



사용자 가이드

# AWS Health



# AWS Health: 사용자 가이드

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

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

# Table of Contents

AWS Health란 무엇인가요? .....	1
AWS Health를 처음 사용하십니까? .....	2
에 대한 개념 AWS Health .....	3
AWS Health 이벤트 .....	3
계정별 이벤트 .....	4
공개 이벤트 .....	4
AWS Health 대시보드 .....	4
AWS Health 대시보드 — 서비스 상태 .....	4
이벤트 유형 코드 .....	5
이벤트 유형 범주 .....	5
이벤트 상태 .....	7
영향을 받는 엔터티 .....	7
AWS Health 아마존 이벤트 EventBridge .....	7
AWS Health API .....	7
조직 보기 .....	8
AWS Health 대시보드 — 서비스 상태 .....	9
계획된 라이프사이클 이벤트 AWS Health .....	12
계획된 수명 주기 이벤트란 무엇입니까? .....	12
계획된 수명 주기 이벤트 알림을 받으면 무엇을 해야 합니까? .....	13
복원성을 위한 공동 책임 모델 .....	15
계획된 수명 주기 이벤트 액세스 .....	15
AWS Health 대시보드 – 계정 상태 .....	17
AWS Health 대시보드에서 계정 이벤트 보기 .....	18
미결 및 최근 문제 .....	18
예약된 변경 .....	19
기타 알림 .....	20
이벤트 로그 .....	20
이벤트 세부 정보 .....	21
이벤트 유형 .....	23
일정 보기 .....	23
영향을 받는 리소스 보기 .....	24
시간대 설정 .....	25
조직 상태 .....	26
Amazon EventBridge 설정 .....	26

AWS Health Aware .....	27
AWS Health 이벤트에 대한 경보 .....	27
AWS Health에 대한 AWS 사용자 알림 구성 .....	28
AWS Health API에 액세스 .....	29
엔드포인트 .....	29
고가용성 엔드포인트 데모 사용 .....	31
Java 데모 사용 .....	31
Python 데모 사용 .....	34
AWS Health API 요청에 서명 .....	37
AWS Health에서 지원되는 작업 .....	37
샘플 Java 코드 .....	39
1단계: 자격 증명 초기화 .....	39
2단계: AWS Health API 클라이언트 초기화 .....	39
3단계: AWS Health API 작업을 사용하여 이벤트 정보 가져오기 .....	40
보안 .....	44
데이터 보호 .....	44
데이터 암호화 .....	45
Identity and Access Management(IAM) .....	46
고객 .....	46
ID를 통한 인증 .....	47
정책을 사용한 액세스 관리 .....	50
IAM의 AWS Health 작동 방식 .....	52
자격 증명 기반 정책 예시 .....	57
문제 해결 .....	69
서비스 링크 역할 사용 .....	71
AWS 에 대한 관리형 정책 AWS Health .....	73
로그인 및 모니터링 AWS Health .....	78
규정 준수 확인 .....	79
복원력 .....	80
인프라 보안 .....	80
구성 및 취약성 분석 .....	81
보안 모범 사례 .....	81
AWS Health 사용자에게 가능한 최소 권한 부여 .....	81
보기 AWS Health Dashboard .....	81
Amazon Chime 또는 AWS Health 슬랙과 통합 .....	81
AWS Health 이벤트 모니터링 .....	81

AWS Health 이벤트 집계 .....	83
필수 조건 .....	83
조직 보기(콘솔) .....	84
조직 보기 활성화(콘솔) .....	85
조직 보기 이벤트 보기(콘솔) .....	86
영향을 받는 계정 및 리소스 보기(콘솔) .....	90
조직 보기 사용 안 함(콘솔) .....	91
조직 보기(CLI) .....	92
조직 보기 활성화(CLI) .....	92
조직 보기 이벤트 보기(CLI) .....	95
조직 보기 사용 안 함(CLI) .....	96
AWS Health 조직 보기 API 작업 .....	97
위임된 관리자 조직 보기 .....	98
조직 보기에 대한 위임된 관리자 등록 .....	98
조직 보기에서 위임된 관리자 제거 .....	99
를 통한 Health 이벤트 모니터링 EventBridge .....	100
에 AWS 리전 대한 정보 AWS Health .....	101
공개 이벤트 정보 AWS Health .....	102
에 대한 이벤트 프로세서 AWS Health .....	103
관련 정보 .....	103
에 대한 EventBridge 규칙 생성 AWS Health .....	104
여러 서비스 및 범주에 대한 규칙 생성 .....	108
AWS Health 이벤트 스키마 Amazon EventBridge .....	110
AWS Health 이벤트 스키마 .....	110
공개 상태 이벤트 - Amazon EC2 운영 문제 .....	136
계정별 AWS Health 이벤트 - Elastic Load Balancing API 문제 .....	137
계정별 AWS Health 이벤트 - Amazon EC2 인스턴스 스토어 드라이브 성능 저하 .....	138
이벤트 페이지 매김 AWS Health EventBridge .....	139
조직 보기 및 위임된 관리자 액세스를 사용하여 이벤트를 집계합니다 AWS Health . .....	139
다음과 같은 이벤트 수신 AWS HealthAWS Chatbot .....	140
필수 조건 .....	140
Amazon EC2 인스턴스에 대한 작업 자동화 .....	142
필수 조건 .....	142
에 대한 규칙을 생성하세요. EventBridge .....	146
SMC 커넥터를 다음과 같이 구성하십시오. AWS Health .....	149
모니터링 AWS Health .....	150

