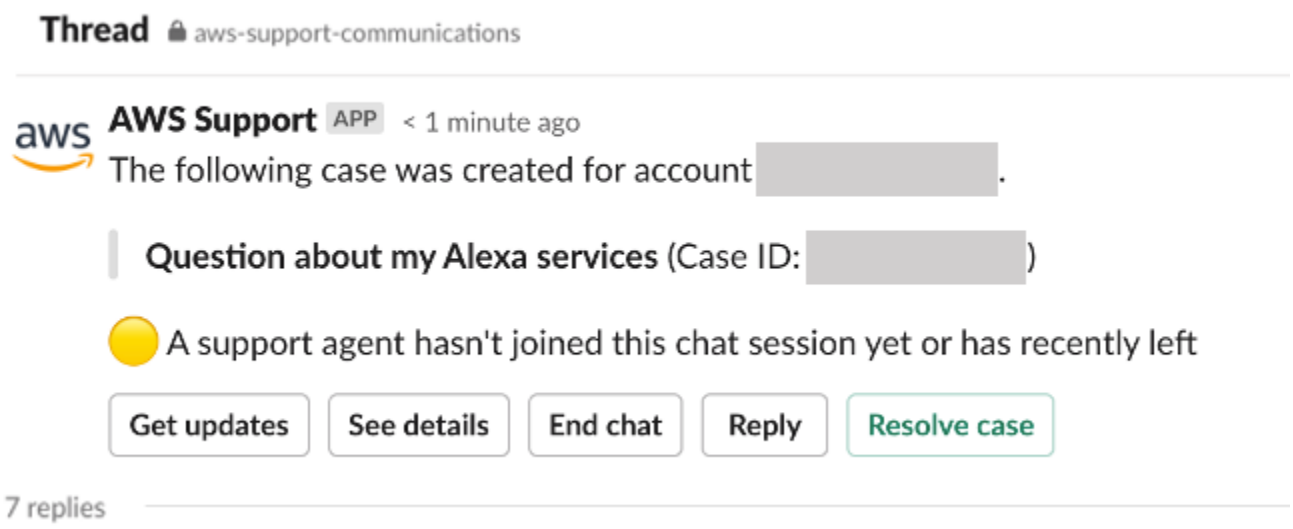
현재 채널의 실시간 채팅 AWS Support 세션에 참여하려면

1. Slack 애플리케이션에서 AWS Support 앱이 채팅에 사용하는 현재 채널의 스레드로 이동합니다. 대부분의 경우 이 스레드는 케이스가 처음 생성되었을 때 시작된 스레드가 됩니다.
2. 지원 에이전트가 스레드에 참여하면 지원 사례에 대해 채팅할 수 있습니다. 지원 에이전트가 스레드에 참여할 때까지 에이전트는 해당 스레드에서 메시지를 볼 수 없으며 채팅이 종료될 때 메시지가 사례 대응 서신에 표시되지 않습니다.

> **Note**
>
> 채팅 스레드 외부에서 이 채널로 전송된 메시지는 채팅이 진행 중인 동안에도 볼 수 없습니다. AWS Support




3. (선택사항) 다른 채널 멤버를 태그하여 채팅 스레드에서 알립니다.
4. 지원 상담원이 채팅에 참여하면 채팅 스레드가 활성화되고 AWS Support 앱이 채팅을 기록합니다. 새로운 채팅 채널 옵션과 유사하게 지원 사례에 대해 에이전트와 채팅하고 첨부 파일을 스레드에 업로드할 수 있습니다. AWS Support 앱은 자동으로 파일 및 채팅 로그를 케이스 서신에 저장합니다.
5. (선택 사항) 실시간 채팅을 중단하려면 이 스레드의 첫 메시지에서 채팅 종료를 선택합니다. 지원 상담원이 스레드를 떠나고 AWS Support 앱은 실시간 채팅 녹화를 중단합니다. 이 지원 사례에 대한 사례 대응 서신에 첨부된 채팅 기록을 찾을 수 있습니다.
6. 문제가 해결된 경우 이 스레드의 초기 메시지에서 Resolve 사례를 선택할 수 있습니다.




# Slack에서 지원 사례 검색

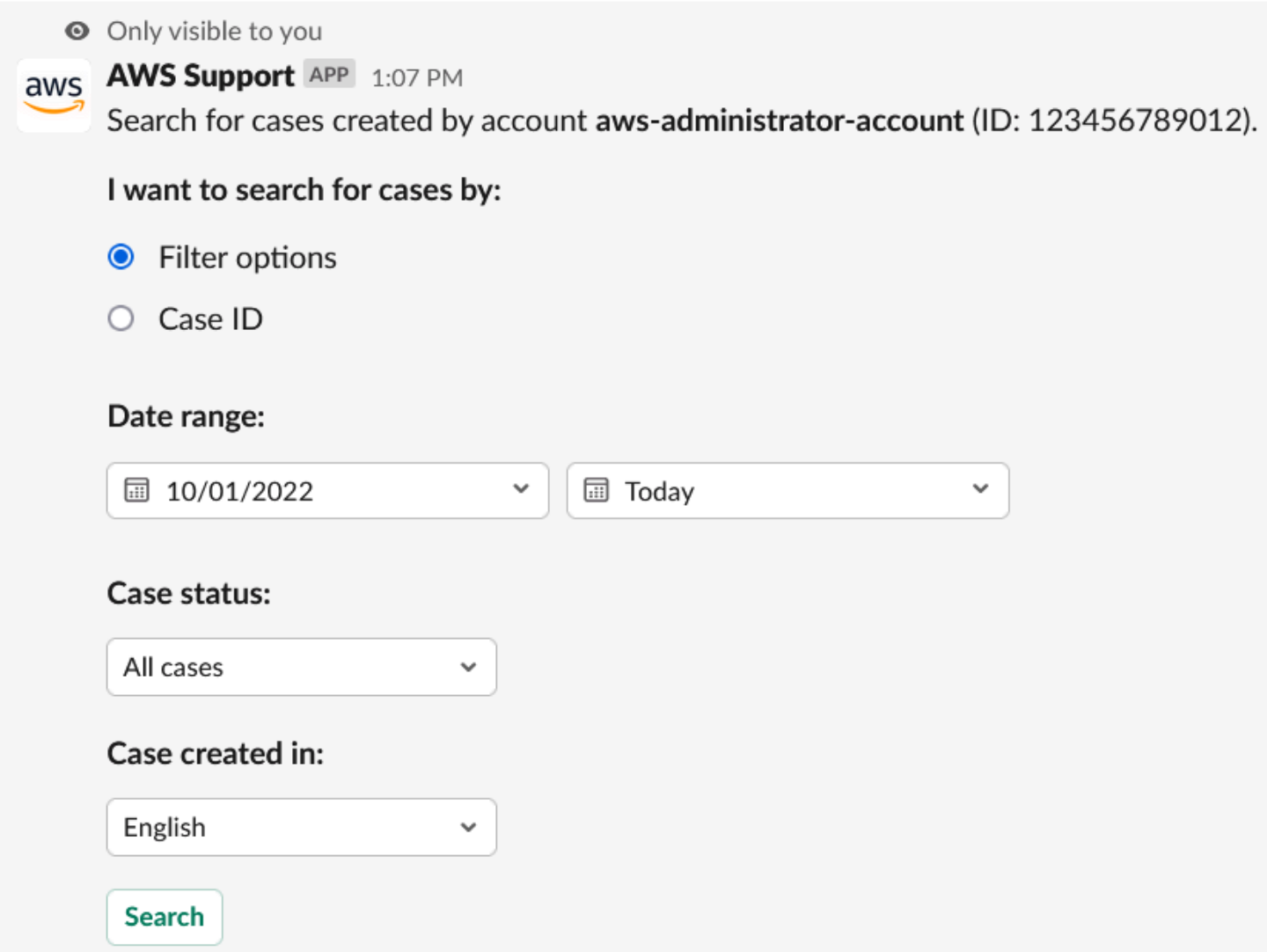
Slack 채널에서 AWS 계정의 지원 사례를 검색할 수도 있고, 동일한 채널 및 작업 영역을 구성한 다른 계정의 지원 사례를 검색할 수 있습니다. 예를 들어 사용자의 계정(123456789012)과 동료의 계정(111122223333)이 AWS Support Center Console에서 동일한 작업 영역 및 채널을 구성한 경우 AWS Support 앱을 사용하여 각 계정의 지원 사례를 검색할 수 있습니다.

결과를 필터링하려면 다음 옵션을 사용하세요.

- 계정 ID
- 사례 ID
- 사례 상태
- 고객 응대 언어
- 날짜 범위

Example : Slack에서 사례 검색

다음 예에서는 날짜 범위, 사례 상태, 고객 응대 언어를 지정하여 단일 계정의 Filter options(필터 옵션)를 기준으로 검색하는 방법을 보여줍니다.




Slack에서 지원 사례를 검색하려면

1. Slack 채널에 다음 명령을 입력합니다.

   ```
   /awssupport search
   ```

2. I want to search for cases by:(케이스 검색 기준:) 옵션에서 다음 중 하나를 선택합니다.

   A. 필터 옵션(Filter options) – 다음 옵션을 사용하여 사례를 필터링할 수 있습니다.

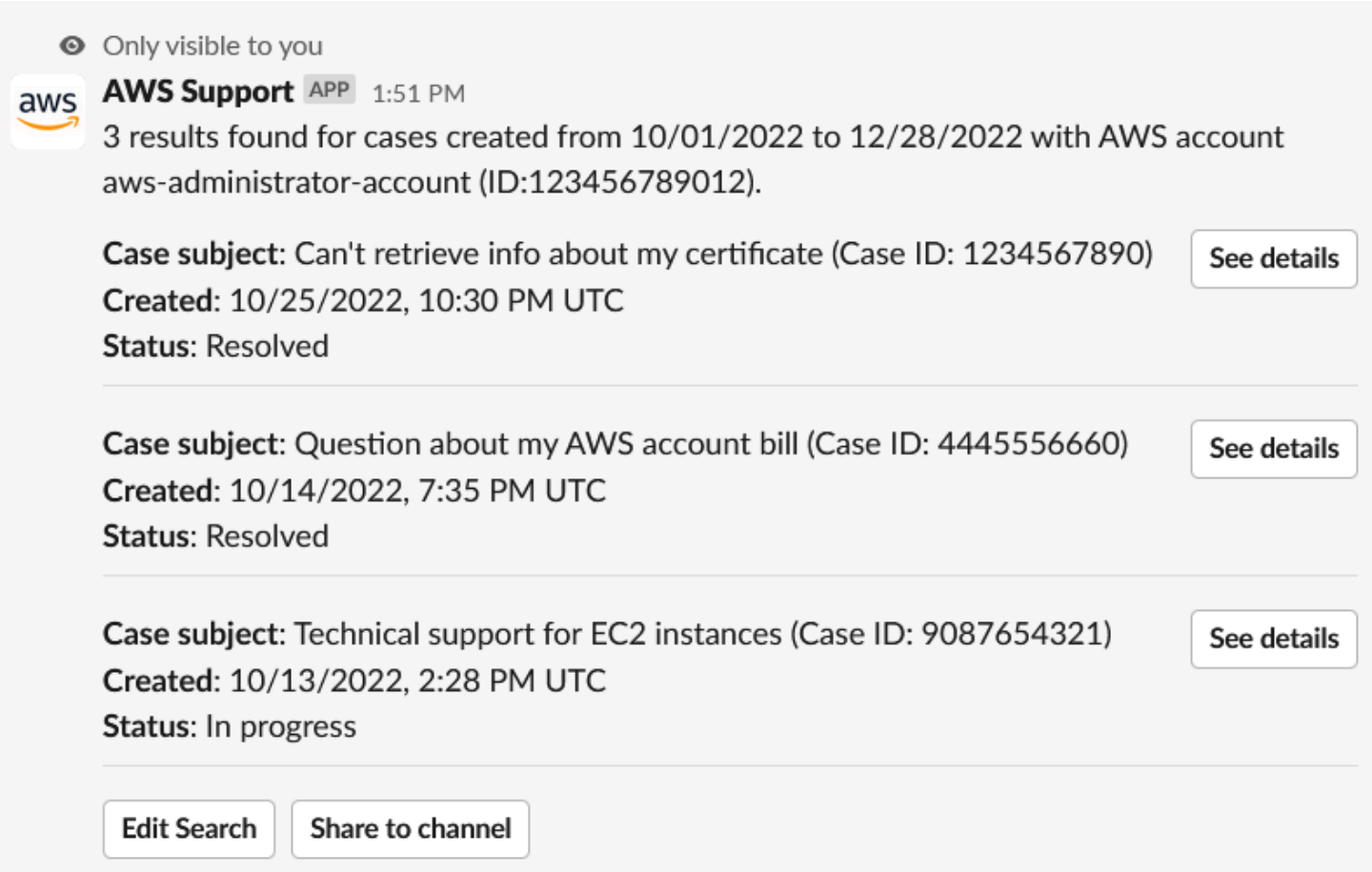
   - AWS 계정 – 이 목록은 이 채널에 여러 계정이 있는 경우에만 표시됩니다.
   - 날짜 범위(Date range) – 사례가 생성된 날짜입니다.
   - 사례 상태(Case status) – 사례 상태(예: 모든 미해결 사례(All open cases) 또는 해결됨(Resolved)입니다.
   - 다음 언어로 생성된 사례(Case created in) – 사례의 고객 응대 언어입니다.

B. 사례 ID(Case ID) – 사례 ID를 입력합니다. 사례 ID는 한 번에 하나만 입력할 수 있습니다. 채널에 계정이 여러 개 있는 경우 AWS 계정을 선택하여 사례를 검색하세요.

3. 검색(Search)을 선택합니다. 검색 결과가 Slack에 표시됩니다.

## 검색 결과 사용

다음 예에서는 하나의 AWS 계정에서 지원 사례 세 개를 반환합니다.




검색 결과를 받은 후 다음을 수행할 수 있습니다.

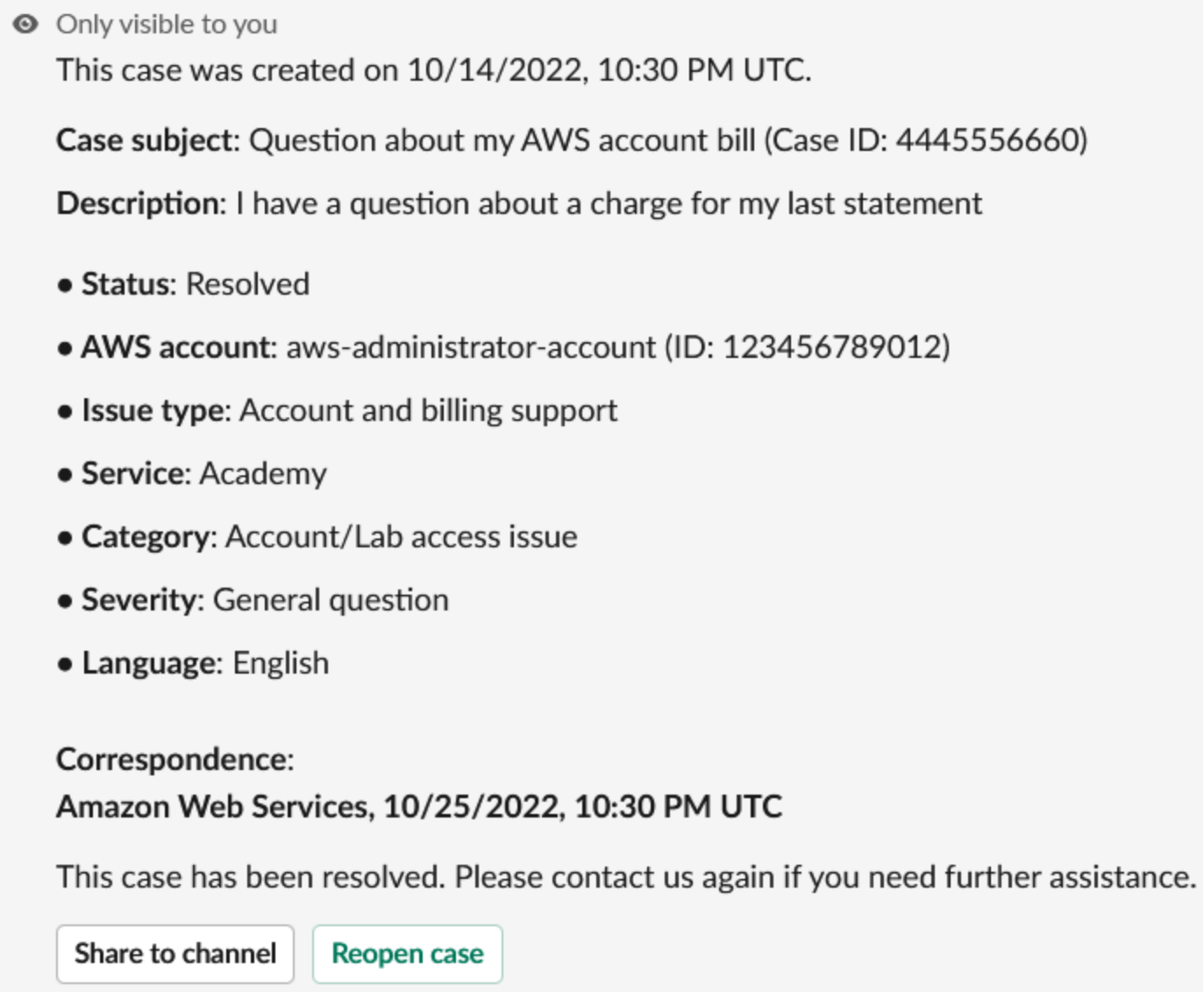
검색 결과를 사용하려면

1. Edit Search(검색 편집)를 선택하여 이전 필터 옵션이나 사례 ID를 변경합니다.
2. Share to channel(채널에 공유)을 선택하여 검색 결과를 채널과 공유할 수 있습니다.
3. See details(세부 정보 보기)를 선택하여 사례에 대한 자세한 정보를 볼 수 있습니다. Show full message(전체 메시지 보기)를 선택하여 나머지 최신 서신을 볼 수 있습니다.

4. Filter options(필터 옵션)로 검색한 경우 검색 결과에 여러 케이스가 반환될 수 있습니다. Next 5 results(다음 5개 결과) 또는 Previous 5 results(이전 5개 결과)를 선택하여 다음 또는 이전 5개 사례를 봅니다.

Example : 해결된 지원 사례

다음 예는 See details(세부 정보 보기)를 선택한 후 계정 및 결제 문제에 대해 해결된 지원 사례를 보여줍니다.

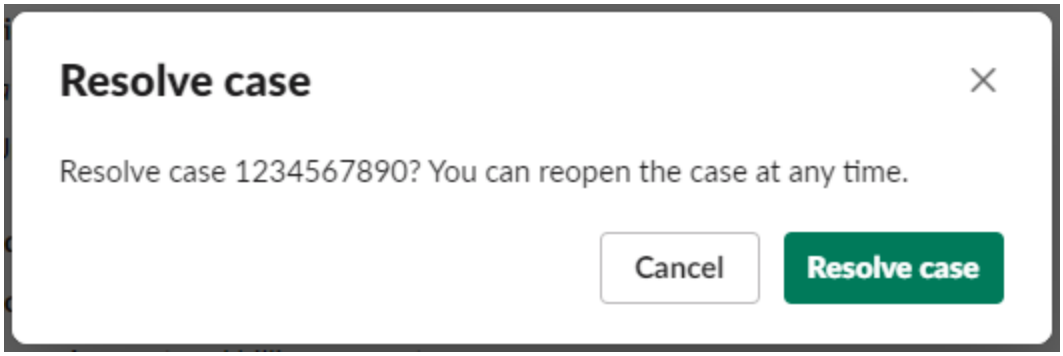


# Slack의 지원 사례 해결

지원 사례가 더 이상 필요하지 않거나 문제를 해결한 경우 Slack에서 직접 지원 사례를 해결할 수 있습니다. 그러면 AWS Support Center Console에서도 사례가 해결됩니다. 사례를 해결한 후 나중에 해당 사례를 다시 열 수 있습니다.

Slack에서 지원 사례를 해결하려면

1. Slack 채널에서 지원 사례로 이동합니다. Slack에서 지원 사례 검색 섹션을 참조하세요.
2. 사례에 대한 See details(세부 정보 보기)를 선택합니다.
3. Resolve case(사례 해결)를 선택합니다.
4. Resolve case(사례 해결) 대화 상자에서 Resolve case(사례 해결)를 선택합니다. Slack 채널 또는 지원 센터 콘솔에서 사례를 다시 열 수 있습니다.

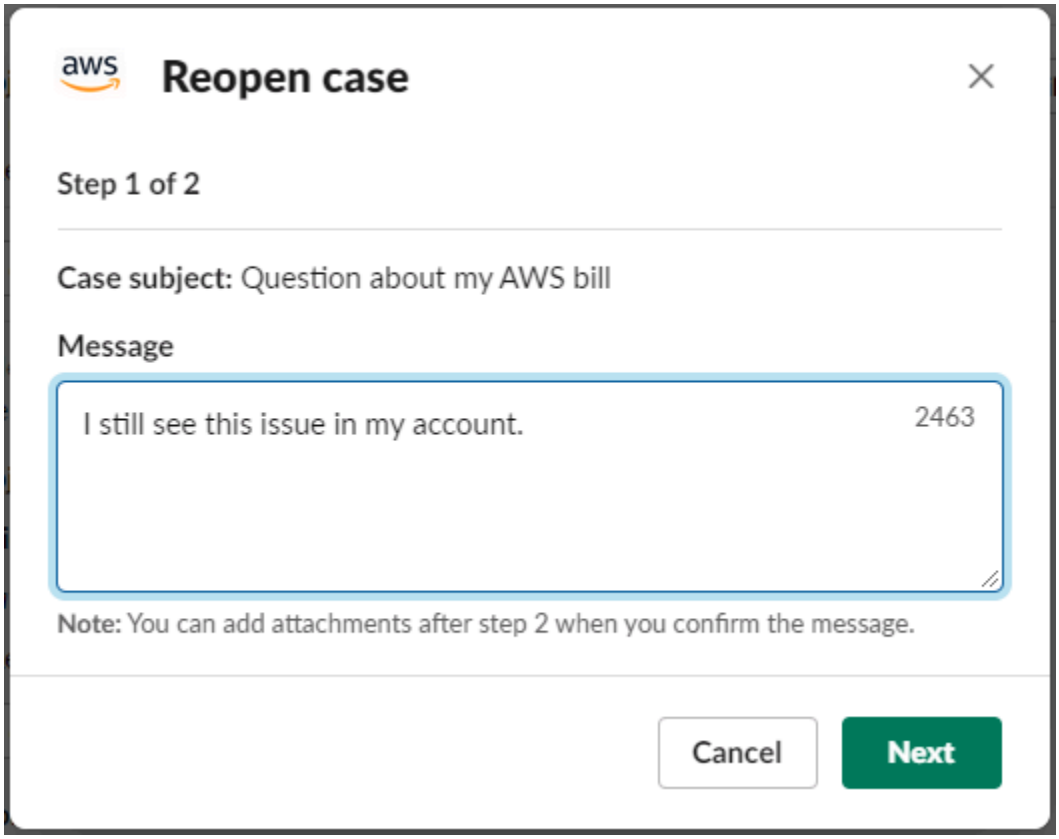



# Slack에서 지원 사례 다시 열기

지원 사례를 해결한 후 Slack에서 해당 사례를 다시 열 수 있습니다.

Slack에서 지원 사례를 다시 열려면

1. Slack에서 다시 열 지원 사례를 찾습니다. Slack에서 지원 사례 검색 섹션을 참조하세요.
2. See details(세부 정보 보기)를 선택합니다.
3. 사례 다시 열기(Reopen case)를 선택합니다.
4. Reopen case(사례 다시 열기) 대화 상자의 Message(메시지) 필드에 문제에 대한 간략한 설명을 입력합니다.
5. Next(다음)를 선택합니다.




6. (선택 사항) 추가 연락처를 입력합니다.
7. Review(검토)를 선택합니다.
8. 사례 세부 정보를 검토한 다음 Send message(메시지 전송)를 선택합니다. 케이스가 다시 열립니다. 지원 에이전트와 새 실시간 채팅을 요청한 경우 Slack에서는 이전 실시간 채팅에 사용된 것과 동일한 채팅 채널 또는 스레드를 사용합니다. 새 채널에서 실시간 채팅을 요청했지만 아직 채팅하지 못한 경우 새 채팅 채널이 열립니다. 현재 채널에서 실시간 채팅을 요청했지만 아직 채팅하지 못한 경우 현재 채널의 스레드가 사용됩니다.

# 서비스 할당량 증가 요청

Slack 채널에서 계정에 대한 서비스 할당량 증가를 요청할 수 있습니다.

서비스 할당량 증가를 요청하려면

1. Slack 채널에 다음 명령을 입력합니다.

   ```
   /awssupport quota
   ```

2. Increase service quota(서비스 할당량 증가) 대화 상자에 다음 정보를 입력합니다.

a. AWS 계정을 선택합니다.

b. AWS 리전을 선택합니다.

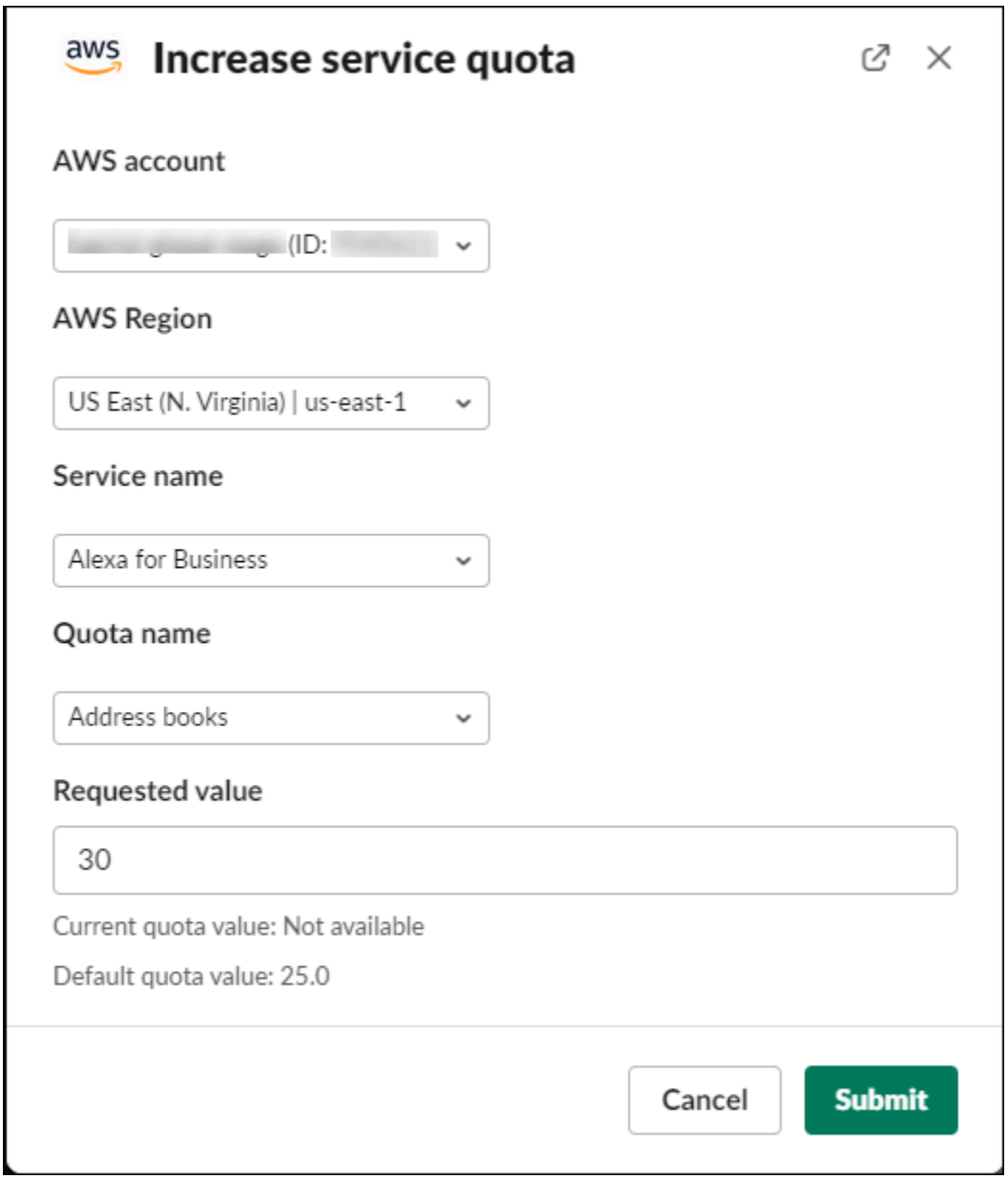
c. Service name(서비스 이름)을 선택합니다.

d. Quota name(할당량 이름)을 선택합니다.

e. 할당량 증가에 대해 Requested value(요청된 값)를 입력합니다. 기본 할당량보다 큰 값을 입력해야 합니다.

3. Submit(제출)을 선택합니다.

Example : Alexa for Business에 대한 할당량 증가




Service Quotas 콘솔에서 요청을 볼 수도 있습니다. 자세한 내용은 Service Quotas User Guide(Service Quotas 사용 설명서)의 Requesting a quota increase(할당량 증가 요청)를 참조하세요.

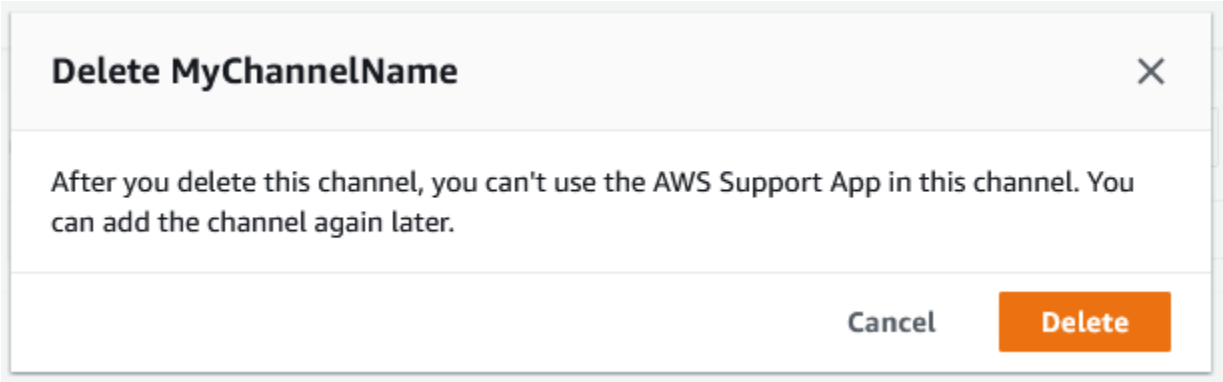
## AWS Support 앱에서 Slack 채널 구성 삭제

AWS Support 앱에서 채널 구성을 삭제할 수 있습니다(필요하지 않은 경우). 이 작업은 AWS Support 앱 및 AWS Support Center Console에서만 채널을 제거합니다. Slack에서는 채널이 삭제되지 않습니다.

AWS 계정당 최대 20개의 채널을 추가할 수 있습니다. 이미 이 할당량에 도달한 경우 다른 채널을 추가하려면 먼저 채널을 삭제해야 합니다.

Slack 채널 구성을 삭제하려면

1. Support Center Console(지원 센터 콘솔)에 로그인하고 Slack configuration(Slack 구성)을 선택합니다.
2. Slack configuration(Slack 구성) 페이지의 Channels(채널)에서 채널 이름을 선택한 다음 Delete(삭제)를 선택합니다.
3. Delete channel name(채널 이름 삭제) 대화 상자에서 Delete(삭제)를 선택합니다. 나중에 이 채널을 AWS Support 앱에 다시 추가할 수 있습니다.




## AWS Support 앱에서 Slack 작업 영역 구성 삭제

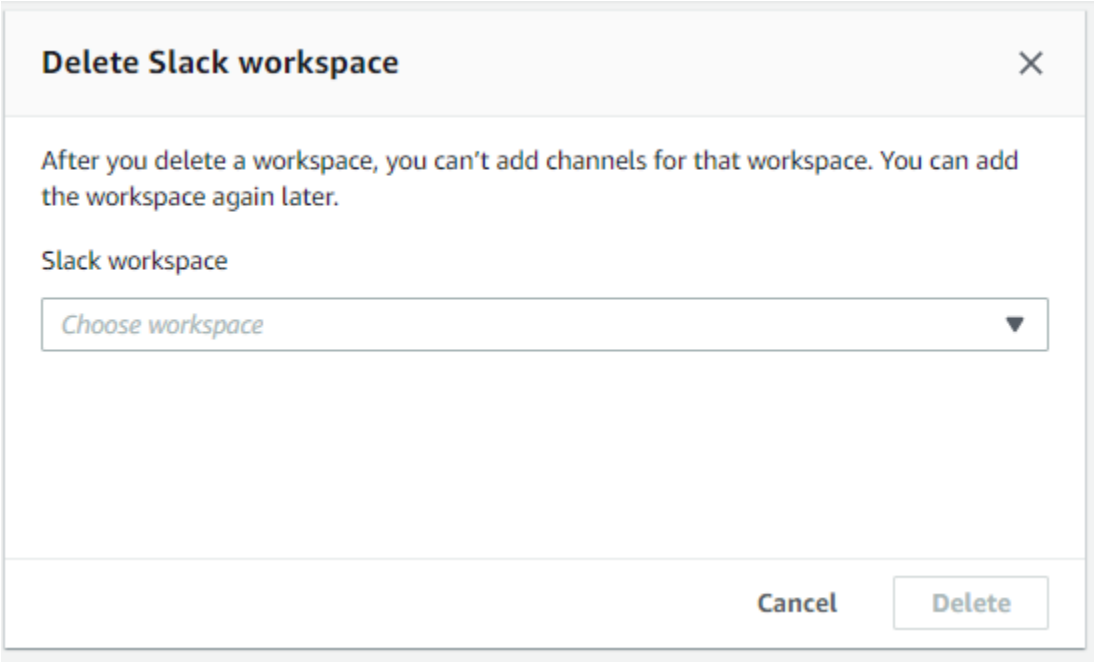
AWS Support 앱에서 작업 영역 구성을 삭제할 수 있습니다(필요하지 않은 경우). 이 작업은 AWS Support 앱 및 AWS Support Center Console에서만 작업 영역을 제거합니다. Slack에서는 작업 영역이 삭제되지 않습니다.

AWS 계정에 대해 최대 5개의 작업 영역을 추가할 수 있습니다. 이미 이 할당량에 도달한 경우 다른 작업 영역을 추가하려면 먼저 Slack 작업 영역을 삭제해야 합니다.

> **Note**
>
> 이 작업 영역의 채널을 AWS Support 앱에 추가한 경우 작업 영역을 삭제하려면 먼저 이 채널을 삭제해야 합니다. AWS Support 앱에서 Slack 채널 구성 삭제 섹션을 참조하세요.

Slack 작업 영역 구성을 삭제하려면

1. AWS Support Center Console에 로그인하고 Slack configuration(Slack 구성)을 선택합니다.
2. Slack configuration(Slack 구성) 페이지의 Slack WorkSpace(Slack 작업 영역)에서 Delete a workspace(작업 영역 삭제)를 선택합니다.
3. Delete Slack workspace(Slack 작업 영역 삭제) 대화 상자에서 Slack 작업 영역 이름을 선택한 다음 Delete(삭제)를 선택합니다. 나중에 작업 영역을 AWS 계정에 다시 추가할 수 있습니다.




# Slack의 AWS Support 앱 명령

## Slack 채널 명령

AWS Support 앱을 초대한 Slack 채널에 다음 명령을 입력할 수 있습니다. 이 Slack 채널 이름은 AWS Support Center Console에 구성된 채널로도 표시됩니다.

`/awssupport create` 또는 `/awssupport create-case`

지원 사례를 생성합니다.

`/awssupport search` 또는 `/awssupport search-case`

사례를 검색합니다. 동일한 Slack 채널에 대한 AWS Support 앱을 구성한 AWS 계정의 지원 사례를 검색할 수 있습니다.

`/awssupport quota` 또는 `/awssupport service-quota-increase`

서비스 할당량 증가를 요청합니다.

## 실시간 채팅 채널 명령

실시간 채팅 채널에서 다음 명령을 입력할 수 있습니다. 이는 AWS Support와(과)의 채팅을 위해 새로운 채널을 선택하면 AWS Support 앱이 생성하는 채널입니다. 채팅 채널에는 지원 사례 ID(예: *awscase-1234567890*)가 포함되어 있습니다.

> **Note**
>
> 현재 채널의 스레드를 실시간 채팅에 사용할 때는 다음 명령을 사용할 수 없습니다. 대신 초기 스레드 메시지에 첨부된 버튼을 사용하여 채팅을 종료하거나, 새 상담원을 초대하거나, 문제를 해결하세요.

`/awssupport endchat`

지원 에이전트를 제거하고 실시간 채팅 세션을 종료합니다.

`/awssupport invite`

새 지원 에이전트를 이 채널에 초대합니다.

`/awssupport resolve`

이 지원 사례를 해결합니다.

# AWS Support Center Console에서 AWS Support 앱 서신 보기

Slack 채널에서 계정에 대한 지원 사례를 생성, 업데이트 또는 해결할 때 지원 센터 콘솔에 로그인하여 사례를 볼 수도 있습니다. 사례 대응 서신을 보고 Slack 채널에서 사례가 업데이트되었는지를 확인하고, 지원 에이전트와의 채팅 기록을 보고, Slack에서 업로드한 첨부 파일을 찾을 수 있습니다.

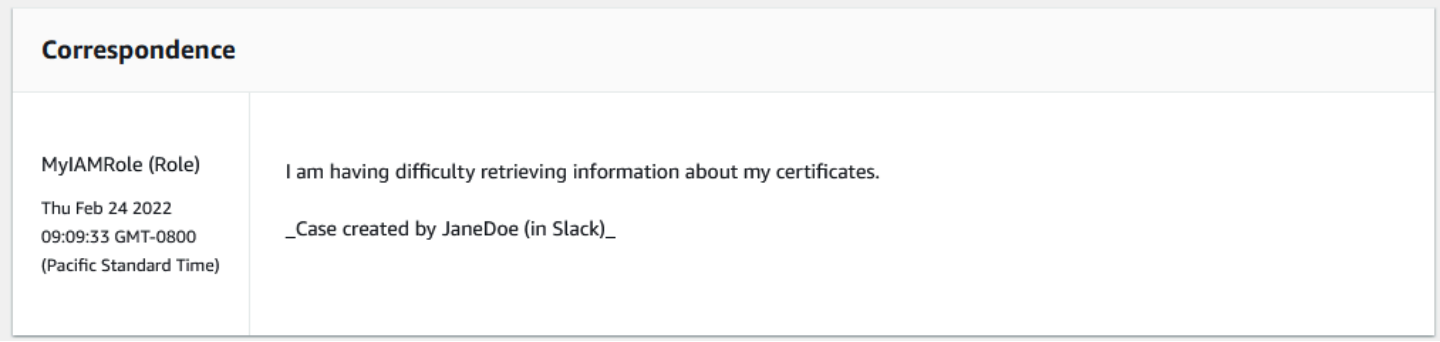
Slack에서 사례 대응 서신을 보려면

1. 계정에 대한 AWS Support Center Console에 로그인합니다.
2. 지원 사례를 선택합니다.

3. Correspondence(서신)에서 Slack 채널에서 사례가 생성되고 업데이트되었는지 확인할 수 있습니다.

Example : 지원 사례

다음 스크린샷에서 Jane Doe는 Slack에서 지원 사례를 다시 열었습니다. 이 서신은 지원 센터 콘솔의 지원 사례에 대해 표시됩니다.




# AWS CloudFormation으로 Slack 리소스에서 AWS Support 앱 생성

Slack의 AWS Support 앱은 리소스 및 인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있도록 AWS 리소스를 모델링하고 설정하는 데 도움이 되는 서비스인 AWS CloudFormation과 통합됩니다. 필요한 모든 AWS 리소스(예: AccountAlias 및 SlackChannelConfiguration)를 설명하는 템플릿을 생성하면 AWS CloudFormation에서 이러한 리소스를 프로비저닝하고 구성합니다.

AWS CloudFormation을 사용할 때 템플릿을 재사용하여 AWS Support 앱 리소스를 일관되고 반복적으로 설정할 수 있습니다. 리소스를 한 번 설명한 후 여러 AWS 계정 및 리전에서 동일한 리소스를 반복적으로 프로비저닝할 수 있습니다.

## AWS Support 앱 및 AWS CloudFormation 템플릿

AWS Support 앱 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML로 서식 지정된 텍스트 파일입니다. 이 템플릿은 AWS CloudFormation 스택에서 프로비저닝할 리소스에 대해 설명합니다. JSON 또는 YAML에 익숙하지 않은 경우 AWS CloudFormation Designer를 사용하면 AWS CloudFormation 템플릿을 시작하는 데 도움이 됩니다. 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS CloudFormation Designer이란 무엇입니까?를 참조하세요.

AWS Support 앱은 AWS CloudFormation에서 AccountAlias 및 SlackChannelConfiguration 생성을 지원합니다. AccountAlias 및 SlackChannelConfiguration 리소스에 대한 JSON 및 YAML 템플릿의 예를

비롯한 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS Support 앱 리소스 유형 참조를 참조하세요.

## 조직을 위한 Slack 구성 리소스 생성

CloudFormation 템플릿을 사용하여 AWS Support 앱에 필요한 리소스를 만들 수 있습니다. 조직의 관리 계정인 경우 템플릿을 사용하여 구성원 계정에 대한 리소스를 AWS Organizations에서 생성할 수 있습니다.

예를 들어 템플릿을 사용하여 조직 내 모든 계정에 대해 동일한 Slack 작업 영역 구성을 생성한 다음 별도의 템플릿을 사용하여 특정 AWS 계정 또는 조직 단위(OU)에 대해 서로 다른 Slack 채널 구성을 생성할 수 있습니다. 또한 템플릿을 사용하여 멤버 계정이 AWS 계정에 대해 원하는 Slack 채널을 구성할 수 있도록 Slack 작업 공간 구성을 생성할 수 있습니다.

CloudFormation 템플릿 사용 여부를 선택할 수 있습니다. CloudFormation 템플릿을 사용하지 않는 경우 다음 수동 단계를 대신 완료할 수 있습니다.

- AWS Support Center Console에서 AWS Support 앱 리소스를 생성합니다.
- AWS Support 앱을 사용하도록 여러 계정에 권한을 부여하려면 AWS Support으로 지원 사례를 생성하세요.
- RegisterSlackWorkspaceForOrganization API 작업을 호출하여 계정에 대한 Slack 작업 영역을 등록합니다. CloudFormation 스택은 이 API 작업을 자동으로 호출합니다.

다음 절차에 따라 조직에 CloudFormation 템플릿을 업로드하세요. AWS Support App resource type reference 페이지에서 예제 템플릿을 사용할 수 있습니다.

템플릿은 CloudFormation에 다음 리소스를 생성하도록 지시합니다.

- Slack 채널 구성.
- Slack 작업 영역 구성.
- `AWSSupportSlackAppCFNRole` 이름이 포함된 IAM 역할. AWSSupportAppFullAccess AWS 관리형 정책이 연결됩니다.

목차


- Slack용 CloudFormation 템플릿 업데이트
- 관리 계정에 대한 스택 만들기

- 조직을 위한 스택 세트 생성

## Slack용 CloudFormation 템플릿 업데이트

시작하려면 다음 템플릿을 사용하여 스택을 생성하세요. 템플릿을 Slack 작업 영역 및 채널의 유효한 값으로 바꿔야 합니다.

> **Note**
>
> 조직의 AccountAlias 리소스를 만들 때는 템플릿을 사용하지 않는 것이 좋습니다. AccountAlias 리소스는 AWS Support 앱에서 AWS 계정을 고유하게 식별합니다. 멤버 계정은 지원 센터 콘솔에 계정 이름을 입력할 수 있습니다. 자세한 내용은 Slack 작업 영역 승인 섹션을 참조하세요.

Slack용 CloudFormation 템플릿을 업데이트하려면

1. 조직의 관리 계정인 경우 멤버 계정이 CloudFormation을 사용하여 리소스를 생성하려면 계정에 대한 Slack 작업 영역을 수동으로 승인해야 합니다. 아직 이를 실행하지 않았다면 Slack 작업 영역 승인 단원을 참조하세요.
2. AWS Support App resource type reference 페이지에서 원하는 리소스의 JSON 또는 YAML 템플릿을 복사합니다.
3. 텍스트 편집기에서 템플릿을 새 파일에 붙여넣습니다.
4. 템플릿에서 원하는 파라미터를 지정합니다. 최소한 다음 필드의 값을 변경합니다.
   - `TeamId`를 Slack 작업 영역 ID로
   - `ChannelId`를 Slack 채널 ID 사용
   - `ChannelName`를 Slack 채널 구성을 식별하는 이름으로

> **Tip**
>
> 작업 영역 및 채널 ID를 찾으려면 브라우저에서 Slack 채널을 여세요. URL에서 워크스페이스 ID는 첫 번째 식별자이고 채널 ID는 두 번째 식별자입니다. 예를 들어, https://app.slack.com/client/T012ABCDEFG/C01234A5BCD에서 T012ABCDEFG는 작업 영역 ID이고 C01234A5BCD는 채널 ID에 해당합니다.

5. 파일을 JSON 또는 YAML 파일으로 저장합니다.

## 관리 계정에 대한 스택 만들기

다음으로 조직의 관리 계정에 대한 스택을 만들어야 합니다. 이 단계에서는 RegisterSlackWorkspaceForOrganization API 작업을 자동으로 호출하고 Slack으로 작업 영역을 승인합니다.

> **Note**
>
> 관리 계정에 대한 이전 절차에서 업데이트한 Slack 작업 영역 구성 템플릿을 업로드하는 것이 좋습니다. AWS Support 앱을 사용하도록 관리 계정도 구성하지 않는 한 Slack 채널 구성 템플릿을 업로드할 필요가 없습니다.

관리 계정에 대한 스택을 생성하려면

1. 조직의 관리 계정으로 AWS Management Console에 로그인합니다.
2. AWS CloudFormation 콘솔(https://console.aws.amazon.com/cloudformation)을 엽니다.
3. 아직 선택하지 않았다면 Region selector(리전 선택기)에서 다음 AWS 리전을 선택합니다.
   - 유럽(프랑크푸르트)
   - 유럽(아일랜드)
   - 유럽(런던)
   - 미국 동부(버지니아 북부)
   - 미국 동부(오하이오)
   - 미국 서부(오레곤)
   - 아시아 태평양(싱가포르)
   - 아시아 태평양(도쿄)
   - 캐나다(중부)
4. 절차에 따라 스택을 생성합니다. 자세한 내용은 AWS CloudFormation 콘솔에서 스택 생성 단원을 참조하세요.

   CloudFormation이 스택을 성공적으로 생성한 후에는 동일한 템플릿을 사용하여 조직의 스택 세트를 만들 수 있습니다.

## 조직을 위한 스택 세트 생성

다음으로 Slack 작업 영역 구성에 동일한 템플릿을 사용하여 `service-managed` 권한이 있는 스택 세트를 생성합니다. 스택 세트를 사용하여 전체 조직을 위한 스택을 만들거나 원하는 OU를 지정할 수 있습니다. 자세한 내용은 스택 세트 생성을 참조하세요.

이 절차는 RegisterSlackWorkspaceForOrganization API 작업도 자동으로 호출합니다. 이 API 작업은 멤버 계정에 대해 Slack으로 작업 영역을 승인합니다.

조직을 위한 스택 세트를 생성하려면

1. 조직의 관리 계정으로 AWS Management Console에 로그인합니다.
2. AWS CloudFormation 콘솔(https://console.aws.amazon.com/cloudformation)을 엽니다.
3. 아직 설정하지 않았다면 Region selector(리전 선택기)에서 이전 절차에서 사용한 것과 동일한 AWS 리전을 선택합니다.
4. 탐색 창에서 StackSets(스택 세트)를 선택합니다.
5. Create StackSet(StackSet 생성)을 선택합니다.
6. Choose a template(템플릿 선택) 페이지에서 다음 옵션의 기본 옵션을 그대로 두세요.
   - Permissions(권한)의 경우 Service-managed permissions(서비스 관리형 권한)를 유지합니다.
   - Prerequisite - Prepare template(사전 조건 - 템플릿 준비)에서 Template is ready(템플릿 준비 완료)를 선택합니다.
7. Specify template(템플릿 지정)에서 Upload a template file(템플릿 파일 업로드)을 선택한 다음 Choose file(파일 선택)을 선택합니다.
8. 파일을 선택한 후 Next(다음)를 선택합니다.
9. Specify stack details(스택 세부 정보 지정) 페이지에서 **`support-app-slack-workspace`** 등의 스택 이름을 입력한 후 설명을 입력하고 Next(다음)를 선택합니다.
10. Configure StackSet options(StackSet 옵션 구성) 페이지에서 기본 옵션을 유지하고 Next(다음)를 선택합니다.
11. Set deployment options(배포 옵션 설정) 페이지에서 Add stacks to stack set(스택 세트에 스택 추가)의 기본 Deploy new stacks(새 스택 배포) 옵션을 그대로 유지합니다.
12. Deployment targets(배포 대상)의 경우 전체 조직 또는 특정 OU에 대한 스택을 생성할지 선택합니다. OU를 선택한 경우 OU ID를 입력합니다.
13. Specify regions(리전 지정)에는 다음 AWS 리전 중 하나만 입력합니다.
    - 유럽(프랑크푸르트)

- 유럽(아일랜드)
- 유럽(런던)
- 미국 동부(버지니아 북부)
- 미국 동부(오하이오)
- 미국 서부(오레곤)
- 아시아 태평양(싱가포르)
- 아시아 태평양(도쿄)
- 캐나다(중부)

> 참고:
>
> - 워크플로를 간소화하려면 3단계에서 선택한 것과 동일한 AWS 리전을 사용하는 것이 좋습니다.
> - 둘 이상의 AWS 리전을 선택하면 스택 생성과 충돌이 발생할 수 있습니다.

14. 배포 옵션(Deployment options)의 경우 내결함성 - 선택 사항(Failure tolerance - optional)에는 CloudFormation이 작업을 중지하기 전에 스택이 실패할 수 있는 계정 수를 입력합니다. 추가하려는 계정 수에서 1을 뺀 수를 입력하는 것이 좋습니다. 예를 들어 지정한 OU에 10개의 멤버 계정이 있는 경우 9를 입력합니다. 즉, CloudFormation이 9번 실패하더라도 하나 이상의 계정이 성공합니다.
15. 다음(Next)을 선택합니다.
16. Review(검토) 페이지에서 옵션을 검토하고 Submit(제출)을 선택하세요. Stack instance(스택 인스턴스) 탭에서 스택의 상태를 확인할 수 있습니다.
17. (선택 사항) 이 절차를 반복하여 Slack 채널 구성용 템플릿을 업로드합니다. 예제 템플릿은 또한 IAM 역할을 생성하고 AWS 관리형 정책을 연결합니다. 이 역할에는 다른 서비스에 액세스하는 데 필요한 권한이 있습니다. 자세한 내용은 AWS Support 앱에 대한 액세스 관리 섹션을 참조하세요.

    Slack 채널 구성을 만들기 위한 스택 세트를 생성하지 않는 경우 멤버 계정에서 Slack 채널을 수동으로 구성할 수 있습니다. 자세한 내용은 Slack 채널 구성 섹션을 참조하세요.

CloudFormation에서 스택을 생성한 후 각 멤버 계정은 지원 센터 콘솔에 로그인하여 구성된 Slack 작업 영역 및 채널을 찾을 수 있습니다. 그런 다음 AWS 계정에서 AWS Support 앱을 사용할 수 있습니다. Slack 채널에서 지원 사례 생성 섹션을 참조하세요.

> **Tip**
>
> 새 템플릿을 업로드해야 하는 경우 이전에 지정한 것과 동일한 AWS 리전을 사용하는 것이 좋습니다.

## CloudFormation에 대해 자세히 알아보기

CloudFormation에 대한 자세한 내용은 다음 리소스를 참조하세요.

- AWS CloudFormation
- AWS CloudFormation 사용 설명서
- AWS CloudFormation API 참조
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

## Terraform을 사용하여 AWS Support 앱 리소스 생성

Terraform을 사용하여 AWS 계정을 위한 AWS Support 앱 리소스를 생성할 수도 있습니다. Terraform은 클라우드 애플리케이션에 사용할 수 있는 코드형 인프라(IaC) 도구입니다. 계정에 CloudFormation 스택을 배포하는 대신 Terraform을 사용하여 AWS Support 앱 리소스를 생성할 수 있습니다.

Terraform을 설치한 후 원하는 AWS Support 앱 리소스를 지정할 수 있습니다. Terraform은 RegisterSlackWorkspaceForOrganization API 작업을 호출하여 사용자를 위한 Slack 작업 영역을 등록하고 리소스를 생성합니다. 그런 다음 지원 센터 콘솔에 로그인하여 구성된 Slack 작업 영역 및 채널을 찾을 수 있습니다.

> **주의**
>
> - 조직의 관리 계정인 경우 멤버 계정이 Terraform을 사용하여 리소스를 생성하려면 계정에 대한 Slack 작업 영역을 수동으로 승인해야 합니다. 아직 이를 실행하지 않았다면 Slack 작업 영역 승인 단원을 참조하세요.
> - CloudFormation 스택 세트와 달리 Terraform을 사용하여 조직의 OU에 대한 AWS Support 앱 리소스를 생성할 수 없습니다.
> - AWS CloudTrail의 Terraform에서 이러한 업데이트에 대한 이벤트 기록을 찾을 수도 있습니다. 이러한 이벤트의 `eventSource`는 `cloudcontrolapi.amazonaws.com` 및

supportapp.amazonaws.com입니다. 자세한 내용은 AWS CloudTrail을 사용하여 Slack API의 AWS Support 앱 호출 로깅 섹션을 참조하세요.

## 자세히 알아보기

Terraform에 대한 자세한 내용은 다음 주제를 참조하세요.

- Terraform 설치
- Terraform 튜토리얼: AWS를 위한 인프라 구축
- awscc_support_app_account_alias
- awscc_supportapp_slack_workspace_configuration
- awscc_supportapp_slack_channel_configuration

# 보안: AWS Support

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스 Amazon Web Services 규정 준수 프로그램별 참조하십시오. AWS Support
- 클라우드에서의 보안 — 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 공동 책임 모델을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 AWS Support됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 AWS Support 충족하도록 구성하는 방법을 보여줍니다. 또한 AWS Support 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 Amazon Web Services를 사용하는 방법도 배웁니다.

주제

- 데이터 보호: AWS Support
- 케이스의 보안 AWS Support
- ID 및 액세스 관리 대상 AWS Support
- 사고 대응
- 로그인 및 모니터링 AWS Support 및 AWS Trusted Advisor
- 규정 준수 검증: AWS Support
- 의 레질리언스 AWS Support
- 의 인프라 보안 AWS Support
- 의 구성 및 취약성 분석 AWS Support

# 데이터 보호: AWS Support

AWS 공동 책임 모델 의 데이터 보호에 적용됩니다 AWS Support. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

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

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 리소스와 통신하세요. AWS TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.

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

## 케이스의 보안 AWS Support

지원 사례를 생성하면 지원 사례에 포함되는 정보를 소유하게 됩니다. AWS 사용자의 허가 없이는 AWS 계정 데이터에 액세스하지 않습니다. AWS 제3자와 정보를 공유하지 않습니다.

지원 사례를 생성할 때 다음 사항에 유의하세요.

- AWS Support `AWSServiceRoleForSupport`서비스 연결 역할에 정의된 권한을 사용하여 고객 문제를 해결해 AWS 서비스 줄 다른 사람에게 전화를 겁니다. 자세한 내용은 서비스 연결 역할 사용 및 관리형 정책을 참조하십시오. AWS SupportAWS AWSSupportServiceRolePolicy
- 에서 AWS Support 발생한 API 호출을 볼 수 있습니다. AWS 계정예를 들어 계정 내 누군가가 지원 사례를 생성하거나 해결할 때 로그 정보를 볼 수 있습니다. 자세한 내용은 AWS Support API 호출 로깅을 참조하십시오 AWS CloudTrail.
- API를 사용하여 AWS Support API를 호출할 수 있습니다. `DescribeCases` 이 API는 사례 ID, 생성 날짜, 해결 날짜, 지원 에이전트와의 서신과 같은 지원 사례 정보를 반환합니다. 사례 생성 후 최대 12개월 동안 사례 세부 정보를 볼 수 있습니다. 자세한 내용은 AWS Support API DescribeCases참조를 참조하십시오.
- 지원 사례는 AWS Support의 규정 준수 확인을 따릅니다.
- 지원 사례를 생성하면 계정에 액세스할 수 AWS 없습니다. 필요한 경우 지원 에이전트는 화면 공유 도구를 사용하여 원격으로 화면을 보고 문제를 식별하고 해결합니다. 이 도구는 보기 전용입니다. AWS Support 에서는 화면 공유 세션 중에 사용자를 대리할 수 없습니다. 지원 에이전트와 화면을 공유하려면 동의해야 합니다. 자세한 내용은 AWS Support FAQ를 참조하십시오.
- AWS Support 플랜을 변경하여 계정에 필요한 도움을 받을 수 있습니다. 자세한 내용은 AWS Support 플랜 비교 및 AWS Support 플랜 변경을 참조하십시오.

# ID 및 액세스 관리 대상 AWS Support

AWS Identity and Access Management (IAM) 은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM 관리자는 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. AWS Support IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- IAM의 AWS Support 작동 방식
- AWS Support ID 기반 정책 예제
- 서비스 링크 역할 사용
- AWS 관리형 정책 대상 AWS Support
- AWS Support 센터 액세스 관리

- 플랜에 대한 액세스 관리 AWS Support
- 액세스 관리: AWS Trusted Advisor
- AWS Trusted Advisor에 대한 예제 서비스 제어 정책
- AWS Support ID 및 액세스 문제 해결

## 고객

사용하는 방식 AWS Identity and Access Management (IAM) 은 수행하는 작업에 따라 다릅니다. AWS Support

서비스 사용자 - AWS Support 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS Support 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AWS Support의 기능에 액세스할 수 없는 경우 AWS Support ID 및 액세스 문제 해결을 참조하세요.

서비스 관리자 — 회사에서 AWS Support 리소스를 담당하는 경우 전체 액세스 권한이 있을 수 AWS Support있습니다. 서비스 사용자가 액세스해야 하는 AWS Support 기능과 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사에서 IAM을 어떻게 사용할 수 있는지 자세히 AWS Support알아보려면 을 참조하십시오IAM의 AWS Support 작동 방식.

IAM 관리자 - IAM 관리자라면 AWS Support에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 AWS Support ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Support ID 기반 정책 예제

## ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 연동 자격 증명으로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

## AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

## IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 가진 사용자 내의 자격 증명입니다. AWS 계정 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하세요.

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

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하세요.

## IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 연동 자격 증명에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 만들기를 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 아이덴티티가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관 짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예컨대, 어떤 서비스에서 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.

- 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하세요.

## 정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

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

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

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

### ID 기반 정책

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

있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

## 기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 보안 인증 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할 자격 증명 기반 정책의 교차 및 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

## 여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

# IAM의 AWS Support 작동 방식

IAM을 사용하여 액세스를 AWS Support관리하기 전에 먼저 사용할 수 있는 IAM 기능이 무엇인지 이해해야 합니다. AWS Support기타 AWS 서비스가 AWS Support IAM과 연동되는 방식을 자세히 알아보려면 IAM 사용 설명서에서 IAM과 연동되는AWS 서비스를 참조하십시오.

IAM을 AWS Support 사용하기 위한 액세스를 관리하는 방법에 대한 자세한 내용은 액세스 관리를 참조하십시오. AWS Support

주제

- AWS Support ID 기반 정책
- AWS Support IAM 역할

## AWS Support ID 기반 정책

IAM 자격 증명 기반 정책을 사용하면 허용 또는 거부할 작업과 리소스뿐 아니라 작업이 허용 또는 거부 조건을 지정할 수 있습니다. AWS Support 는 특정 작업을 지원합니다. JSON 정책에서 사용하는 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

작업

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

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

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

정책 조치는 조치 앞에 다음 접두사를 AWS Support 사용합니다. `support:` 예를 들어 누군가에게 Amazon EC2 `RunInstances` API 작업을 통해 Amazon EC2 인스턴스를 실행할 권한을 부여하려면 해당 정책에 `ec2:RunInstances` 작업을 포함하세요. 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. AWS Support 는 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 집합을 정의합니다.

명령문 하나에 여러 태스크를 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
```

```
      "ec2:action1",
      "ec2:action2"
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, Describe라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "ec2:Describe*"
```

AWS Support 작업 목록을 보려면 IAM 사용 설명서의 정의된 AWS Support작업을 참조하십시오.

예제

AWS Support ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Support ID 기반 정책 예제

## AWS Support IAM 역할

IAM 역할은 AWS 계정 내에서 특정 권한을 가진 엔티티입니다.

임시 자격 증명 사용: AWS Support

임시 보안 인증을 사용하여 페더레이션을 통해 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. AssumeRole또는 GetFederationToken과 같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 얻습니다.

AWS Support 임시 자격 증명 사용을 지원합니다.

서비스 연결 역할

서비스 연결 역할을 사용하면 AWS 서비스가 다른 서비스의 리소스에 액세스하여 사용자를 대신하여 작업을 완료할 수 있습니다. 서비스 연결 역할은 IAM 계정에 나타나고 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수 없습니다.

AWS Support 서비스 연결 역할을 지원합니다. AWS Support 서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. AWS Support에 서비스 연결 역할 사용

서비스 역할

이 기능을 사용하면 서비스가 사용자를 대신하여 서비스 역할을 수임할 수 있습니다. 이 역할을 사용하면 서비스가 다른 서비스의 리소스에 액세스해 사용자를 대신해 작업을 완료할 수 있습니다. 서비스 역할은 IAM 계정에 나타나고, 해당 계정이 소유합니다. 즉, IAM 관리자가 이 역할에 대한 권한을 변경할 수 있습니다. 그러나 권한을 변경하면 서비스의 기능이 손상될 수 있습니다.

AWS Support 서비스 역할을 지원합니다.

## AWS Support ID 기반 정책 예제

기본적으로 IAM 사용자 및 역할은 AWS Support 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI, 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. IAM 관리자는 지정된 리소스에서 특정 API 작업을 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 정책을 연결해야 합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 JSON 탭에서 정책 생성을 참조하세요.

주제

- 정책 모범 사례
- AWS Support 콘솔 사용
- 사용자가 자신이 권한을 볼 수 있도록 허용

### 정책 모범 사례

자격 증명 기반 정책은 매우 강력합니다. 계정에서 다른 사람이 AWS Support 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르십시오.

- AWS 관리형 정책 사용 시작하기 — 관리형 정책을 AWS Support 빠르게 사용하려면 AWS 관리형 정책을 사용하여 직원에게 필요한 권한을 부여하세요. 이 정책은 이미 계정에서 사용할 수 있으며 AWS에 의해 유지 관리 및 업데이트됩니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책으로 권한 사용 시작하기를 참조하십시오.
- 최소 권한 부여 – 사용자 지정 정책을 생성할 때는 작업을 수행하는 데 필요한 권한만 부여합니다. 최소한의 권한 조합으로 시작하여 필요에 따라 추가 권한을 부여합니다. 처음부터 권한을 많이 부여한 후 나중에 줄이는 방법보다 이 방법이 안전합니다. 자세한 정보는 IAM 사용 설명서의 최소 권한 부여를 참조하세요.
- 민감한 작업에 대해 MFA 활성화 – 보안을 강화하기 위해 IAM 사용자가 중요한 리소스 또는 API 작업에 액세스하려면 멀티 팩터 인증(MFA)을 사용해야 합니다. 자세한 정보는 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.
- 보안 강화를 위해 정책 조건 사용 – 실제로 가능한 경우, 자격 증명 기반 정책이 리소스에 대한 액세스를 허용하는 조건을 정의합니다. 예를 들어 요청을 할 수 있는 IP 주소의 범위를 지정하도록 조건

을 작성할 수 있습니다. 지정된 날짜 또는 시간 범위 내에서만 요청을 허용하거나, SSL 또는 MFA를 사용해야 하는 조건을 작성할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.

## AWS Support 콘솔 사용

AWS Support 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 AWS 계정의 AWS Support 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다. 최소 필수 권한보다 더 제한적인 보안 인증 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(IAM 사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

해당 엔티티가 AWS Support 콘솔을 계속 사용할 수 있도록 하려면 다음 AWS 관리형 정책도 엔티티에 연결하십시오. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

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

## 사용자가 자신이 권한을 볼 수 있도록 허용

이 예시는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

# 서비스 링크 역할 사용

AWS Support 그리고 AWS Identity and Access Management (IAM) 서비스 연결 역할을 AWS Trusted Advisor 사용하십시오. 서비스 연결 역할은 및 에 직접 연결된 고유한 IAM 역할입니다. AWS Support Trusted Advisor각각의 경우 서비스 연결 역할은 사전 정의된 역할입니다. 이 역할에는 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 Trusted Advisor 필요한 모든 권한이 포함됩니다. AWS Support 다음 항목에서는 서비스 연결 역할이 어떤 역할을 하며, 및 에서 AWS Support 해당 역할을 어떻게 사용하는지에 대해 설명합니다. Trusted Advisor

주제

- AWS Support에 서비스 연결 역할 사용
- Trusted Advisor의 서비스 링크 역할 사용

## AWS Support에 서비스 연결 역할 사용

AWS Support 도구는 API 호출을 통해 AWS 리소스에 대한 정보를 수집하여 고객 서비스 및 기술 지원을 제공합니다. 지원 활동의 투명성과 감사 가능성을 높이기 위해 AWS Identity and Access Management (IAM) 서비스 연결 역할을 AWS Support 사용합니다.

`AWSServiceRoleForSupport`서비스 연결 역할은 직접 연결된 고유한 IAM 역할입니다. AWS Support이 서비스 연결 역할은 미리 정의되어 있으며, 사용자를 대신하여 다른 서비스를 호출하는 데 AWS Support 필요한 권한을 포함합니다. AWS

`AWSServiceRoleForSupport` 서비스 연결 역할은 역할을 수임하기 위해 `support.amazonaws.com` 서비스를 신뢰합니다.

이러한 서비스를 제공하기 위해 역할의 사전 정의된 권한은 고객 데이터가 아닌 리소스 메타데이터에 AWS Support 대한 액세스 권한을 부여합니다. AWS Support 도구만 이 역할을 맡을 수 있으며, 이 역할은 AWS 계정 내에 있습니다.

당사는 고객 데이터가 포함될 수 있는 필드를 삭제합니다. 예를 들어 AWS Step Functions API 호출 GetExecution기록의 `Input` 및 `Output` 필드는 에 표시되지 않습니다 AWS Support. 민감한 필드는 AWS KMS keys 를 사용하여 암호화됩니다. 이러한 필드는 API 응답에서 수정되며 AWS Support 상담원에게는 보이지 않습니다.

> **Note**
>
> AWS Trusted Advisor 별도의 IAM 서비스 연결 역할을 사용하여 계정의 AWS 리소스에 액세스하여 모범 사례 권장 사항 및 검사를 제공합니다. 자세한 정보는 Trusted Advisor의 서비스 링크 역할 사용을 참조하세요.

`AWSServiceRoleForSupport`서비스 연결 역할을 사용하면 모든 AWS Support API 호출을 통해 고객이 볼 수 있습니다. AWS CloudTrail이렇게 하면 사용자 대신 AWS Support 수행하는 작업을 투명하게 이해할 수 있으므로 요구 사항을 모니터링하고 감사하는 데 도움이 됩니다. 에 대한 CloudTrail 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

AWS Support에 대한 서비스 연결 역할 권한

이 역할은 `AWSSupportServiceRolePolicy` AWS 관리형 정책을 사용합니다. 이 관리형 정책은 역할에 연결되어 사용자 대신 작업을 완료할 역할 권한을 허용합니다.

이러한 업데이트에는 다음과 같은 작업이 포함됩니다.

- 청구, 관리, 지원 및 기타 고객 서비스 — AWS 고객 서비스에서는 관리형 정책에서 부여한 권한을 사용하여 지원 계획의 일환으로 여러 서비스를 수행합니다. 여기에는 계정 및 결제 관련 질문 조사 및 답변, 계정에 대한 관리 지원 제공, 서비스 제한 증가, 추가 고객 지원 제공이 포함됩니다.
- AWS 계정의 서비스 특성 및 사용 데이터를 처리하는 경우 관리형 정책에서 부여한 권한을 사용하여 AWS 계정의 서비스 특성 및 사용 데이터에 액세스할 AWS Support 수 있습니다. 이 정책을 통해 AWS Support 계정에 대한 청구, 관리 및 기술 지원을 제공할 수 있습니다. 서비스 속성에는 계정의 리소스 식별자, 메타데이터 태그, 역할 및 권한이 포함됩니다. 사용 데이터에는 사용 정책, 사용 통계 및 분석이 포함됩니다.
- 계정 및 해당 리소스의 운영 상태 유지 — 자동화된 도구를 AWS Support 사용하여 운영 및 기술 지원과 관련된 조치를 수행합니다.

허용되는 서비스 및 작업에 대한 자세한 내용은 IAM 콘솔의 AWSSupportServiceRolePolicy 정책을 참조하세요.

> **Note**
>
> AWS Support 한 달에 한 번 `AWSSupportServiceRolePolicy` 정책을 자동으로 업데이트하여 새 AWS 서비스 및 작업에 대한 권한을 추가합니다.

자세한 정보는 AWS 관리형 정책 대상 AWS Support을 참조하세요.

에 대한 서비스 연결 역할 생성 AWS Support

`AWSServiceRoleForSupport` 역할을 수동으로 생성할 필요가 없습니다. AWS 계정을 생성하면 이 역할이 자동으로 생성되고 구성됩니다.

> **Important**
>
> 서비스 연결 역할 지원을 AWS Support 시작하기 전에 사용한 경우 계정에 `AWSServiceRoleForSupport` 역할을 AWS 생성한 것입니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

에 대한 서비스 연결 역할 편집 및 삭제 AWS Support

IAM을 사용하여 `AWSServiceRoleForSupport` 서비스 연결 역할에 대한 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

이 `AWSServiceRoleForSupport` 역할은 계정에 대한 관리, 운영 및 기술 지원을 제공하는 AWS Support 데 필요합니다. 따라서 IAM 콘솔, API 또는 AWS Command Line Interface (AWS CLI) 를 통해 이 역할을 삭제할 수 없습니다. 지원 서비스를 관리하기 위해 필요한 권한을 실수로 제거할 수 없으므로 AWS 계정이 보호됩니다.

`AWSServiceRoleForSupport` 역할 또는 그 용도에 대한 자세한 내용은 AWS Support에 문의하세요.

## Trusted Advisor의 서비스 링크 역할 사용

AWS Trusted Advisor AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결된 고유한 IAM 역할입니다. AWS Trusted Advisor서비스 연결 역할은 에서 미리 정의되며 서비스에서 사용자를 대신하여 Trusted Advisor다른 서비스를 호출하는 데 필요한

모든 권한을 포함합니다. AWS Trusted Advisor 이 역할을 사용하여 전체 AWS 사용량을 확인하고 환경 개선을 위한 권장 사항을 제공합니다. AWS 예를 들어, Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스 사용을 Trusted Advisor 분석하여 비용 절감, 성능 향상, 장애 허용 및 보안 개선을 지원합니다.

> **Note**
>
> AWS Support 별도의 IAM 서비스 연결 역할을 사용하여 계정 리소스에 액세스하여 청구, 관리 및 지원 서비스를 제공합니다. 자세한 정보는 AWS Support에 서비스 연결 역할 사용을 참조하세요.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스 단원을 참조하세요. 서비스 연결 역할(Service-linked role) 열에서 예(Yes)라고 표시된 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

주제

- Trusted Advisor에 대한 서비스 링크 역할 권한
- 서비스 연결 역할 권한 관리
- Trusted Advisor에 대한 서비스 링크 역할 생성
- Trusted Advisor에 대한 서비스 연결 역할 편집
- Trusted Advisor에 대한 서비스 링크 역할 삭제

### Trusted Advisor에 대한 서비스 링크 역할 권한

Trusted Advisor 두 가지 서비스 연결 역할을 사용합니다.

- AWSServiceRoleForTrustedAdvisor— 이 역할은 서비스가 사용자를 대신하여 Trusted Advisor AWS 서비스에 액세스하는 역할을 맡을 것으로 신뢰합니다. 역할 권한 정책은 모든 AWS 리소스에 대한 Trusted Advisor 읽기 전용 액세스를 허용합니다. 이 역할을 사용하면 필요한 권한을 추가할 필요가 없으므로 AWS 계정을 쉽게 시작할 수 있습니다. Trusted Advisor AWS 계정을 개설하면 이 역할이 자동으로 Trusted Advisor 생성됩니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함됩니다. 권한 정책은 다른 어떤 IAM 엔터티에도 연결할 수 없습니다.

  연결된 정책에 대한 자세한 내용은 을 참조하십시오 AWSTrustedAdvisorServiceRolePolicy.
- AWSServiceRoleForTrustedAdvisorReporting - 이 역할은 조직 보기 기능에 대한 역할을 맡도록 Trusted Advisor 서비스를 신뢰합니다. 이 역할을 AWS Organizations 조직에서 신뢰할 수 있는

Trusted Advisor 서비스로 사용할 수 있습니다. Trusted Advisor 조직 보기를 활성화하면 이 역할을 대신 생성합니다.

연결 정책에 대한 자세한 내용은 AWSTrustedAdvisorReportingServiceRolePolicy 단원을 참조하세요.

조직 보기를 사용하여 조직 내 모든 계정의 Trusted Advisor 검사 결과에 대한 보고서를 만들 수 있습니다. 이 기능에 대한 자세한 내용은 AWS Trusted Advisor에 대한 조직 보기 단원을 참조하세요.

### 서비스 연결 역할 권한 관리

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성해야 합니다. 다음은 `AWSServiceRoleForTrustedAdvisor` 서비스 연결 역할을 사용한 예입니다.

Example IAM 엔터티가 **`AWSServiceRoleForTrustedAdvisor`** 서비스 연결 역할을 생성하도록 허용

이 단계는 Trusted Advisor 계정이 비활성화되고, 서비스 연결 역할이 삭제되고, 사용자가 역할을 다시 생성하여 다시 활성화해야 하는 경우에만 필요합니다. Trusted Advisor

서비스 연결 역할을 생성하기 위해 IAM 엔터티의 권한 정책에 다음 명령문을 추가합니다.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example IAM 엔터티가 **`AWSServiceRoleForTrustedAdvisor`** 서비스 연결 역할의 설명을 편집할 수 있도록 허용

`AWSServiceRoleForTrustedAdvisor` 역할에 관한 설명만 편집할 수 있습니다. 서비스 연결 역할의 설명을 편집하기 위해 IAM 개체의 권한 정책에 다음 명령문을 추가할 수 있습니다.

```
{
```

```
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example IAM 엔터티가 **AWSServiceRoleForTrustedAdvisor** 서비스 연결 역할을 삭제하도록 허용

서비스 연결 역할을 삭제하기 위해 IAM 개체의 권한 정책에 다음 문장을 추가할 수 있습니다.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

와 같은 AWS AdministratorAccess관리형 정책을 사용하여 에 대한 전체 액세스 권한을 제공할 수도 있습니다. Trusted Advisor

Trusted Advisor에 대한 서비스 링크 역할 생성

AWSServiceRoleForTrustedAdvisor 서비스 연결 역할을 수동으로 생성할 필요가 없습니다. AWS 계정을 개설하면 서비스 연결 역할이 자동으로 Trusted Advisor 생성됩니다.

> **Important**
>
> Trusted Advisor 서비스 연결 역할을 지원하기 전에 서비스를 사용하고 있었다면 계정에 역할이 Trusted Advisor 이미 생성되어 있는 AWSServiceRoleForTrustedAdvisor 것입니다. 자세한 내용은 IAM 사용 설명서의 내 IAM 계정에 표시되는 새 역할을 참조하세요.

계정에 AWSServiceRoleForTrustedAdvisor 서비스 연결 역할이 없는 경우, Trusted Advisor 는 정상 작동하지 않습니다. 계정의 누군가가 Trusted Advisor 를 비활성화한 후 서

비스 연결 역할을 삭제한 경우 이러한 상황이 발생할 수 있습니다. 이럴 경우 IAM을 사용하여 AWSServiceRoleForTrustedAdvisor 서비스 연결 역할을 생성하고 Trusted Advisor를 다시 활성화하세요.

활성화하려면 Trusted Advisor (콘솔)

1. IAM 콘솔 또는 IAM API를 사용하여 서비스 연결 역할을 생성합니다. AWS CLI Trusted Advisor자세한 내용은 서비스 연결 역할 만들기를 참조하세요.
2. 에 로그인한 다음 에서 콘솔로 이동합니다. AWS Management Console Trusted Advisor https://console.aws.amazon.com/trustedadvisor

   비활성화된 Trusted Advisor(Disabled Trusted Advisor) 상태 배너가 콘솔에 표시됩니다.
3. 상태 배너에서 Trusted Advisor 역할 활성화를 선택합니다. 필요한 AWSServiceRoleForTrustedAdvisor가 감지되지 않을 경우 비활성화됨 상태 배너가 유지됩니다.

Trusted Advisor에 대한 서비스 연결 역할 편집

서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에서비스 연결 역할 이름을 변경할 수 없습니다. 하지만 IAM 콘솔이나 IAM API를 사용하여 역할 설명을 편집할 수 있습니다. AWS CLI자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Trusted Advisor에 대한 서비스 링크 역할 삭제

의 Trusted Advisor기능이나 서비스를 사용할 필요가 없는 경우 역할을 삭제할 수 있습니다. AWSServiceRoleForTrustedAdvisor 이 서비스 연결 역할을 삭제하려면 Trusted Advisor 먼저 비활성화해야 합니다. 이로써 Trusted Advisor 작업에 필요한 권한을 제거하는 일을 방지할 수 있습니다. Trusted Advisor비활성화하면 오프라인 처리 및 알림을 비롯한 모든 서비스 기능을 사용할 수 없게 됩니다. 또한 회원 계정을 Trusted Advisor 비활성화하면 별도의 지급인 계정도 영향을 받기 때문에 비용 절감 방법을 식별하는 Trusted Advisor 수표를 받지 못하게 됩니다. Trusted Advisor 콘솔에 액세스할 수 없습니다. 액세스 거부 오류를 Trusted Advisor 반환하기 위한 API 호출

먼저 계정에 AWSServiceRoleForTrustedAdvisor 서비스 연결 역할을 다시 생성해야 Trusted Advisor를 다시 활성화할 수 있습니다.

AWSServiceRoleForTrustedAdvisor서비스 연결 역할을 삭제하려면 먼저 Trusted Advisor 콘솔에서 비활성화해야 합니다.

비활성화하려면 Trusted Advisor

1. 에 AWS Management Console 로그인하고 에서 Trusted Advisor 콘솔로 이동합니다https://console.aws.amazon.com/trustedadvisor.
2. 탐색 창에서 Preferences(기본 설정)를 선택합니다.
3. Service Linked Role Permissions 섹션에서 Disable Trusted Advisor를 선택합니다.
4. 확인 대화 상자에서확인(OK)을 클릭하여 Trusted Advisor비활성화 여부를 확인합니다.

Trusted Advisor비활성화하면 모든 Trusted Advisor 기능이 비활성화되고 Trusted Advisor 콘솔에는 비활성화된 상태 배너만 표시됩니다.

그런 다음 IAM 콘솔 AWS CLI, 또는 IAM API를 사용하여 이름이 지정된 Trusted Advisor 서비스 연결 역할을 삭제할 수 있습니다. `AWSServiceRoleForTrustedAdvisor` 자세한 내용은 IAM 사용 설명서에서 서비스 연결 역할 삭제를 참조하세요.

## AWS 관리형 정책 대상 AWS Support

AWS 관리형 정책은 에서 생성하고 관리하는 독립 실행형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

주제

- AWS 관리형 정책은 다음과 같습니다. AWS Support
- AWS Slack의 AWS Support 앱에 대한 관리형 정책

- AWS 관리형 정책: AWS Trusted Advisor
- AWSAWS Support 플랜의 관리형 정책

## AWS 관리형 정책은 다음과 같습니다. AWS Support

AWS Support 에는 다음과 같은 관리형 정책이 있습니다.

목차

- AWS 관리형 정책: AWSSupportServiceRolePolicy
- AWS SupportAWS 관리형 정책 업데이트
- AWSSupportServiceRolePolicy에 대한 권한 변경

### AWS 관리형 정책: AWSSupportServiceRolePolicy

AWS Support AWSSupportServiceRolePolicy AWS 관리형 정책을 사용합니다. 이 관리형 정책은 `AWSServiceRoleForSupport` 서비스 연결 역할에 연결됩니다. 이 정책은 서비스 연결 역할이 사용자를 대신하여 작업을 완료할 수 있도록 허용합니다. IAM 엔터티에 이 정책을 연결할 수 없습니다. 자세한 정보는 AWS Support에 대한 서비스 연결 역할 권한을 참조하세요.

정책 변경 사항 목록은 AWS SupportAWS 관리형 정책 업데이트 및 AWSSupportServiceRolePolicy에 대한 권한 변경 단원을 참조하세요.

### AWS SupportAWS 관리형 정책 업데이트

해당 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Support 이후의 AWS 관리형 정책 업데이트에 대한 세부 정보를 볼 수 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 문서 기록 페이지에서 RSS 피드를 구독하십시오.

다음 표에는 2022년 2월 17일 이후 AWS Support 관리형 정책에 대한 중요 업데이트가 설명되어 있습니다.