를 AWS Health 사용하여 API 호출을 로깅합니다. AWS CloudTrail .....	150
AWS Health 자세한 내용은 CloudTrail .....	151
예: AWS Health 로그 파일 항목 .....	152
사용 설명서 기록 .....	154
이전 업데이트 .....	158
AWS 용어집 .....	160
.....	clxi

# AWS Health란 무엇인가요?

AWS Health는 리소스 성능과 사용자 AWS 서비스 및 계정의 가용성에 대한 지속적인 가시성을 제공합니다. AWS Health 이벤트를 사용하여 서비스 및 리소스 변경이 AWS에서 실행 중인 애플리케이션에 어떤 영향을 미칠 수 있는지 알아볼 수 있습니다. AWS Health는 진행 중인 이벤트를 관리하는 데 도움이 되는 관련성 있고 시기적절한 정보를 제공합니다. 또한 AWS Health는 계획된 활동을 파악하고 이에 대비하는 데도 도움을 줍니다. 이 서비스는 AWS 리소스의 상태가 변경되면 경고 및 알림을 트리거하므로, 사용자는 이벤트 정보와 지침을 거의 즉각적으로 파악하고 문제를 신속하게 해결할 수 있습니다.

모든 고객은 AWS Health API로 구동되는 [AWS Health 대시보드](#)를 사용할 수 있습니다. 대시보드는 별도의 설정이 필요하지 않으며 [인증된 AWS 사용자](#)가 바로 사용할 수 있습니다. 더 많은 서비스 하이라이트는 [AWS Health 대시보드 세부 정보 페이지](#)

AWS Health의 기본 사항 및 사용 방법을 알아보려면 [AWS Health를 처음 사용하십니까?](#) 항목을 참조하세요.

AWS Health를 사용할 때 표시되는 용어 목록은 [에 대한 개념 AWS Health](#) 항목을 참조하세요.

## 주의

- 모든 AWS 고객은 추가 비용 없이 AWS Health 대시보드를 사용할 수 있습니다.
- 모든 AWS 고객은 추가 비용 없이 Amazon EventBridge를 통해 AWS Health 이벤트를 수신할 수 있습니다.
- Business, Enterprise On-Ramp 또는 Enterprise Support 플랜을 사용하는 경우에는 AWS Health API를 사용하여 사내 및 타사 시스템과 통합할 수 있습니다. 자세한 내용은 [AWS Health API 참조](#)를 참조하세요.
- 사용 가능한 AWS Support 플랜에 대한 자세한 내용은 [AWS Support](#)을(를) 참조하세요.

# AWS Health를 처음 사용하십니까?

AWS Health를 처음 사용하시는 경우 먼저 다음 단원을 읽어 보세요.

- [AWS Health란 무엇인가요?](#) - 이 섹션에서는 기본 데이터 모델, 이 모델이 지원하는 작업 및 서비스와 상호 작용하는 데 사용할 수 있는 AWS SDK에 대해 설명합니다.
- [에 대한 개념 AWS Health](#) - 서비스를 사용하는 동안 접하게 되는 AWS Health에 대한 기본 사항과 용어에 대해 알아보세요.
- [AWS Health 대시 보드 시작하기 - 계정 상태](#) - 이벤트 및 영향을 받는 엔터티를 확인하고 고급 필터링을 수행하는 방법을 알아봅니다. 이 대시보드에는 사용자 계정 및 조직별 이벤트가 포함됩니다.
- [AWS Health 대시보드 - 서비스 상태](#) - AWS 계정이 없는 경우 각 AWS 리전에 대한 상태와 AWS 서비스 상태에 대한 정보를 확인할 수 있습니다.
- [Amazon을 통한 AWS Health 이벤트 모니터링 EventBridge](#) - Amazon EventBridge를 사용하여 AWS Health에서 푸시 알림을 수신할 수 있습니다.
- [AWS Health API에 액세스](#) - AWS Health API 섹션에서는 이벤트 및 엔터티에 대한 정보를 검색하는 작업을 설명합니다.