## AWS Support

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy - 기존 정책에 대한 업데이트 | 청구, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있는 17개의 새 권한이 다음 서비스에 추가되었습니다.<br>• Amazon CloudWatch 네트워크 모니터 — 네트워크 모니터 서비스와 관련된 문제를 해결합니다.<br>• 아마존 CloudWatch 로그 — 아마존 로그와 관련된 문제를 CloudWatch 디버깅합니다.<br>• 아파치 Kafka용 아마존 매니지드 스트리밍 — 아파치 Kafka용 아마존 매니지드 스트리밍과 관련된 문제를 디버깅하기 위함입니다.<br>• Prometheus용 Amazon 관리형 서비스 — Prometheus용 Amazon 관리형 서비스와 관련된 문제를 해결합니다. | 2024년 3월 22일 |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 청구, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있는 63개의 새 권한을 다음 서비스에 추가했습니다.<br>• AWS 클린룸 — 클린룸과 관련된 문제를 해결합니다. AWS | 2024년 1월 17일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • CodeConnections — 관련 문제를 해결합니다. CodeConnections<br>• 아마존 EKS — 아마존 EKS와 관련된 문제를 디버깅하기 위함입니다.<br>• Image Builder — Image Builder와 관련된 문제를 디버깅합니다.<br>• 아마존 인스펙터2 — 아마존 인스펙터2와 관련된 문제를 해결합니다.<br>• 아마존 인스펙터 스캔 — 아마존 인스펙터 스캔과 관련된 문제를 디버깅합니다.<br>• Amazon CloudWatch 로그 — Amazon CloudWatch Logs와 관련된 문제를 해결하기 위한 것입니다.<br>• AWS Outposts — 와 관련된 문제를 해결합니다. AWS Outposts<br>• Amazon RDS - Amazon RDS와 관련된 문제를 디버깅합니다.<br>• AWS IAM Identity Center — 와 관련된 문제를 해결합니다. AWS IAM Identity Center<br>• 아마존 S3 익스프레스 — 아마존 S3 익스프레스와 관련된 문제를 디버깅하기 위함입니다. | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • AWS Trusted Advisor — 와 관련된 문제를 해결합니다. AWS Trusted Advisor | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 청구, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있는 126개의 새 권한을 다음 서비스에 추가했습니다.<br>• AWS Direct Connect — 서비스와 관련된 문제를 해결합니다. AWS Direct Connect<br>• Amazon SageMaker — Amazon SageMaker 서비스와 관련된 문제를 해결합니다.<br>• Amazon AppStream — 아마존과 관련된 문제를 디버깅합니다. AppStream<br>• AWS 리소스 탐색기 — 와 관련된 문제를 디버깅합니다. AWS 리소스 탐색기<br>• Amazon Redshift 서버리스 — Amazon Redshift 서버리스와 관련된 문제를 해결합니다.<br>• Amazon ElastiCache — 아마존과 관련된 문제를 디버깅합니다. ElastiCache<br>• Amazon Comprehend – Amazon Comprehend와 관련된 문제를 해결합니다.<br>• Amazon EC2 — Amazon EC2와 관련된 문제를 해결합니다. | 2023년 12월 6일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • 아마존 엘라스틱 쿠버네티스 서비스 — 아마존 엘라스틱 쿠버네티스 서비스와 관련된 문제를 디버깅하기 위함입니다.<br>• AWS Elastic Disaster Recovery — 와 관련된 문제를 해결합니다. AWS Elastic Disaster Recovery<br>• AWS AppSync — 관련 문제를 디버깅합니다. AWS AppSync<br>• Amazon CloudWatch 로그 — Amazon CloudWatch Logs와 관련된 문제를 해결하기 위한 것입니다.<br>• AWS Health — 서비스와 관련된 문제를 디버깅합니다. AWS Health<br>• 아마존 커넥트 — 아마존 커넥트와 관련된 문제를 디버깅하기 위함입니다.<br>• AWS Snowball — 와 관련된 문제를 해결합니다. AWS Snowball<br>• AWS Health이미징 — 이미징과 관련된 AWS Health문제를 해결합니다. | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 권한 163개가 다음 서비스에 추가되었습니다.<br>• Amazon CloudFront — CloudFront 서비스와 관련된 문제를 해결합니다.<br>• Amazon EC2 - Amazon EC2 서비스와 관련된 문제를 해결합니다.<br>• Amazon AppStream — 아마존과 관련된 문제를 디버깅합니다. AppStream<br>• AWS WAF — AWS 웹 애플리케이션 방화벽과 관련된 문제를 디버깅합니다.<br>• Amazon Connect - Amazon Connect와 관련된 문제를 해결합니다.<br>• AWS IoT — 와 관련된 문제를 디버깅합니다. AWS IoT<br>• Amazon Route 53 - Amazon Route 53과 관련된 문제를 해결합니다.<br>• AWS 검증된 액세스 — AWS 검증된 액세스 서비스와 관련된 문제를 해결합니다.<br>• Amazon 심플 이메일 서비스 - Amazon 심플 이메일 서비스와 관련된 문제를 디버깅합니다. | 2023년 10월 27일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • AWS Elastic Beanstalk — 와 관련된 문제를 해결합니다. AWS Elastic Beanstalk<br>• Amazon DynamoDB - Amazon DynamoDB와 관련된 문제를 디버깅합니다.<br>• AWS EC2 이미지 빌더 — EC2 이미지 빌더와 AWS 관련된 문제를 해결합니다.<br>• AWS Outposts — 서비스와 관련된 문제를 디버깅합니다. AWS Outposts<br>• AWS Glue — 와 관련된 문제를 디버깅합니다. AWS Glue<br>• AWS Directory Service — 관련 문제를 해결합니다. AWS Directory Service<br>• AWS Elastic Disaster Recovery — 관련 문제를 해결합니다. AWS Elastic Disaster Recovery<br>• AWS Step Functions — 관련 문제를 디버깅합니다. AWS Step Functions<br>• Amazon EMR - Amazon EMR과 관련된 문제를 해결합니다.<br>• Amazon 관계형 데이터베이스 서비스 - Amazon 관계형 데이터베이스 서비스와 관련된 문제를 해결합니다. | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • Amazon EC2 Systems Manager - Amazon EC2 Systems Manager와 관련된 문제를 디버깅합니다. | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 권한 176개가 다음 서비스에 추가되었습니다.<br>• AWS Glue — 서비스 관련 문제 해결 AWS Glue<br>• Amazon EMR - Amazon EMR 서비스와 관련된 문제를 해결합니다.<br>• Amazon Security Lake - Amazon Security Lake와 관련된 문제를 디버깅합니다.<br>• AWS Systems Manager — Systems Manager 서비스와 관련된 문제를 디버깅합니다.<br>• Amazon Verified Permissions - Amazon Verified Permissions과 관련된 문제를 해결합니다.<br>• AWS IAM 액세스 분석기 - IAM 액세스 분석기 서비스와 관련된 문제를 디버깅합니다.<br>• AWS Backup — 와 관련된 문제를 해결합니다. AWS Backup<br>• AWS Database Migration Service — DMS 서비스와 관련된 문제를 해결합니다. | 2023년 8월 28일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • Amazon DynamoDB - Dynamo DB와 관련된 문제를 디버깅합니다.<br>• Amazon Elastic Container Registry(Amazon ECR) - Amazon Elastic Container Registry(Amazon ECR)와 관련된 문제를 해결합니다.<br>• Amazon Elastic 컨테이너 서비스 - Amazon Elastic 컨테이너 서비스와 관련된 문제를 디버깅합니다.<br>• Amazon Elastic Kubernetes Service - Amazon Elastic Kubernetes 서비스와 관련된 문제를 해결합니다.<br>• Amazon EMR Serverless - Amazon EMR Serverless 서비스와 관련된 문제를 디버깅합니다.<br>• AWS Identity and Access Management — 와 관련된 문제를 해결합니다. AWS Identity and Access Management<br>• AWS Network Firewall - 네트워크 방화벽과 관련된 AWS 문제를 해결합니다.<br>• AWS HealthOmics — 관련 문제를 디버깅합니다. AWS HealthOmics | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • Amazon QuickSight — 아마존과 관련된 문제를 디버깅합니다. QuickSight<br>• Amazon 관계형 데이터베이스 서비스 - Amazon 관계형 데이터베이스 서비스와 관련된 문제를 해결합니다.<br>• Amazon Redshift - Amazon Redshift와 관련된 문제를 해결합니다.<br>• Amazon Redshift Serverless - Amazon Redshift Serverless와 관련된 문제를 디버깅합니다.<br>• Amazon SageMaker — 아마존과 관련된 문제를 디버깅합니다. SageMaker | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 권한 141개가 다음 서비스에 추가되었습니다.<br>• Lambda - Lambda 서비스와 관련된 문제를 해결합니다.<br>• Amazon Lex - Amazon Lex 서비스와 관련된 문제를 해결합니다.<br>• AWS 전송 — 전송 서비스와 관련된 문제를 디버깅합니다.<br>• AWS Amplify — Amplify 서비스와 관련된 문제를 디버깅합니다.<br>• Amazon EventBridge Pipes — Pipes와 관련된 권한 및 청구 문제를 해결합니다.<br>• Amazon EventBridge — 아마존 관련 문제를 디버깅하려면 EventBridge<br>• Amazon CloudWatch 로그 — Amazon CloudWatch Logs와 관련된 문제를 해결하기 위한 것입니다.<br>• AWS Systems Manager — Systems Manager와 관련된 문제를 해결합니다.<br>• Amazon CloudWatch — 관련된 CloudWatch 문제를 디버깅합니다. | 2023년 6월 26일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • Amazon ElastiCache — 아마존과 관련된 문제를 해결하기 위함입니다. ElastiCache<br>• Amazon Athena - Athena와 관련된 문제를 디버깅합니다.<br>• AWS Elastic Disaster Recovery — Elastic 재해 복구와 관련된 문제를 해결합니다.<br>• Amazon CloudWatch — Amazon의 구성 문제를 해결하기 위해서입니다. CloudWatch<br>• Amazon EC2 - EC2 서비스와 관련된 문제를 디버깅합니다.<br>• AWS Certificate Manager — Certificate Manager와 관련된 문제를 해결합니다.<br>• Amazon EventBridge 스케줄러 — 스케줄러와 관련된 EventBridge 문제를 해결합니다.<br>• Amazon OpenSearch 서비스 — 관련 문제를 OpenSearch 해결합니다.<br>• Amazon EventBridge 스키마 — 스키마와 관련된 EventBridge 문제를 디버깅합니다. | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • AWS 사용자 알림 — 사용자 알림과 관련된 문제를 해결합니다.<br>• Amazon CloudWatch 애플리케이션 인사이트 — CloudWatch 애플리케이션 인사이트와 관련된 문제를 해결합니다.<br>• Amazon DynamoDB - DynamoDB와 관련된 문제를 해결합니다.<br>• Amazon DocumentDB Elastic Clusters - DocumentDB Elastic Clusters와 관련된 문제를 해결합니다. | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 권한 53개가 다음 서비스에 추가되었습니다.<br>• Auto Scaling - Auto Scaling 서비스와 관련된 문제를 해결합니다.<br>• Amazon CloudWatch — 아마존과 관련된 문제를 해결하기 위함입니다. CloudWatch<br>• AWS Compute Optimizer — Compute Optimizer와 관련된 문제를 해결합니다.<br>• Amazon은 CloudWatch 분명히 — Evidenly와 관련된 문제를 해결하기 위함입니다.<br>• EC2 Image Builder - Image Builder 서비스와 관련된 문제를 해결합니다.<br>• AWS IoT TwinMaker — 와 관련된 문제를 해결합니다. AWS IoT TwinMaker<br>• Amazon CloudWatch 로그 — Amazon CloudWatch Logs와 관련된 문제를 해결하기 위한 것입니다.<br>• Amazon Pinpoint – Amazon Pinpoint와 관련된 문제를 해결합니다. | 2023년 5월 2일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • AWS OAM 링크 — OAM 리소스와 관련된 문제를 디버깅합니다.<br>• AWS Outposts — 관련 문제를 해결합니다. AWS Outposts<br>• Amazon RDS - Amazon RDS와 관련된 문제를 디버깅합니다.<br>• AWS 리소스 탐색기 — 리소스 탐색기와 관련된 문제를 해결합니다.<br>• Amazon CloudWatch RUM — RUM 서비스 리소스의 구성 문제를 해결합니다.<br>• Amazon SNS - Amazon SNS와 관련된 문제를 해결합니다.<br>• 아마존 CloudWatch 신세틱스 — 신세틱스와 관련된 문제를 해결하기 위해서입니다. CloudWatch | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 권한 52개가 다음 서비스에 추가되었습니다.<br>• AWS Backup gateway — Backup 게이트웨이와 관련된 문제를 해결합니다.<br>• Amazon S3 - Amazon S3와 관련된 문제를 디버깅합니다.<br>• AWS Application Migration Service — 애플리케이션 마이그레이션 서비스와 관련된 문제를 해결합니다.<br>• AWS 클린룸 — 클린룸과 관련된 AWS 문제를 디버깅합니다.<br>• AWS Systems Manager SAP용 — AWS Systems Manager SAP용 관련 문제를 해결합니다.<br>• Amazon VPC Lattice - Amazon VPC Lattice와 관련된 문제를 디버깅합니다. | 2023년 3월 16일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 권한 220개가 다음 서비스에 추가되었습니다.<br>• Amazon Athena — Athena와 관련된 쿼리를 통해 AWS Support 고객을 지원하는 데 사용할 수 있는 도구를 개발할 수 있도록 하기 위함입니다.<br>• Amazon Chime - Amazon Chime와 관련된 문제를 해결합니다.<br>• Amazon CloudWatch 인터넷 모니터 — 인터넷 모니터와 관련된 문제를 디버깅합니다.<br>• Amazon Comprehend – Amazon Comprehend와 관련된 문제를 해결합니다.<br>• Amazon Elastic Compute Cloud — Transit Gateway Connect 및 멀티캐스트 기능과 관련된 문제를 디버깅합니다.<br>• Amazon Pipes — EventBridge EventBridge 파이프와 관련된 문제를 해결합니다.<br>• Amazon 대화형 비디오 서비스 — Amazon IVS 리소스를 AWS Support 쿼리하여 고객 | 2023년 1월 10일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | 문제를 해결할 수 있도록 합니다.<br>• Amazon FSx — Amazon FSx 데이터 리포지토리의 가져오기 및 내보내기를 지원하는 도구를 개발할 수 AWS Support 있도록 합니다.<br>• Amazon GameLift — 아마존과 관련된 문제를 해결하기 위함입니다. GameLift<br>• AWS Glue– AWS Glue Data Quality와 관련된 문제를 해결합니다.<br>• Amazon Kinesis Video Streams– Kinesis Video Streams와 관련된 문제를 해결합니다.<br>• Amazon Managed Service for Prometheus – Amazon Managed Service for Prometheus와 관련된 문제를 해결합니다.<br>• Amazon Managed Streaming for Apache Kafka – Amazon MSK Connect와 관련된 문제를 해결합니다.<br>• AWS Network Manager — 네트워크 관리자와 관련된 문제를 해결합니다.<br>• Amazon Nimble Studio – Nimble Studio와 관련된 문제를 디버깅합니다. | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | • Amazon Personalize – Amazon Personalize와 관련된 문제를 디버깅합니다.<br>• Amazon Pinpoint – Amazon Pinpoint와 관련된 문제를 해결합니다.<br>• AWS HealthOmics — 와 관련된 문제를 해결합니다. HealthOmics<br>• Amazon Transcribe – Amazon Transcribe와 관련된 문제를 디버깅합니다. | |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 권한 47개가 다음 서비스에 추가되었습니다.<br>• AWS Application Migration Service — 복제 및 실행 문제를 해결합니다.<br>• AWS CloudFormation 후크 - 문제 AWS Support 해결에 도움이 되는 자동화 도구를 개발할 수 있도록 합니다.<br>• Amazon Elastic Kubernetes Service - Amazon EKS와 관련된 문제를 해결합니다.<br>• AWS IoT FleetWise - AWS IoT FleetWise 관련 문제를 해결합니다.<br>• AWS Mainframe Modernization — 메인프레임 현대화와 관련된 문제를 디버깅합니다.<br>• AWS Outposts — 전용 호스트 및 AWS Support 자산 목록을 얻는 데 도움이 됩니다.<br>• AWS Private 5G - Private 5G 관련 문제를 해결합니다.<br>• AWS Tiros - Tiros 관련 문제를 디버깅합니다. | 2022년 10월 4일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 46개의 새로운 권한이 다음 서비스에 추가되었습니다.<br>• Amazon Managed Streaming for Apache Kafka – Amazon MSK와 관련된 문제를 해결합니다.<br>• AWS DataSync — 와 관련된 DataSync 문제를 해결합니다.<br>• AWS Elastic Disaster Recovery — 복제 및 실행 문제를 해결합니다.<br>• Amazon GameSparks — 관련 문제를 GameSparks 해결합니다.<br>• AWS IoT TwinMaker — 관련 문제를 디버깅합니다. AWS IoT TwinMaker<br>• AWS Lambda — 함수 URL의 구성을 보고 문제를 해결합니다.<br>• Amazon Lookout for Equipment - Lookout for Equipment와 관련된 문제를 해결합니다.<br>• Amazon Route 53 및 Amazon Route 53 리졸버 — VPC의 DNS 확인 동작을 확인할 AWS Support 수 있는 | 2022년 8월 17일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | 리졸버 구성을 확보하기 위함입니다. | |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 다음 서비스에 새 권한이 추가되었습니다:<br>• Amazon CloudWatch Logs — CloudWatch 로그 관련 문제를 해결하는 데 도움이 됩니다.<br>• Amazon 대화형 비디오 서비스 — 기존 Amazon IVS 리소스에서 사기 또는 손상된 계정과 관련된 지원 사례를 AWS Support 확인할 수 있도록 지원합니다.<br>• Amazon Inspector - Amazon Inspector 관련 문제를 해결하는 데 사용됩니다.<br><br>Amazon과 같은 서비스에 대한 권한이 WorkLink 제거되었습니다. WorkLink 아마존은 2022년 4월 19일에 지원 중단되었습니다. | 2022년 6월 23일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 권한 25개가 다음 서비스에 추가되었습니다:<br>• AWS Amplify UI Builder — 구성 요소 및 테마 생성과 관련된 문제를 해결합니다.<br>• Amazon AppStream — 최근에 출시된 기능에 대한 리소스를 검색하여 문제를 해결합니다.<br>• AWS Backup — 백업 작업과 관련된 문제를 해결합니다.<br>• AWS CloudFormation — IAM, 확장 및 버전 관리와 관련된 문제에 대한 진단을 수행합니다.<br>• Amazon Kinesis — Kinesis와 관련된 문제를 해결합니다.<br>• AWS Transfer Family — Transfer Family와 관련된 문제를 해결합니다. | 2022년 4월 27일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 권한 54개가 다음 서비스에 추가되었습니다.<br>• Amazon Elastic Compute Cloud<br>  • 고객 및 AWS관리형 접두사 목록과 관련된 문제를 해결합니다.<br>  • Amazon VPC IP 주소 관리자(IPAM)와 관련된 문제를 해결합니다.<br>• AWS 네트워크 관리자 — 네트워크 관리자와 관련된 문제를 해결합니다.<br>• Savings Plan - 미해결된 Savings Plan 약정에 대한 메타데이터를 가져옵니다.<br>• AWS Serverless Application Repository — 지원 사례 조사 및 해결의 일환으로 대응 조치를 개선하고 지원합니다.<br>• Amazon WorkSpaces Web — 웹 서비스 관련 문제를 디버깅하고 해결합니다. WorkSpaces | 2022년 3월 14일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy-기존 정책 업데이트 | 결제, 관리 및 기술 지원과 관련된 고객 문제를 해결하는 데 도움이 되는 작업을 수행할 수 있도록 권한 74개가 다음 서비스에 추가되었습니다.<br>• AWS Application Migration Service — 애플리케이션 마이그레이션 서비스에서 에이전트 없는 복제를 지원합니다.<br>• AWS CloudFormation — IAM, 확장 및 버전 관리 관련 문제에 대한 진단을 수행합니다.<br>• Amazon CloudWatch Logs — 리소스 정책을 검증합니다.<br>• Amazon EC2 휴지통 – 휴지통 보존 규칙에 대한 메타데이터를 가져옵니다.<br>• AWS Elastic Disaster Recovery — 고객 계정의 복제 및 시작 문제를 해결합니다.<br>• Amazon FSx – Amazon FSx 스냅샷에 대한 설명을 봅니다.<br>• Amazon Lightsail – Lightsail 버킷에 대한 메타데이터 및 구성 세부 정보를 봅니다.<br>• Amazon Macie – 분류 작업, 사용자 지정 데이터 식별자, | 2022년 2월 17일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | 정규 표현식 및 검색 결과와 같은 Macie 구성을 봅니다.<br>• Amazon S3 – Amazon S3 버킷에 대한 메타데이터 및 구성을 수집합니다.<br>• AWS Storage Gateway — 고객의 자동 테이프 생성 정책에 대한 메타데이터를 보려면<br>• Elastic Load Balancing – Service Quotas 콘솔을 사용할 때 리소스 제한에 대한 설명을 봅니다.<br><br>자세한 정보는 AWSSupportServiceRolePolicy에 대한 권한 변경을 참조하세요. | |
| 변경 로그 게시 | AWS Support 관리형 정책의 변경 로그. | 2022년 2월 17일 |

AWSSupportServiceRolePolicy에 대한 권한 변경

동일한 이름의 API 작업을 AWS Support 호출할 `AWSSupportServiceRolePolicy` 수 있도록 대부분의 권한이 추가되었습니다. 그러나 일부 API 작업에는 이름이 다른 권한이 필요합니다.

다음 표에는 다른 이름의 권한이 필요한 API 작업만 나와 있습니다. 이 표에서는 2022년 2월 17일부터 시작하는 이러한 차이점에 대해 설명합니다.

| 날짜 | API 작업 이름 | 필요한 정책 권한 |
| --- | --- | --- |
| 2022년 2월 17일에 권한 추가 | `s3.GetBucketAnalyticsConfiguration` | `s3:GetAnalyticsConfiguration` |

| 날짜 | API 작업 이름 | 필요한 정책 권한 |
| --- | --- | --- |
| | s3.ListBucketAnalyticsConfiguration | |
| | s3.GetBucketNotificationConfiguration | s3:GetBucketNotification |
| | s3.GetBucketEncryption | s3:GetEncryptionConfiguration |
| | s3.GetBucketIntelligentTieringConfiguration<br><br>s3.ListBucketIntelligentTieringConfiguration | s3:GetIntelligentTieringConfiguration |
| | s3.GetBucketInventoryConfiguration<br><br>s3.ListBucketInventoryConfiguration | s3:GetInventoryConfiguration |
| | s3.GetBucketLifecycleConfiguration | s3:GetLifecycleConfiguration |
| | s3.GetBucketMetricsConfiguration<br><br>s3.ListBucketMetricsConfiguration | s3:GetMetricsConfiguration |
| | s3.GetBucketReplication | s3:GetReplicationConfiguration |
| | s3.HeadBucket | s3:ListBucket |
| | s3.ListObjects | |

| 날짜 | API 작업 이름 | 필요한 정책 권한 |
| --- | --- | --- |
| | s3.ListBuckets | s3:ListAllMyBuckets |
| | s3.ListMultipartUploads | s3:ListBucketMultipartUploads |
| | s3.ListObjectVersions | s3:ListBucketVersions |
| | s3.ListParts | s3:ListMultipartUploadParts |

## AWS Slack의 AWS Support 앱에 대한 관리형 정책

> **Note**
>
> 의 지원 사례를 액세스하고 AWS Support Center Console보려면 을 참조하십시오AWS Support 센터 액세스 관리.

AWS Support 앱에는 다음과 같은 관리형 정책이 있습니다.

목차


- AWS 관리형 정책: AWSSupportAppFullAccess
- AWS 관리형 정책: AWSSupportAppReadOnlyAccess
- AWS SupportAWS 관리형 정책에 대한 앱 업데이트


### AWS 관리형 정책: AWSSupportAppFullAccess

AWSSupportAppFullAccess 관리형 정책을 사용하여 IAM 역할에 Slack 채널 구성에 대한 권한을 부여할 수 있습니다. AWSSupportAppFullAccess 정책을 IAM 엔터티에 연결할 수도 있습니다.

자세한 정보는 AWS Support 슬랙의 앱을 참조하세요.

이 정책은 엔티티가 앱에 대한 Service Quotas 및 IAM 작업을 수행할 AWS Support수 있는 권한을 부여합니다. AWS Support

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `servicequotas` - 기존 Service Quotas 및 요청을 설명하고 계정에 대한 서비스 할당량 증가를 생성합니다.
- `support` - 지원 사례를 생성, 업데이트 및 해결합니다. 파일 첨부, 서신, 심각도 수준 등 사례에 대한 정보를 업데이트하고 설명합니다. 지원 에이전트와 실시간 채팅 세션을 시작합니다.
- `iam` - Service Quotas에 대한 서비스 연결 역할을 생성합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
```

```
            }
        }
    ]
}
```

자세한 정보는 AWS Support 앱에 대한 액세스 관리을 참조하세요.

AWS 관리형 정책: AWSSupportAppReadOnlyAccess

AWSSupportAppReadOnlyAccess정책은 엔티티가 읽기 전용 AWS Support 앱 작업을 수행할 수 있는 권한을 부여합니다. 자세한 정보는 AWS Support 슬랙의 앱을 참조하세요.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `support` - 지원 사례에 추가된 지원 사례 세부 정보 및 커뮤니케이션에 대해 설명합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeCases",
                "support:DescribeCommunications"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS SupportAWS 관리형 정책에 대한 앱 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 AWS Support 앱에 대한 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하세요. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 문서 기록 페이지에서 RSS 피드를 구독하십시오.

다음 표에는 2022년 8월 17일 이후 AWS Support 앱 관리형 정책의 중요 업데이트가 설명되어 있습니다.

AWS Support 앱

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportAppFullAccess그리고 AWSSupportAppReadOnlyAccess<br><br>AWS Support 앱을 위한 새로운 AWS 관리형 정책 | Slack 채널 구성에 대해 구성한 IAM 역할에 이러한 정책을 사용할 수 있습니다.<br><br>자세한 정보는 AWS Support 앱에 대한 액세스 관리을 참조하세요. | 2022년 8월 19일 |
| 변경 로그 게시 | AWS Support 앱 관리 정책의 변경 로그. | 2022년 8월 19일 |

## AWS 관리형 정책: AWS Trusted Advisor

Trusted Advisor 에는 다음과 같은 AWS 관리형 정책이 있습니다.

목차


- AWS 관리형 정책: AWSTrustedAdvisorPriorityFullAccess
- AWS 관리형 정책: AWSTrustedAdvisorPriorityReadOnlyAccess
- AWS 관리형 정책: AWSTrustedAdvisorServiceRolePolicy
- AWS 관리형 정책: AWSTrustedAdvisorReportingServiceRolePolicy
- AWS 관리형 정책으로Trusted Advisor 업데이트


### AWS 관리형 정책: AWSTrustedAdvisorPriorityFullAccess

이 AWSTrustedAdvisorPriorityFullAccess정책은 Trusted Advisor Priority에 대한 전체 액세스 권한을 부여합니다. 또한 이 정책을 통해 사용자는 신뢰할 수 있는 Trusted Advisor 서비스로 AWS Organizations 추가하고 Trusted Advisor Priority에 위임된 관리자 계정을 지정할 수 있습니다.

권한 세부 정보

첫 번째 문의 정책에 `trustedadvisor`에 대한 다음 권한이 포함되어 있습니다.

- 계정 및 조직에 대해 설명합니다.
- Trusted Advisor Priority에서 식별된 위험에 대해 설명합니다. 권한을 활용하여 위험 상태를 다운로드하고 업데이트할 수 있습니다.
- Trusted Advisor Priority 이메일 알림의 구성을 설명합니다. 권한을 활용하여 이메일 알림을 구성하고 위임된 관리자의 이메일 알림을 비활성화할 수 있습니다.
- 계정에서 활성화할 수 Trusted Advisor 있도록 설정합니다 AWS Organizations.

두 번째 문의 정책에 `organizations`에 대한 다음 권한이 포함되어 있습니다.

- Trusted Advisor 계정 및 조직에 대해 설명합니다.
- AWS 서비스 Organizations를 사용하도록 설정한 항목을 나열합니다.

세 번째 문의 정책에 `organizations`에 대한 다음 권한이 포함되어 있습니다.

- Trusted Advisor 우선순위에 대해 위임된 관리자를 나열합니다.
- Organizations와 상호 신뢰할 수 있는 액세스를 활성화 및 비활성화합니다.

네 번째 문의 정책에 `iam`에 대한 다음 권한이 포함되어 있습니다.

- `AWSServiceRoleForTrustedAdvisorReporting` 서비스 연결 역할을 생성합니다.

다섯 번째 문의 정책에 `organizations`에 대한 다음 권한이 포함되어 있습니다.

- Trusted Advisor Priority에 대해 위임된 관리자를 등록 및 등록 취소할 수 있습니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityFullAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:UpdateRiskStatus",
```

```
    "trustedadvisor:DescribeNotificationConfigurations",
    "trustedadvisor:UpdateNotificationConfigurations",
    "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
    "trustedadvisor:SetOrganizationAccess"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AllowCreateServiceLinkedRole",
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
   "Condition": {
    "StringLike": {
     "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
    }
```

```
    }
   },
   {
    "Sid": "AllowRegisterDelegatedAdministrators",
    "Effect": "Allow",
    "Action": [
     "organizations:RegisterDelegatedAdministrator",
     "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource": "arn:aws:organizations::*:*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "reporting.trustedadvisor.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

AWS 관리형 정책: AWSTrustedAdvisorPriorityReadOnlyAccess

이 AWSTrustedAdvisorPriorityReadOnlyAccess정책은 위임된 관리자 계정을 볼 수 있는 권한을 포함하여 Trusted Advisor Priority에 읽기 전용 권한을 부여합니다.

권한 세부 정보

첫 번째 문의 정책에 `trustedadvisor`에 대한 다음 권한이 포함되어 있습니다.

- Trusted Advisor 계정 및 조직에 대해 설명합니다.
- Trusted Advisor Priority에서 식별된 위험을 설명하고 다운로드할 수 있습니다.
- Trusted Advisor Priority 이메일 알림의 구성을 설명합니다.

두 번째 및 세 번째 문의 정책에 `organizations`에 대한 다음 권한이 포함되어 있습니다.

- Organizations를 사용하여 조직을 설명합니다.
- AWS 서비스 Organizations를 사용하도록 설정한 항목을 나열합니다.
- 우선 순위에 대해 위임된 관리자를 나열합니다 Trusted Advisor .

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityReadOnlyAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:DescribeNotificationConfigurations"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

## AWS 관리형 정책: AWSTrustedAdvisorServiceRolePolicy

이 정책은 `AWSServiceRoleForTrustedAdvisor` 서비스 역할에 연결됩니다. 이 정책을 사용하면 서비스 연결 역할이 사용자를 대신하여 작업을 수행할 수 있습니다. AWSTrustedAdvisorServiceRolePolicy를 AWS Identity and Access Management (IAM) 엔터티에 연결할 수 없습니다. 자세한 정보는 Trusted Advisor의 서비스 링크 역할 사용을 참조하세요.

이 정책은 서비스 연결 역할이 AWS 서비스에 액세스할 수 있도록 하는 관리 권한을 부여합니다. 이러한 권한을 통해 검사를 Trusted Advisor 통해 계정을 평가할 수 있습니다.

### 권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `accessanalyzer`— AWS Identity and Access Management Access Analyzer 리소스에 대해 설명합니다.
- `Auto Scaling` - Amazon EC2 Auto Scaling 계정 할당량 및 리소스에 관해 설명합니다
- `cloudformation`— AWS CloudFormation (CloudFormation) 계정 할당량 및 스택에 대해 설명합니다.
- `cloudfront`— Amazon CloudFront 배포판에 대해 설명합니다.
- `cloudtrail`— AWS CloudTrail (CloudTrail) 트레일에 대해 설명합니다.
- `dynamodb` - Amazon DynamoDB 계정 할당량 및 리소스에 관해 설명합니다
- `dynamodbaccelerator`— DynamoDB 액셀러레이터 리소스에 대해 설명합니다.
- `ec2` - Amazon Elastic Compute Cloud(Amazon EC2) 계정 할당량 및 리소스에 관해 설명합니다
- `elasticloadbalancing` - Elastic Load Balancing(ELB) 계정 할당량 및 리소스에 관해 설명합니다
- `iam` - 자격 증명, 암호 정책 및 인증서와 같은 IAM 리소스를 가져옵니다
- `networkfirewall`— 리소스에 대해 설명합니다. AWS Network Firewall
- `kinesis` - Amazon Kinesis(Kinesis) 계정 할당량에 관해 설명합니다
- `rds` – Amazon Relational Database Service(Amazon RDS) 리소스에 관해 설명합니다
- `redshift` - Amazon Redshift 리소스에 관해 설명합니다
- `route53` - Amazon Route 53 계정 할당량 및 리소스에 관해 설명합니다

- `s3` - Amazon Simple Storage Service(Amazon S3) 리소스에 관해 설명합니다
- `ses` – Amazon Simple Email Service(Amazon SES) 전송 할당량을 가져옵니다
- `sqs` – Amazon Simple Queue Service(Amazon SQS) 대기열을 목록으로 만듭니다
- `cloudwatch`— Amazon CloudWatch 이벤트 (CloudWatch 이벤트) 지표 통계를 가져옵니다.
- `ce` - Cost Explorer 서비스(Cost Explorer) 권장 사항을 가져옵니다
- `route53resolver`— Amazon Route 53 Resolver 리졸버 엔드포인트 및 리소스를 가져옵니다.
- `kafka` - Amazon Managed Streaming for Apache Kafka 리소스 확보
- `ecs`— Amazon ECS 리소스를 가져옵니다.
- `outposts`— 리소스 확보 AWS Outposts

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "access-analyzer:ListAnalyzers"
                "autoscaling:DescribeAccountLimits",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetTrail",
                "cloudtrail:ListTrails",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "dax:DescribeClusters",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
```

```
                "ec2:DescribeReservedInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeNatGateways",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:GetManagedPrefixListEntries",
                "ecs:DescribeTaskDefinition",
                "ecs:ListTaskDefinitions"
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "iam:ListSAMLProviders",
                "kinesis:DescribeLimits",
                "kafka:DescribeClusterV2",
                "kafka:ListClustersV2",
                "kafka:ListNodes",
                "network-firewall:ListFirewalls",
                "network-firewall:DescribeFirewall",
                "outposts:GetOutpost",
                "outposts:ListAssets",
                "outposts:ListOutposts",
```

```
                "rds:DescribeAccountAttributes",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroupOptions",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribeReservedDBInstances",
                "rds:DescribeReservedDBInstancesOfferings",
                "rds:ListTagsForResource",
                "redshift:DescribeClusters",
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "route53:GetAccountLimit",
                "route53:GetHealthCheck",
                "route53:GetHostedZone",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "ses:GetSendQuota",
                "sqs:GetQueueAttributes",
                "sqs:ListQueues"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AWSTrustedAdvisorReportingServiceRolePolicy

이 정책은 조직 보기 기능에 대한 작업을 수행할 수 Trusted Advisor 있는 `AWSServiceRoleForTrustedAdvisorReporting` 서비스 연결 역할에 연결됩니다. AWSTrustedAdvisorReportingServiceRolePolicy를 IAM 엔터티에 연결할 수 없습니다. 자세한 정보는 Trusted Advisor의 서비스 링크 역할 사용을 참조하세요.

이 정책은 서비스 연결 역할이 작업을 수행할 수 있도록 허용하는 관리 권한을 부여합니다. AWS Organizations

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `organizations` – 조직을 설명하고 서비스 액세스, 계정, 상위, 하위 및 조직 단위를 나열합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책으로Trusted Advisor 업데이트

해당 서비스가 이러한 변경 사항을 추적하기 시작한 Trusted Advisor 이후 AWS Support 및 AWS 관리형 정책에 대한 업데이트에 대한 세부 정보를 확인하세요. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 문서 기록 페이지에서 RSS 피드를 구독하십시오.

다음 표에는 2021년 8월 10일 이후 Trusted Advisor 관리형 정책에 대한 중요 업데이트가 설명되어 있습니다.

Trusted Advisor

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSTrustedAdvisorServiceRolePolicy<br><br>기존 정책 업데이트. | Trusted Advisor `access-analyzer:ListAnalyzers` `,,,,,, cloudwatch:ListMetrics` `dax:DescribeClusters` `, ec2:DescribeNatGateways` `ec2:DescribeRouteTables` `ec2:DescribeVpcEndpoints` `ec2:GetManagedPrefixListEntries` `elasticloadbalancing:DescribeTargetHealth` `iam:ListSAMLProviders` `, kafka:DescribeClus` | 2024년 6월 11일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| | terV2 network-firewall:ListFirewalls network-firewall:DescribeFirewall 및 sqs:GetQueueAttributes 권한을 부여하는 새 작업을 추가했습니다. | |
| AWSTrustedAdvisorServiceRolePolicy<br><br>기존 정책 업데이트. | Trusted Advisor cloudtrail:GetTrail cloudtrail:ListTrails cloudtrail:GetEventSelectors outposts:GetOutpost , outposts:ListAssets 및 outposts:ListOutposts 권한을 부여하는 새 작업을 추가했습니다. | 2024년 1월 18일 |
| AWSTrustedAdvisorPriorityFullAccess<br><br>기존 정책 업데이트. | Trusted Advisor 명령문 ID를 포함하도록 AWSTrustedAdvisorPriorityFullAccess AWS 관리형 정책을 업데이트했습니다. | 2023년 12월 6일 |
| AWSTrustedAdvisorPriorityReadOnlyAccess<br><br>기존 정책 업데이트. | Trusted Advisor 명령문 ID를 포함하도록 AWSTrustedAdvisorPriorityReadOnlyAccess AWS 관리형 정책을 업데이트했습니다. | 2023년 12월 6일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSTrustedAdvisorServiceRolePolicy-기존 정책 업데이트 | Trusted Advisor `ec2:DescribeRegions` `s3:GetLifecycleConfiguration` `ecs:DescribeTaskDefinition` 및 `ecs:ListTaskDefinitions` 권한을 부여하는 새 작업을 추가했습니다. | 2023년 11월 9일 |
| AWSTrustedAdvisorServiceRolePolicy-기존 정책 업데이트 | Trusted Advisor 새 복원력 검사를 `kafka:ListNodes` 온보딩하기 위해 새 IAM 작업 `route53resolver:ListResolverEndpoints` `route53resolver:ListResolverEndpointIpAddresses` `ec2:DescribeSubnets` ,,, `kafka:ListClustersV2` 를 추가했습니다. | 2023년 9월 14일 |
| AWSTrustedAdvisorReportingServiceRolePolicy<br><br>서비스 연결 역할에 연결된 관리형 정책의 V2 Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` | Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` 서비스 연결 역할의 AWS 관리형 정책을 V2로 업그레이드하세요. V2에는 IAM 작업 `organizations:ListDelegatedAdministrators` 이(가) 하나 더 추가됩니다. | 2023년 2월 28일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSTrustedAdvisorPriorityFullAccess 및 AWSTrustedAdvisorPriorityReadOnlyAccess<br><br>에 대한 새로운 AWS 관리형 정책 Trusted Advisor | Trusted Advisor Trusted Advisor Priority에 대한 액세스를 제어하는 데 사용할 수 있는 두 개의 새로운 관리형 정책이 추가되었습니다. | 2022년 8월 17일 |
| AWSTrustedAdvisorServiceRolePolicy-기존 정책 업데이트 | Trusted Advisor `DescribeTargetGroups` 및 `GetAccountPublicAccessBlock` 권한을 부여하는 새 작업을 추가했습니다.<br><br>`DescribeTargetGroup` 권한은 Auto Scaling 그룹 상태 확인이 Auto Scaling 그룹에 연결된 비클래식 로드 밸런서를 검색하는 데 필요합니다.<br><br>`GetAccountPublicAccessBlock` 권한은 Amazon S3 버킷 권한 검사가 AWS 계정에 대한 퍼블릭 액세스 차단 설정을 검색하는 데 필요합니다. | 2021년 8월 10일 |
| 변경 로그 게시 | Trusted Advisor AWS 관리형 정책의 변경 사항 추적을 시작했습니다. | 2021년 8월 10일 |

## AWSAWS Support 플랜의 관리형 정책

AWS Support 플랜에는 다음과 같은 관리형 정책이 있습니다.

목차

- AWS 관리형 정책: AWSSupportPlansFullAccess
- AWS 관리형 정책: AWSSupportPlansReadOnlyAccess
- AWS Support 계획, AWS 관리형 정책 업데이트

AWS 관리형 정책: AWSSupportPlansFullAccess

AWS Support 플랜은 AWSSupportPlansFullAccess AWS 관리형 정책을 사용합니다. IAM 엔터티는 이 정책을 사용하여 다음 Support 플랜 작업을 완료합니다.

- 다음 지원 플랜을 확인하세요. AWS 계정
- 지원 플랜 변경 요청 상태에 대한 세부 정보 보기
- 다음 지원 플랜을 변경하세요. AWS 계정
- 다음을 위한 지원 계획 일정을 만드세요. AWS 계정

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule"
            ],
            "Resource": "*"
        }
    ]
}
```

정책 변경 사항 목록은 AWS Support 계획, AWS 관리형 정책 업데이트 단원을 참조하세요.

AWS 관리형 정책: AWSSupportPlansReadOnlyAccess

AWS Support 플랜은 AWSSupportPlansReadOnlyAccess AWS 관리형 정책을 사용합니다. IAM 엔터티는 이 정책을 사용하여 다음 읽기 전용 Support 플랜 작업을 완료합니다.

- 다음 지원 플랜을 확인하세요. AWS 계정

- 지원 플랜 변경 요청 상태에 대한 세부 정보 보기

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

정책 변경 사항 목록은 AWS Support 계획, AWS 관리형 정책 업데이트 단원을 참조하세요.

AWS Support 계획, AWS 관리형 정책 업데이트

Support Plans에서 이러한 변경 사항을 추적하기 시작한 이후 Support Plan의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 문서 기록 페이지에서 RSS 피드를 구독하십시오.

다음 표에서는 2022년 9월 29일부터의 Support Plans 관리형 정책에 대한 중요 업데이트에 대해 설명합니다.

AWS Support

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSSupportPlansFullAccess - 기존 정책에 대한 업데이트 | `AWSSupportPlansFullAccess` 관리형 정책에 `CreateSupportPlanSchedule` 조치를 추가합니다. | 2023년 5월 8일 |
| 변경 로그 게시 | Support Plans 관리형 정책에 대한 변경 로그. | 2022년 9월 29일 |

# AWS Support 센터 액세스 관리

지원 센터에 액세스하고 지원 사례를 생성할 수 있는 권한이 있어야 합니다.

다음 옵션 중 하나를 사용하여 지원 센터에 액세스할 수 있습니다.

- AWS 계정과 연결된 이메일 주소와 비밀번호를 사용하세요. 이 ID를 AWS 계정 루트 사용자라고 합니다.
- 사용 AWS Identity and Access Management (IAM).

비즈니스, 엔터프라이즈 온램프 또는 Enterprise Support 플랜을 사용하는 경우 AWS Support API를 사용하여 프로그래밍 방식으로 AWS Support 액세스하고 Trusted Advisor 운영할 수도 있습니다. 자세한 내용은 AWS Support API 참조를 참조하세요.

> **Note**
>
> 지원 센터에 로그인할 수 없는 경우 문의처페이지를 대신 사용할 수 있습니다. 이 페이지에서 결제 및 계정 문제에 대하여 도움받을 수 있습니다.

## AWS 계정

AWS 계정 이메일 주소와 암호를 사용하여 Support Center에 로그인하고 액세스할 수 있습니다. AWS Management Console 이 ID를 AWS 계정 루트 사용자라고 합니다. 그러나 일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 않는 것이 좋습니다. 대신 IAM을 사용하는 것이 좋은데, 이를 통해 계정에서 특정 작업을 수행할 수 있는 사용자를 제어할 수 있습니다.

## AWS 지원 조치

콘솔에서 다음 AWS Support 작업을 수행할 수 있습니다. IAM 정책에서 이러한 AWS Support 작업을 지정하여 특정 작업을 허용하거나 거부할 수도 있습니다.

> **Note**
>
> IAM 정책에서 아래 조치 중 하나라도 거부하면 지원 사례를 생성하거나 지원 사례와 상호 작용할 때 지원 센터에서 의도하지 않은 동작이 발생할 수 있습니다.

| 작업 | 설명 |
| --- | --- |
| DescribeSupportLevel | AWS 계정 식별자에 대한 지원 수준을 반환하는 권한을 부여합니다. 이 정보는 AWS Support 센터 내부적으로 지원 수준을 파악하는 데 사용됩니다. |
| InitiateCallForCase | Center에서 AWS Support 통화를 시작할 수 있는 권한을 부여합니다. 이는 AWS Support 센터 내부적으로 사용자를 대신하여 통화를 시작하는 데 사용됩니다. |
| InitiateChatForCase | AWS Support 센터에서 채팅을 시작하는 권한을 부여합니다. 이는 AWS Support 센터 내부적으로 사용자를 대신하여 채팅을 시작하는 데 사용됩니다. |
| RateCaseCommunication | AWS Support 케이스 커뮤니케이션에 등급을 매길 권한을 부여합니다. |
| DescribeCaseAttributes | 보조 서비스에  AWS Support 사례 속성을 읽을 수 있는 권한을 부여합니다. 이는 AWS Support 센터 내부적으로 케이스에 태그가 지정된 속성을 가져오는 데 사용됩니다. |
| DescribeIssueTypes | AWS Support  사례에 대한 문제 유형을 반환하는 권한을 부여합니다. 이는 AWS Support 센터 내부적으로 사용자 계정에 사용할 수 있는 문제 유형을 가져오는 데 사용됩니다. |
| SearchForCases | 입력한 내용과 일치하는 AWS Support 사례 목록을 반환할 권한을 부여합니다. 이 정보는 AWS Support 센터 내부적으로 검색된 사례를 찾는 데 사용됩니다. |
| PutCaseAttributes | 보조 서비스가 AWS Support 케이스에 속성을 첨부할 수 있는 권한을 부여합니다. 이는 AWS |

| 작업 | 설명 |
| --- | --- |
| | Support 센터 내부적으로 AWS Support 케이스에 운영 태그를 추가하는 데 사용됩니다. |

## IAM

기본적으로 IAM 사용자는 지원 센터에 액세스할 수 없습니다. IAM을 사용하여 개별 사용자 또는 그룹을 생성할 수 있습니다. 그런 다음 이러한 개체에 IAM 정책을 연결하여 해당 개체가 Support Center 사례를 열고 AWS Support API를 사용하는 등의 작업을 수행하고 리소스에 액세스할 수 있는 권한을 갖도록 합니다.

IAM 사용자를 생성하면 해당 사용자에게 개별 암호와 계정별 로그인 페이지를 제공할 수 있습니다. 그러면 담당자가 사용자 AWS 계정에 로그인하여 Support Center에서 작업할 수 있습니다. AWS Support 액세스 권한이 있는 IAM 사용자는 계정에 대해 생성된 모든 사례를 볼 수 있습니다.

자세한 내용은 IAM 사용 설명서의 IAM AWS Management Console 사용자로 로그인을 참조하십시오.

권한을 부여하는 가장 쉬운 방법은 AWS 관리형 정책을 AWSSupportAccess사용자, 그룹 또는 역할에 연결하는 것입니다. AWS Support 작업 수준 권한을 통해 특정 AWS Support 작업에 대한 액세스를 제어할 수 있습니다. AWS Support 리소스 수준 액세스를 제공하지 않으므로 `Resource` 요소는 항상 로 설정됩니다. * 특정 지원 사례에 대한 액세스를 허용하거나 거부할 수 없습니다.

Example : 모든 작업에 대한 액세스 허용 AWS Support

AWS 관리형 정책은 IAM 사용자에게 액세스 권한을 AWSSupportAccess AWS Support부여합니다. 이 정책을 사용하는 IAM 사용자는 모든 AWS Support 작업과 리소스에 액세스할 수 있습니다.

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

AWSSupportAccess 정책을 엔터티에 연결하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 자격 증명 권한 추가(콘솔)를 참조하세요.

Example : 작업을 제외한 모든 작업에 대한 액세스를 허용합니다. ResolveCase

또한 IAM의 고객 관리형 정책을 생성하여 허용 또는 거부할 작업을 지정할 수 있습니다. 다음 정책 설명문은 IAM 사용자가 사례 해결을 AWS Support 제외한 모든 작업을 수행할 수 있도록 허용합니다.

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "support:*",
      "Resource": "*"
   },
   {
       "Effect": "Deny",
       "Action": "support:ResolveCase",
       "Resource": "*"
    }]
}
```

고객 관리형 IAM 정책을 생성하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 정책 생성(콘솔)단원을 참조하세요.

사용자 또는 그룹에 이미 정책이 있는 경우 해당 정책에 AWS Support특정 정책 설명을 추가할 수 있습니다.

**Important**

- 지원 센터에서 사례를 볼 수 없는 경우 필요한 권한이 있는지 확인합니다. IAM 관리자에게 문의해야 할 수도 있습니다. 자세한 정보는 ID 및 액세스 관리 대상 AWS Support을 참조하세요.

## 액세스 대상 AWS Trusted Advisor

AWS Management Console에서는 별도의 trustedadvisor IAM 네임스페이스가 액세스를 제어합니다. Trusted Advisor AWS Support API에서 support IAM 네임스페이스는 에 대한 액세스를 제어합니다. Trusted Advisor자세한 정보는 액세스 관리: AWS Trusted Advisor을 참조하세요.

# 플랜에 대한 액세스 관리 AWS Support

주제


- Support 플랜 콘솔에 대한 권한
- Support 플랜 작업
- Support 플랜에 대한 예제 IAM 정책
- 문제 해결


## Support 플랜 콘솔에 대한 권한

Support Plans 콘솔에 액세스하려면 사용자에게 최소 권한 집합이 있어야 합니다. 이러한 권한은 사용자가 AWS 계정에서 Support Plans 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다.

`supportplans`네임스페이스로 AWS Identity and Access Management (IAM) 정책을 생성할 수 있습니다. 이 정책을 사용하여 작업 및 리소스에 대한 권한을 지정할 수 있습니다.

정책을 생성할 때 서비스의 네임스페이스를 지정하여 작업을 허용하거나 거부할 수 있습니다. Support 플랜의 네임스페이스는 `supportplans`입니다.

AWS 관리형 정책을 사용하고 이를 IAM 개체에 연결할 수 있습니다. 자세한 정보는 AWSAWS Support 플랜의 관리형 정책을 참조하세요.

## Support 플랜 작업

콘솔에서 다음 Support Plans 작업을 수행할 수 있습니다. IAM 정책에 이러한 Support Plans 작업을 지정하여 특정 작업을 허용하거나 거부할 수도 있습니다.

| 작업 | 설명 |
| --- | --- |
| `GetSupportPlan` | 이 AWS 계정에 대한 현재 지원 플랜에 대한 자세한 정보를 확인할 권한을 부여합니다. |
| `GetSupportPlanUpdateStatus` | 지원 플랜 업데이트 요청에 대한 자세한 상태 정보를 확인할 권한을 부여합니다. |
| `StartSupportPlanUpdate` | 이 AWS 계정에 대한 지원 플랜 업데이트 요청을 시작할 권한을 부여합니다. |

| 작업 | 설명 |
| --- | --- |
| CreateSupportPlanSchedule | 이 AWS 계정에 대한 지원 플랜 스케줄을 생성할 수 있는 권한을 부여합니다. |

## Support 플랜에 대한 예제 IAM 정책

다음 정책 예제를 사용하면 Support Plans에 대한 액세스를 관리할 수 있습니다.

Support 플랜에 대한 모든 액세스

다음 정책은 사용자의 Support Plans에 대한 모든 액세스를 허용합니다.

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

Support 플랜에 대한 읽기 전용 액세스

다음 정책은 Support Plans에 대한 읽기 전용 액세스를 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "supportplans:Get*",
            "Resource": "*"
        }
    ]
}
```

Support 플랜에 대한 액세스 거부

다음 정책은 사용자의 Support Plans에 대한 모든 액세스를 허용하지 않습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "supportplans:*",
            "Resource": "*"
        }
    ]
}
```

## 문제 해결

다음 항목을 참조하여 Support 플랜에 대한 액세스를 관리합니다.

지원 플랜을 보거나 변경하려고 하면 Support 플랜 콘솔에 **GetSupportPlan** 권한이 누락되었다고 표시됩니다.

IAM 사용자에게는 Support 플랜 콘솔에 액세스하는 데 필요한 권한이 있어야 합니다. 누락된 권한을 포함하도록 IAM 정책을 업데이트하거나 AWSSupportPlansFullAccess 또는 AWSSupportPlansReadOnlyAccess와 같은 AWS 관리형 정책을 사용할 수 있습니다. 자세한 정보는 AWSAWS Support 플랜의 관리형 정책을 참조하세요.

IAM 정책을 업데이트할 수 있는 액세스 권한이 없는 경우 AWS 계정 관리자에게 문의하세요.

관련 정보

자세한 설명은 IAM 사용자 가이드에서 다음 주제를 참조하십시오:

- IAM 정책 시뮬레이터로 IAM 정책 테스트
- 액세스 거부 오류 메시지 문제 해결

올바른 Support 플랜 권한이 있지만 여전히 같은 오류가 발생합니다.

소속된 회원 AWS 계정 계정인 경우 서비스 제어 정책 (SCP) 을 업데이트해야 할 수 있습니다. AWS Organizations SCP는 조직의 권한을 관리하는 정책 유형입니다.

Support 플랜은 글로벌 서비스이기 때문에 AWS 리전 제한 정책으로 인해 회원 계정에서 지원 플랜을 보거나 변경하지 못할 수 있습니다. IAM 및 Support 플랜과 같은 글로벌 서비스를 조직에 허용하려면 해당 SCP의 제외 목록에 서비스를 추가해야 합니다. 즉, SCP가 지정된 서비스를 거부하더라도 조직의 계정은 이러한 서비스에 액세스할 수 있습니다. AWS 리전

Support 플랜을 예외로 추가하려면 SCP의 "NotAction" 목록에 "supportplans:*"을 입력하세요.

```
"supportplans:*",
```

SCP는 다음 정책 스니펫으로 표시될 수 있습니다.

Example : 조직 내 Support 플랜 액세스를 허용하는 SCP

```
{ "Version":  "2012-10-17",
   "Statement": [
     { "Sid":  "GRREGIONDENY",
       "Effect":  "Deny",
       "NotAction": [
         "aws-portal:*",
         "budgets:*",
         "chime:*"
         "iam:*",
         "supportplans:*",
         ....
```

멤버 계정이 있지만 SCP를 업데이트할 수 없는 경우 AWS 계정 관리자에게 문의하세요. 관리 계정은 모든 멤버 계정이 Support 플랜에 액세스할 수 있도록 SCP를 업데이트해야 할 수 있습니다.

에 대한 참고 사항 AWS Control Tower

- 조직에서 SCP를 사용하는 경우 요청된 AWS 리전제어 (일반적으로 지역 거부 제어라고 함)를 AWS 기반으로 액세스 거부를 업데이트할 수 있습니다. AWS Control Tower
- AWS Control Tower 허용하도록 SCP를 업데이트한 경우supportplans, 드리프트를 복구하면 SCP에 대한 업데이트가 제거됩니다. 자세한 내용은 드리프트 인 감지 및 해결을 참조하십시오. AWS Control Tower

관련 정보

자세한 정보는 다음 주제를 참조하세요.

- AWS Organizations 사용 설명서의 서비스 제어 정책(SCP)
- AWS Control Tower 사용 설명서의 리전 거부 제어 구성
- 사용 설명서의 요청에 AWSAWS 리전따라 액세스를 거부하십시오AWS Control Tower .

## 액세스 관리: AWS Trusted Advisor

AWS Trusted Advisor 에서 액세스할 수 있습니다. AWS Management Console모든 AWS 계정 사용자가 엄선된 핵심 Trusted Advisor 검사를 이용할 수 있습니다. Business, Enterprise On-Ramp 또는 Enterprise Support 플랜을 보유한 경우, 모든 검사에 액세스할 수 있습니다. 더 자세한 정보는 AWS Trusted Advisor 참조 확인 단원을 참조하세요.

AWS Identity and Access Management (IAM) 을 사용하여 액세스를 Trusted Advisor제어할 수 있습니다.

주제

- Trusted Advisor 콘솔에 대한 권한
- Trusted Advisor 액션
- IAM 정책 예시
- 다음 사항도 참조하세요.

### Trusted Advisor 콘솔에 대한 권한

Trusted Advisor 콘솔에 액세스하려면 사용자에게 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 사용자는 내 Trusted Advisor 리소스의 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다.

다음 옵션을 사용하여 Trusted Advisor에 대한 액세스를 제어할 수 있습니다.

- Trusted Advisor 콘솔의 태그 필터 기능을 사용하십시오. 사용자 또는 역할에 태그와 연결된 권한이 있어야 합니다.

  AWS 관리형 정책 또는 사용자 지정 정책을 사용하여 태그별로 권한을 할당할 수 있습니다. 자세한 내용은 태그를 사용하여 IAM 사용자 및 역할에 대한 액세스 제어를 참조하세요.
- `trustedadvisor` 네임스페이스를 사용하여 IAM 정책을 생성합니다. 이 정책을 사용하여 작업 및 리소스에 대한 권한을 지정할 수 있습니다.

정책을 생성할 때 서비스의 네임스페이스를 지정하여 작업을 허용하거나 거부할 수 있습니다. 의 네임스페이스는 입니다. Trusted Advisor `trustedadvisor` 하지만 `trustedadvisor` 네임스페이스를 사용하여 API에서 Trusted Advisor API 작업을 허용하거나 거부할 수는 없습니다. AWS Support 대신 AWS Support 에 대해 `support` 네임스페이스를 사용해야 합니다.

> **Note**
>
> AWS SupportAPI에 대한 권한이 있는 경우 의 Trusted Advisor 위젯에 결과의 요약 보기가 AWS Management Console 표시됩니다. Trusted Advisor Trusted Advisor 콘솔에서 결과를 보려면 `trustedadvisor` 네임스페이스에 대한 권한이 있어야 합니다.

## Trusted Advisor 액션

콘솔에서 다음 Trusted Advisor 작업을 수행할 수 있습니다. IAM 정책에서 이러한 Trusted Advisor 작업을 지정하여 특정 작업을 허용하거나 거부할 수도 있습니다.

| 작업 | 설명 |
| --- | --- |
| `DescribeAccount` | AWS Support 계획 및 다양한 Trusted Advisor 기본 설정을 볼 수 있는 권한을 부여합니다. |
| `DescribeAccountAccess` | AWS 계정 가 활성화되었는지 비활성화되었는지 여부를 볼 수 있는 권한을 Trusted Advisor부여합니다. |
| `DescribeCheckItems` | 검사 항목에 대한 세부 정보를 볼 수 있는 권한을 부여합니다. |
| `DescribeCheckRefreshStatuses` | Trusted Advisor 검사에 대한 새로 고침 상태를 볼 수 있는 권한을 부여합니다. |
| `DescribeCheckSummaries` | Trusted Advisor 검사 요약을 볼 수 있는 권한을 부여합니다. |
| `DescribeChecks` | Trusted Advisor 검사 세부 정보를 볼 수 있는 권한을 부여합니다. |

| 작업 | 설명 |
| --- | --- |
| DescribeNotificationPreferences | AWS 계정에 대한 알림 기본 설정을 볼 수 있는 권한을 부여합니다. |
| ExcludeCheckItems | Trusted Advisor 검사에 대한 권장 사항을 제외할 수 있는 권한을 부여합니다. |
| IncludeCheckItems | Trusted Advisor 검사에 대한 권장 사항을 포함시킬 수 있는 권한을 부여합니다. |
| RefreshCheck | Trusted Advisor 수표를 새로 고칠 수 있는 권한을 부여합니다. |
| SetAccountAccess | 계정을 활성화하거나 Trusted Advisor 비활성화할 수 있는 권한을 부여합니다. |
| UpdateNotificationPreferences | Trusted Advisor에 대한 알림 기본 설정을 업데이트할 수 있는 권한을 부여합니다. |
| DescribeCheckStatusHistoryChanges | 지난 30일 동안에 나타난 검사 결과 및 변경된 상태를 확인할 수 있는 권한을 부여합니다. |

Trusted Advisor 조직 보기를 위한 조치

조직 보기 기능을 위한 Trusted Advisor 작업은 다음과 같습니다. 자세한 정보는 AWS Trusted Advisor에 대한 조직 보기을 참조하세요.

| 작업 | 설명 |
| --- | --- |
| DescribeOrganization | 조직 보기 기능을 사용하기 위한 요구 사항을 AWS 계정 충족하는지 여부를 볼 수 있는 권한을 부여합니다. |
| DescribeOrganizationAccounts | 조직에 있는 연결된 AWS 계정을 볼 수 있는 권한을 부여합니다. |

| 작업 | 설명 |
| --- | --- |
| `DescribeReports` | 보고서 이름, 런타임, 생성 날짜, 상태 및 형식과 같은 조직 보기 보고서의 세부 정보를 볼 수 있는 권한을 부여합니다. |
| `DescribeServiceMetadata` | 검사 범주 AWS 리전, 검사 이름 및 자원 상태와 같은 조직 보기 보고서에 대한 정보를 볼 수 있는 권한을 부여합니다. |
| `GenerateReport` | 조직의 Trusted Advisor 점검을 위한 보고서를 만들 수 있는 권한을 부여합니다. |
| `ListAccountsForParent` | Trusted Advisor 콘솔에서 루트 또는 OU (조직 구성 단위) 에 포함된 AWS 조직의 모든 계정을 볼 수 있는 권한을 부여합니다. |
| `ListOrganizationalUnitsForParent` | Trusted Advisor 콘솔에서 상위 조직 단위 또는 루트의 모든 OU (조직 단위) 를 볼 수 있는 권한을 부여합니다. |
| `ListRoots` | Trusted Advisor 콘솔에서 AWS 조직에 정의된 모든 루트를 볼 수 있는 권한을 부여합니다. |
| `SetOrganizationAccess` | 에 대한 조직 보기 기능을 활성화할 권한을 Trusted Advisor부여합니다. |

Trusted Advisor 우선순위 조치

계정에 Trusted Advisor Priority를 활성화한 경우 콘솔에서 다음 Trusted Advisor 작업을 수행할 수 있습니다. IAM 정책에 이러한 Trusted Advisor 작업을 추가하여 특정 작업을 허용하거나 거부할 수도 있습니다. 자세한 정보는 Trusted Advisor Priority에 대한 예제 IAM 정책을 참조하세요.

> **Note**
>
> Trusted Advisor Priority에 나타나는 위험은 기술 계정 관리자 (TAM) 가 계정에 대해 확인한 권장 사항입니다. 수표와 같은 서비스의 권장 사항은 자동으로 생성됩니다. Trusted Advisor TAM

의 권장 사항은 수동으로 생성됩니다. 그런 다음 TAM이 이러한 권장 사항을 전송하여 해당 권장 사항이 계정의 Trusted Advisor 우선 순위에 표시되도록 합니다.

자세한 정보는 AWS Trusted Advisor Priority 시작하기을 참조하세요.

| 작업 | 설명 |
| --- | --- |
| `DescribeRisks` | Trusted Advisor Priority에서 위험을 볼 수 있는 권한을 부여합니다. |
| `DescribeRisk` | Trusted Advisor Priority에서 위험 세부 정보를 볼 수 있는 권한을 부여합니다. |
| `DescribeRiskResources` | Trusted Advisor Priority 내 위험으로부터 영향을 받는 리소스를 볼 수 있는 권한을 부여합니다. |
| `DownloadRisk` | Trusted Advisor Priority에서 위험에 대한 세부 정보가 포함된 파일을 다운로드할 수 있는 권한을 부여합니다. |
| `UpdateRiskStatus` | Trusted Advisor Priority 내 위험 상태를 업데이트할 수 있는 권한을 부여합니다. |
| `DescribeNotificationConfigurations` | Trusted Advisor Priority에 대한 이메일 알림 환경설정을 가져올 수 있는 권한을 부여합니다. |
| `UpdateNotificationConfigurations` | Trusted Advisor Priority에 대한 이메일 알림 기본 설정을 생성 또는 업데이트할 수 있는 권한을 부여합니다. |
| `DeleteNotificationConfigurationForDelegatedAdmin` | Trusted Advisor Priority의 위임된 관리자 계정에서 이메일 알림 기본 설정을 삭제할 수 있는 권한을 조직 관리 계정에 부여합니다. |

Trusted Advisor 조치 참여

계정에 Trusted Advisor Engage를 활성화한 경우 콘솔에서 다음 Trusted Advisor 작업을 수행할 수 있습니다. IAM 정책에 이러한 Trusted Advisor 작업을 추가하여 특정 작업을 허용하거나 거부할 수도 있습니다. 자세한 정보는 Trusted Advisor 참여에 대한 예제 IAM 정책을 참조하세요.

자세한 정보는 AWS Trusted Advisor 참여(미리 보기) 시작하기을 참조하세요.

| 작업 | 설명 |
| --- | --- |
| `CreateEngagement` | Engage에서 Trusted Advisor 인게이지먼트를 생성할 수 있는 권한을 부여합니다. |
| `CreateEngagementAttachment` | Trusted Advisor Engage에서 참여 첨부 파일을 만들 수 있는 권한을 부여합니다. |
| `CreateEngagementCommunication` | Trusted Advisor Engage에서 참여 커뮤니케이션을 만들 수 있는 권한을 부여합니다. |
| `GetEngagement` | Engage에서 Trusted Advisor 참여를 볼 수 있는 권한을 부여합니다. |
| `GetEngagementAttachment` | Engage에서 인게이지먼트 첨부 파일을 볼 수 있는 권한을 부여합니다. Trusted Advisor |
| `GetEngagementType` | Engage에서 Trusted Advisor 특정 참여 유형을 볼 수 있는 권한을 부여합니다. |
| `ListEngagementCommunications` | Trusted Advisor 참여의 참여에 대한 모든 커뮤니케이션을 볼 수 있는 권한을 부여합니다. |
| `ListEngagements` | Engage의 모든 참여를 볼 수 있는 Trusted Advisor 권한을 부여합니다. |
| `ListEngagementTypes` | Engage의 모든 참여 유형을 볼 수 있는 Trusted Advisor 권한을 부여합니다. |
| `UpdateEngagement` | Trusted Advisor Engage에서 참여 세부 정보를 업데이트할 수 있는 권한을 부여합니다. |

| 작업 | 설명 |
| --- | --- |
| `UpdateEngagementStatus` | Trusted Advisor Engage의 참여 상태를 업데이트할 수 있는 권한을 부여합니다. |

## IAM 정책 예시

다음 정책은 Trusted Advisor에 대한 액세스를 허용 및 거부하는 방법을 보여 줍니다. 다음 정책 중 하나를 사용하여 IAM 콘솔에서 고객 관리형 정책을 생성할 수 있습니다. 예를 들어 예제 정책을 복사한 다음 IAM 콘솔의 JSON 탭에 붙여넣을 수 있습니다. 그런 다음 정책을 IAM 사용자, 그룹 또는 역할에 연결할 수 있습니다.

IAM 정책을 생성하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

예제

- 전체 액세스 권한 Trusted Advisor
- Trusted Advisor에 대한 읽기 전용 액세스
- 액세스 거부: Trusted Advisor
- 특정 작업 허용 및 거부
- 에 대한 AWS Support API 작업에 대한 액세스를 제어합니다. Trusted Advisor
- Trusted Advisor Priority에 대한 예제 IAM 정책
- Trusted Advisor 참여에 대한 예제 IAM 정책

### 전체 액세스 권한 Trusted Advisor

다음 정책을 통해 사용자는 Trusted Advisor 콘솔의 모든 Trusted Advisor 검사를 보고 모든 작업을 수행할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
```

```
        }
    ]
}
```

Trusted Advisor에 대한 읽기 전용 액세스

다음 정책은 사용자에게 Trusted Advisor 콘솔에 대한 읽기 전용 액세스를 허용합니다. 사용자는 점검 새로 고침 또는 알림 기본 설정 변경과 같은 변경 작업을 수행할 수 없습니다.

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

액세스 거부: Trusted Advisor

다음 정책은 사용자가 Trusted Advisor 콘솔에서 Trusted Advisor 확인 작업을 보거나 조치를 취하는 것을 허용하지 않습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

특정 작업 허용 및 거부

다음 정책은 사용자가 Trusted Advisor 콘솔에서 모든 Trusted Advisor 검사를 볼 수 있도록 허용하지만 검사 내용을 새로 고치는 것은 허용하지 않습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:RefreshCheck",
            "Resource": "*"
        }
    ]
}
```

에 대한 AWS Support API 작업에 대한 액세스를 제어합니다. Trusted Advisor

AWS Management Console에서는 별도의 `trustedadvisor` IAM 네임스페이스가 액세스를 제어합니다. Trusted Advisor`trustedadvisor`네임스페이스를 사용하여 API에서 API 작업을 허용하거나 Trusted Advisor 거부할 수 없습니다. AWS Support 대신 `support` 네임스페이스를 사용합니다. 프로그래밍 방식으로 AWS Support 호출하려면 API에 대한 권한이 있어야 합니다. Trusted Advisor

예를 들어 RefreshTrustedAdvisorCheck작업을 호출하려면 정책에 이 작업에 대한 권한이 있어야 합니다.

Example : Trusted Advisor API 작업만 허용

다음 정책은 사용자가 AWS Support API 작업의 나머지 부분에 대한 Trusted Advisor API 작업에는 액세스할 수 있도록 허용하지만 나머지 AWS Support API 작업에는 액세스할 수 없습니다. 예를 들어 사용자는 API를 사용하여 검사를 보거나 새로 고칠 수 있습니다. AWS Support 케이스를 생성, 조회, 업데이트 또는 해결할 수 없습니다.

이 정책을 사용하여 프로그래밍 방식으로 Trusted Advisor API 작업을 호출할 수 있지만 Trusted Advisor 콘솔에서 검사를 보거나 새로 고치는 데는 이 정책을 사용할 수 없습니다.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:RefreshTrustedAdvisorCheck",
                "trustedadvisor:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeAttachment",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:ResolveCase"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM이 AWS Support 및 Trusted Advisor에서 작동하는 방식에 대한 자세한 내용은 을 참조하십시오. 작업

Trusted Advisor Priority에 대한 예제 IAM 정책

다음 AWS 관리형 정책을 사용하여 Trusted Advisor Priority에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 AWS 관리형 정책: AWS Trusted Advisor 및 AWS Trusted Advisor Priority 시작하기 섹션을 참조하세요.

Trusted Advisor 참여에 대한 예제 IAM 정책

> **Note**
>
> Trusted Advisor Engage는 프리뷰 릴리즈 중이며 현재 AWS 관리형 정책이 없습니다. 다음 정책 중 하나를 사용하여 IAM 콘솔에서 고객 관리형 정책을 생성할 수 있습니다.

Trusted Advisor Engage에서 읽기 및 쓰기 권한을 부여하는 정책의 예는 다음과 같습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Trusted Advisor Engage에서 읽기 전용 액세스 권한을 부여하는 정책의 예는 다음과 같습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Trusted Advisor Engage에서 읽기 및 쓰기 액세스 권한을 부여하고 신뢰할 수 있는 액세스를 활성화하는 기능을 제공하는 정책의 예는 다음과 같습니다. Trusted Advisor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:SetOrganizationAccess",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
```

```
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
                }
            }
        }
    ]
}
```

### 다음 사항도 참조하세요.

Trusted Advisor 권한에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- IAM 사용 설명서의 AWS Trusted Advisor에서 정의한 작업.
- Trusted Advisor 콘솔에 대한 액세스 제어

## AWS Trusted Advisor에 대한 예제 서비스 제어 정책

AWS Trusted Advisor SCP (서비스 제어 정책) 를 지원합니다. SCP는 조직 내 구성 요소에 연결하여 해당 조직 내의 권한을 관리하는 정책입니다. SCP는 SCP를 연결하는 요소 아래의 모든 AWS 계정에 적용됩니다. SCP는 조직의 모든 계정에 사용 가능한 최대 권한을 중앙에서 제어합니다. 이를 통해 AWS 계정이 조직의 액세스 제어 지침을 준수하도록 할 수 있습니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.

주제

- 사전 조건
- 예제 서비스 제어 정책

### 사전 조건

SCP를 사용하려면 먼저 다음 사항을 수행해야 합니다.

- 조직 내에서 모든 기능을 활성화합니다. 자세한 내용은AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하세요.
- 조직에 대해 SCP를 활성화합니다. 자세한 내용은 AWS Organizations 사용 설명서의 정책 유형 활성화 및 비활성화를 참조하세요.
- 필요한 SCP를 생성합니다. SCP를 생성하는 방법에 대한 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책 생성, 업데이트 및 삭제를 참조하세요.

## 예제 서비스 제어 정책

다음 예에서는 조직에서 리소스 공유의 다양한 측면을 제어할 수 있는 방법을 보여줍니다.

Example : 사용자가 Engage에서 참여를 만들거나 편집하지 못하도록 방지 Trusted Advisor

다음 SCP는 사용자가 새 계약을 만들거나 기존 계약을 편집하지 못하도록 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:CreateEngagement",
        "trustedadvisor:UpdateEngagement*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Example : Trusted Advisor 참여 거부 및 우선 액세스 Trusted Advisor

다음 SCP는 사용자가 Trusted Advisor Engage and Trusted Advisor Priority에서 액세스하거나 작업을 수행하는 것을 방지합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:ListEngagement*",
        "trustedadvisor:GetEngagement*",
        "trustedadvisor:CreateEngagement*",
        "trustedadvisor:UpdateEngagement*",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:UpdateRisk*",
        "trustedadvisor:DownloadRisk"
```

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

# AWS Support ID 및 액세스 문제 해결

다음 정보를 사용하면 및 IAM을 사용할 때 발생할 수 있는 일반적인 문제를 AWS Support 진단하고 해결하는 데 도움이 됩니다.

주제

- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 액세스 키를 보아야 합니다.
- 저는 관리자이며 다른 사람들이 액세스할 수 있도록 허용하고 싶습니다. AWS Support
- 내 AWS 계정 외부의 사용자가 내 리소스에 액세스할 수 있도록 허용하고 싶습니다. AWS Support

## 저는 IAM을 수행할 권한이 없습니다. PassRole

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AWS Support에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 AWS 서비스 수 있는 기능도 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 AWS Support에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우 Mary가 `iam:PassRole`작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

### 액세스 키를 보아야 합니다.

IAM 사용자 액세스 키를 생성한 후에는 언제든지 액세스 키 ID를 볼 수 있습니다. 하지만 보안 액세스 키는 다시 볼 수 없습니다. 보안 액세스 키를 잃어버린 경우 새로운 액세스 키 페어를 생성해야 합니다.

액세스 키는 액세스 키 ID(예: `AKIAIOSFODNN7EXAMPLE`)와 보안 액세스 키(예: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`)의 두 가지 부분으로 구성됩니다. 사용자 이름 및 암호와 같이 액세스 키 ID와 보안 액세스 키를 함께 사용하여 요청을 인증해야 합니다. 사용자 이름과 암호를 관리하는 것처럼 안전하게 액세스 키를 관리합니다.

> **Important**
>
> 정식 사용자 ID를 찾는 데 도움이 되더라도 액세스 키를 타사에 제공하지 마시기 바랍니다. 이렇게 하면 다른 사람에게 내 계정에 대한 영구 액세스 권한을 부여할 수 있습니다 AWS 계정.

액세스 키 페어를 생성할 때는 액세스 키 ID와 보안 액세스 키를 안전한 위치에 저장하라는 메시지가 나타납니다. 보안 액세스 키는 생성할 때만 사용할 수 있습니다. 하지만 보안 액세스 키를 잃어버린 경우 새로운 액세스 키를 IAM 사용자에게 추가해야 합니다. 최대 두 개의 액세스 키를 가질 수 있습니다. 이미 두 개가 있는 경우 새로 생성하려면 먼저 키 페어 하나를 삭제해야 합니다. 지침을 보려면 IAM 사용 설명서의 액세스 키 관리 단원을 참조하십시오.

### 저는 관리자이며 다른 사람들이 액세스할 수 있도록 허용하고 싶습니다. AWS Support

다른 사람이 액세스할 수 있도록 하려면 액세스가 AWS Support필요한 개인 또는 애플리케이션을 위한 IAM 엔티티 (사용자 또는 역할) 를 생성해야 합니다. 다른 사용자들은 해당 엔터티에 대한 보안 인증을 사용해 AWS에 액세스합니다. 그런 다음 AWS Support에 대한 올바른 권한을 부여하는 정책을 엔터티에 연결해야 합니다.

바로 시작하려면 IAM 사용 설명서의 첫 번째 IAM 위임 사용자 및 그룹 생성을 참조하십시오.

### 내 AWS 계정 외부의 사용자가 내 리소스에 액세스할 수 있도록 허용하고 싶습니다. AWS Support

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 이러한 기능의 AWS Support 지원 여부를 알아보려면 을 참조하십시오IAM의 AWS Support 작동 방식.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서에서 자신이 소유한 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 교차 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

# 사고 대응

사고 AWS Support 대응은 AWS 책임입니다. AWS 사고 대응을 관리하는 공식적이고 문서화된 정책 및 프로그램이 있습니다. 자세한 내용은 AWS 보안 사고 대응 소개 백서를 참조하십시오.

다음 옵션을 사용하여 운영 문제에 대해 알립니다.

- AWS Service Health Dashboard에서 광범위한 영향을 미치는 AWS 운영 문제를 확인하십시오. 예를 들어, 계정에 국한되지 않고 서비스 또는 리전에 영향을 주는 이벤트입니다.
- 개별 계정에 대한 운영 문제는 AWS Health Dashboard에서 볼 수 있습니다. 예를 들어, 해당 계정의 서비스 또는 리소스에 영향을 주는 이벤트입니다. 자세한 내용은 AWS Health 사용 설명서에서 AWS Health Dashboard시작하기를 참조하세요.

# 로그인 및 모니터링 AWS Support 및 AWS Trusted Advisor

모니터링은 및 기타 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 AWS Trusted Advisor 있어 중요한 부분입니다. AWS Support AWS 문제가 발생한 경우 이를 AWS Support 관찰하고 보고하고 AWS Trusted Advisor적절한 경우 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- Amazon은 실행 중인 AWS 리소스와 애플리케이션을 AWS 실시간으로 CloudWatch 모니터링합니다. 지표를 수집 및 추적하고, 맞춤 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임계값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스의 CPU 사용량 또는 기타 지표를 CloudWatch 추적

하고 필요할 때 새 인스턴스를 자동으로 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

- EventBridgeAmazon은 AWS 리소스 변경을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 제공합니다. EventBridge 특정 이벤트를 감시하고 이러한 이벤트가 발생할 경우 다른 AWS 서비스에서 자동화된 작업을 트리거하는 규칙을 작성할 수 있으므로 자동화된 이벤트 기반 컴퓨팅을 지원합니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하십시오.
- AWS CloudTrail계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon Simple Storage Service (Amazon S3) 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 전화를 걸었는지, 언제 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

자세한 내용은 AWS Support의 모니터링 및 로깅 및 AWS Trusted Advisor의 모니터링 및 로깅 단원을 참조하세요.

# 규정 준수 검증: AWS Support

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

## 의 레질리언스 AWS Support

AWS 글로벌 인프라는 AWS 지역 및 가용 영역을 중심으로 구축됩니다. AWS 지역은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이러한 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 지역 및 가용 영역에 대한 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

## 의 인프라 보안 AWS Support

관리형 서비스로서 Amazon Web Services: 보안 프로세스 개요 백서에 설명된 AWS 글로벌 네트워크 보안 절차에 따라 보호됩니다. AWS Support

AWS 게시된 API 호출을 사용하여 네트워크를 AWS Support 통해 액세스합니다. 클라이언트가 전송 계층 보안(TLS) 1.0 이상을 지원해야 합니다. TLS 1.2 이상을 권장합니다. 클라이언트는 Ephemeral

Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 PFS(전달 완전 보안, Perfect Forward Secrecy)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

# 의 구성 및 취약성 분석 AWS Support

를 위해 AWS Trusted Advisor, 게스트 운영 체제 (OS) 및 데이터베이스 패치, 방화벽 구성, 재해 복구와 같은 기본 보안 작업을 AWS 처리합니다.

구성 및 IT 제어는 고객과 고객 간의 AWS 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하십시오.

# AWS SDK AWS Support 사용을 위한 코드 예제

다음 코드 예제는 AWS 소프트웨어 개발 키트 (SDK) AWS Support 와 함께 사용하는 방법을 보여줍니다.

작업은 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 작업은 개별 서비스 함수를 호출하는 방법을 보여 주며 관련 시나리오와 교차 서비스 예시에서 컨텍스트에 맞는 작업을 볼 수 있습니다.

시나리오는 동일한 서비스 내에서 여러 함수를 호출하여 특정 태스크를 수행하는 방법을 보여주는 코드 예시입니다.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

시작하기

## 안녕하세요. AWS Support

다음 코드 예제에서는 AWS Support의 사용을 시작하는 방법을 보여 줍니다.

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있어요 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using Amazon.AWSSupport;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

public static class HelloSupport
{
    static async Task Main(string[] args)
    {
```

```
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        // You must have one of the following AWS Support plans: Business,
 Enterprise On-Ramp, or Enterprise. Otherwise, an exception will be thrown.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>()
            ).Build();

        // Now the client is available for injection.
        var supportClient =
 host.Services.GetRequiredService<IAmazonAWSSupport>();

        // You can use await and any of the async methods to get a response.
        var response = await supportClient.DescribeServicesAsync();
        Console.WriteLine($"\tHello AWS Support! There are
 {response.Services.Count} services available.");
    }
}
```

- API 세부 정보는 AWS SDK for .NET API DescribeServices참조를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> 자세한 내용은 다음과 같습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SupportException;
```

```
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following task:
 *
 * 1. Gets and displays available services.
 *
 *
 * NOTE: To see multiple operations, see SupportScenario.
 */

public class HelloSupport {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();

        System.out.println("***** Step 1. Get and display available services.");
        displayServices(supportClient);
    }

    // Return a List that contains a Service name and Category name.
    public static void displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                    .language("en")
                    .build();
```

```
            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());

                // Display the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                }
                index++;
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- API 세부 정보는 AWS SDK for Java 2.x API DescribeServices참조를 참조하십시오.

JavaScript

JavaScript (v3) 용 SDK

> **Note**
>
> 더 많은 내용이 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

`main ()`을 간접적으로 호출하여 예제를 실행합니다.

```
import {
  DescribeServicesCommand,
  SupportClient,
} from "@aws-sdk/client-support";

// Change the value of 'region' to your preferred AWS Region.
const client = new SupportClient({ region: "us-east-1" });

const getServiceCount = async () => {
  try {
    const { services } = await client.send(new DescribeServicesCommand({}));
    return services.length;
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

export const main = async () => {
  try {
    const count = await getServiceCount();
    console.log(`Hello, AWS Support! There are ${count} services available.`);
  } catch (err) {
    console.error("Failed to get service count: ", err.message);
  }
};
```

- API 세부 정보는 AWS SDK for JavaScript API DescribeServices참조를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> 자세한 내용은 다음과 같습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following task:

1. Gets and displays available services.
 */

suspend fun main() {
    displaySomeServices()
}

// Return a List that contains a Service name and Category name.
suspend fun displaySomeServices() {
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
```

```
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is: " + service.name)

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                index++
            }
        }
    }
}
```

- API 세부 정보는 Kotlin API용AWS SDK 레퍼런스를 참조하세요 DescribeServices.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 여기에서 확인할 수 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


def hello_support(support_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Support client and count
```

```
    the available services in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param support_client: A Boto3 Support Client object.
    """
    try:
        print("Hello, AWS Support! Let's count the available Support services:")
        response = support_client.describe_services()
        print(f"There are {len(response['services'])} services available.")
    except ClientError as err:
        if err.response["Error"]["Code"] == "SubscriptionRequiredException":
            logger.info(
                "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                "examples."
            )
        else:
            logger.error(
                "Couldn't count services. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


if __name__ == "__main__":
    hello_support(boto3.client("support"))
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 DescribeServices.

코드 예시

- SDK 사용을 위한 조치 AWS SupportAWS
  - AWS SDK 또는 AddAttachmentsToSet CLI와 함께 사용
  - AWS SDK 또는 AddCommunicationToCase CLI와 함께 사용
  - AWS SDK 또는 CreateCase CLI와 함께 사용

- AWS SDK 또는 DescribeAttachment CLI와 함께 사용
- AWS SDK 또는 DescribeCases CLI와 함께 사용
- AWS SDK 또는 DescribeCommunications CLI와 함께 사용
- AWS SDK 또는 DescribeServices CLI와 함께 사용
- AWS SDK 또는 DescribeSeverityLevels CLI와 함께 사용
- AWS SDK 또는 DescribeTrustedAdvisorCheckRefreshStatuses CLI와 함께 사용
- AWS SDK 또는 DescribeTrustedAdvisorCheckResult CLI와 함께 사용
- AWS SDK 또는 DescribeTrustedAdvisorCheckSummaries CLI와 함께 사용
- AWS SDK 또는 DescribeTrustedAdvisorChecks CLI와 함께 사용
- AWS SDK 또는 RefreshTrustedAdvisorCheck CLI와 함께 사용
- AWS SDK 또는 ResolveCase CLI와 함께 사용
- SDK AWS Support 사용 AWS 시나리오
  - AWS SDK를 사용하여 AWS Support 케이스를 시작하세요.

# SDK 사용을 위한 조치 AWS SupportAWS

다음 코드 예제는 AWS SDK로 개별 AWS Support 작업을 수행하는 방법을 보여줍니다. 이 발췌문은 AWS Support API를 호출하며 컨텍스트에서 실행해야 하는 대규모 프로그램에서 발췌한 코드입니다. 각 예제에는 코드 설정 및 실행 지침을 찾을 수 있는 링크가 포함되어 있습니다. GitHub

다음 예제에는 가장 일반적으로 사용되는 작업만 포함되어 있습니다. 전체 목록은 AWS Support API 참조를 참조하세요.

예제

- AWS SDK 또는 AddAttachmentsToSet CLI와 함께 사용
- AWS SDK 또는 AddCommunicationToCase CLI와 함께 사용
- AWS SDK 또는 CreateCase CLI와 함께 사용
- AWS SDK 또는 DescribeAttachment CLI와 함께 사용
- AWS SDK 또는 DescribeCases CLI와 함께 사용
- AWS SDK 또는 DescribeCommunications CLI와 함께 사용
- AWS SDK 또는 DescribeServices CLI와 함께 사용
- AWS SDK 또는 DescribeSeverityLevels CLI와 함께 사용

- AWS SDK 또는 DescribeTrustedAdvisorCheckRefreshStatuses CLI와 함께 사용
- AWS SDK 또는 DescribeTrustedAdvisorCheckResult CLI와 함께 사용
- AWS SDK 또는 DescribeTrustedAdvisorCheckSummaries CLI와 함께 사용
- AWS SDK 또는 DescribeTrustedAdvisorChecks CLI와 함께 사용
- AWS SDK 또는 RefreshTrustedAdvisorCheck CLI와 함께 사용
- AWS SDK 또는 ResolveCase CLI와 함께 사용

## AWS SDK 또는 **AddAttachmentsToSet** CLI와 함께 사용

다음 코드 예제는 AddAttachmentsToSet의 사용 방법을 보여줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 사례 시작하기

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Add an attachment to a set, or create a new attachment set if one does
not exist.
    /// </summary>
    /// <param name="data">The data for the attachment.</param>
    /// <param name="fileName">The file name for the attachment.</param>
    /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
    /// <returns>The setId of the attachment.</returns>
    public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
```

```
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }
```

- API 세부 정보는 AWS SDK for .NET API AddAttachmentsToSet참조를 참조하십시오.

## CLI

### AWS CLI

#### 세트에 첨부 파일 추가하기

다음 `add-attachments-to-set` 예시에서는 세트에 이미지를 추가한 다음 AWS 계정의 지원 사례에 대해 이 이미지를 지정할 수 있습니다.

```
aws support add-attachments-to-set \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE" \
    --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string
```

출력:

```
{
    "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE",
    "expiryTime": "2020-05-14T17:04:40.790+0000"
}
```

자세한 내용은 AWS Support 사용 설명서의 사례 관리를 참조하세요.

- API 세부 정보는 AWS CLI 명령 AddAttachmentsToSet참조를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
       try {
           File myFile = new File(fileAttachment);
           InputStream sourceStream = new FileInputStream(myFile);
           SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

           Attachment attachment = Attachment.builder()
                   .fileName(myFile.getName())
                   .data(sourceBytes)
                   .build();

           AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                   .attachments(attachment)
                   .build();

           AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
           return response.attachmentSetId();

       } catch (SupportException | FileNotFoundException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- API 세부 정보는 AWS SDK for Java 2.x API AddAttachmentsToSet참조를 참조하십시오.

JavaScript

JavaScript (v3) 용 SDK

> **Note**
>
> 더 많은 내용이 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import { AddAttachmentsToSetCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new attachment set or add attachments to an existing set.
    // Provide an 'attachmentSetId' value to add attachments to an existing set.
    // Use AddCommunicationToCase or CreateCase to associate an attachment set
 with a support case.
    const response = await client.send(
      new AddAttachmentsToSetCommand({
        // You can add up to three attachments per set. The size limit is 5 MB
 per attachment.
        attachments: [
          {
            fileName: "example.txt",
            data: new TextEncoder().encode("some example text"),
          },
        ],
      }),
    );
    // Use this ID in AddCommunicationToCase or CreateCase.
    console.log(response.attachmentSetId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API 세부 정보는 AWS SDK for JavaScript API AddAttachmentsToSet참조를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> 자세한 내용은 다음과 같습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal =
        Attachment {
            fileName = myFile.name
            data = sourceBytes
        }

    val setRequest =
        AddAttachmentsToSetRequest {
            attachments = listOf(attachmentVal)
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

- API 세부 정보는 Kotlin API용AWS SDK 레퍼런스를 참조하세요 AddAttachmentsToSet.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 여기에서 확인할 수 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
 not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
 support case.",
```

```
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 AddAttachmentsToSet.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **AddCommunicationToCase** CLI와 함께 사용

다음 코드 예제는 AddCommunicationToCase의 사용 방법을 보여줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 사례 시작하기

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }
```

- API 세부 정보는 AWS SDK for .NET API AddCommunicationToCase참조를 참조하십시오.

CLI

AWS CLI

사례에 커뮤니케이션 추가하기

다음 add-communication-to-case 예는 AWS 계정의 지원 사례에 커뮤니케이션을 추가합니다.

```
aws support add-communication-to-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --communication-body "I'm attaching a set of images to this case." \
    --cc-email-addresses "myemail@example.com" \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE"
```

출력:

```
{
    "result": true
}
```

자세한 내용은 AWS Support 사용 설명서의 사례 관리를 참조하세요.

- API 세부 정보는 AWS CLI 명령 AddCommunicationToCase참조를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
       try {
           AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
```

```
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API AddCommunicationToCase참조를 참조하십시오.

JavaScript

JavaScript (v3) 용 SDK

> **Note**
>
> 더 많은 내용이 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import { AddCommunicationToCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  let attachmentSetId;
```

```
  try {
    // Add a communication to a case.
    const response = await client.send(
      new AddCommunicationToCaseCommand({
        communicationBody: "Adding an attachment.",
        // Set value to an existing support case id.
        caseId: "CASE_ID",
        // Optional. Set value to an existing attachment set id to add
 attachments to the case.
        attachmentSetId,
      }),
    );
    console.log(response);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API 세부 정보는 AWS SDK for JavaScript API AddCommunicationToCase참조를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> 자세한 내용은 다음과 같습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
```

```
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}
```

- API 세부 정보는 Kotlin API용AWS SDK 레퍼런스를 참조하세요 AddCommunicationToCase.

PowerShell

다음을 위한 도구 PowerShell

예 1: 이메일 통신 본문을 지정된 대/소문자에 추가합니다.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

예 2: 이메일 통신 본문을 지정된 대/소문자에 추가하고 이메일의 CC 라인에 포함된 하나 이상의 이메일 주소를 추가합니다.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CcEmailAddress @("email1@address.com", "email2@address.com") -CommunicationBody
 "Some text about the case"
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조를 참조하십시오 AddCommunicationToCase.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 다음과 같습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
 support case.",
                attachmentSetId=attachment_set_id,
            )
```

```
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 AddCommunicationToCase.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **CreateCase** CLI와 함께 사용

다음 코드 예제는 CreateCase의 사용 방법을 보여줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 사례 시작하기

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Create a new support case.
    /// </summary>
    /// <param name="serviceCode">Service code for the new case.</param>
    /// <param name="categoryCode">Category for the new case.</param>
    /// <param name="severityCode">Severity code for the new case.</param>
    /// <param name="subject">Subject of the new case.</param>
    /// <param name="body">Body text of the new case.</param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
    /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
    /// <returns>The caseId of the new support case.</returns>
    public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
        string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
    {
        var response = await _amazonSupport.CreateCaseAsync(
            new CreateCaseRequest()
            {
                ServiceCode = serviceCode,
                CategoryCode = categoryCode,
                SeverityCode = severityCode,
                Subject = subject,
                Language = language,
                AttachmentSetId = attachmentSetId,
                IssueType = issueType,
```

```
                CommunicationBody = body
            });
        return response.CaseId;
    }
```

- API 세부 정보는 AWS SDK for .NET API CreateCase참조를 참조하십시오.

CLI

AWS CLI

사례를 생성하는 방법

다음 `create-case` 예시는 AWS 계정에 대한 지원 사례를 생성합니다.

```
aws support create-case \
    --category-code "using-aws" \
    --cc-email-addresses "myemail@example.com" \
    --communication-body "I want to learn more about an AWS service." \
    --issue-type "technical" \
    --language "en" \
    --service-code "general-info" \
    --severity-code "low" \
    --subject "Question about my account"
```

출력:

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

자세한 내용은 AWS Support 사용 설명서의 사례 관리를 참조하세요.

- API 세부 정보는 AWS CLI 명령 CreateCase참조를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
       try {
           String serviceCode = sevCatList.get(0);
           String caseCat = sevCatList.get(1);
           CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                   .categoryCode(caseCat.toLowerCase())
                   .serviceCode(serviceCode.toLowerCase())
                   .severityCode(sevLevel.toLowerCase())
                   .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                   .subject("Test case, please ignore")
                   .language("en")
                   .issueType("technical")
                   .build();

           CreateCaseResponse response = supportClient.createCase(caseRequest);
           return response.caseId();

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- API 세부 정보는 AWS SDK for Java 2.x API CreateCase참조를 참조하십시오.

JavaScript

JavaScript (v3) 용 SDK

> **Note**
>
> 더 많은 내용이 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import { CreateCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new case and log the case id.
    // Important: This creates a real support case in your account.
    const response = await client.send(
      new CreateCaseCommand({
        // The subject line of the case.
        subject: "IGNORE: Test case",
        // Use DescribeServices to find available service codes for each service.
        serviceCode: "service-quicksight-end-user",
        // Use DescribeSecurityLevels to find available severity codes for your
 support plan.
        severityCode: "low",
        // Use DescribeServices to find available category codes for each
 service.
        categoryCode: "end-user-support",
        // The main description of the support case.
        communicationBody: "This is a test. Please ignore.",
      }),
    );
    console.log(response.caseId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API 세부 정보는 AWS SDK for JavaScript API CreateCase참조를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> 자세한 내용은 다음과 같습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun createSupportCase(
    sevCatListVal: List<String>,
    sevLevelVal: String
): String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest =
        CreateCaseRequest {
            categoryCode = caseCategory.lowercase(Locale.getDefault())
            serviceCode = serCode.lowercase(Locale.getDefault())
            severityCode = sevLevelVal.lowercase(Locale.getDefault())
            communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
            subject = "Test case, please ignore"
            language = "en"
            issueType = "technical"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}
```

- API 세부 정보는 Kotlin API용AWS SDK 레퍼런스를 참조하세요 CreateCase.

PowerShell

다음을 위한 도구 PowerShell

예 1: AWS Support 센터에서 새 케이스를 생성합니다. - ServiceCode 및 - CategoryCode 매개 변수의 값은 Get-asaService cmdlet을 사용하여 가져올 수 있습니다. - SeverityCode 매개 변수의 값은 Get-ASA cmdlet을 사용하여 가져올 수 있습니다. SeverityLevel - IssueType 매개 변수 값은 “고객 서비스” 또는 “기술”일 수 있습니다. 성공하면 AWS Support 케이스 번호가 출력됩니다. 기본적으로 케이스는 영어로 처리되며, 일본어를 사용하려면 -Language “ja” 매개변수를 추가하십시오. -ServiceCode, -CategoryCode, -제목 및 - CommunicationBody 매개변수는 필수입니다.

```
New-ASACase -ServiceCode "amazon-cloudfront" -CategoryCode "APIs" -SeverityCode
 "low" -Subject "subject text" -CommunicationBody "description of the case" -
CcEmailAddress @("email1@domain.com", "email2@domain.com") -IssueType "technical"
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조를 참조하십시오 CreateCase.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 다음과 같습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
```

```
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 CreateCase.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **DescribeAttachment** CLI와 함께 사용

다음 코드 예제는 DescribeAttachment의 사용 방법을 보여줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 사례 시작하기

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
```

```
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }
```

- API 세부 정보는 AWS SDK for .NET API DescribeAttachment참조를 참조하십시오.

CLI

AWS CLI

첨부 파일을 설명하는 방법

다음 describe-attachment 예시에서는 지정된 ID를 가진 첨부 파일에 대한 정보를 반환합니다.

```
aws support describe-attachment \
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

출력:

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
    }
}
```

자세한 내용은 AWS Support 사용 설명서의 사례 관리를 참조하세요.

- API 세부 정보는 AWS CLI 명령 DescribeAttachment참조를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static void describeAttachment(SupportClient supportClient, String
attachId) {
       try {
           DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                   .attachmentId(attachId)
                   .build();

           DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
           System.out.println("The name of the file is " +
response.attachment().fileName());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- API 세부 정보는 AWS SDK for Java 2.x API DescribeAttachment참조를 참조하십시오.

JavaScript

JavaScript (v3) 용 SDK

> **Note**
>
> 더 많은 내용이 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import { DescribeAttachmentCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the metadata and content of an attachment.
    const response = await client.send(
      new DescribeAttachmentCommand({
        // Set value to an existing attachment id.
        // Use DescribeCommunications or DescribeCases to find an attachment id.
        attachmentId: "ATTACHMENT_ID",
      }),
    );
    console.log(response.attachment?.fileName);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API 세부 정보는 AWS SDK for JavaScript API DescribeAttachment참조를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> 자세한 내용은 다음과 같습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
```

```
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}
```

- API 세부 정보는 Kotlin API용AWS SDK 레퍼런스를 참조하세요 DescribeAttachment.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 여기에서 확인할 수 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
```

```
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 DescribeAttachment.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **DescribeCases** CLI와 함께 사용

다음 코드 예제는 DescribeCases의 사용 방법을 보여줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 사례 시작하기

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
```

```
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }
```

- API 세부 정보는 AWS SDK for .NET API DescribeCases참조를 참조하십시오.

## CLI

### AWS CLI

#### 사례를 설명하는 방법

다음 `describe-cases` 예시는 AWS 계정의 지정된 지원 사례에 대한 정보를 반환합니다.

```
aws support describe-cases \
    --display-id "1234567890" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --include-resolved-cases \
    --language "en" \
    --no-include-communications \
    --max-item 1
```

출력:

```
{
    "cases": [
        {
            "status": "resolved",
            "ccEmailAddresses": [],
            "timeCreated": "2020-03-23T21:31:47.774Z",
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "severityCode": "low",
```

```
            "language": "en",
            "categoryCode": "using-aws",
            "serviceCode": "general-info",
            "submittedBy": "myemail@example.com",
            "displayId": "1234567890",
            "subject": "Question about my account"
        }
    ]
}
```

자세한 내용은 AWS Support 사용 설명서의 사례 관리를 참조하세요.

- API 세부 정보는 AWS CLI 명령 DescribeCases참조를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
```

```
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API DescribeCases참조를 참조하십시오.

## JavaScript

### JavaScript (v3) 용 SDK

> **Note**
>
> 더 많은 내용이 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import { DescribeCasesCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all of the unresolved cases in your account.
    // Filter or expand results by providing parameters to the
 DescribeCasesCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecasescommandinput.html
    const response = await client.send(new DescribeCasesCommand({}));
    const caseIds = response.cases.map((supportCase) => supportCase.caseId);
    console.log(caseIds);
    return response;
  } catch (err) {
```

```
    console.error(err);
  }
};
```

- API 세부 정보는 AWS SDK for JavaScript API DescribeCases참조를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 20
            afterTime = yesterday.toString()
            beforeTime = now.toString()
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}
```

- API 세부 정보는 Kotlin API용AWS SDK 레퍼런스를 참조하세요 DescribeCases.

PowerShell

다음을 위한 도구 PowerShell

예 1: 모든 지원 사례의 세부 정보를 반환합니다.

```
Get-ASACase
```

예 2: 지정된 날짜 및 시간 이후 모든 지원 사례의 세부 정보를 반환합니다.

```
Get-ASACase -AfterTime "2013-09-10T03:06Z"
```

예 3: 해결된 지원 사례를 포함하여 처음 10개 지원 사례의 세부 정보를 반환합니다.

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

예 4: 지정된 단일 지원 사례의 세부 정보를 반환합니다.

```
Get-ASACase -CaseIdList "case-12345678910-2013-c4c1d2bf33c5cf47"
```

예 5: 지정된 지원 사례의 세부 정보를 반환합니다.

```
Get-ASACase -CaseIdList @("case-12345678910-2013-c4c1d2bf33c5cf47",
 "case-18929034710-2011-c4fdeabf33c5cf47")
```

예 6: 수동 페이징을 사용하여 모든 지원 사례를 반환합니다. 케이스는 20개씩 배치로 검색됩니다.

```
$nextToken = $null
do {
  Get-ASACase -NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조를 참조하십시오 DescribeCases.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 다음과 같습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
```

```
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 DescribeCases.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **DescribeCommunications** CLI와 함께 사용

다음 코드 예제는 DescribeCommunications의 사용 방법을 보여줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 사례 시작하기

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }
```

- API 세부 정보는 AWS SDK for .NET API DescribeCommunications참조를 참조하십시오.

CLI

AWS CLI

사례에 대한 최신 커뮤니케이션을 설명하는 방법

다음 describe-communications 예시는 AWS 계정의 지정된 지원 사례에 대한 최신 커뮤니케이션을 반환합니다.

```
aws support describe-communications \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

출력:

```
{
    "communications": [
        {
            "body": "I want to learn more about an AWS service.",
            "attachmentSet": [],
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "timeCreated": "2020-05-12T23:12:35.000Z",
            "submittedBy": "Amazon Web Services"
        }
    ],
    "NextToken":
 "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

자세한 내용은 AWS Support 사용 설명서의 사례 관리를 참조하세요.

- API 세부 정보는 AWS CLI 명령 DescribeCommunications참조를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static String listCommunications(SupportClient supportClient, String
caseId) {
       try {
           String attachId = null;
           DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                   .caseId(caseId)
                   .maxResults(10)
                   .build();

           DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
           List<Communication> communications = response.communications();
           for (Communication comm : communications) {
               System.out.println("the body is: " + comm.body());

               // Get the attachment id value.
               List<AttachmentDetails> attachments = comm.attachmentSet();
               for (AttachmentDetails detail : attachments) {
                   attachId = detail.attachmentId();
               }
           }
           return attachId;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- API 세부 정보는 AWS SDK for Java 2.x API DescribeCommunications참조를 참조하십시오.

JavaScript

JavaScript (v3) 용 SDK

> **Note**
>
> 더 많은 내용이 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import { DescribeCommunicationsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all communications for the support case.
    // Filter results by providing parameters to the
 DescribeCommunicationsCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecommunicationscommandinput.html
    const response = await client.send(
      new DescribeCommunicationsCommand({
        // Set value to an existing case id.
        caseId: "CASE_ID",
      }),
    );
    const text = response.communications.map((item) => item.body).join("\n");
    console.log(text);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API 세부 정보는 AWS SDK for JavaScript API DescribeCommunications참조를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
        DescribeCommunicationsRequest {
            caseId = caseIdVal
            maxResults = 10
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}
```

- API 세부 정보는 Kotlin API용AWS SDK 레퍼런스를 참조하세요 DescribeCommunications.

PowerShell

다음을 위한 도구 PowerShell

예 1: 지정된 케이스에 대한 모든 통신을 반환합니다.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

예 2: 지정된 케이스에 대해 2012년 1월 1일 자정 UTC 이후의 모든 통신을 반환합니다.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime
 "2012-01-10T00:00Z"
```

예 3: 수동 페이징을 사용하여 지정된 케이스에 대해 2012년 1월 1일 자정 UTC 이후 모든 통신을 반환합니다. 통신은 20개씩 일괄 검색됩니다.

```
$nextToken = $null
do {
  Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조를 참조하십시오 DescribeCommunications.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 다음과 같습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
```

```
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 DescribeCommunications.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **DescribeServices** CLI와 함께 사용

다음 코드 예제는 DescribeServices의 사용 방법을 보여줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 사례 시작하기

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
```

```
        return response.Services;
    }
```

- API 세부 정보는 AWS SDK for .NET API DescribeServices참조를 참조하십시오.

## CLI

### AWS CLI

#### AWS 서비스 및 서비스 범주를 나열하려면

다음 `describe-services` 예시에서는 일반 정보를 요청하는 데 사용할 수 있는 서비스 범주를 나열합니다.

```
aws support describe-services \
    --service-code-list "general-info"
```

출력:

```
{
    "services": [
        {
            "code": "general-info",
            "name": "General Info and Getting Started",
            "categories": [
                {
                    "code": "charges",
                    "name": "How Will I Be Charged?"
                },
                {
                    "code": "gdpr-queries",
                    "name": "Data Privacy Query"
                },
                {
                    "code": "reserved-instances",
                    "name": "Reserved Instances"
                },
                {
                    "code": "resource",
                    "name": "Where is my Resource?"
```

```
                },
                {
                    "code": "using-aws",
                    "name": "Using AWS & Services"
                },
                {
                    "code": "free-tier",
                    "name": "Free Tier"
                },
                {
                    "code": "security-and-compliance",
                    "name": "Security & Compliance"
                },
                {
                    "code": "account-structure",
                    "name": "Account Structure"
                }
            ]
        }
    ]
}
```

자세한 내용은 AWS Support 사용 설명서의 사례 관리를 참조하세요.

- API 세부 정보는 AWS CLI 명령 DescribeServices참조를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    // Return a List that contains a Service name and Category name.
    public static List<String> displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                    .language("en")
```

```
                    .build();

            DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
            String serviceCode = null;
            String catName = null;
            List<String> sevCatList = new ArrayList<>();
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();

                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API DescribeServices참조를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
```

```
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- API 세부 정보는 Kotlin API용AWS SDK 레퍼런스를 참조하세요 DescribeServices.

PowerShell

다음을 위한 도구 PowerShell

예 1: 사용 가능한 모든 서비스 코드, 이름 및 카테고리를 반환합니다.

```
Get-ASAService
```

예 2: 지정된 코드를 사용하여 서비스의 이름 및 범주를 반환합니다.

```
Get-ASAService -ServiceCodeList "amazon-cloudfront"
```

예 3: 지정된 서비스 코드의 이름과 범주를 반환합니다.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

예 4: 지정된 서비스 코드의 이름 및 범주 (일본어) 를 반환합니다. 현재 영어 (“en”) 및 일본어 (“ja”) 언어 코드가 지원됩니다.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch") -
Language "ja"
```

- API에 대한 자세한 내용은 AWS Tools for PowerShell Cmdlet 참조를 참조하십시오 DescribeServices.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 다음과 같습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
 language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
```

```
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 DescribeServices.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **DescribeSeverityLevels** CLI와 함께 사용

다음 코드 예제는 DescribeSeverityLevels의 사용 방법을 보여줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 사례 시작하기

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 DescribeSeverity 레벨을 참조하십시오.

CLI

AWS CLI

사용 가능한 심각도 수준을 나열하는 방법

다음 `describe-severity-levels` 예시에서는 지원 사례에 사용할 수 있는 심각도 수준을 나열합니다.

```
aws support describe-severity-levels
```

출력:

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
        {
            "code": "high",
            "name": "High"
        },
        {
            "code": "urgent",
            "name": "Urgent"
        },
        {
            "code": "critical",
            "name": "Critical"
        }
    ]
}
```

자세한 내용은 AWS Support 사용 설명서의 심각도 선택을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 DescribeSeverity 수준을 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    public static String displaySevLevels(SupportClient supportClient) {
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 DescribeSeverity 레벨을 참조하십시오.

## JavaScript

### JavaScript (v3) 용 SDK

> **Note**
>
> 더 많은 내용이 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import { DescribeSeverityLevelsCommand } from "@aws-sdk/client-support";
```

```
import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the list of severity levels.
    // The available values depend on the support plan for the account.
    const response = await client.send(new DescribeSeverityLevelsCommand({}));
    console.log(response.severityLevels);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API 세부 정보는 AWS SDK for JavaScript API 참조의 DescribeSeverity 레벨을 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
```

```
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}
```

- API 세부 정보는 Kotlin API 레퍼런스용AWS SDK의 DescribeSeverity 레벨을 참조하세요.

PowerShell

다음을 위한 도구 PowerShell

예 1: AWS Support 사례에 할당할 수 있는 심각도 수준 목록을 반환합니다.

```
Get-ASASeverityLevel
```

예 2: AWS Support 사례에 할당할 수 있는 심각도 수준 목록을 반환합니다. 레벨 이름은 일본어로 반환됩니다.

```
Get-ASASeverityLevel -Language "ja"
```

- API에 대한 세부 정보는 AWS Tools for PowerShell Cmdlet 참조의 DescribeSeverity수준을 참조하십시오.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 에서 확인할 수 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
```

```
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
```

```
                raise
        else:
            return severity_levels
```

- API에 대한 자세한 내용은 파이썬용AWS SDK의 DescribeSeverity레벨 (Boto3) API 레퍼런스를 참조하십시오.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **DescribeTrustedAdvisorCheckRefreshStatuses** CLI와 함께 사용

다음 코드 예제는 DescribeTrustedAdvisorCheckRefreshStatuses의 사용 방법을 보여줍니다.

CLI

AWS CLI

AWS Trusted Advisor 검사의 새로 고침 상태를 나열하려면

다음 describe-trusted-advisor-check-refresh-statuses 예제에서는 두 가지 Trusted Advisor 검사 (Amazon S3 버킷 권한 및 IAM 사용) 의 새로 고침 상태를 나열합니다.

```
aws support describe-trusted-advisor-check-refresh-statuses \
    --check-id "Pfx0RwqBli" "zXCkfM1nI3"
```

출력:

```
{
    "statuses": [
        {
            "checkId": "Pfx0RwqBli",
            "status": "none",
            "millisUntilNextRefreshable": 0
        },
        {
```

```
            "checkId": "zXCkfM1nI3",
            "status": "none",
            "millisUntilNextRefreshable": 0
        }
    ]
}
```

자세한 내용은 AWS 지원 사용 설명서의AWS Trusted Advisor를 참조하십시오.

- API 세부 정보는 AWS CLI 명령 DescribeTrustedAdvisorCheckRefreshStatuses참조를 참조하십시오.

PowerShell

도구: PowerShell

예 1: 지정된 검사에 대한 새로 고침 요청의 현재 상태를 반환합니다. Request-ASA는 검사의 상태 정보를 새로 고치도록 요청하는 데 사용할 TrustedAdvisorCheckRefresh 수 있습니다.

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

- API 세부 정보는 Cmdlet 참조를 참조하십시오 DescribeTrustedAdvisorCheckRefreshStatuses.AWS Tools for PowerShell

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **DescribeTrustedAdvisorCheckResult** CLI와 함께 사용

다음 코드 예제는 DescribeTrustedAdvisorCheckResult의 사용 방법을 보여줍니다.

CLI

AWS CLI

AWS Trusted Advisor 검사 결과를 나열하려면

다음 describe-trusted-advisor-check-result 예는 IAM Use 검사의 결과를 나열합니다.

```
aws support describe-trusted-advisor-check-result \
    --check-id "zXCkfM1nI3"
```

출력:

```
{
    "result": {
        "checkId": "zXCkfM1nI3",
        "timestamp": "2020-05-13T21:38:05Z",
        "status": "ok",
        "resourcesSummary": {
            "resourcesProcessed": 1,
            "resourcesFlagged": 0,
            "resourcesIgnored": 0,
            "resourcesSuppressed": 0
        },
        "categorySpecificSummary": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "flaggedResources": [
            {
                "status": "ok",
                "resourceId": "47DEQpj8HBSa-_TImW-5JCeuQeRkm5NMpJWZEXAMPLE",
                "isSuppressed": false
            }
        ]
    }
}
```

자세한 내용은 AWS 지원 사용 설명서의AWS Trusted Advisor를 참조하십시오.

- API 세부 정보는 AWS CLI 명령 참조 DescribeTrusted AdvisorCheck 결과를 참조하십시오.

PowerShell

에 대한 도구 PowerShell

예 1: Trusted Advisor 검사 결과를 반환합니다. 사용 가능한 Trusted Advisor 검사 목록은 Get-ASA TrustedAdvisor 검사를 사용하여 확인할 수 있습니다. 출력은 검사의 전체 상태, 검사가 마

지막으로 실행된 타임스탬프, 특정 검사의 고유한 검사 ID입니다. 결과를 일본어로 출력하려면 -Language “ja” 매개 변수를 추가하십시오.

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

- API에 대한 세부 정보는 AWS Tools for PowerShell Cmdlet 참조의 DescribeTrustedAdvisorCheck결과를 참조하십시오.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **DescribeTrustedAdvisorCheckSummaries** CLI와 함께 사용

다음 코드 예제는 DescribeTrustedAdvisorCheckSummaries의 사용 방법을 보여줍니다.

CLI

AWS CLI

AWS Trusted Advisor 검사 요약을 나열하려면

다음 describe-trusted-advisor-check-summaries 예제는 두 가지 Trusted Advisor 검사 (Amazon S3 버킷 권한 및 IAM 사용) 의 결과를 나열합니다.

```
aws support describe-trusted-advisor-check-summaries \
    --check-ids "Pfx0RwqBli" "zXCkfM1nI3"
```

출력:

```
{
    "summaries": [
        {
            "checkId": "Pfx0RwqBli",
            "timestamp": "2020-05-13T21:38:12Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 44,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
```

```
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        },
        {
            "checkId": "zXCkfM1nI3",
            "timestamp": "2020-05-13T21:38:05Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 1,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        }
    ]
}
```

자세한 내용은 AWS 지원 사용 설명서의AWS Trusted Advisor를 참조하십시오.

- API 세부 정보는 AWS CLI 명령 참조의 DescribeTrusted AdvisorCheck 요약을 참조하십시오.

PowerShell

에 대한 도구 PowerShell

예 1: 지정된 Trusted Advisor 검사의 최신 요약을 반환합니다.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

예 2: 지정된 Trusted Advisor 검사의 최신 요약을 반환합니다.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조의 DescribeTrustedAdvisorCheck요약을 참조하십시오.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **DescribeTrustedAdvisorChecks** CLI와 함께 사용

다음 코드 예제는 DescribeTrustedAdvisorChecks의 사용 방법을 보여줍니다.

CLI

AWS CLI

사용 가능한 AWS Trusted Advisor 검사를 나열하려면

다음 describe-trusted-advisor-checks 예에는 AWS 계정에서 사용 가능한 Trusted Advisor 검사 목록이 나와 있습니다. 이 정보에는 검사 이름, ID, 설명, 범주 및 메타데이터가 포함됩니다. 가독성을 위해 출력 내용이 짧아졌음을 참고하십시오.

```
aws support describe-trusted-advisor-checks \
    --language "en"
```

출력:

```
{
    "checks": [
        {
            "id": "zXCkfM1nI3",
            "name": "IAM Use",
            "description": "Checks for your use of AWS Identity and Access
 Management (IAM). You can use IAM to create users, groups, and roles in
 AWS, and you can use permissions to control access to AWS resources. \n<br>
\n<br>\n<b>Alert Criteria</b><br>\nYellow: No IAM users have been created
 for this account.\n<br>\n<br>\n<b>Recommended Action</b><br>\nCreate one or
 more IAM users and groups in your account. You can then create additional
 users whose permissions are limited to perform specific tasks in your AWS
 environment. For more information, see <a href=\"https://docs.aws.amazon.com/
```

```
IAM/latest/UserGuide/IAMGettingStarted.html\" target=\"_blank\">Getting
 Started</a>. \n<br><br>\n<b>Additional Resources</b><br>\n<a href=\"https://
docs.aws.amazon.com/IAM/latest/UserGuide/IAM_Introduction.html\" target=\"_blank
\">What Is IAM?</a>",
            "category": "security",
            "metadata": []
        }
    ]
}
```

자세한 내용은 AWS 지원 사용 설명서의AWS Trusted Advisor를 참조하십시오.

- API 세부 정보는 AWS CLI 명령 DescribeTrustedAdvisorChecks참조를 참조하십시오.

PowerShell

에 대한 도구 PowerShell

예 1: Trusted Advisor 검사 컬렉션을 반환합니다. 영어 출력의 경우 “en”, 일본어 출력의 경우 “ja”를 받아들일 수 있는 언어 매개 변수를 지정해야 합니다.

```
Get-ASATrustedAdvisorCheck -Language "en"
```

- API에 대한 자세한 내용은 AWS Tools for PowerShell Cmdlet 참조를 참조하십시오 DescribeTrustedAdvisorChecks.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **RefreshTrustedAdvisorCheck** CLI와 함께 사용

다음 코드 예제는 RefreshTrustedAdvisorCheck의 사용 방법을 보여줍니다.

CLI

AWS CLI

AWS Trusted Advisor 검사를 새로 고치려면

다음 refresh-trusted-advisor-check 예는 AWS 계정의 Amazon S3 버킷 권한 Trusted Advisor 확인을 새로 고칩니다.

```
aws support refresh-trusted-advisor-check \
    --check-id "Pfx0RwqBli"
```

출력:

```
{
    "status": {
        "checkId": "Pfx0RwqBli",
        "status": "enqueued",
        "millisUntilNextRefreshable": 3599992
    }
}
```

자세한 내용은 AWS 지원 사용 설명서의AWS Trusted Advisor를 참조하십시오.

- API 세부 정보는 AWS CLI 명령 RefreshTrustedAdvisorCheck참조를 참조하십시오.

PowerShell

에 대한 도구 PowerShell

예 1: 지정된 Trusted Advisor 검사의 새로 고침을 요청합니다.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조를 참조하십시오 RefreshTrustedAdvisorCheck.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

## AWS SDK 또는 **ResolveCase** CLI와 함께 사용

다음 코드 예제는 ResolveCase의 사용 방법을 보여줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 사례 시작하기

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/// <summary>
/// Resolve a support case by caseId.
/// </summary>
/// <param name="caseId">Id for the support case.</param>
/// <returns>The final status of the case after resolving.</returns>
public async Task<string> ResolveCase(string caseId)
{
    var response = await _amazonSupport.ResolveCaseAsync(
        new ResolveCaseRequest()
        {
            CaseId = caseId
        });
    return response.FinalCaseStatus;
}
```

- API 세부 정보는 AWS SDK for .NET API ResolveCase참조를 참조하십시오.

CLI

AWS CLI

지원 사례를 해결하는 방법

다음 `resolve-case` 예시는 AWS 계정의 지원 사례를 해결합니다.

```
aws support resolve-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

출력:

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
}
```

자세한 내용은 AWS Support 사용 설명서의 사례 관리를 참조하세요.

- API 세부 정보는 AWS CLI 명령 ResolveCase참조를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
       try {
           ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                   .caseId(caseId)
                   .build();

           ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
           System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- API 세부 정보는 AWS SDK for Java 2.x API ResolveCase참조를 참조하십시오.

JavaScript

JavaScript (v3) 용 SDK

> **Note**
>
> 더 많은 내용이 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import { ResolveCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

const main = async () => {
  try {
    const response = await client.send(
      new ResolveCaseCommand({
        caseId: "CASE_ID",
      }),
    );

    console.log(response.finalCaseStatus);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API 세부 정보는 AWS SDK for JavaScript API ResolveCase참조를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> 자세한 내용은 에서 확인할 수 GitHub 있습니다. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}
```

- API 세부 정보는 Kotlin API용AWS SDK 레퍼런스를 참조하세요 ResolveCase.

PowerShell

다음을 위한 도구 PowerShell

예 1: 지정된 케이스의 초기 상태와 해결 호출이 완료된 후의 현재 상태를 반환합니다.

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

- API에 대한 자세한 내용은 AWS Tools for PowerShell Cmdlet 참조를 참조하십시오 ResolveCase.

Python

SDK for Python(Boto3)

> **Note**
>
> 자세한 내용은 다음과 같습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
```

```
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status
```

- API에 대한 자세한 내용은 파이썬용AWS SDK (Boto3) API 레퍼런스를 참조하십시오 ResolveCase.

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오. AWS SupportAWS SDK와 함께 사용 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

# SDK AWS Support 사용 AWS 시나리오

다음 코드 예제는 AWS SDK를 사용하여 일반적인 시나리오를 구현하는 방법을 보여줍니다. AWS Support 이 시나리오는 내에서 여러 함수를 호출하여 특정 작업을 수행하는 방법을 보여줍니다. AWS Support각 시나리오에는 코드 설정 및 실행 방법에 대한 지침을 찾을 수 있는 링크가 포함되어 있습니다. GitHub

예제

- AWS SDK를 사용하여 AWS Support 케이스를 시작하세요.

## AWS SDK를 사용하여 AWS Support 케이스를 시작하세요.

다음 코드 예제에서는 다음과 같은 작업을 수행하는 방법을 보여줍니다.

- 사용 가능한 서비스 및 사례의 심각도 수준을 가져와서 표시합니다.
- 선택한 서비스, 범주 및 심각도 수준을 사용하여 지원 사례를 만듭니다.
- 현재 일자의 미해결 사례 목록을 가져와서 표시합니다.
- 새로운 사례에 첨부 파일 세트와 통신을 추가합니다.
- 해당 사례에 대한 새로운 첨부 파일과 통신을 설명하세요.
- 사건을 해결하세요.
- 현재 일자의 해결된 사례 목록을 가져와서 표시합니다.

.NET

AWS SDK for .NET

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

명령 프롬프트에서 대화형 시나리오를 실행합니다.

```
/// <summary>
/// Hello AWS Support example.
/// </summary>
public static class SupportCaseScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.
    To use the AWS Support API, you must have one of the following AWS Support
 plans: Business, Enterprise On-Ramp, or Enterprise.

    This .NET example performs the following tasks:
    1.  Get and display services. Select a service from the list.
    2.  Select a category from the selected service.
    3.  Get and display severity levels and select a severity level from the
 list.
    4.  Create a support case using the selected service, category, and severity
 level.
    5.  Get and display a list of open support cases for the current day.
    6.  Create an attachment set with a sample text file to add to the case.
    7.  Add a communication with the attachment to the support case.
    8.  List the communications of the support case.
    9.  Describe the attachment set.
    10. Resolve the support case.
    11. Get a list of resolved cases for the current day.
   */

    private static SupportWrapper _supportWrapper = null!;

    static async Task Main(string[] args)
```

```
    {
        // Set up dependency injection for the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>(new AWSOptions()
{ Profile = "default" })
                    .AddTransient<SupportWrapper>()
            )
            .Build();

        var logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger(typeof(SupportCaseScenario));

        _supportWrapper = host.Services.GetRequiredService<SupportWrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the AWS Support case example scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            var apiSupported = await _supportWrapper.VerifySubscription();
            if (!apiSupported)
            {
                logger.LogError("You must have a Business, Enterprise On-Ramp, or
Enterprise Support " +
                                "plan to use the AWS Support API. \n\tPlease
upgrade your subscription to run these examples.");
                return;
            }

            var service = await DisplayAndSelectServices();

            var category = DisplayAndSelectCategories(service);
```

```
            var severityLevel = await DisplayAndSelectSeverity();

            var caseId = await CreateSupportCase(service, category,
severityLevel);

            await DescribeTodayOpenCases();

            var attachmentSetId = await CreateAttachmentSet();

            await AddCommunicationToCase(attachmentSetId, caseId);

            var attachmentId = await ListCommunicationsForCase(caseId);

            await DescribeCaseAttachment(attachmentId);

            await ResolveCase(caseId);

            await DescribeTodayResolvedCases();

            Console.WriteLine(new string('-', 80));
            Console.WriteLine("AWS Support case example scenario complete.");
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
    }

    /// <summary>
    /// List some available services from AWS Support, and select a service for
the example.
    /// </summary>
    /// <returns>The selected service.</returns>
    private static async Task<Service> DisplayAndSelectServices()
    {
        Console.WriteLine(new string('-', 80));
        var services = await _supportWrapper.DescribeServices();
        Console.WriteLine($"AWS Support client returned {services.Count}
services.");

        Console.WriteLine($"1. Displaying first 10 services:");
        for (int i = 0; i < 10 && i < services.Count; i++)
```

```
        {
            Console.WriteLine($"\t{i + 1}. {services[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > services.Count)
        {
            Console.WriteLine(
                "Select an example support service by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return services[choiceNumber - 1];
    }

    /// <summary>
    /// List the available categories for a service and select a category for the
example.
    /// </summary>
    /// <param name="service">Service to use for displaying categories.</param>
    /// <returns>The selected category.</returns>
    private static Category DisplayAndSelectCategories(Service service)
    {
        Console.WriteLine(new string('-', 80));

        Console.WriteLine($"2. Available support categories for Service
\"{service.Name}\":");
        for (int i = 0; i < service.Categories.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {service.Categories[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > service.Categories.Count)
        {
            Console.WriteLine(
                "Select an example support category by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
```

```
        Console.WriteLine(new string('-', 80));

        return service.Categories[choiceNumber - 1];
    }

    /// <summary>
    /// List available severity levels from AWS Support, and select a level for
the example.
    /// </summary>
    /// <returns>The selected severity level.</returns>
    private static async Task<SeverityLevel> DisplayAndSelectSeverity()
    {
        Console.WriteLine(new string('-', 80));
        var severityLevels = await _supportWrapper.DescribeSeverityLevels();

        Console.WriteLine($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {severityLevels[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > severityLevels.Count)
        {
            Console.WriteLine(
                "Select an example severity level by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return severityLevels[choiceNumber - 1];
    }

    /// <summary>
    /// Create an example support case.
    /// </summary>
    /// <param name="service">Service to use for the new case.</param>
    /// <param name="category">Category to use for the new case.</param>
    /// <param name="severity">Severity to use for the new case.</param>
    /// <returns>The caseId of the new support case.</returns>
    private static async Task<string> CreateSupportCase(Service service,
```

```
        Category category, SeverityLevel severity)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. Create an example support case" +
                          $" with the following settings:" +
                          $" \n\tService: {service.Name}, Category:
{category.Name} " +
                          $"and Severity Level: {severity.Name}.");
        var caseId = await _supportWrapper.CreateCase(service.Code,
category.Code, severity.Code,
            "Example case for testing, ignore.", "This is my example support
case.");

        Console.WriteLine($"\tNew case created with ID {caseId}");

        Console.WriteLine(new string('-', 80));

        return caseId;
    }

    /// <summary>
    /// List open cases for the current day.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task DescribeTodayOpenCases()
    {
        Console.WriteLine($"5. List the open support cases for the current
day.");
        // Describe the cases. If it is empty, try again and allow time for the
new case to appear.
        List<CaseDetails> currentOpenCases = null!;
        while (currentOpenCases == null || currentOpenCases.Count == 0)
        {
            Thread.Sleep(1000);
            currentOpenCases = await _supportWrapper.DescribeCases(
                new List<string>(),
                null,
                false,
                false,
                DateTime.UtcNow.Date,
                DateTime.UtcNow);
        }

        foreach (var openCase in currentOpenCases)
```

```
        {
            Console.WriteLine($"\tCase: {openCase.CaseId} created
 {openCase.TimeCreated}");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Create an attachment set for a support case.
    /// </summary>
    /// <returns>The attachment set id.</returns>
    private static async Task<string> CreateAttachmentSet()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Create an attachment set for a support case.");
        var fileName = "example_attachment.txt";

        // Create the file if it does not already exist.
        if (!File.Exists(fileName))
        {
            await using StreamWriter sw = File.CreateText(fileName);
            await sw.WriteLineAsync(
                "This is a sample file for attachment to a support case.");
        }

        await using var ms = new MemoryStream(await
 File.ReadAllBytesAsync(fileName));

        var attachmentSetId = await _supportWrapper.AddAttachmentToSet(
            ms,
            fileName);

        Console.WriteLine($"\tNew attachment set created with id: \n
\t{attachmentSetId.Substring(0, 65)}...");

        Console.WriteLine(new string('-', 80));

        return attachmentSetId;
    }

    /// <summary>
    /// Add an attachment set and communication to a case.
    /// </summary>
```

```
    /// <param name="attachmentSetId">Id of the attachment set.</param>
    /// <param name="caseId">Id of the case to receive the attachment set.</
param>
    /// <returns>Async task.</returns>
    private static async Task AddCommunicationToCase(string attachmentSetId,
 string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Add attachment set and communication to
 {caseId}.");

        await _supportWrapper.AddCommunicationToCase(
            caseId,
            "This is an example communication added to a support case.",
            attachmentSetId);

        Console.WriteLine($"\tNew attachment set and communication added to
 {caseId}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List the communications for a case.
    /// </summary>
    /// <param name="caseId">Id of the case to describe.</param>
    /// <returns>An attachment id.</returns>
    private static async Task<string> ListCommunicationsForCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. List communications for case {caseId}.");

        var communications = await
 _supportWrapper.DescribeCommunications(caseId);
        var attachmentId = "";
        foreach (var communication in communications)
        {
            Console.WriteLine(
                $"\tCommunication created on: {communication.TimeCreated} has
 {communication.AttachmentSet.Count} attachments.");
            if (communication.AttachmentSet.Any())
            {
                attachmentId = communication.AttachmentSet.First().AttachmentId;
            }
```

```
        }

        Console.WriteLine(new string('-', 80));
        return attachmentId;
    }

    /// <summary>
    /// Describe an attachment by id.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment to describe.</param>
    /// <returns>Async task.</returns>
    private static async Task DescribeCaseAttachment(string attachmentId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Describe the attachment set.");

        var attachment = await _supportWrapper.DescribeAttachment(attachmentId);
        var data = Encoding.ASCII.GetString(attachment.Data.ToArray());
        Console.WriteLine($"\tAttachment includes {attachment.FileName} with
data: \n\t{data}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Resolve the support case.
    /// </summary>
    /// <param name="caseId">Id of the case to resolve.</param>
    /// <returns>Async task.</returns>
    private static async Task ResolveCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Resolve case {caseId}.");

        var status = await _supportWrapper.ResolveCase(caseId);
        Console.WriteLine($"\tCase {caseId} has final status {status}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List resolved cases for the current day.
    /// </summary>
    /// <returns>Async Task.</returns>
```

```
    private static async Task DescribeTodayResolvedCases()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"11. List the resolved support cases for the current
 day.");
        var currentCases = await _supportWrapper.DescribeCases(
            new List<string>(),
            null,
            false,
            true,
            DateTime.UtcNow.Date,
            DateTime.UtcNow);

        foreach (var currentCase in currentCases)
        {
            if (currentCase.Status == "resolved")
            {
                Console.WriteLine(
                    $"\tCase: {currentCase.CaseId}: status
 {currentCase.Status}");
            }
        }

        Console.WriteLine(new string('-', 80));
    }
}
```

시나리오에서 AWS Support 액션에 사용하는 래퍼 메서드.

```
/// <summary>
/// Wrapper methods to use AWS Support for working with support cases.
/// </summary>
public class SupportWrapper
{
    private readonly IAmazonAWSSupport _amazonSupport;
    public SupportWrapper(IAmazonAWSSupport amazonSupport)
    {
        _amazonSupport = amazonSupport;
    }
```

```
    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }



    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }



    /// <summary>
    /// Create a new support case.
    /// </summary>
    /// <param name="serviceCode">Service code for the new case.</param>
    /// <param name="categoryCode">Category for the new case.</param>
```

```
    /// <param name="severityCode">Severity code for the new case.</param>
    /// <param name="subject">Subject of the new case.</param>
    /// <param name="body">Body text of the new case.</param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
    /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
    /// <returns>The caseId of the new support case.</returns>
    public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
        string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
    {
        var response = await _amazonSupport.CreateCaseAsync(
            new CreateCaseRequest()
            {
                ServiceCode = serviceCode,
                CategoryCode = categoryCode,
                SeverityCode = severityCode,
                Subject = subject,
                Language = language,
                AttachmentSetId = attachmentSetId,
                IssueType = issueType,
                CommunicationBody = body
            });
        return response.CaseId;
    }



    /// <summary>
    /// Add an attachment to a set, or create a new attachment set if one does
not exist.
    /// </summary>
    /// <param name="data">The data for the attachment.</param>
    /// <param name="fileName">The file name for the attachment.</param>
    /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
    /// <returns>The setId of the attachment.</returns>
    public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
```

```
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }



    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }



    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
```

```
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }



    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
```

```
            results.Add(communications);
        }
        return results;
    }



    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
```

```
        {
            results.Add(cases);
        }
        return results;
    }



    /// <summary>
    /// Resolve a support case by caseId.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }



    /// <summary>
    /// Verify the support level for AWS Support API access.
    /// </summary>
    /// <returns>True if the subscription level supports API access.</returns>
    public async Task<bool> VerifySubscription()
    {
        try
        {
            var response = await _amazonSupport.DescribeServicesAsync(
                new DescribeServicesRequest()
                {
                    Language = "en"
                });
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Amazon.AWSSupport.AmazonAWSSupportException ex)
        {
            if (ex.ErrorCode == "SubscriptionRequiredException")
            {
                return false;
```

```
            }
            else throw;
        }
    }
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 다음 주제를 참조하십시오.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverity레벨
  - ResolveCase

Java

SDK for Java 2.x

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

다양한 AWS Support 작업을 실행하세요.

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetResponse;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseRequest;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseResponse;
```

```
import software.amazon.awssdk.services.support.model.Attachment;
import software.amazon.awssdk.services.support.model.AttachmentDetails;
import software.amazon.awssdk.services.support.model.CaseDetails;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.Communication;
import software.amazon.awssdk.services.support.model.CreateCaseRequest;
import software.amazon.awssdk.services.support.model.CreateCaseResponse;
import software.amazon.awssdk.services.support.model.DescribeAttachmentRequest;
import software.amazon.awssdk.services.support.model.DescribeAttachmentResponse;
import software.amazon.awssdk.services.support.model.DescribeCasesRequest;
import software.amazon.awssdk.services.support.model.DescribeCasesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsResponse;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsResponse;
import software.amazon.awssdk.services.support.model.ResolveCaseRequest;
import software.amazon.awssdk.services.support.model.ResolveCaseResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SeverityLevel;
import software.amazon.awssdk.services.support.model.SupportException;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetRequest;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
```

```
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following tasks:
 *
 * 1. Gets and displays available services.
 * 2. Gets and displays severity levels.
 * 3. Creates a support case by using the selected service, category, and
 * severity level.
 * 4. Gets a list of open cases for the current day.
 * 5. Creates an attachment set with a generated file.
 * 6. Adds a communication with the attachment to the support case.
 * 7. Lists the communications of the support case.
 * 8. Describes the attachment set included with the communication.
 * 9. Resolves the support case.
 * 10. Gets a list of resolved cases for the current day.
 */
public class SupportScenario {

    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <fileAttachment>Where:
                    fileAttachment - The file can be a simple saved .txt file to
 use as an email attachment.\s
                """;

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

        String fileAttachment = args[0];
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();
```

```
        System.out.println(DASHES);
        System.out.println("***** Welcome to the AWS Support case example
scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. Get and display available services.");
        List<String> sevCatList = displayServices(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. Get and display Support severity levels.");
        String sevLevel = displaySevLevels(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. Create a support case using the selected service,
category, and severity level.");
        String caseId = createSupportCase(supportClient, sevCatList, sevLevel);
        if (caseId.compareTo("") == 0) {
            System.out.println("A support case was not successfully created!");
            System.exit(1);
        } else
            System.out.println("Support case " + caseId + " was successfully
created!");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Get open support cases.");
        getOpenCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Create an attachment set with a generated file to
add to the case.");
        String attachmentSetId = addAttachment(supportClient, fileAttachment);
        System.out.println("The Attachment Set id value is" + attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Add communication with the attachment to the
support case.");
        addAttachSupportCase(supportClient, caseId, attachmentSetId);
```

```
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. List the communications of the support case.");
        String attachId = listCommunications(supportClient, caseId);
        System.out.println("The Attachment id value is" + attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Describe the attachment set included with the
communication.");
        describeAttachment(supportClient, attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Resolve the support case.");
        resolveSupportCase(supportClient, caseId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get a list of resolved cases for the current
day.");
        getResolvedCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("***** This Scenario has successfully completed");
        System.out.println(DASHES);
    }

    public static void getResolvedCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(30)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .includeResolvedCases(true)
                    .build();
```

```
            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                if (sinCase.status().compareTo("resolved") == 0)
                    System.out.println("The case status is " + sinCase.status());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
        try {
            ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                    .caseId(caseId)
                    .build();

            ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
            System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeAttachment(SupportClient supportClient, String
attachId) {
        try {
            DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                    .attachmentId(attachId)
                    .build();

            DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
```

```
            System.out.println("The name of the file is " +
response.attachment().fileName());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String listCommunications(SupportClient supportClient, String
caseId) {
        try {
            String attachId = null;
            DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                    .caseId(caseId)
                    .maxResults(10)
                    .build();

            DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
            List<Communication> communications = response.communications();
            for (Communication comm : communications) {
                System.out.println("the body is: " + comm.body());

                // Get the attachment id value.
                List<AttachmentDetails> attachments = comm.attachmentSet();
                for (AttachmentDetails detail : attachments) {
                    attachId = detail.attachmentId();
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
        try {
```

```
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
        try {
            File myFile = new File(fileAttachment);
            InputStream sourceStream = new FileInputStream(myFile);
            SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

            Attachment attachment = Attachment.builder()
                    .fileName(myFile.getName())
                    .data(sourceBytes)
                    .build();

            AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                    .attachments(attachment)
                    .build();

            AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
            return response.attachmentSetId();

        } catch (SupportException | FileNotFoundException e) {
```

```
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
        try {
            String serviceCode = sevCatList.get(0);
            String caseCat = sevCatList.get(1);
            CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                    .categoryCode(caseCat.toLowerCase())
                    .serviceCode(serviceCode.toLowerCase())
                    .severityCode(sevLevel.toLowerCase())
```

```
                    .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                    .subject("Test case, please ignore")
                    .language("en")
                    .issueType("technical")
                    .build();

            CreateCaseResponse response = supportClient.createCase(caseRequest);
            return response.caseId();

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static String displaySevLevels(SupportClient supportClient) {
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    // Return a List that contains a Service name and Category name.
```

```
   public static List<String> displayServices(SupportClient supportClient) {
       try {
           DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                   .language("en")
                   .build();

           DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
           String serviceCode = null;
           String catName = null;
           List<String> sevCatList = new ArrayList<>();
           List<Service> services = response.services();

           System.out.println("Get the first 10 services");
           int index = 1;
           for (Service service : services) {
               if (index == 11)
                   break;

               System.out.println("The Service name is: " + service.name());
               if (service.name().compareTo("Account") == 0)
                   serviceCode = service.code();

               // Get the Categories for this service.
               List<Category> categories = service.categories();
               for (Category cat : categories) {
                   System.out.println("The category name is: " + cat.name());
                   if (cat.name().compareTo("Security") == 0)
                       catName = cat.name();
               }
               index++;
           }

           // Push the two values to the list.
           sevCatList.add(serviceCode);
           sevCatList.add(catName);
           return sevCatList;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return null;
```

```
    }
}
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 다음 주제를 참조하십시오.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverity레벨
  - ResolveCase

JavaScript

JavaScript (v3) 용 SDK

> **Note**
>
> 더 많은 내용이 있습니다. GitHub AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

터미널에서 대화형 시나리오를 실행합니다.

```
import {
  AddAttachmentsToSetCommand,
  AddCommunicationToCaseCommand,
  CreateCaseCommand,
  DescribeAttachmentCommand,
  DescribeCasesCommand,
  DescribeCommunicationsCommand,
  DescribeServicesCommand,
  DescribeSeverityLevelsCommand,
  ResolveCaseCommand,
  SupportClient,
```

```
} from "@aws-sdk/client-support";
import * as inquirer from "@inquirer/prompts";
import { retry } from "@aws-doc-sdk-examples/lib/utils/util-timers.js";

const wrapText = (text, char = "=") => {
  const rule = char.repeat(80);
  return `${rule}\n    ${text}\n${rule}\n`;
};

const client = new SupportClient({ region: "us-east-1" });

// Verify that the account has a Support plan.
export const verifyAccount = async () => {
  const command = new DescribeServicesCommand({});

  try {
    await client.send(command);
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

/**
 * Select a service from the list returned from DescribeServices.
 */
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const selectedService = await inquirer.select({
    message:
      "Select a service. Your support case will be created for this service. The
 list of services is truncated for readability.",
    choices: services.slice(0, 10).map((s) => ({ name: s.name, value: s })),
  });
  return selectedService;
};

/**
 * @param {{ categories: import('@aws-sdk/client-support').Category[]}} service
```

```
 */
export const getCategory = async (service) => {
  const selectedCategory = await inquirer.select({
    message: "Select a category.",
    choices: service.categories.map((c) => ({ name: c.name, value: c })),
  });
  return selectedCategory;
};

// Get the available severity levels for the account.
export const getSeverityLevel = async () => {
  const command = new DescribeSeverityLevelsCommand({});
  const { severityLevels } = await client.send(command);
  const selectedSeverityLevel = await inquirer.select({
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

/**
 * Create a new support case
 * @param {{
 *  selectedService: import('@aws-sdk/client-support').Service
 *  selectedCategory: import('@aws-sdk/client-support').Category
 *  selectedSeverityLevel: import('@aws-sdk/client-support').SeverityLevel
 * }} selections
 * @returns
 */
export const createCase = async ({
  selectedService,
  selectedCategory,
  selectedSeverityLevel,
}) => {
  const command = new CreateCaseCommand({
    subject: "IGNORE: Test case",
    communicationBody: "This is a test. Please ignore.",
    serviceCode: selectedService.code,
    categoryCode: selectedCategory.code,
    severityCode: selectedSeverityLevel.code,
  });
  const { caseId } = await client.send(command);
  return caseId;
};
```

```
// Get a list of open support cases created today.
export const getTodaysOpenCases = async () => {
  const d = new Date();
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
  });

  const { cases } = await client.send(command);

  if (cases.length === 0) {
    throw new Error(
      "Unexpected number of cases. Expected more than 0 open cases.",
    );
  }
  return cases;
};

// Create an attachment set.
export const createAttachmentSet = async () => {
  const command = new AddAttachmentsToSetCommand({
    attachments: [
      {
        fileName: "example.txt",
        data: new TextEncoder().encode("some example text"),
      },
    ],
  });
  const { attachmentSetId } = await client.send(command);
  return attachmentSetId;
};

export const linkAttachmentSetToCase = async (attachmentSetId, caseId) => {
  const command = new AddCommunicationToCaseCommand({
    attachmentSetId,
    caseId,
    communicationBody: "Adding attachment set to case.",
  });
  await client.send(command);
};

// Get all communications for a support case.
```

```
export const getCommunications = async (caseId) => {
  const command = new DescribeCommunicationsCommand({
    caseId,
  });
  const { communications } = await client.send(command);
  return communications;
};

/**
 * @param {import('@aws-sdk/client-support').Communication[]} communications
 */
export const getFirstAttachment = (communications) => {
  const firstCommWithAttachment = communications.find(
    (c) => c.attachmentSet.length > 0,
  );
  return firstCommWithAttachment?.attachmentSet[0].attachmentId;
};

// Get an attachment.
export const getAttachment = async (attachmentId) => {
  const command = new DescribeAttachmentCommand({
    attachmentId,
  });
  const { attachment } = await client.send(command);
  return attachment;
};

// Resolve the case matching the given case ID.
export const resolveCase = async (caseId) => {
  const shouldResolve = await inquirer.confirm({
    message: `Do you want to resolve ${caseId}?`,
  });

  if (shouldResolve) {
    const command = new ResolveCaseCommand({
      caseId: caseId,
    });

    await client.send(command);
    return true;
  }
  return false;
};
```

```
/**
 * Find a specific case in the list of provided cases by case ID.
 * If the case is not found, and the results are paginated, continue
 * paging through the results.
 * @param {{
 *   caseId: string,
 *   cases: import('@aws-sdk/client-support').CaseDetails[]
 *   nextToken: string
 * }} options
 * @returns
 */
export const findCase = async ({ caseId, cases, nextToken }) => {
  const foundCase = cases.find((c) => c.caseId === caseId);

  if (foundCase) {
    return foundCase;
  }

  if (nextToken) {
    const response = await client.send(
      new DescribeCasesCommand({
        nextToken,
        includeResolvedCases: true,
      }),
    );
    return findCase({
      caseId,
      cases: response.cases,
      nextToken: response.nextToken,
    });
  }

  throw new Error(`${caseId} not found.`);
};

// Get all cases created today.
export const getTodaysResolvedCases = async (caseIdToWaitFor) => {
  const d = new Date("2023-01-18");
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
    includeResolvedCases: true,
  });
```

```
  const { cases, nextToken } = await client.send(command);
  await findCase({ cases, caseId: caseIdToWaitFor, nextToken });
  return cases.filter((c) => c.status === "resolved");
};

const main = async () => {
  let caseId;
  try {
    console.log(wrapText("Welcome to the AWS Support basic usage scenario."));

    // Verify that the account is subscribed to support.
    await verifyAccount();

    // Provided a truncated list of services and prompt the user to select one.
    const selectedService = await getService();

    // Provided the categories for the selected service and prompt the user to
 select one.
    const selectedCategory = await getCategory(selectedService);

    // Provide the severity available severity levels for the account and prompt
 the user to select one.
    const selectedSeverityLevel = await getSeverityLevel();

    // Create a support case.
    console.log("\nCreating a support case.");
    caseId = await createCase({
      selectedService,
      selectedCategory,
      selectedSeverityLevel,
    });
    console.log(`Support case created: ${caseId}`);

    // Display a list of open support cases created today.
    const todaysOpenCases = await retry(
      { intervalInMs: 1000, maxRetries: 15 },
      getTodaysOpenCases,
    );
    console.log(
      `\nOpen support cases created today: ${todaysOpenCases.length}`,
    );
    console.log(todaysOpenCases.map((c) => `${c.caseId}`).join("\n"));

    // Create an attachment set.
```

```
    console.log("\nCreating an attachment set.");
    const attachmentSetId = await createAttachmentSet();
    console.log(`Attachment set created: ${attachmentSetId}`);

    // Add the attachment set to the support case.
    console.log(`\nAdding attachment set to ${caseId}`);
    await linkAttachmentSetToCase(attachmentSetId, caseId);
    console.log(`Attachment set added to ${caseId}`);

    // List the communications for a support case.
    console.log(`\nListing communications for ${caseId}`);
    const communications = await getCommunications(caseId);
    console.log(
      communications
        .map(
          (c) =>
            `Communication created on ${c.timeCreated}. Has
${c.attachmentSet.length} attachments.`,
        )
        .join("\n"),
    );

    // Describe the first attachment.
    console.log(`\nDescribing attachment ${attachmentSetId}`);
    const attachmentId = getFirstAttachment(communications);
    const attachment = await getAttachment(attachmentId);
    console.log(
      `Attachment is the file '${
        attachment.fileName
      }' with data: \n${new TextDecoder().decode(attachment.data)}`,
    );

    // Confirm that the support case should be resolved.
    const isResolved = await resolveCase(caseId);
    if (isResolved) {
      // List the resolved cases and include the one previously created.
      // Resolved cases can take a while to appear.
      console.log(
        "\nWaiting for case status to be marked as resolved. This can take some
time.",
      );
      const resolvedCases = await retry(
        { intervalInMs: 20000, maxRetries: 15 },
        () => getTodaysResolvedCases(caseId),
```

```
      );
      console.log("Resolved cases:");
      console.log(resolvedCases.map((c) => c.caseId).join("\n"));
    }
  } catch (err) {
    console.error(err);
  }
};
```

- API 세부 정보는 AWS SDK for JavaScript API 참조의 다음 주제를 참조하십시오.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverity레벨
  - ResolveCase

Kotlin

SDK for Kotlin

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
```

```
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following tasks:
1. Gets and displays available services.
2. Gets and displays severity levels.
3. Creates a support case by using the selected service, category, and severity
 level.
4. Gets a list of open cases for the current day.
5. Creates an attachment set with a generated file.
6. Adds a communication with the attachment to the support case.
7. Lists the communications of the support case.
8. Describes the attachment set included with the communication.
9. Resolves the support case.
10. Gets a list of resolved cases for the current day.
*/

suspend fun main(args: Array<String>) {
    val usage = """
    Usage:
        <fileAttachment>
    Where:
         fileAttachment - The file can be a simple saved .txt file to use as an
 email attachment.
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val fileAttachment = args[0]
    println("***** Welcome to the AWS Support case example scenario.")
    println("***** Step 1. Get and display available services.")
    val sevCatList = displayServices()

    println("***** Step 2. Get and display Support severity levels.")
    val sevLevel = displaySevLevels()

    println("***** Step 3. Create a support case using the selected service,
 category, and severity level.")
```

```
    val caseIdVal = createSupportCase(sevCatList, sevLevel)
    if (caseIdVal != null) {
        println("Support case $caseIdVal was successfully created!")
    } else {
        println("A support case was not successfully created!")
        exitProcess(1)
    }

    println("***** Step 4. Get open support cases.")
    getOpenCase()

    println("***** Step 5. Create an attachment set with a generated file to add
 to the case.")
    val attachmentSetId = addAttachment(fileAttachment)
    println("The Attachment Set id value is $attachmentSetId")

    println("***** Step 6. Add communication with the attachment to the support
 case.")
    addAttachSupportCase(caseIdVal, attachmentSetId)

    println("***** Step 7. List the communications of the support case.")
    val attachId = listCommunications(caseIdVal)
    println("The Attachment id value is $attachId")

    println("***** Step 8. Describe the attachment set included with the
 communication.")
    describeAttachment(attachId)

    println("***** Step 9. Resolve the support case.")
    resolveSupportCase(caseIdVal)

    println("***** Step 10. Get a list of resolved cases for the current day.")
    getResolvedCase()
    println("***** This Scenario has successfully completed")
}

suspend fun getResolvedCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 30
```

```
            afterTime = yesterday.toString()
            beforeTime = now.toString()
            includeResolvedCases = true
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}

suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}

suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
        DescribeCommunicationsRequest {
            caseId = caseIdVal
            maxResults = 10
        }
```

```
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}

suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}

suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal =
        Attachment {
            fileName = myFile.name
            data = sourceBytes
```

```
        }

    val setRequest =
        AddAttachmentsToSetRequest {
            attachments = listOf(attachmentVal)
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}

suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 20
            afterTime = yesterday.toString()
            beforeTime = now.toString()
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun createSupportCase(
    sevCatListVal: List<String>,
    sevLevelVal: String
): String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest =
        CreateCaseRequest {
            categoryCode = caseCategory.lowercase(Locale.getDefault())
```

```
            serviceCode = serCode.lowercase(Locale.getDefault())
            severityCode = sevLevelVal.lowercase(Locale.getDefault())
            communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
            subject = "Test case, please ignore"
            language = "en"
            issueType = "technical"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}

suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}

// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }
```

```
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- API 세부 정보는 AWS SDK for Kotlin API reference의 다음 주제를 참조하세요.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications

- DescribeServices
- DescribeSeverity레벨
- ResolveCase

Python

SDK for Python(Boto3)

> **Note**
>
> 더 많은 정보가 있습니다 GitHub. AWS 코드 예제 리포지토리에서 전체 예제를 찾고 설정 및 실행하는 방법을 배워보세요.

명령 프롬프트에서 대화형 시나리오를 실행합니다.

```
class SupportCasesScenario:
    """Runs an interactive scenario that shows how to get started using AWS
 Support."""

    def __init__(self, support_wrapper):
        """
        :param support_wrapper: An object that wraps AWS Support actions.
        """
        self.support_wrapper = support_wrapper

    def display_and_select_service(self):
        """
        Lists support services and prompts the user to select one.

        :return: The support service selected by the user.
        """
        print("-" * 88)
        services_list = self.support_wrapper.describe_services("en")
        print(f"AWS Support client returned {len(services_list)} services.")
        print("Displaying first 10 services:")

        service_choices = [svc["name"] for svc in services_list[:10]]
        selected_index = q.choose(
            "Select an example support service by entering a number from the
 preceding list:",
```

```
            service_choices,
        )
        selected_service = services_list[selected_index]
        print("-" * 88)
        return selected_service

    def display_and_select_category(self, service):
        """
        Lists categories for a support service and prompts the user to select
one.

        :param service: The service of the categories.
        :return: The selected category.
        """
        print("-" * 88)
        print(
            f"Available support categories for Service {service['name']}
{len(service['categories'])}:"
        )
        categories_choices = [category["name"] for category in
service["categories"]]
        selected_index = q.choose(
            "Select an example support category by entering a number from the
preceding list:",
            categories_choices,
        )
        selected_category = service["categories"][selected_index]
        print("-" * 88)
        return selected_category

    def display_and_select_severity(self):
        """
        Lists available severity levels and prompts the user to select one.

        :return: The selected severity level.
        """
        print("-" * 88)
        severity_levels_list =
self.support_wrapper.describe_severity_levels("en")
        print(f"Available severity levels:")
        severity_choices = [level["name"] for level in severity_levels_list]
        selected_index = q.choose(
            "Select an example severity level by entering a number from the
preceding list:",
```

```
            severity_choices,
        )
        selected_severity = severity_levels_list[selected_index]
        print("-" * 88)
        return selected_severity

    def create_example_case(self, service, category, severity_level):
        """
        Creates an example support case with the user's selections.

        :param service: The service for the new case.
        :param category: The category for the new case.
        :param severity_level: The severity level for the new case.
        :return: The caseId of the new support case.
        """
        print("-" * 88)
        print(f"Creating new case for service {service['name']}.")
        case_id = self.support_wrapper.create_case(service, category,
severity_level)
        print(f"\tNew case created with ID {case_id}.")
        print("-" * 88)
        return case_id

    def list_open_cases(self):
        """
        List the open cases for the current day.
        """
        print("-" * 88)
        print("Let's list the open cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        open_cases = self.support_wrapper.describe_cases(start_time, end_time,
False)
        for case in open_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def create_attachment_set(self):
        """
        Create an attachment set with a sample file.

        :return: The attachment set ID of the new attachment set.
        """
        print("-" * 88)
```

```
        print("Creating attachment set with a sample file.")
        attachment_set_id = self.support_wrapper.add_attachment_to_set()
        print(f"\tNew attachment set created with ID {attachment_set_id}.")
        print("-" * 88)
        return attachment_set_id

    def add_communication(self, case_id, attachment_set_id):
        """
        Add a communication with an attachment set to the case.

        :param case_id: The ID of the case for the communication.
        :param attachment_set_id: The ID of the attachment set to
        add to the communication.
        """
        print("-" * 88)
        print(f"Adding a communication and attachment set to the case.")
        self.support_wrapper.add_communication_to_case(attachment_set_id,
case_id)
        print(
            f"Added a communication and attachment set {attachment_set_id} to the
case {case_id}."
        )
        print("-" * 88)

    def list_communications(self, case_id):
        """
        List the communications associated with a case.

        :param case_id: The ID of the case.
        :return: The attachment ID of an attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attachment_id = ""
        communications =
self.support_wrapper.describe_all_case_communications(case_id)
        for communication in communications:
            print(
                f"\tCommunication created on {communication['timeCreated']} "
                f"has {len(communication['attachmentSet'])} attachments."
            )
            if len(communication["attachmentSet"]) > 0:
                attachment_id = communication["attachmentSet"][0]["attachmentId"]
        print("-" * 88)
```

```
        return attachment_id

    def describe_case_attachment(self, attachment_id):
        """
        Describe an attachment associated with a case.

        :param attachment_id: The ID of the attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attached_file = self.support_wrapper.describe_attachment(attachment_id)
        print(f"\tAttachment includes file {attached_file}.")
        print("-" * 88)

    def resolve_case(self, case_id):
        """
        Shows how to resolve an AWS Support case by its ID.

        :param case_id: The ID of the case to resolve.
        """
        print("-" * 88)
        print(f"Resolving case with ID {case_id}.")
        case_status = self.support_wrapper.resolve_case(case_id)
        print(f"\tFinal case status is {case_status}.")
        print("-" * 88)

    def list_resolved_cases(self):
        """
        List the resolved cases for the current day.
        """
        print("-" * 88)
        print("Let's list the resolved cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        resolved_cases = self.support_wrapper.describe_cases(start_time,
end_time, True)
        for case in resolved_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def run_scenario(self):
        logging.basicConfig(level=logging.INFO, format="%(levelname)s:
%(message)s")
```

```
        print("-" * 88)
        print("Welcome to the AWS Support get started with support cases demo.")
        print("-" * 88)

        selected_service = self.display_and_select_service()
        selected_category = self.display_and_select_category(selected_service)
        selected_severity = self.display_and_select_severity()
        new_case_id = self.create_example_case(
            selected_service, selected_category, selected_severity
        )
        wait(10)
        self.list_open_cases()
        new_attachment_set_id = self.create_attachment_set()
        self.add_communication(new_case_id, new_attachment_set_id)
        new_attachment_id = self.list_communications(new_case_id)
        self.describe_case_attachment(new_attachment_id)
        self.resolve_case(new_case_id)
        wait(10)
        self.list_resolved_cases()

        print("\nThanks for watching!")
        print("-" * 88)


if __name__ == "__main__":
    try:
        scenario = SupportCasesScenario(SupportWrapper.from_client())
        scenario.run_scenario()
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

지원 클라이언트 작업을 래핑하는 클래스를 정의합니다.

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client
```

```
    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services


    def describe_severity_levels(self, language):
```

```
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
```

```
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
support case.",
```

```
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
```

```
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications
```

```
    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
```

```
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
```

```
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 다음 주제를 참조하십시오.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverity레벨
  - ResolveCase

AWS SDK 개발자 가이드 및 코드 예제의 전체 목록은 을 참조하십시오AWS SupportAWS SDK와 함께 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

# AWS Support의 모니터링 및 로깅

AWS Support 및 다른 AWS 솔루션의 안정성, 가용성 및 성능을 유지하려면 모니터링이 중요합니다. AWS는 AWS Support를 모니터링하고, 이상이 있을 때 이를 보고하고, 필요한 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 제공합니다.

- Amazon EventBridge는 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 제공합니다. EventBridge는 특정 이벤트를 감시하는 규칙을 작성하고 이러한 이벤트가 발생할 때 다른 AWS 서비스에서 자동화된 작업을 트리거할 수 있으므로 자동화된 이벤트 기반 컴퓨팅이 가능합니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.
- AWS CloudTrail은 직접 수행하거나 AWS 계정을 대신하여 수행한 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 호출했는지, 어떤 소스 IP 주소에 호출이 이루어졌는지, 언제 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

주제


- Amazon을 통한 AWS Support 사례 모니터링 EventBridge
- AWS CloudTrail을 사용하여 AWS Support API 호출 로깅
- AWS CloudTrail을 사용하여 Slack API의 AWS Support 앱 호출 로깅


## Amazon을 통한 AWS Support 사례 모니터링 EventBridge

EventBridge Amazon을 사용하여 AWS Support 사례의 변경 사항을 감지하고 이에 대응할 수 있습니다. 그런 다음 생성한 규칙에 따라 이벤트가 규칙에 지정한 값과 일치할 때 하나 이상의 대상 작업을 EventBridge 호출합니다.

이벤트에 따라 알림을 보내거나, 이벤트 정보를 캡처하거나, 교정 작업을 수행하거나, 이벤트를 시작하거나, 기타 작업을 수행할 수 있습니다. 예를 들어 계정에서 다음 작업이 발생할 때마다 알림을 받을 수 있습니다.

- 지원 사례 생성
- 기존 지원 사례에 사례 대응 추가
- 지원 사례 해결
- 지원 사례 다시 열기

> **Note**
>
> AWS Support은 최선의 작업을 기반으로 이벤트를 전달합니다. 이벤트가 항상 EventBridge에 전달되도록 보장되는 것은 아닙니다.

## AWS Support 사례에 대한 EventBridge 규칙 생성

EventBridge 규칙을 생성하여 AWS Support 사례 이벤트에 대한 알림을 받을 수 있습니다. 이 규칙은 사용자, IAM 사용자 또는 지원 에이전트가 수행하는 작업을 포함하여 계정의 지원 사례에 대한 업데이트를 모니터링합니다. AWS Support 사례 이벤트에 대한 규칙을 생성하기 전에 다음을 수행해야 합니다.

- 에서 이벤트, 규칙, 대상을 숙지하세요. EventBridge 자세한 내용은 Amazon이란 무엇입니까 EventBridge? 를 참조하십시오. Amazon EventBridge 사용 설명서에서 확인할 수 있습니다.
- 이벤트 규칙에 사용할 대상을 만듭니다. 예를 들어 지원 사례가 업데이트될 때마다 문자 메시지 또는 이메일을 수신하도록 Amazon Simple Notification Service(Amazon SNS) 주제를 만들 수 있습니다. 자세한 내용은 EventBridge 대상을 참조하세요.

> **Note**
>
> AWS Support는 전역적 서비스입니다. 지원 사례에 대한 업데이트를 받으려면 미국 동부(버지니아 북부) 리전, 미국 서부(오레곤) 리전 또는 유럽(아일랜드) 리전 중 하나를 사용할 수 있습니다.

AWS Support케이스 이벤트에 대한 EventBridge 규칙을 만들려면

1. https://console.aws.amazon.com/events/ 에서 아마존 EventBridge 콘솔을 엽니다.
2. 아직 수행하지 않은 경우 페이지 오른쪽 상단에서 리전 선택기를 사용하여 미국 동부(버지니아 북부)를 선택합니다.
3. 탐색 창에서 규칙을 선택합니다.
4. 규칙 생성을 선택합니다.
5. 규칙 세부 정보 정의(Define rule detail) 페이지에서 규칙의 이름과 설명을 입력합니다.
6. 이벤트 버스(Event bus)와 규칙 유형(Rule type)의 기본값을 유지하고 다음(Next)을 선택합니다.

7. 이벤트 패턴 빌드 페이지에서 이벤트 소스로 이벤트 또는 EventBridge 파트너 AWS 이벤트를 선택합니다.
8. 이벤트 패턴(Event pattern)에서 AWS 서비스의 기본값을 유지합니다.
9. AWS 서비스에서 지원(Support)를 선택합니다.
10. 이벤트 유형(Event type)에서 지원 사례 업데이트(Support Case Update)를 선택합니다.
11. 다음을 선택합니다.
12. 대상 선택(Select targets) 섹션에서 이 규칙에 대해 만든 대상을 선택한 후 해당 유형에 필요한 모든 추가 옵션을 구성합니다. 예를 들어 Amazon SNS를 선택하는 경우 이메일이나 SMS를 통해 알림을 받을 수 있도록 SNS 주제가 올바르게 구성되어 있는지 확인합니다.
13. 다음을 선택합니다.
14. (선택 사항) 태그 구성(Configure tags) 페이지에서 태그를 추가하고 다음(Next)을 선택합니다.
15. 검토 및 생성(Review and create) 페이지에서 규칙 설정을 검토하여 이벤트 모니터링 요구 사항을 충족하는지 확인합니다.
16. 규칙 생성(Create rule)을 선택합니다. 이제 규칙이 AWS Support 사례 이벤트를 모니터링한 다음 지정한 대상에 이벤트를 보냅니다.

> **참고**
>
> - 이벤트를 수신하면 사용자 또는 AWS Support 에이전트가 지원 사례에 사례 대응을 추가했는지 여부를 확인하는 `origin` 파라미터를 사용할 수 있습니다. `origin`의 값은 `CUSTOMER` 또는 `AWS`가 될 수 있습니다.
>
>   현재 `AddCommunicationToCase` 작업에 대한 이벤트만 이 값을 갖습니다.
> - 이벤트 패턴 생성에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 이벤트 패턴을 참조하십시오.
> - CloudTrail이벤트 유형을 통해 AWS API 호출에 대한 다른 규칙을 생성할 수도 있습니다. 이 규칙은 계정에서 AWS Support API 호출에 대한 AWS CloudTrail 로그를 모니터링합니다.

## AWS Support 이벤트 예제

다음 이벤트는 계정에서 지원 작업이 발생할 때 생성됩니다.

Example : 지원 사례 생성

지원 사례가 생성되면 다음 이벤트가 생성됩니다.

```
{
    "version": "0",
    "id": "3433df007-9285-55a3-f6d1-536944be45d7",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "CreateCase",
        "origin": ""
    }
}
```

Example : 지원 사례 업데이트

AWS Support에서 지원 사례에 회신할 때 다음 이벤트가 생성됩니다.

```
{
    "version": "0",
    "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
        "event-name": "AddCommunicationToCase",
        "origin": "AWS"
    }
}
```

Example : 지원 사례 해결

지원 사례가 해결되면 다음 이벤트가 생성됩니다.

```
{
    "version": "0",
    "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ResolveCase",
        "origin": ""
    }
}
```

Example : 지원 사례 다시 열기

지원 사례를 다시 열면 다음 이벤트가 생성됩니다.

```
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

## 다음 사항도 참조하십시오.

EventBridge with AWS Support 사용 방법에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- 아마존에서 AWS Support API를 자동화하는 방법 EventBridge
- AWS Support사례 활동 알림: 켜짐 GitHub

# AWS CloudTrail을 사용하여 AWS Support API 호출 로깅

AWS Support는 AWS Support에서 사용자, 역할, 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail와 통합됩니다. CloudTrail은 AWS Support에 대한 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Support 콘솔로부터의 호출과 AWS Support API 작업에 대한 코드 호출이 포함됩니다.

추적을 생성하면 AWS Support에 대한 이벤트를 포함한 CloudTrail 이벤트를 Amazon Simple Storage Service(Amazon S3) 버킷에 지속적으로 전송할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 Event history(이벤트 기록)에서 최신 이벤트를 볼 수 있습니다.

CloudTrail에서 수집한 정보를 사용하여 AWS Support에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

구성 및 사용 방법을 포함하여 CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

## CloudTrail의 AWS Support 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. 지원되는 이벤트 활동이 AWS Support에서 발생하면, 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

AWS Support에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요

- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 수신 및 여러 계정에서 CloudTrail 로그 파일 수신

모든 AWS Support API 작업은 CloudTrail이 기록하고 AWS Support API 참조에 문서화됩니다.

예를 들어, `CreateCase`, `DescribeCases` 및 `ResolveCase` 작업에 대한 호출은 CloudTrail 로그 파일의 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 했는지.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

또한 여러 AWS 리전 및 여러 AWS 계정의 AWS Support 로그 파일을 하나의 Amazon S3 버킷으로 통합할 수도 있습니다.

## CloudTrail 로그 기록의 AWS Trusted Advisor 정보

Trusted Advisor는 비용 절감, 보안 강화, 계정 최적화를 위해 AWS 계정을 검사하는 데 사용할 수 있는 AWS Support 서비스입니다.

모든 Trusted Advisor API 작업은 CloudTrail이 기록하고 AWS Support API 참조에 문서화됩니다.

예를 들어, `DescribeTrustedAdvisorCheckRefreshStatuses`, `DescribeTrustedAdvisorCheckResult` 및 `RefreshTrustedAdvisorCheck` 작업에 대한 호출은 CloudTrail 로그 파일의 항목을 생성합니다.

> **Note**
>
> CloudTrail은 Trusted Advisor 콘솔 작업도 로그합니다. 를 AWS Trusted Advisor 사용하여 콘솔 작업 로깅 AWS CloudTrail 단원을 참조하세요.

# AWS Support 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 의미합니다. 여기에는 요청된 작업에 대한 정보, 작업 날짜 및 시간, 요청 파라미터 등이 포함됩니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

Example : CreateCase에 대한 로그 항목

다음 예제는 CreateCase 작업에 대한 CloudTrail 로그 항목을 보여줍니다.


```
{
   "Records": [
      {
         "eventVersion": "1.04",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/janedoe",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "janedoe",
            "sessionContext": {
               "attributes": {
                  "mfaAuthenticated": "false",
                  "creationDate": "2016-04-13T17:51:37Z"
               }
            },
            "invokedBy": "signin.amazonaws.com"
         },
         "eventTime": "2016-04-13T18:05:53Z",
         "eventSource": "support.amazonaws.com",
         "eventName": "CreateCase",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "198.51.100.15",
         "userAgent": "signin.amazonaws.com",
         "requestParameters": {
            "severityCode": "low",
            "categoryCode": "other",
            "language": "en",
            "serviceCode": "support-api",
            "issueType": "technical"
```

```
        },
        "responseElements": {
           "caseId": "case-111122223333-muen-2016-c3f2077e504940f2"
        },
        "requestID": "58c257ef-01a2-11e6-be2a-01c031063738",
        "eventID": "5aa34bfc-ad5b-4fb1-8a55-2277c86e746a",
        "eventType": "AwsApiCall",
        "recipientAccountId": "111122223333"
      }
   ],
   ...
}
```

Example : RefreshTrustedAdvisorCheck에 대한 로그 항목

다음 예제는 RefreshTrustedAdvisorCheck 작업에 대한 CloudTrail 로그 항목을 보여 줍니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Admin"
    },
    "eventTime": "2020-10-21T16:34:13Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "RefreshTrustedAdvisorCheck",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "checkId": "Pfx0RwqBli"
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

# AWS CloudTrail을 사용하여 Slack API의 AWS Support 앱 호출 로깅

Slack의 AWS Support 앱은 AWS CloudTrail과 통합됩니다. CloudTrail은 AWS Support 앱에서 사용자, 역할 또는 AWS 서비스가 수행한 작업 기록을 제공합니다. 이 기록을 생성하기 위해 CloudTrail은 AWS Support 앱에 대한 모든 퍼블릭 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Support 앱 콘솔로부터의 호출과 AWS Support 앱 퍼블릭 API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 여기에는 AWS Support 앱에 대한 이벤트가 포함됩니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집하는 정보를 사용하여 AWS Support 앱에 대한 요청을 확인할 수 있습니다. 또한 어떤 IP 주소에서 호출했는지, 누가 언제 요청했는지 등의 추가 세부 정보도 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

## CloudTrail의 AWS Support 앱 정보

AWS 계정를 생성할 때 계정에서 CloudTrail을 활성화합니다. AWS Support 앱에서 퍼블릭 API 활동이 발생하면 해당 활동이 이벤트 기록(Event history)의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

AWS Support 앱에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 지역에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

CloudTrail은 모든 퍼블릭 AWS Support 앱 작업을 로깅합니다. 이러한 조치는 Slack API의 AWS Support 앱 참조에도 설명되어 있습니다. 예를 들어 `CreateSlackChannelConfiguration`, `GetAccountAlias`, `UpdateSlackChannelConfiguration` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 했는지.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

## AWS Support 앱 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 정렬된 스택 트레이스가 아닙니다. 즉, 로그가 특정 순서로 표시되지 않습니다.

Example : **`CreateSlackChannelConfiguration`**에 대한 로그 예

다음 예제는 CreateSlackChannelConfiguration 작업에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:JaneDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Administrator/JaneDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Administrator",
                "accountId": "111122223333",
                "userName": "Administrator"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-26T01:37:57Z",
```

```
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-02-26T01:48:20Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "CreateSlackChannelConfiguration",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
        "notifyOnCreateOrReopenCase": true,
        "teamId": "T012ABCDEFG",
        "notifyOnAddCorrespondenceToCase": true,
        "notifyOnCaseSeverity": "all",
        "channelName": "troubleshooting-channel",
        "notifyOnResolveCase": true,
        "channelId": "C01234A5BCD",
        "channelRoleArn": "arn:aws:iam::111122223333:role/AWSSupportAppRole"
    },
    "responseElements": null,
    "requestID": "d06df6ca-c233-4ffb-bbff-63470c5dc255",
    "eventID": "0898ce29-a396-444a-899d-b068f390c361",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : **`ListSlackChannelConfigurations`**에 대한 로그 예

다음 예제는 ListSlackChannelConfigurations 작업에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:AWSSupportAppRole",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
```

```
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:06:32Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:06:46Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "ListSlackChannelConfigurations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.131",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "20f81d63-31c5-4351-bd02-9eda7f76e7b8",
    "eventID": "70acb7fe-3f84-47cd-8c28-cc148ad06d21",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example : **`GetAccountAlias`**에 대한 로그 예

다음 예제는 GetAccountAlias 작업에 대한 CloudTrail 로그 항목을 보여줍니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:devdsk",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole/devdsk",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
```

```
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:31:27Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:31:47Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "GetAccountAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.142",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a225966c-0906-408b-b8dd-f246665e6758",
    "eventID": "79ebba8d-3285-4023-831a-64af7de8d4ad",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

# AWS Support 플랜의 모니터링 및 로깅

Support 플랜 및 다른 AWS 솔루션의 안정성, 가용성 및 성능을 유지하려면 모니터링이 중요합니다. AWS는 Support 플랜을 모니터링하고, 이상이 있을 때 이를 보고하고, 필요한 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 제공합니다.

- AWS CloudTrail은 직접 수행하거나 AWS 계정을 대신하여 수행한 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 호출했는지, 어떤 소스 IP 주소에 호출이 이루어졌는지, 언제 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

주제

- AWS CloudTrail을 사용하여 AWS Support 플랜 API 호출 로깅

# AWS CloudTrail을 사용하여 AWS Support 플랜 API 호출 로깅

AWS Support 플랜은 사용자, 역할, 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 AWS Support 플랜에 대한 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Support 플랜 콘솔로부터의 호출과 AWS Support 플랜 API 작업에 대한 호출이 포함됩니다.

추적을 생성하면 AWS Support 플랜에 대한 이벤트를 포함한 CloudTrail 이벤트를 Amazon Simple Storage Service(S3) 버킷에 지속적으로 전송할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다.

CloudTrail에서 수집한 정보를 사용하여 AWS Support 플랜에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

구성 및 사용 방법을 포함하여 CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

## CloudTrail의 AWS Support 플랜 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. 지원되는 이벤트 활동이 AWS Support 플랜에서 발생하면, 해당 활동이 이벤트 기록(Event history)의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

AWS Support 플랜에 대한 이벤트를 포함하여 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 수신 및 여러 계정에서 CloudTrail 로그 파일 수신

모든 AWS Support 플랜 API 작업이 CloudTrail에서 로깅됩니다. 모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 했는지.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

여러 AWS 리전 및 여러 계정의 AWS Support 플랜 로그 파일을 하나의 Amazon S3 버킷으로 통합할 수도 있습니다.

## AWS Support 플랜 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 의미합니다. 여기에는 요청된 작업에 대한 정보, 작업 날짜 및 시간, 요청 파라미터 등이 포함됩니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

Example : **`GetSupportPlan`**에 대한 로그 항목

다음 예제는 `GetSupportPlan` 작업에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:11Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlan",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7665c39a-d6bf-4d0d-8010-2f59740b8ecb",
    "eventID": "b711bc30-16a5-4579-8f0d-9ada8fe6d1ce",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

### Example : **GetSupportPlanUpdateStatus**에 대한 로그 항목

다음 예제는 GetSupportPlanUpdateStatus 작업에 대한 CloudTrail 로그 항목을 보여줍니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:02Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlanUpdateStatus",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "responseElements": null,
    "requestID": "75e5c767-8703-4ed3-b01e-4dda28020322",
    "eventID": "28d1c0e3-ccb6-4fd1-8793-65be010114cc",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : **StartSupportPlanUpdate**에 대한 로그 항목

다음 예제는 StartSupportPlanUpdate 작업에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:38:55Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "StartSupportPlanUpdate",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "98add111-dcc9-464d-8722-438d697fe242",
        "update": {
            "supportLevel": "BASIC"
        }
    },
```

```
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "requestID": "e5ff9382-5fb8-4764-9993-0f33fb0b1e17",
    "eventID": "5dba89f8-2e5b-42b9-9b8f-395580c52962",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example : **`CreateSupportPlanSchedule`**에 대한 로그 항목

다음 예제는 `CreateSupportPlanSchedule` 작업에 대한 CloudTrail 로그 항목을 보여줍니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-09T16:30:04Z",
    "eventSource": "supportplans.amazonaws.com",
```

```
    "eventName": "CreateSupportPlanSchedule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "b998de5e-ad1c-4448-90db-2bf86d6d9e9a",
        "scheduleCreationDetails": {
            "startLevel": "BUSINESS",
            "startOffer": "TrialPlan7FB93B",
            "startTimestamp": "2023-06-03T17:23:56.109Z",
            "endLevel": "BUSINESS",
            "endOffer": "StandardPlan2074BB",
            "endTimestamp": "2023-09-03T17:23:55.109Z"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanschedule/
b9a9a4336a3974950a6e670f7dab79b77a4b104db548a0d57050ce4544721d4b"
    },
    "requestID": "150450b8-e61a-4b15-93a8-c3b557a1ca48",
    "eventID": "a2a1ba44-610d-4dc8-bf16-29f1635b57a9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


## AWS Support 계획에 대한 변경 사항 로깅

> **Important**
>
> 2022년 8월 3일부터 다음 작업은 더 이상 사용되지 않고 새 CloudTrail 로그에 표시되지 않습니다. 지원되는 작업 목록은 AWS Support 플랜 로그 파일 항목 이해 항목을 참조하십시오.

- `DescribeSupportLevelSummary` - 이 작업은 Support 플랜 페이지를 열 때 로그에 나타납니다.

- `UpdateProbationAutoCancellation` - 개발자 지원 또는 비즈니스 지원에 가입한 후 30일 이내에 취소를 시도하면 해당 기간이 끝날 때 플랜이 자동으로 취소됩니다. 이 작업은 Support 플랜 페이지에 나타나는 배너에서 자동 취소 거부(Opt-out of automatic cancellation)를 선택하면 로그에 나타납니다. 개발자 지원 또는 비즈니스 지원에 대한 플랜을 재개하게 됩니다.
- `UpdateSupportLevel` - 이 작업은 Support 플랜을 변경할 때 로그에 나타납니다.

> **Note**
>
> `eventSource` 필드에는 해당 작업에 대한 `support-subscription.amazonaws.com` 네임스페이스가 있습니다.

Example : DescribeSupportLevelSummary에 대한 로그 항목

다음 예제는 `DescribeSupportLevelSummary` 작업에 대한 CloudTrail 로그 항목을 표시합니다.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:07Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "DescribeSupportLevelSummary",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
```

```
  },
  "responseElements": null,
  "requestID": "b423b84d-829b-4090-a239-2b639b123abc",
  "eventID": "e1eeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Example : UpdateProbationAutoCancellation에 대한 로그 항목

다음 예제는 UpdateProbationAutoCancellation 작업에 대한 CloudTrail 로그 항목을 표시합니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2021-01-07T23:28:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateProbationAutoCancellation",
  "awsRegion": "us-east-1", "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "5492206a-e200-4c33-9fcf-4162d4123abc",
  "eventID": "f4a58c09-0bb0-4ba2-a8d3-df6909123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Example : UpdateSupportLevel에 대한 로그 항목

다음 예제는 UpdateSupportLevel 작업을 개발자 지원으로 변경하는 CloudTrail 로그 항목을 보여 줍니다.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.247",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "supportLevel": "new_developer"
  },
  "responseElements": {
    "aispl": false,
    "supportLevel": "new_developer"
  },
  "requestID": "5df3da3a-61cd-4a3c-8f41-e5276b123abc",
  "eventID": "c69fb149-c206-47ce-8766-8df6ec123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

# AWS Trusted Advisor의 모니터링 및 로깅

Trusted Advisor 및 다른 AWS 솔루션의 안정성, 가용성 및 성능을 유지하려면 모니터링이 중요합니다. AWS는 Trusted Advisor를 모니터링하고, 이상이 있을 때 이를 보고하고, 필요한 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 제공합니다.

- Amazon EventBridge는 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 제공합니다. EventBridge는 특정 이벤트를 감시하는 규칙을 작성하고 이러한 이벤트가 발생할 때 다른 AWS 서비스에서 자동화된 작업을 트리거할 수 있으므로 자동화된 이벤트 기반 컴퓨팅이 가능합니다.

  예를 들어 Trusted Advisor에서는 Amazon S3 버킷 권한 검사를 제공합니다. 이 점검은 열린 액세스 권한이 있거나 인증된 AWS 사용자에 대한 액세스를 허용하는 버킷이 있는지 여부를 식별합니다. 버킷 권한이 변경되면 Trusted Advisor 검사의 상태가 변경됩니다. EventBridge에서는 이 이벤트를 감지한 다음, 조치를 취할 수 있도록 알림을 보냅니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하세요.
- AWS Trusted Advisor 검사는 비용을 절감하고 성능을 향상시키며 AWS 계정의 보안을 강화할 수 있는 방법을 파악합니다. EventBridge를 사용하여 Trusted Advisor 점검 상태를 모니터링할 수 있습니다. 그런 다음 Amazon CloudWatch를 사용하여 Trusted Advisor 지표에 경보를 생성할 수 있습니다. 이러한 경보는 업데이트된 리소스 또는 서비스 할당량에 도달한 것과 같이 Trusted Advisor 검사에 대한 상태가 변경될 때 사용자에게 알립니다.
- AWS CloudTrail은 직접 수행하거나 AWS 계정을 대신하여 수행한 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 호출했는지, 어떤 소스 IP 주소에 호출이 이루어졌는지, 언제 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

주제

- Amazon을 통한 AWS Trusted Advisor 검사 결과 모니터링 EventBridge
- AWS Trusted Advisor 지표를 모니터링하여 Amazon CloudWatch 경보 생성
- 를 AWS Trusted Advisor 사용하여 콘솔 작업 로깅 AWS CloudTrail

# Amazon을 통한 AWS Trusted Advisor 검사 결과 모니터링 EventBridge

상태를 확인하는 시기를 감지하는 EventBridge 데 사용할 수 있습니다. Trusted Advisor 그런 다음 생성한 규칙에 따라 상태가 규칙에 지정된 값으로 변경될 때 하나 이상의 대상 작업을 EventBridge 호출합니다.

상태 변경에 따라 알림을 보내거나, 상태 정보를 캡처하거나, 교정 작업을 수행하거나, 이벤트를 시작하거나, 기타 작업을 수행할 수 있습니다. 예를 들어 문제가 감지되지 않음(녹색)에서 권장 조치(빨간색)로 검사 상태가 변경되는 경우 다음 대상 유형을 지정할 수 있습니다.

- AWS Lambda 함수를 사용하여 Slack 채널에 알림을 전달합니다.
- 검사에 대한 데이터를 Amazon Kinesis stream으로 푸시하여 포괄적인 실시간 상태 모니터링을 지원합니다.
- Amazon Simple Notification Service 주제를 이메일로 보냅니다.
- Amazon CloudWatch 알람 조치로 알림을 받으세요.

Lambda 함수를 사용하여 EventBridge 응답을 자동화하는 방법에 Trusted Advisor 대한 자세한 내용은 의 도구를 참조하십시오. Trusted Advisor GitHub

> **참고**
>
> - Trusted Advisor은 최선의 작업을 기반으로 이벤트를 전달합니다. 이벤트가 항상 EventBridge에 전달되도록 보장되는 것은 아닙니다.
> - Trusted Advisor 검사 규칙을 만들려면 Business, Enterprise On-Ramp 또는 Enterprise AWS Support 계획을 이용해야 합니다. 자세히 알아보려면 AWS Support 플랜 변경의 내용을 참조하세요.
> - 글로벌 서비스처럼 Trusted Advisor 모든 이벤트는 미국 동부 (버지니아 EventBridge 북부) 지역으로 전송됩니다.

다음 절차에 따라 EventBridge 규칙을 생성하십시오. Trusted Advisor 이벤트 규칙을 생성하기 전에 다음을 수행해야 합니다.

- 에서 이벤트, 규칙, 대상을 숙지하세요. EventBridge 자세한 내용은 Amazon이란 무엇입니까 EventBridge? 를 참조하십시오. Amazon EventBridge 사용 설명서에서 확인할 수 있습니다.

- 이벤트 규칙에 사용할 대상을 생성합니다.

에 대한 EventBridge 규칙을 만들려면 Trusted Advisor

1. https://console.aws.amazon.com/events/ 에서 아마존 EventBridge 콘솔을 엽니다.
2. 리전을 변경하려면 페이지의 오른쪽 상단에 있는 리전 선택기를 사용하고 미국 동부(버지니아 북부)를 선택합니다.
3. 탐색 창에서 규칙을 선택합니다.
4. 규칙 생성을 선택합니다.
5. 규칙 세부 정보 정의(Define rule detail) 페이지에서 규칙의 이름과 설명을 입력합니다.
6. 이벤트 버스(Event bus)와 규칙 유형(Rule type)의 기본값을 유지하고 다음(Next)을 선택합니다.
7. 이벤트 패턴 빌드 페이지에서 이벤트 소스로 이벤트 또는 EventBridge 파트너 AWS 이벤트를 선택합니다.
8. 이벤트 패턴(Event pattern)에서 AWS 서비스의 기본값을 유지합니다.
9. AWS 서비스에는 Trusted Advisor를 선택합니다.
10. 이벤트 유형(Event type)에서 항목 새로 고침 상태 검사(Check Item Refresh Status)를 선택합니다.
11. 검사 상태에 대해 다음 옵션 중 하나를 선택합니다.
    - 모든 상태(Any status)를 선택하여 상태 변경을 모니터링하는 규칙을 생성합니다.
    - 특정 상태(Specific status(es))를 선택한 후 규칙에서 모니터링할 값을 선택합니다.
        - ERROR – Trusted Advisor가 검사에 대한 작업을 권장합니다.
        - INFO – Trusted Advisor가 검사 상태를 확인할 수 없습니다.
        - OK – Trusted Advisor가 검사에서 문제를 감지하지 않습니다.
        - WARN – Trusted Advisor가 검사에 발생 가능한 문제를 감지하고 조사를 권장합니다.
12. 검사에 대해 다음 옵션 중 하나를 선택합니다.
    - 모든 검사(Any check)를 선택합니다.
    - 특정 검사(Specific check(s))를 선택한 후 목록에서 검사 이름을 한 개 이상 선택합니다.
13. AWS 리소스에서 다음 옵션 중 하나를 선택합니다.
    - 모든 리소스 ID(Any resource ID)을 선택하여 모든 리소스를 모니터링하는 규칙을 만듭니다.
    - ARN별 특정 리소스 ID(Specific resource ID(s) by ARN)를 선택한 후 원하는 Amazon 리소스 이름 (ARN)을 입력합니다.

14. 다음을 선택합니다.
15. 대상 선택(Select targets) 페이지에서 이 규칙에 대해 생성한 대상 유형을 선택한 후, 해당 유형에 필요한 모든 추가 옵션을 구성합니다. 예를 들어 이벤트를 Amazon SQS 대기열 또는 Amazon SNS 주제로 보낼 수 있습니다.
16. 다음을 선택합니다.
17. (선택 사항) 태그 구성(Configure tags) 페이지에서 태그를 추가하고 다음(Next)을 선택합니다.
18. 검토 및 생성(Review and create) 페이지에서 규칙 설정을 검토하여 이벤트 모니터링 요구 사항을 충족하는지 확인합니다.
19. 규칙 생성(Create rule)을 선택합니다. 이제 규칙이 Trusted Advisor 검사를 모니터링한 다음 지정한 대상에 이벤트를 보냅니다.

# AWS Trusted Advisor 지표를 모니터링하여 Amazon CloudWatch 경보 생성

AWS Trusted Advisor에서 검사를 새로 고치면 Trusted Advisor는 검사 결과에 대한 지표를 CloudWatch에 게시합니다. CloudWatch에서 이러한 지표를 검토할 수 있습니다. 또한 경보를 생성하여 Trusted Advisor 검사에 대한 상태 변경, 리소스에 대한 상태 변경, 서비스 할당량 사용(이전에는 제한이라고 지칭)을 감지할 수 있습니다. 예를 들어 서비스 한도(Service Limits) 범주에서 검사의 상태 변경을 추적하는 경보를 생성할 수 있습니다. 그러면 경보가 AWS 계정의 서비스 할당량에 도달하거나 할당량을 초과할 때 사용자에게 알립니다.

다음 절차에 따라 특정 Trusted Advisor 지표에 대한 CloudWatch 경보를 생성하세요.

주제


- 필수 조건
- Trusted Advisor의 CloudWatch 지표
- Trusted Advisor 지표 및 차원


## 필수 조건

Trusted Advisor 지표에 대한 CloudWatch 경보를 생성하기 전에 다음 정보를 검토하세요.

- CloudWatch가 지표 및 경보를 사용하는 방식을 이해하세요. 자세한 내용은 Amazon CloudWatch 사용 설명서의 CloudWatch 작동 방법을 참조하세요.

- Trusted Advisor 콘솔 또는AWS Support API를 사용하여 검사를 새로 고치고 최신 검사 결과를 얻을 수 있습니다. 자세한 내용은 검사 결과 새로 고침 단원을 참조하세요,

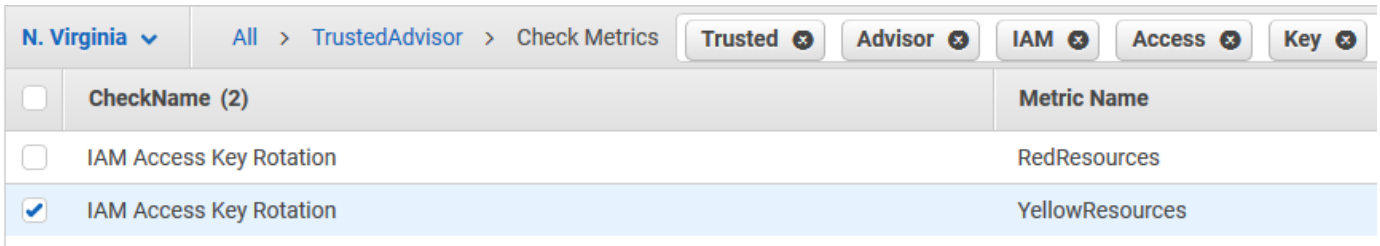
Trusted Advisor 지표에 대한 CloudWatch 경보를 생성하려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 여세요.
2. 리전 선택기(Region selector)를 사용해 미국 동부(버지니아 북부)(US East (N. Virginia)) AWS 리전을 선택하세요.
3. 탐색 창에서 경보(Alarms)를 선택하세요.
4. 경보 생성(Create alarm)을 선택하세요.
5. 지표 선택(Select metric)을 선택하세요.
6. 지표(Metrics)에서, 지표 목록을 필터링할 차원 값을 하나 이상 입력하세요. 예를 들어 지표 이름 ServiceLimitUsage 또는 차원(예: Trusted Advisor 검사 이름)을 입력할 수 있습니다.

   > **Tip**
   >
   > - **`Trusted Advisor`**를 검색하여 서비스에 대한 모든 지표를 나열할 수 있습니다.
   > - 사용 가능한 지표와 차원 이름의 목록은 Trusted Advisor 지표 및 차원를 참조하세요.

7. 결과 표에서 원하는 지표가 있는 선택 상자를 선택합니다.

   다음 예제에서 검사 이름은 IAM 액세스 키 교체이고 지표 이름은YellowResources입니다.

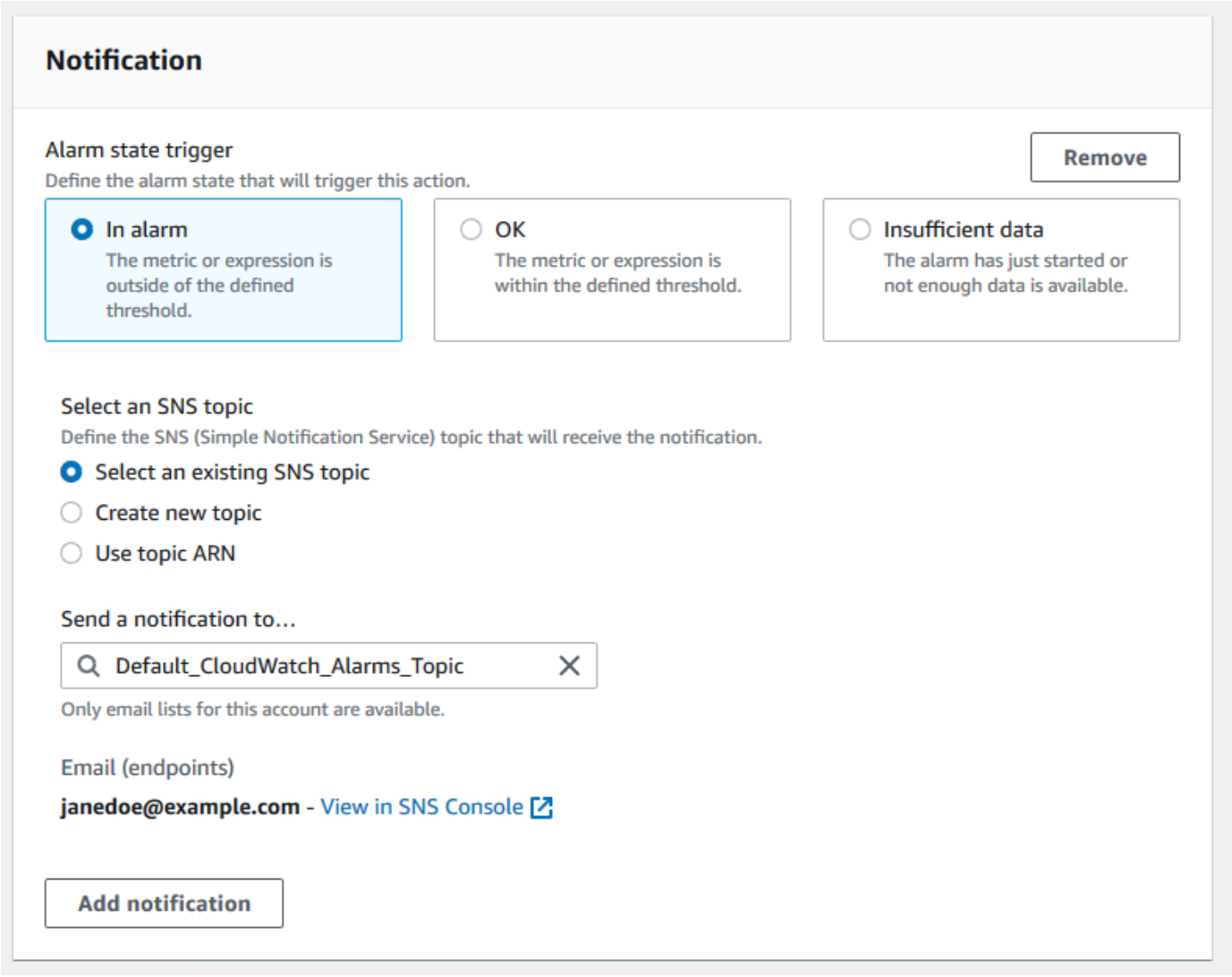



8. 지표 선택(Select metric)을 선택하세요.
9. 지표 및 조건 지정(Specify metric and conditions) 페이지에서, 사용자가 선택한 지표 이름(Metric name) 및 검사 이름(CheckName)이 이 페이지에 나타나는지 확인하세요.
10. 기간(Period)에는 검사 상태가 변경될 때 경보를 시작하는 데 필요한 기간(예: 5분)을 지정할 수 있습니다.
11. 조건(Conditions)에서 고정(Static)을 선택한 다음 경보가 시작되어야 하는 시기에 대한 경보 조건을 선택하세요.

예를 들어, 크거나 같음 >=임계값(Greater/Equal >=threshold)을 선택하고 임계값에 **1**을 입력하면 Trusted Advisor가 지난 90일 동안 교체되지 않은 IAM 액세스 키를 하나 이상 감지했을 때 경보가 시작되는 것을 의미합니다.

> **주의**
>
> - GreenChecks, RedChecks, YellowChecks, RedResources 및 YellowResources 지표에서는 0 이상의 모든 정수로 임계값을 지정할 수 있습니다.
> - Trusted Advisor는 Trusted Advisor가 아무런 문제를 감지하지 못한 리소스인 GreenResources에 대해 지표를 보내지 않습니다.

12. Next를 선택하세요.
13. 작업 구성(Configure actions) 페이지의 경보 상태 트리거(Alarm state trigger)에서 경보 상태(In alarm)를 선택하세요.
14. SNS 주제 선택(Select an SNS topic)에서 기존 Amazon Simple Notification Service(Amazon SNS) 주제를 선택하거나 새로 생성합니다.




15. Next를 선택하세요.
16. 이름 및 설명(Name and Description)에서, 경보에 대한 이름과 설명을 입력하세요.
17. Next를 선택하세요.
18. 미리 보기 및 만들기(Preview and create) 페이지에서 경보 세부 정보를 검토한 다음경보 생성(Create alarm)을 선택하세요.

    IAM 액세스 키 교체(IAM Access Key Rotation) 검사의 상태가 5분 동안 빨간색으로 변경되었다면 경보가 SNS 주제로 알림을 보내게 됩니다.

Example : CloudWatch 경보에 대한 이메일 알림

다음 이메일 메시지는 경보가 IAM 액세스 키 교체 검사에 대한 변경 사항을 감지했음을 보여 줍니다.

```
You are receiving this email because your Amazon CloudWatch Alarm
 "IAMAcessKeyRotationCheckAlarm" in the US East (N. Virginia) region has entered the
 ALARM state,
because "Threshold Crossed: 1 out of the last 1 datapoints [9.0 (26/03/21 22:44:00)]
 was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM
 transition)." at "Friday 26 March, 2021 22:49:42 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAcessKeyRotationCheckAlarm

Alarm Details:
- Name:                       IAMAcessKeyRotationCheckAlarm
- Description:                This alarm starts when one or more AWS access keys in my
 AWS account have not been rotated in the last 90 days.
- State Change:               INSUFFICIENT_DATA -> ALARM
- Reason for State Change:    Threshold Crossed: 1 out of the last 1 datapoints [9.0
 (26/03/21 22:44:00)] was greater than or equal to the threshold (1.0) (minimum 1
 datapoint for OK -> ALARM transition).
- Timestamp:                  Friday 26 March, 2021 22:49:42 UTC
- AWS Account:                123456789012
- Alarm Arn:                  arn:aws:cloudwatch:us-
east-1:123456789012:alarm:IAMAcessKeyRotationCheckAlarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0
 for 300 seconds.

Monitored Metric:
- MetricNamespace:                    AWS/TrustedAdvisor
- MetricName:                         RedResources
- Dimensions:                         [CheckName = IAM Access Key Rotation]
- Period:                             300 seconds
- Statistic:                          Average
- Unit:                               not specified
- TreatMissingData:                   missing


State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:123456789012:Default_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:
```

# Trusted Advisor의 CloudWatch 지표

CloudWatch 콘솔 또는 AWS Command Line Interface(AWS CLI)를 사용하여 Trusted Advisor에 사용할 수 있는 지표를 찾을 수 있습니다.

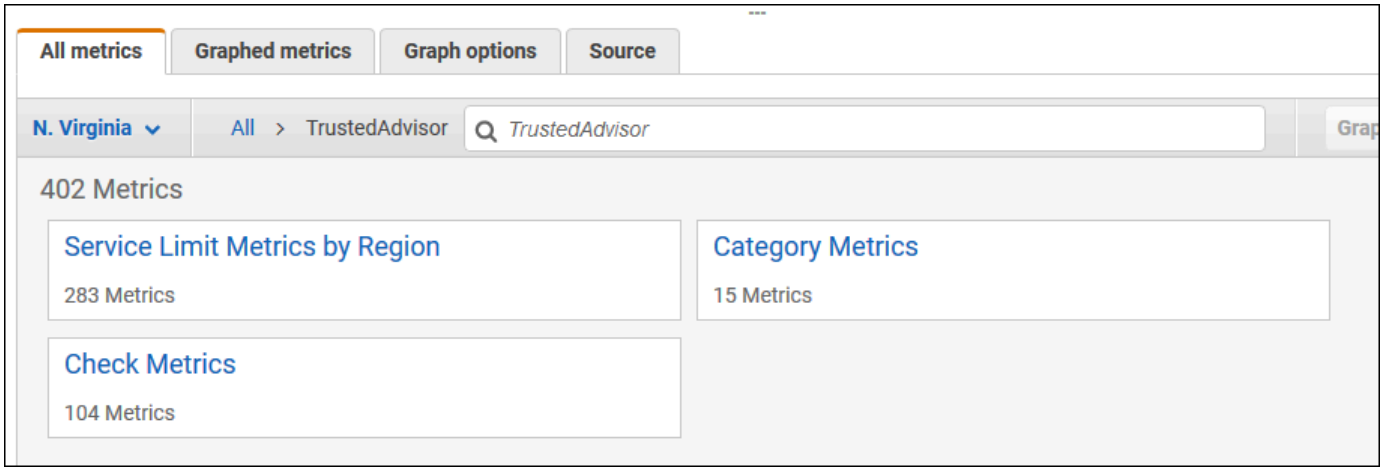
지표를 게시하는 모든 서비스의 네임스페이스, 지표 및 차원 목록은 Amazon CloudWatch 사용 설명서의 CloudWatch 지표를 게시하는 AWS 서비스를 참조하세요.

## Trusted Advisor 지표 보기(콘솔)

CloudWatch 콘솔에 로그인하여 Trusted Advisor에 사용 가능한 지표를 볼 수 있습니다.

사용 가능한 Trusted Advisor 지표를 보려면(콘솔)

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 여세요.
2. 리전 선택기(Region selector)를 사용해 미국 동부(버지니아 북부)(US East (N. Virginia)) AWS 리전을 선택하세요.
3. 탐색 창에서 지표(Metrics)를 선택하세요.
4. **`TrustedAdvisor`** 등의 지표 네임스페이스를 입력하세요.
5. 검사 지표(Check Metrics) 등의 지표 차원을 선택하세요.



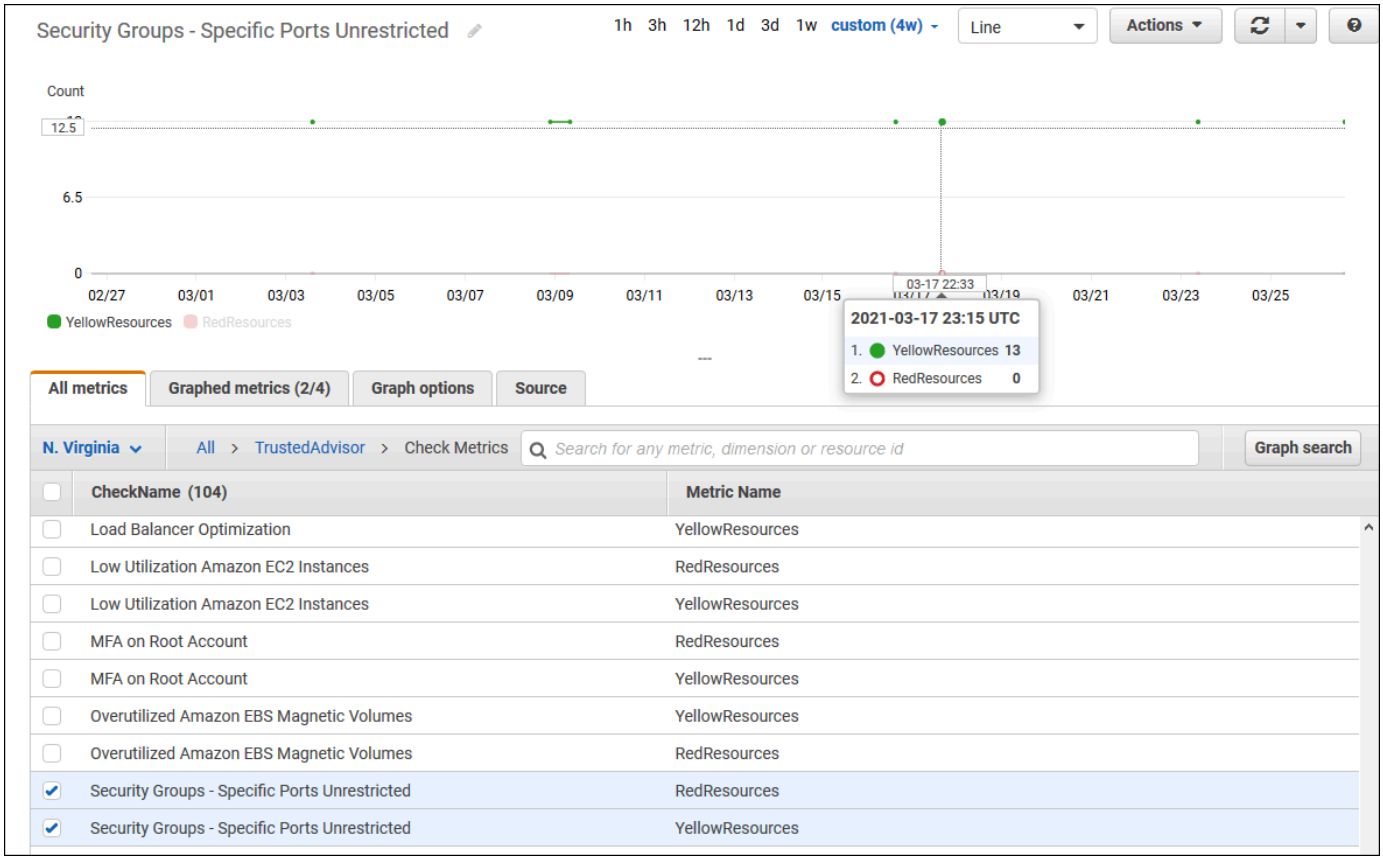

6. 모든 지표(All metrics) 탭에서 네임스페이스의 해당 차원에 대한 지표가 표시됩니다. 다음을 수행할 수 있습니다.

   a. 테이블을 정렬하려면 열 머리글을 선택합니다.

   b. 측정치를 그래프로 표시하려면 측정치 옆에 있는 확인란을 선택하세요. 모든 지표를 선택하려면 테이블의 머리글 행에 있는 확인란을 선택하세요.

   c. 지표로 필터링하려면 지표 이름을 선택한 후 검색에 추가를 선택하세요.

다음 예제는 보안 그룹 - 제한 없는 특정 포트(Security Groups - Specific Ports Unrestricted) 검사의 결과를 보여줍니다. 이 검사는 노란색으로 표시된 13개의 리소스를 식별합니다. Trusted Advisor는 노란색 검사를 조사할 것을 권장합니다.




7. (선택 사항) CloudWatch 대시보드에 이 그래프를 추가하려면 작업(Actions)을 선택한 후 대시보드에 추가(Add to dashboard)를 선택하세요.

   지표를 보기 위해 그래프를 만드는 방법에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 지표 그래프 작성을 참조하세요.

## Trusted Advisor 지표 보기(CLI)

list-metrics AWS CLI 명령을 사용하여 Trusted Advisor에 사용 가능한 지표를 볼 수 있습니다.

Example : Trusted Advisor에 대한 모든 지표 나열

다음 예제는 Trusted Advisor에 대한 모든 지표를 볼 수 있도록 `AWS/TrustedAdvisor` 네임스페이스를 지정합니다.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

출력은 다음과 같을 수 있습니다.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Magnetic (standard) volume storage (TiB)"
                },
                {
                    "Name": "Region",
                    "Value": "ap-northeast-2"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Overutilized Amazon EBS Magnetic Volumes"
                }
            ],
            "MetricName": "YellowResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
```

```
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "eu-west-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "ap-south-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : 차원에 대한 모든 지표 나열

다음 예제에서는 지정된 AWS 리전에 사용 가능한 지표만 보도록 AWS/TrustedAdvisor 네임스페이스와 Region 차원을 지정합니다.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions
 Name=Region,Value=us-east-1
```

출력은 다음과 같을 수 있습니다.

```
{
    "Metrics": [
```

```
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "SES"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Daily sending quota"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "AutoScaling"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Launch configurations"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "CloudFormation"
                },
                {
```

```
                    "Name": "ServiceLimit",
                    "Value": "Stacks"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : 특정 지표 이름에 대한 지표 나열

다음 예제는 이 특정 지표의 결과만 보도록 AWS/TrustedAdvisor 네임스페이스와 RedResources 지표 이름을 지정합니다.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

출력은 다음과 같을 수 있습니다.

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Amazon RDS Security Group Access Risk"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Exposed Access Keys"
                }
```

```
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Large Number of Rules in an EC2 Security Group"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Auto Scaling Group Health Check"
                }
            ],
            "MetricName": "RedResources"
        },
    ...
  ]
}
```

## Trusted Advisor 지표 및 차원

CloudWatch 경보 및 그래프에 사용할 수 있는 Trusted Advisor 지표와 차원은 다음 표를 참조하세요.

### Trusted Advisor 검사 수준 지표

Trusted Advisor 검사에 다음 지표를 사용할 수 있습니다.

| 지표 | 설명 |
| --- | --- |
| RedResources | 빨간색 상태(작업 권장)인 리소스의 수. |
| YellowResources | 노란색 상태(조사 권장)인 리소스의 수. |

## Trusted Advisor 범주 수준 지표

Trusted Advisor 범주에 다음 지표를 사용할 수 있습니다.

| 지표 | 설명 |
| --- | --- |
| GreenChecks | 녹색 상태(발견된 문제가 없음)인 Trusted Advisor 검사의 수. |
| RedChecks | 빨간색 상태(작업 권장)인 Trusted Advisor 검사의 수. |
| YellowChecks | 노란색 상태(조사 권장)인 Trusted Advisor 검사의 수. |

## Trusted Advisor 서비스 할당량 수준 지표

AWS 서비스할당량에 다음 지표를 사용할 수 있습니다:

| 지표 | 설명 |
| --- | --- |
| ServiceLimitUsage | 서비스 할당량(이전에는 제한이라고 지칭)에 대한 리소스 사용량의 백분율입니다. |

## 검사 수준 지표의 차원

Trusted Advisor 검사에서 다음 차원을 사용할 수 있습니다.

| 차원 | 설명 |
| --- | --- |
| CheckName | Trusted Advisor 검사의 이름입니다.<br><br>Trusted Advisor 콘솔 또는 AWS Trusted Advisor 참조 확인에서 모든 검사 이름을 찾을 수 있습니다. |

## 범주 수준 지표의 차원

Trusted Advisor 검사 범주에서 다음 차원을 사용할 수 있습니다.

| 차원 | 설명 |
| --- | --- |
| `Category` | Trusted Advisor 검사 범주의 이름입니다.<br><br>모든 검사 범주를 Trusted Advisor 콘솔 또는 검사 범주 보기 페이지에서 찾을 수 있습니다. |

### 서비스 할당량 지표의 차원

Trusted Advisor 서비스 할당량 지표에 다음 차원을 사용할 수 있습니다.

| 차원 | 설명 |
| --- | --- |
| `Region` | service quota에 대한 AWS 리전입니다. |
| `ServiceName` | AWS 서비스의 이름입니다. |
| `ServiceLimit` | 서비스 할당량의 이름입니다.<br><br>서비스 할당량에 대한 자세한 내용은 AWS 일반 참조의 AWS 서비스 할당량을 참조하세요. |

## 를 AWS Trusted Advisor 사용하여 콘솔 작업 로깅 AWS CloudTrail

Trusted Advisor 에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합됩니다 Trusted Advisor. CloudTrail Trusted Advisor as 이벤트의 작업을 캡처합니다. 캡처된 통화에는 Trusted Advisor 콘솔에서 걸려온 통화가 포함됩니다. 트레일을 생성하면 Amazon Simple Storage Service (Amazon S3) 버킷으로 CloudTrail 이벤트를 지속적으로 전송할 수 있습니다. 여기에는 에 대한 이벤트가 포함됩니다. Trusted Advisor트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람 Trusted Advisor, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

구성 및 활성화 방법을 CloudTrail 포함하여 자세한 내용은 사용 AWS CloudTrail 설명서를 참조하십시오.

# Trusted Advisor 자세한 내용은 CloudTrail

CloudTrail 계정을 만들 때 AWS 계정에서 활성화됩니다. Trusted Advisor 콘솔에서 지원되는 이벤트 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. AWS 계정에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

에 대한 이벤트를 포함하여 AWS 계정에서 진행 중인 이벤트의 기록을 보려면 Trusted Advisor트레일을 생성하세요. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 지역에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 트레일 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

Trusted Advisor Trusted Advisor 콘솔 작업의 일부를 CloudTrail 로그 파일에 이벤트로 기록할 수 있습니다. CloudTrail 다음 작업을 기록합니다.

- `BatchUpdateRecommendationResourceExclusion`
- `CreateEngagement`
- `CreateEngagementAttachment`
- `CreateEngagementCommunication`
- `CreateExcelReport`
- `DescribeAccount`
- `DescribeAccountAccess`
- `DescribeCheckItems`
- `DescribeCheckRefreshStatuses`
- `DescribeCheckSummaries`
- `DescribeChecks`
- `DescribeNotificationPreferences`

- DescribeOrganization
- DescribeOrganizationAccounts
- DescribeReports
- DescribeServiceMetadata
- ExcludeCheckItems
- GenerateReport
- GetEngagement
- GetEngagementAttachment
- GetEngagementType
- GetExcelReport
- GetOrganizationRecommendation
- GetRecommendation
- IncludeCheckItems
- ListAccountsForParent
- ListChecks
- ListEngagementCommunications
- ListEngagementTypes
- ListEngagements
- ListOrganizationRecommendationAccounts
- ListOrganizationRecommendationResources
- ListOrganizationRecommendations
- ListOrganizationalUnitsForParent
- ListRecommendationResources
- ListRecommendations
- ListRoots
- RefreshCheck
- SetAccountAccess
- SetOrganizationAccess
- UpdateEngagement
- UpdateEngagementStatus

- UpdateNotificationPreferences
- UpdateOrganizationRecommendationLifecycle
- UpdateRecommendationLifecycle

Trusted Advisor 콘솔 작업의 전체 목록은 을 참조하십시오Trusted Advisor 액션.

> **Note**
>
> CloudTrail 또한 API 참조에 Trusted AdvisorAWS Support API 작업을 기록합니다. 자세한 내용은 AWS CloudTrail을 사용하여 AWS Support API 호출 로깅 섹션을 참조하세요.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 연동 사용자를 위한 임시 보안 인증으로 요청을 생성하였는지.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail 사용자 ID 요소를 참조하십시오.

## 예: 로그 파일 항목 Trusted Advisor

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일은 하나 이상의 로그 항목을 포함합니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

Example : 로그 항목 대상 RefreshCheck

다음 예제는 Amazon S3 버킷 버전 관리 검사 (IDR365s2Qddf) RefreshCheck 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
```

```
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:06:33Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"RefreshCheck",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.136",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "checkId":"R365s2Qddf"
        },
        "responseElements":{
        "status":{
        "checkId":"R365s2Qddf",
        "status":"enqueued",
        "millisUntilNextRefreshable":3599993
        }
        },
        "requestID":"d23ec729-8995-494c-8054-dedeaEXAMPLE",
        "eventID":"a49d5202-560f-4a4e-b38a-02f1cEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```


Example : 로그 입력 대상 UpdateNotificationPreferences

다음 예제는 UpdateNotificationPreferences 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.


```
{
        "eventVersion":"1.04",
        "userIdentity":{
```

```
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:09:49Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"UpdateNotificationPreferences",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.167",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "contacts":[
        {
        "id":"billing",
        "type":"email",
        "active":false
        },
        {
        "id":"operational",
        "type":"email",
        "active":false
        },
        {
        "id":"security",
        "type":"email",
        "active":false
        }
        ],
        "language":"en"
        },
        "responseElements":null,
        "requestID":"695295f3-c81c-486e-9404-fa148EXAMPLE",
        "eventID":"5f923d8c-d210-4037-bd32-997c6EXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
```

```
        }
```

Example : 로그 입력 대상 GenerateReport

다음 예제는 GenerateReport 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. 이 작업을 수행하면 AWS 조직의 보고서가 생성됩니다.

```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-11-03T13:03:10Z"
        }
        }
        },
        "eventTime":"2020-11-03T13:04:29Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"GenerateReport",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.36.171",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "refresh":false,
        "includeSuppressedResources":false,
        "language":"en",
        "format":"JSON",
        "name":"organizational-view-report",
        "preference":{
        "accounts":[

        ],
        "organizationalUnitIds":[
        "r-j134"
        ],
```

```
        "preferenceName":"organizational-view-report",
        "format":"json",
        "language":"en"
        }
        },
        "responseElements":{
        "status":"ENQUEUED"
        },
        "requestID":"bb866dc1-60af-47fd-a660-21498EXAMPLE",
        "eventID":"2606c89d-c107-47bd-a7c6-ec92fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

# 문제 해결 리소스

일반적인 문제 해결 질문에 대한 답변은 AWS Support 지식 센터를 참조하십시오.

Windows의 경우 Amazon EC2는 고객이 Windows 인스턴스를 검사하여 일반적인 문제를 식별하고, 로그 파일을 수집하고, 문제를 해결하는 데 도움을 주는 AWS Support EC2Rescue를 제공합니다. 또한 작동하지 않는 인스턴스의 부트 볼륨을 분석하는 데 EC2Rescue를 사용할 수도 있습니다. 자세한 내용은 EC2 Windows 인스턴스에서 문제를 해결하고 일반적인 문제를 수정하는 데 EC2Rescue를 사용하는 방법은 무엇입니까?를 참조하세요.

## 서비스별 문제 해결

대부분의 AWS 서비스 설명서에는 문의하기 전에 시작할 수 있는 문제 해결 항목이 포함되어 있습니다. AWS Support다음 표는 서비스별로 정리된 문제 해결 항목에 대한 링크를 제공합니다.

> **Note**
>
> 다음 표에서는 가장 일반적인 서비스의 목록을 확인할 수 있습니다. 그 밖의 문제 해결 관련 주제를 검색하려면 AWS 설명서 랜딩 페이지의 검색 텍스트 상자를 사용하세요.

| Service | 링크 |
| --- | --- |
| Amazon Web Services | AWS 시그니처 버전 4 오류 문제 해결 |
| Amazon API Gateway | HTTP API 관련 문제 해결 |
| 아마존 AppStream | 아마존 문제 해결 AppStream |
| Amazon Athena | Athena의 문제 해결 |
| Amazon Aurora MySQL | Amazon Aurora 문제 해결 |
| Amazon Aurora PostgreSQL | Amazon Aurora 문제 해결 |
| Amazon EC2 Auto Scaling | Auto Scaling 문제 해결 |
| AWS Certificate Manager (ACM) | 문제 해결 |

| Service | 링크 |
| --- | --- |
| AWS CloudFormation | AWS CloudFormation문제 해결 |
| 아마존 CloudFront | 문제 해결 \| RTMP 배포 문제 해결 |
| AWS CloudHSM | 문제 해결 |
| 아마존 CloudSearch | 아마존 문제 해결 CloudSearch |
| AWS CodeDeploy | AWS CodeDeploy문제 해결 |
| 아마존 CloudWatch | https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-metric-streams-troubleshoot.html 문제 해결 |
| AWS Database Migration Service | 의 마이그레이션 작업 문제 해결 AWS Database Migration Service |
| AWS Data Pipeline | 문제 해결 |
| AWS Direct Connect | AWS Direct Connect문제 해결 |
| AWS Directory Service | AWS Directory Service 관리 문제 해결 |
| Amazon DynamoDB | 문제 해결 \| SSL/TLS 연결 설정 문제 해결 |
| AWS Elastic Beanstalk | 문제 해결 |
| Amazon Elastic Compute Cloud(Amazon EC2) | 인스턴스 문제 해결 \| Windows 인스턴스 문제 해결 \| VM Import/Export 문제 해결 \| API 요청 오류 문제 해결 \| AWS 관리 팩 문제 해결\| Microsoft SCVMM용 AWS Systems Manager 문제 해결 \| Microsoft Windows Server용AWS 진단 |
| Amazon Elastic Container Service(Amazon ECS) | Amazon ECS 문제 해결 |
| Amazon Elastic Kubernetes Service(Amazon EKS) | Amazon EKS 문제 해결 |

| Service | 링크 |
| --- | --- |
| Elastic Load Balancing | 애플리케이션 로드 밸런서 문제 해결 \| Classic Load Balancer 문제 해결 |
| ElastiCache 멤캐시드를 위한 Amazon | 애플리케이션 문제 해결 |
| 아마존 포 ElastiCache 레디스용 | 애플리케이션 문제 해결 |
| Amazon EMR | 클러스터 문제 해결 |
| AWS Flow Framework | 문제 해결 및 디버깅 팁 |
| AWS Glue | 문제 해결 AWS Glue |
| AWS Glue DataBrew | AWS Glue DataBrew자격 증명 및 액세스 문제 해결 |
| AWS GovCloud (US) | 문제 해결 |
| AWS Identity and Access Management (IAM) | IAM 문제 해결 |
| Amazon Keyspaces(Apache Cassandra용) | Amazon Keyspaces(Apache Cassandra용) 문제 해결 |
| Amazon Kinesis Data Streams | Amazon Kinesis Data Streams 생산자 문제 해결 \| Amazon Kinesis Data Streams 소비자 문제 해결 |
| Amazon Managed Service for Apache Flink | 성능 문제 해결 \| SQL 애플리케이션용 Amazon Managed Service for Apache Flink 문제 해결 |
| Amazon Data Firehose | Amazon Data Firehose 문제 해결 |
| AWS Lambda | 다음과 같은 문제 해결 및 모니터링 AWS Lambda 기능 CloudWatch |
| 아마존 OpenSearch 서비스 | 아마존 OpenSearch 서비스 문제 해결 |
| AWS OpsWorks | 디버깅 및 문제 해결 안내서 |

| Service | 링크 |
| --- | --- |
| Amazon Personalize | 문제 해결 |
| Amazon QLDB | Amazon QLDB 문제 해결 |
| 아마존 QuickSight | Amazon 문제 해결 QuickSight \| 건너뛰는 행 오류 문제 해결 |
| AWS Resource Access Manager (AWS RAM) | AWS RAM관련 문제 해결 |
| Amazon Redshift | 쿼리 문제 해결 \| 데이터 로드 문제 해결 \| Amazon Redshift의 연결 문제 해결 \| Amazon Redshift 감사 로깅 문제 해결 \| Amazon Redshift Spectrum의 쿼리 문제 해결 |
| Amazon Relational Database Service(Amazon RDS) | 문제 해결 \| Amazon RDS의 애플리케이션 문제 해결 \| Amazon RDS Custom에 대한 DB 문제 해결 |
| Amazon Route 53 | Amazon Route 53 문제 해결 |
| 아마존 SageMaker | 오류 문제 해결 \| Amazon SageMaker 스튜디오 문제 해결 |
| Amazon Silk | 문제 해결 |
| Amazon Simple Email Service(Amazon SES) | Amazon SES 문제 해결 |
| Amazon Simple Storage Service(S3) | 문제 해결 |
| Amazon Simple Workflow Service(Amazon SWF) | AWS Java용 플로우 프레임워크: 문제 해결 및 디버깅 팁 \| Ruby용AWS 플로우 프레임워크: 워크플로 문제 해결 및 디버깅 |
| AWS Storage Gateway | 게이트웨이 문제 해결 |
| AWS Systems Manager | SSM 에이전트 문제 해결 |
| Amazon Virtual Private Cloud(Amazon VPC) | 문제 해결 |

| Service | 링크 |
| --- | --- |
| AWS Virtual Private Network (AWS VPN) | 고객 게이트웨이 디바이스 문제 해결 |
| AWS WAF | 보호 기능 테스트 및 조정 AWS WAF |
| 아마존 WorkMail | Amazon WorkMail 웹 애플리케이션 문제 해결 |
| 아마존 WorkSpaces | Amazon WorkSpaces 문제 해결 \| Amazon WorkSpaces 클라이언트 문제 해결 |

# 문서 기록

다음 표에는 서비스의 마지막 릴리스 이후 설명서에 대한 중요한 변경 사항이 설명되어 있습니다. AWS Support

- AWS Support API 버전: 2013-04-15
- AWS Support 앱 API 버전: 2021-08-20

다음 표에는 2021년 5월 10일부터 적용되는 AWS Support 및 AWS Trusted Advisor 설명서의 중요 업데이트가 설명되어 있습니다. 이제 RSS 피드를 구독하여 업데이트에 관한 알림을 받을 수 있습니다.

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWSTrustedAdvisorServiceRolePolicy 와 관련하여 업데이트된 설명서 | 새 검사를 sqs:GetQueueAttributes 온보딩하기 위한 새 IAM 작업 access-analyzer:ListAnalyzers cloudwatch:ListMetrics dax:DescribeClusters ec2:DescribeNatGateways ec2:DescribeRouteTables ec2:DescribeVpcEndpoints ,ec2:GetManagedPrefixListEntries ,elasticloadbalancing:DescribeTargetHealth ,iam:ListSAMLProviders ,,,, kafka:DescribeClusterV2 network-firewall:ListFirewalls network-firewall:DescribeFi | 2024년 6월 11일 |

| | | |
|---|---|---|
| | rewall 등이 추가되었습니다. 자세한 내용은 AWS 관리형 정책AWSTrustedAdvisorServiceRolePolicy 단원을 참조하십시오. | |
| 권장 사항에 대한 설명서가 추가되었습니다. AWS Support | AWS Support 권장 사항에 대한 설명서가 추가되었습니다. | 2024년 5월 22일 |
| 문서에서 5개의 AWS Trusted Advisor 체크를 제거했습니다. | 지금은 더 이상 AWS Trusted Advisor 사용되지 않는 검사 5개를 제거했습니다. 자세한 내용은 체크를 위한 변경 로그를 참조하십시오. AWS Trusted Advisor | 2024년 5월 15일 |
| 문서에 새 AWS Trusted Advisor 보안 검사 1개를 추가했습니다. | 문서에 새 AWS Trusted Advisor 보안 검사 1개를 추가했습니다. 자세한 내용은 AWS Trusted Advisor 검사를 위한 변경 로그를 참조하십시오. | 2024년 5월 15일 |
| 설명서에서 내결함성 검사 3개를 제거했습니다. | 현재는 더 이상 사용되지 않는 Fault Tolerance 검사 3개를 제거했습니다. 자세한 내용은 검사를 위한 변경 로그를 참조하십시오. AWS Trusted Advisor | 2024년 4월 25일 |
| 내결함성 및 보안 검사 설명서가 업데이트되었습니다. | 내결함성 검사 1개가 새로 추가되었습니다. 내결함성 1개와 보안 검사 1개를 업데이트했습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2024년 3월 29일 |

| | | |
|---|---|---|
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2024년 3월 22일 |
| AWS Support 계획에 대한 업데이트된 설명서 | AWS Support 플랜 기능 업데이트. 자세한 내용은 AWS Support 플랜을 참조하십시오. | 2024년 3월 11일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 내결함성 검사 1개가 추가되었습니다. 자세한 내용은 AWS Trusted Advisor 검사를 위한 변경 로그를 참조하십시오. | 2024년 2월 29일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 내결함성 검사 1개가 추가되었습니다. 자세한 내용은 AWS Trusted Advisor 검사를 위한 변경 로그를 참조하십시오. | 2024년 1월 31일 |
| AWSTrustedAdvisorServiceRolePolicy 에 대한 설명서 업데이트 | 새 검사를 outposts:ListOutposts 온보딩하기 위해 새 IAM 작업 cloudtrail:GetTrail cloudtrail:ListTrails cloudtrail:GetEventSelectors outposts:GetOutpost ,,, outposts:ListAssets 를 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSTrustedAdvisorServiceRolePolicy 단원을 참조하십시오. | 2024년 1월 18일 |

| | | |
|---|---|---|
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2024년 1월 17일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 제목과 설명을 수정하기 위해 내결함성 검사를 1개 업데이트했습니다. 자세한 내용은 AWS Trusted Advisor 검사를 위한 변경 로그를 참조하십시오. | 2024년 1월 8일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 지원 중단 기간의 변경을 반영하여 보안 검사 1건을 업데이트했습니다. 자세한 내용은 검사를 위한 변경 로그를 참조하십시오. AWS Trusted Advisor | 2023년 12월 21일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 보안 검사 2개와 성능 검사 2개가 추가되었습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2023년 12월 20일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 보안 검사 1개가 추가되었습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2023년 12월 15일 |
| Trusted Advisor Engage 설명서가 업데이트되었습니다. | 이메일 알림 옵션이 변경되어 Trusted Advisor Engage 설명서가 업데이트되었습니다. | 2023년 12월 14일 |

| | | |
|---|---|---|
| Trusted Advisor Engage 설명서가 업데이트되었습니다. | 예정된 계약의 변경 사항을 포함하여 Trusted Advisor Engage 설명서가 업데이트되었습니다. | 2023년 12월 11일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 내결함성 검사 2개와 비용 최적화 검사 1개가 새로 추가되었습니다. 자세한 내용은 AWS Trusted Advisor 검사를 위한 변경 로그를 참조하십시오. | 2023년 12월 7일 |
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2023년 12월 6일 |
| 에 대한 AWS 관리형 정책이 업데이트되었습니다. Trusted Advisor | 명령문 ID를 포함하도록 AWSTrustedAdvisorPriorityFullAccess 및 AWSTrustedAdvisorPriorityReadOnlyAccess AWS 관리형 정책을 업데이트했습니다. 자세한 내용은 AWS Trusted Advisor에 대한AWS 관리형 정책을 참조하십시오. | 2023년 12월 6일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 내결함성 검사 3개가 새로 추가되었습니다. 자세한 내용은 AWS Trusted Advisor 검사를 위한 변경 로그를 참조하십시오. | 2023년 11월 17일 |

| | | |
|---|---|---|
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Amazon RDS에 대한 37개의 새로운 검사를 추가했습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2023년 11월 15일 |
| AWSTrustedAdvisorServiceRolePolicy 에 대한 설명서 업데이트 | 새 IAM 작업을 추가하고 새 ec2:DescribeRegions 검사를 s3:GetLifecycleConfiguration ecs:ListTaskDefinitions 온보딩하도록 했습니다. ecs:DescribeTaskDefinition 자세한 내용은 AWS 관리형 정책AWSTrustedAdvisorServiceRolePolicy 단원을 참조하십시오. | 2023년 11월 9일 |
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2023년 10월 27일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 에서 64개의 새 검사를 AWS Config통합했습니다. 자세한 내용은 AWS Trusted Advisor 검사 변경 로그를 참조하십시오. | 2023년 10월 26일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 여섯 개의 새로운 내결함성 체크인을 추가했습니다 Trusted Advisor. 자세한 내용은 AWS Trusted Advisor 체크를 위한 변경 로그를 참조하십시오. | 2023년 10월 12일 |

| | | |
|---|---|---|
| AWSTrustedAdvisorServiceRolePolicy 에 대한 설명서 업데이트 | 새 복원력 검사를 온보딩하기 위해 새 IAM 작업 route53resolver:ListResolverEndpoints , route53resolver:ListResolverEndpointIpAddresses , ec2:DescribeSubnets , kafka:ListClustersV2 및 kafka:ListNodes 을(를) 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSTrustedAdvisorServiceRolePolicy 단원을 참조하십시오. | 2023년 9월 14일 |
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2023년 8월 28일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 에 대한 1개의 새로운 서비스 한도 검사를 추가했습니다 AWS Lambda. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2023년 8월 17일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Lambda에 대한 한 가지 새로운 내결함성 검사를 추가했습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2023년 8월 3일 |

| | | |
|---|---|---|
| Trusted Advisor Engage 설명서가 업데이트되었습니다. | 계약 생성 및 편집을 위한 양식이 변경되어 Trusted Advisor 참여 설명서가 업데이트되었습니다. 에 대한 서비스 제어 정책 예시가 있는 페이지가 추가되었습니다 AWS Trusted Advisor. | 2023년 7월 27일 |
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2023년 6월 26일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Amazon MQ에 대한 두 가지 새로운 내결함성 검사를 추가했습니다. Amazon Elastic File System에 대한 내결함성 검사 1개와 성능 검사 1개를 추가했습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2023년 6월 1일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | NAT 게이트웨이에 대한 두 가지 새로운 내결함성 검사를 추가했습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2023년 5월 16일 |

| | | |
|---|---|---|
| AWS Support 플랜 설명서가 업데이트되었습니다. | 지원 계획 일정 생성을 위한 새 권한 및 CloudTrail 설명서가 추가되었습니다. 자세한 내용은 계획에 대한 액세스 관리, AWS SupportAWS Support 계획에 대한AWS 관리형 정책 및 계획 API 호출 AWS Support 로깅을 참조하십시오 AWS CloudTrail. | 2023년 5월 8일 |
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2023년 5월 2일 |
| Trusted Advisor 참여 및 Trusted Advisor 우선 순위에 대한 설명서가 업데이트되었습니다. | Trusted Advisor 참여 및 우선 순위에 대한 사전 요구 사항을 명확히 했습니다. Trusted Advisor Trusted Advisor 참여를 사용하고 Trusted Advisor에 신뢰할 수 있는 액세스를 활성화할 수 있는 예제 IAM 정책을 추가했습니다. | 2023년 4월 28일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | AWS Resilience Hub 및 인시던트 관리자에 대한 두 개의 새로운 내결함성 검사를 추가했습니다. 자세한 내용은 변경 로그에서 AWS Trusted Advisor 검사를 참조하십시오. | 2023년 4월 27일 |

| | | |
|---|---|---|
| Trusted Advisor Engage에 대한 설명서가 추가되었습니다. | Engage를 사용하면 모든 사전 AWS Trusted Advisor 참여를 쉽게 확인, 요청 및 추적하고 진행 중인 계약에 대해 AWS 계정 팀과 소통할 수 있어 AWS Support 플랜을 최대한 활용할 수 있습니다. 자세한 내용은 AWS Trusted Advisor 참여 시작하기를 참조하세요. | 2023년 4월 6일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Amazon ECS에 대한 두 가지 새로운 내결함성 검사를 추가했습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2023년 3월 30일 |
| `AWSSupportServiceRolePolicy` 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2023년 3월 16일 |
| Trusted Advisor 우선 순위에 대한 설명서가 추가되었습니다. | Trusted Advisor 프라이어리티 콘솔 업데이트:<br>• 승인 및 취소 버튼이 수락 및 거부 버튼을 대체했습니다.<br>• 추천을 승인, 해결, 취소 또는 다시 열기 위해 직함이나 이름을 입력할 필요가 없습니다.<br><br>자세한 내용은 Trusted Advisor Priority 시작하기를 참조하십시오. | 2023년 2월 16일 |

| | | |
|---|---|---|
| 에 대한 코드 예제가 업데이트되었습니다. AWS Support | AWS 소프트웨어 개발 키트(SDK) 와 AWS Support 함께 사용하는 방법을 보여주는 .NET, Java, Kotlin 코드 예제가 추가되었습니다. 자세한 내용은 SDK 사용을 위한 코드 예제를 참조하세요. AWS Support AWS | 2023년 1월 16일 |
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2023년 1월 10일 |
| 앱 설명서가 업데이트되었습니다. AWS Support | 필터 옵션을 사용하거나 사례 ID로 검색하여 Slack에서 지원 사례를 검색할 수 있습니다. 자세한 내용은 Slack에서 지원 사례 검색을 참조하세요. | 2022년 12월 29일 |
| AWS Support 앱 설명서 업데이트 | Terraform을 사용하여 앱용 리소스를 만들 수도 있습니다. AWS Support 자세한 내용은 Terraform을 사용하여 AWS Support 앱 리소스 만들기를 참조하십시오. | 2022년 12월 22일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | AmazonMemoryDB ElastiCache, Amazon 및 에 대한 세 가지 새로운 내결함성 검사를 추가했습니다. AWS CloudHSM 자세한 내용은 확인을 위한 변경 로그를 참조하십시오. AWS Trusted Advisor | 2022년 12월 15일 |

| | | |
|---|---|---|
| Slack의 AWS Support 앱 설명서가 업데이트되었습니다. | 이제 다음 옵션에 대한 실시간 채팅 지원을 요청할 수 있습니다.<br>• 계정 및 결제 지원 사례.<br>• 기술 지원 사례에 대한 일본어 지원.<br>• 자세한 내용은 Slack 채널에서 지원 사례 생성을 참조하세요. | 2022년 12월 14일 |
| 에 대한 설명서가 업데이트되었습니다. AWS Support | AWS Support API의 새 엔드포인트에 대한 설명서가 추가되었습니다. 자세한 내용은 AWS Support API 정보를 참조하세요. | 2022년 12월 14일 |
| Slack에서 AWS Support 앱에 사용할 AWS CloudFormation 템플릿에 대한 설명서가 추가되었습니다. | CloudFormation 템플릿을 사용하여 in을 위한 Slack 구성 작업 영역 및 채널을 만들 수 있습니다. AWS 계정 AWS Organizations자세한 내용은 를 AWS Support 사용하여 앱 리소스 만들기를 참조하십시오. AWS CloudFormation | 2022년 12월 5일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 에 대한 두 개의 새로운 내결함성 검사를 추가했습니다 AWS Resilience Hub. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2022년 11월 17일 |

| | | |
|---|---|---|
| AWS Security Hub 조사 결과에 대한 설명서가 에 추가되었습니다. Trusted Advisor | Security Hub 컨트롤의 검색 결과가 Trusted Advisor 더 빠름에서 삭제되었습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2022년 11월 17일 |
| 에 대한 설명서가 업데이트되었습니다. AWS Trusted Advisor | Trusted Advisor 권장 사항에 대한 설명서가 추가되었습니다. 자세한 내용은 AWS Trusted Advisor 체크를 위한 변경 로그를 참조하십시오. | 2022년 11월 16일 |
| Slack의 AWS Support 앱 설명서가 업데이트되었습니다. | 일본어 지원에 대한 설명서가 추가되었습니다. 자세한 내용은 Slack 채널에서 지원 사례 생성을 참조하세요. | 2022년 11월 11일 |
| 플랜 설명서 업데이트 AWS Support | 조직 내 Support 플랜 액세스를 허용하는 문제 해결 정보를 추가했습니다. 자세한 설명은 문제 해결을 참조하십시오. | 2022년 11월 9일 |
| Slack의 AWS Support 앱 설명서가 업데이트되었습니다. | `supportapp` 권한에 대한 설명서가 추가되었습니다. 자세한 내용은 AWS Support 앱을 Slack에 연결하는 데 필요한 권한을 참조하십시오. | 2022년 11월 1일 |

| | | |
|---|---|---|
| Slack의 AWS Support 앱 설명서가 업데이트되었습니다. | `RegisterSlackWorkspaceForOrganization` API 작업을 사용하여 AWS 계정에 대한 Slack 작업 영역을 등록할 수 있습니다. 이 API를 호출하려면 계정이 AWS Organizations의 조직에 속해야 합니다. 자세한 내용을 알아보려면 AWS Support App in Slack API Reference를 참조하세요. | 2022년 10월 19일 |
| `AWSSupportServiceRolePolicy` 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2022년 10월 4일 |
| Support 플랜에 대한 업데이트된 설명서 | 이제 AWS Identity and Access Management (IAM) 을 사용하여 지원 플랜을 변경하기 위한 권한을 관리할 수 있습니다. AWS 계정자세한 정보는 다음 주제를 참조하세요.<br>• 플랜 액세스 관리 AWS Support<br>• AWSAWS Support 플랜에 대한 관리형 정책<br>• AWS Support 계획 변경<br>• 다음을 사용한 로깅 AWS Support 계획 API 호출 AWS CloudTrail | 2022년 9월 29일 |

| | | |
|---|---|---|
| Slack의 AWS Support 앱 설명서가 업데이트되었습니다. | AWS Support 앱과 함께 사용할 공개 또는 비공개 채널을 구성하는 방법에 대한 설명서가 추가되었습니다. 자세한 내용은 Slack 채널 구성을 참조하세요. | 2022년 9월 22일 |
| 에 대한 설명서가 업데이트되었습니다. AWS Support | 지원 사례 보안에 대한 새 단원이 추가되었습니다. 자세한 내용은 AWS Support 케이스의 보안을 참조하십시오. | 2022년 9월 9일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Amazon EC2에 대한 새로운 보안 검사가 추가되었습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2022년 9월 1일 |
| Slack의 AWS Support 앱 설명서가 업데이트되었습니다. | 다음 주제를 참조하십시오.<br><br>AWS Support 앱을 사용하여 지원 사례를 관리하고, 서비스 할당량 증가를 요청하고, Slack 채널에서 지원 담당자와 직접 채팅할 수 있습니다. 자세한 내용은 Slack의AWS Support 앱 설명서를 참조하세요.<br><br>IAM 역할에 AWS 관리형 정책을 추가하여 앱을 사용할 수 있습니다. AWS Support 자세한 내용은 Slack의 AWS Support 앱에 대한AWS 관리형 정책을 참조하십시오.<br><br>AWS Support 앱에 대한 새 API 레퍼런스. AWS Support 앱 API 참조를 참조하세요. | 2022년 8월 24일 |

| | | |
|---|---|---|
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2022년 8월 17일 |
| Trusted Advisor 우선순위에 대한 설명서가 추가되었습니다. | Trusted Advisor Priority는 다음 기능에 대한 지원을 추가합니다.<br>• 위임된 관리자<br>• 권장 사항 요약에 대한 일간 및 주간 이메일 알림<br>• 해결되거나 거부된 권장 사항 다시 열기<br>• AWS 관리형 정책<br>자세한 내용은 Trusted Advisor Priority 시작하기를 참조하십시오. | 2022년 8월 17일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Trusted Advisor 콘솔의 기본 설정 페이지가 업데이트되었습니다. 자세한 내용은 시작하기를 참조하십시오 AWS Trusted Advisor. | 2022년 7월 15일 |

| | | |
|---|---|---|
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 다음 정보를 포함하도록 검사를 업데이트했습니다.<br>• 알림 기준<br>• 권장 조치<br>• 추가 리소스<br>• 보고서 열<br><br>자세한 내용은 AWS Trusted Advisor 검사 참조를 참조하세요. | 2022년 7월 7일 |
| 에 대한 설명서가 업데이트되었습니다. AWS Support | 지원 사례를 관리하는 방법을 설명하는 설명서를 추가했습니다.<br>• 기존 지원 사례 업데이트<br>• 문제 해결 | 2022년 6월 28일 |
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하도록 권한을 업데이트했습니다. 자세한 내용은 AWS 관리형 정책 AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2022년 6월 23일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Trusted Advisor 에서 가져온 AWS 추가 기본 보안 모범 사례 보안 표준 제어를 지원합니다. AWS Security Hub자세한 내용은 확인을 위한 변경 로그를 참조하십시오. AWS Trusted Advisor | 2022년 6월 23일 |

| | | |
|---|---|---|
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 서비스 할당량 증가를 요청하는 방법에 대한 정보를 추가했습니다. 자세한 내용은 서비스 한도를 참조하세요. | 2022년 6월 21일 |
| 에 대한 설명서가 업데이트되었습니다. AWS Support | 사례 생성 환경이 지원 센터 콘솔에서 업데이트되었습니다. 자세한 내용은 지원 사례 및 사례 관리 생성을 참조하세요. | 2022년 5월 18일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Amazon EBS 및 AWS Lambda에 대한 네 가지 검사가 추가되었습니다. 자세한 내용은 Trusted Advisor 검사 추가 AWS Compute Optimizer 옵트인을 참조하십시오. | 2022년 5월 4일 |
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2022년 4월 27일 |
| 노출된 액세스 키 검사에 대한 업데이트된 설명서 | 이 검사는 이제 자동으로 새로 고침됩니다. 자세한 내용은 AWS Trusted Advisor 검사 로그 변경을 참조하십시오. | 2022년 4월 25일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 내결함성 범주의 AWS Direct Connect 검사가 업데이트되었습니다. 자세한 내용은 AWS Trusted Advisor 검사를 위한 변경 로그를 참조하십시오. | 2022년 3월 29일 |

| | | |
|---|---|---|
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2022년 3월 14일 |
| Trusted Advisor 우선순위에 대한 설명서가 추가되었습니다. | Trusted Advisor Priority를 사용하여 기술 계정 관리자 (TAM)의 우선 순위가 지정된 권장 사항 목록을 볼 수 있습니다. 자세한 내용은 Priority 시작하기를 참조하십시오. Trusted Advisor | 2022년 2월 28일 |
| Amazon 사용에 대한 설명서가 업데이트되었습니다 EventBridge . Trusted Advisor | Trusted Advisor 수표의 변경 사항을 모니터링하는 EventBridge 규칙을 생성할 수 있습니다. 자세한 내용은 AWS Trusted Advisor 검사 결과 모니터링을 참조하십시오 EventBridge. | 2022년 2월 21일 |
| Amazon을 사용하여 AWS Support 사례를 EventBridge 모니터링하기 위한 새로운 설명서 | EventBridge 규칙을 생성하여 지원 사례를 모니터링하고 관련 알림을 받을 수 있습니다. 자세한 내용은 다음을 통한 AWS Support 사례 모니터링을 참조하십시오 EventBridge. | 2022년 2월 21일 |
| AWSSupportServiceRolePolicy 와 관련하여 업데이트된 설명서 | 서비스 연결 역할에 결제, 관리 및 지원 서비스를 제공하기 위한 새로운 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책AWSSupportServiceRolePolicy 단원을 참조하십시오. | 2022년 2월 17일 |

| | | |
|---|---|---|
| 통합을 위한 설명서가 추가되었습니다. AWS Security Hub | 이제 Trusted Advisor 콘솔에서 AWS 기본 보안 모범 사례 보안 표준의 일부인 Security Hub 컨트롤에 대한 결과를 볼 수 있습니다. 자세한 내용은 콘솔에서 AWS Security HubAWS Trusted Advisor 컨트롤 보기를 참조하십시오. | 2022년 1월 18일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Microsoft SQL Server를 실행하는 Amazon EC2 인스턴스에 대한 새로운 세 가지 검사를 추가했습니다.<br>• Microsoft SQL Server용 Amazon EC2 인스턴스 통합<br>• Microsoft SQL Server에 대해 과다 프로비저닝된 Amazon EC2 인스턴스<br>• Microsoft SQL Server를 사용하는 Amazon EC2 인스턴스 지원 종료<br>자세한 내용은 AWS Trusted Advisor 검사 참조를 참조하세요. | 2021년 12월 20일 |

| | | |
|---|---|---|
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Trusted Advisor 에 대한 네 가지 새로운 검사 추가 AWS Well-Architected<br>• 비용 최적화에 대한 AWS Well-Architected 위험도 높음 문제<br>• 성능에 대한 AWS Well-Architected 위험도 높음 문제<br>• 보안에 대한 AWS Well-Architected 위험도 높음 문제<br>• 안정성에 대한 AWS Well-Architected 위험도 높음 문제<br>자세한 내용은 AWS Trusted Advisor 검사 참조를 참조하세요. | 2021년 12월 20일 |
| 업데이트된 설명서 | Enterprise On-Ramp Support 플랜을 사용하는 경우 모든 Trusted Advisor 검사 및 API 에 액세스할 수 있습니다. AWS Support | 2021년 11월 24일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Trusted Advisor Amazon Comprehend에 대한 두 개의 새로운 검사를 추가했습니다. 자세한 내용은 AWS Trusted Advisor 검사 참조를 참조하세요. | 2021년 9월 29일 |

| | | |
|---|---|---|
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Amazon OpenSearch Service Reserved Instance Optimization에 대한 검사 이름이 업데이트되었습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2021년 9월 8일 |
| Trusted Advisor 점검에 대한 설명서가 업데이트되었습니다. | 모든 Trusted Advisor 검사에 대한 참조 항목이 추가되었습니다. 자세한 내용은 AWS Trusted Advisor 검사 참조를 참조하세요. | 2021년 9월 1일 |
| Trusted Advisor 관리형 정책에 대한 설명서가 업데이트되었습니다. | Trusted Advisor 관리형 정책에 대한 설명서가 업데이트되었습니다. 자세한 내용은 AWS Support 및 에 대한AWS 관리형 정책을 참조하십시오 AWS Trusted Advisor. | 2021년 8월 10일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Trusted Advisor 콘솔 설명서가 업데이트되었습니다. 자세한 내용은 시작하기를 참조하십시오 AWS Trusted Advisor. | 2021년 7월 16일 |
| AWS Support 사례 생성을 위한 설명서가 업데이트되었습니다. | 영구적으로 종료된 사례와 관련된 지원 사례를 만드는 방법을 설명서로 추가했습니다. 자세한 내용은 닫힌 사례 다시 열기 및 관련 사례 만들기를 참조하세요. | 2021년 6월 8일 |

| | | |
|---|---|---|
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Trusted Advisor Amazon Elastic Block Store (Amazon EBS) 볼륨 스토리지에 대한 두 가지 새로운 검사를 추가했습니다. 자세한 내용은 AWS Trusted Advisor 확인을 위한 변경 로그를 참조하십시오. | 2021년 6월 8일 |
| 업데이트된 설명서 | 다음 주제가 업데이트되었습니다.<br>• 절차를 업데이트하고 AWS Trusted Advisor 지표 모니터링을 위한 Amazon CloudWatch 경보 생성 주제에 콘텐츠를 추가했습니다.<br>• API 섹션의 서비스 할당량을 추가했습니다. AWS Support | 2021년 5월 12일 |

# 이전 업데이트

| 변경 사항 | 설명 | 날짜 |
|---|---|---|
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | 검사 결과를 필터링, 새로 고침 및 다운로드하는 설명서가 추가되었습니다. 자세한 내용은 다음 단원을 참조하세요.<br>• 검사 필터링<br>• 검사 결과 새로 고침<br>• 검사 결과 다운로드 | 2021년 3월 16일 |
| AWS 관리형 정책에 대한 문서 업데이트 | `AWSSupportServiceRolePolicy` AWS 관리형 정책에 대한 정보가 추가되었습니다. 자세한 내용은 AWS Support에 서비스 연결 역할 사용 단원을 참조하세요. | 2021년 3월 16일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| 에 대한 검사가 추가되었습니다. AWS Lambda | 에서 Lambda에 대한 네 가지 AWS Trusted Advisor 검사를 추가했습니다. 로그 변경 대상 AWS Trusted Advisor | 2021년 3월 8일 |
| Amazon Elastic Block Store와 관련하여 서비스 한도 검사가 업데이트됨 | 에서 Amazon EBS에 대한 다섯 가지 AWS Trusted Advisor 검사를 업데이트했습니다. 로그 변경 대상 AWS Trusted Advisor | 2021년 3월 5일 |
| 로깅 설명서가 업데이트되었습니다. CloudTrail | CloudTrail AWS Support 플랜 변경 시 콘솔 작업에 대한 로깅을 지원합니다. 자세한 정보는 AWS Support 계획에 대한 변경 사항 로깅을 참조하세요. | 2021년 2월 9일 |
| 에 대한 설명서가 업데이트되었습니다. Trusted Advisor | Trusted Advisor 권장 사항 시작하기 주제를 업데이트했습니다. | 2021년 1월 29일 |
| Trusted Advisor 보고서 설명서가 업데이트되었습니다. | Trusted Advisor 보고서를 다른 AWS 서비스와 함께 사용하기 위한 문제 해결 섹션이 추가되었습니다. | 2020년 12월 4일 |
| AWS CloudTrail 로깅 AWS Trusted Advisor 지원이 추가되었습니다. | CloudTrail Trusted Advisor 콘솔 작업의 하위 집합에 대한 로깅을 지원합니다. 자세한 정보는 를 AWS Trusted Advisor 사용하여 콘솔 작업 로깅 AWS CloudTrail을 참조하세요. | 2020년 11월 23일 |
| 변경 로그 주제가 추가됨 | 에서 AWS Trusted Advisor 검사 및 범주에 대한 변경 내용을 볼 수 있습니다. 로그 변경 대상 AWS Trusted Advisor | 2020년 11월 18일 |
| 조직 단위에 대한 지원이 추가됨 | 이제 조직 단위 (OU) Trusted Advisor 점검에 대한 보고서를 만들 수 있습니다. 자세한 정보는 조직 보기 보고서 생성을 참조하세요. | 2020년 11월 17일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| AWS CloudTrail 주제로 로깅을 업데이트했습니다. | Trusted Advisor API 작업에 대한 예제 로그 항목이 추가되었습니다. CloudTrail 로그 기록의 AWS Trusted Advisor 정보 단원을 참조하세요. | 2020년 10월 22일 |
| AWS Support 할당량 추가 | AWS Support의 현재 할당량 및 제한에 대한 정보를 추가했습니다. AWS 일반 참조에서 AWS Support 엔드포인트와 할당량을 확인하세요. | 2020년 8월 4일 |
| 에 대한 조직 보기 AWS Trusted Advisor | 이제 소속된 계정에 대한 Trusted Advisor 점검 보고서를 만들 수 AWS Organizations있습니다. AWS Trusted Advisor에 대한 조직 보기 단원을 참조하세요. | 2020년 7월 17일 |
| 보안 및 AWS Support | AWS Support 및 Trusted Advisor사용 시 보안 고려 사항에 대한 정보를 업데이트했습니다. 보안: AWS Support 단원 참조 | 2020년 5월 5일 |
| 보안 및 AWS Support | AWS Support사용 시 보안 고려 사항에 대한 정보를 추가했습니다. | 2020년 1월 10일 |
| 웹 Trusted Advisor 서비스로 사용 | Trusted Advisor 검사 목록을 가져온 후 Trusted Advisor 데이터를 새로 고치는 지침이 업데이트되었습니다. | 2018년 11월 1일 |
| 서비스 연결 역할 사용 | 새로운 단원을 추가했습니다. | 2018년 7월 11일 |
| 시작하기: 문제 해결 | Route 53 및 AWS Certificate Manager에 대한 문제 해결 링크를 추가했습니다. | 2017년 9월 1일 |
| 사례 관리 예: 사례 생성 | 기본 지원 플랜을 보유한 사용자를 위해 CC 상자에 대한 참고 사항을 추가했습니다. | 2017년 8월 1일 |
| CloudWatch 이벤트를 통한 Trusted Advisor 검사 결과 모니터링 | 새로운 단원을 추가했습니다. | 2016년 11월 18일 |
| 사례 관리 | 사례 심각도 수준의 이름을 업데이트했습니다. | 2016년 10월 27일 |

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| 를 사용한 AWS Support 통화 기록 AWS CloudTrail | 새로운 단원을 추가했습니다. | 2016년 4월 21일 |
| 시작하기: 문제 해결 | 더 많은 문제 해결 링크를 추가했습니다. | 2015년 5월 19일 |
| 시작하기: 문제 해결 | 더 많은 문제 해결 링크를 추가했습니다. | 2014년 11월 18일 |
| 시작하기: 사례 관리 | AWS Management Console에 Service Catalog를 반영하도록 업데이트되었습니다. | 2014년 10월 30일 |
| AWS Support 케이스 수명 프로그래밍 | 사례에 첨부 파일 추가 및 사례 기록 검색 시 사례 통신 생략을 위해 새로운 API 요소에 대한 정보를 추가했습니다. | 2014년 7월 16일 |
| 액세스 AWS Support | 이름이 지정된 지원 연락처를 액세스 방식으로 제거했습니다. | 2014년 5월 28일 |
| 시작하기 | 시작하기 단원을 추가했습니다. | 2013년 12월 13일 |
| 최초 게시 | 새 AWS Support 서비스가 출시되었습니다. | 2013년 4월 30일 |

# AWS 용어집

최신 AWS 용어는 AWS 용어집 참조의 AWS 용어집을 참조하세요.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.