AWS Health에서는 모든 고객에게 AWS Health 대시보드라는 콘솔을 제공합니다. 대시보드를 설정하기 위해 코드를 작성하거나 작업을 수행할 필요는 없습니다.

Amazon EventBridge에서 AWS Health 이벤트를 수신하도록 EventBridge 규칙을 설정할 수 있습니다. 이러한 방법으로 시 알림을 사용해 Amazon EventBridge 규칙을 생성하여 조치를 취함으로써 AWS Health 이벤트 관리를 자동화할 수 있습니다.

Business, Enterprise On-Ramp 또는 Enterprise Support 요금제를 사용하는 경우 대시보드에 표시되는 정보에 프로그래밍 방식으로 액세스할 수 있습니다. AWS Command Line Interface(AWS CLI)을(를) 사용하거나 코드를 작성하여 요청을 할 수 있습니다(REST API를 직접 사용하거나 AWS SDK 사용).

Amazon EventBridge에서 AWS Health 이벤트를 사용하는 방법에 대한 자세한 내용은 [Amazon을 통한 AWS Health 이벤트 모니터링 EventBridge](#)을(를) 참조하세요. AWS Health과(와) AWS CLI을(를) 함께 사용하는 방법에 대한 자세한 내용은 [AWS Health에 대한 AWS CLI 참조](#) 단원을 참조하세요. AWS CLI 설치에 대한 지침은 [AWS Command Line Interface 설치](#)를 참조하세요.



# 에 대한 개념 AWS Health

AWS Health 개념에 대해 알아보고 서비스를 사용하여 내 애플리케이션, 서비스 및 리소스의 상태를 유지하는 방법을 이해하십시오 AWS 계정.

## 주제

- [AWS Health 이벤트](#)
- [AWS Health 대시보드](#)
- [이벤트 유형 코드](#)
- [이벤트 유형 범주](#)
- [이벤트 상태](#)
- [영향을 받는 엔터티](#)
- [AWS Health 아마존 이벤트 EventBridge](#)
- [AWS Health API](#)
- [조직 보기](#)

## AWS Health 이벤트

AWS Health Health 이벤트라고도 하는 이벤트는 다른 AWS 서비스를 대신하여 AWS Health 보내는 알림입니다. 이러한 이벤트를 통해 계정에 영향을 미칠 수 있는 예정된 변경 사항이나 예약된 변경 사항에 대해 알아볼 수 있습니다. 예를 들어 AWS Identity and Access Management (IAM) 이 관리형 정책을 더 이상 사용하지 않거나 관리형 규칙을 더 이상 사용하지 않을 AWS Config 계획인 경우 이벤트를 전송할 AWS Health 수 있습니다. AWS Health 또한 에 서비스 가용성 문제가 있는 경우 이벤트를 전송합니다. AWS 리전이벤트 설명을 검토하여 문제를 파악하고, 영향을 받는 리소스를 식별하고, 권장되는 조치를 취할 수 있습니다.

상태 이벤트에는 다음과 같은 두 가지 유형이 있습니다.

## 목차

- [계정별 이벤트](#)
- [공개 이벤트](#)

## 계정별 이벤트

계정별 이벤트는 사용자 AWS 계정 또는 조직의 특정 AWS 계정에서 로컬로 발생합니다. 예를 들어, 사용하는 지역의 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스 유형에 문제가 있는 경우 AWS Health, 이벤트에 대한 정보와 영향을 받는 리소스의 이름을 제공합니다.

[AWS Health 대시보드](#) 또는 [AWS Health API에서](#) 계정별 이벤트를 찾거나 [Amazon CloudWatch Events](#)를 사용하여 알림을 받을 수 있습니다.

## 공개 이벤트

공개 이벤트는 계정에 국한되지 않고 보고되는 서비스 이벤트입니다. 예를 들어 미국 동부 (오하이오) 지역의 Amazon Simple Storage Service (Amazon S3) 에 대한 서비스 문제가 있는 경우 AWS Health, 해당 서비스를 사용하지 않거나 해당 지역에 S3 버킷이 있더라도 이벤트에 대한 정보를 제공합니다. 공개 알림에 대해 조치를 취하기 전에 먼저 공개 알림을 검토하는 것이 좋습니다.

AWS Health 대시보드와 대시보드 — 서비스 상태에서 공개 이벤트를 찾을 수 있습니다. AWS Health 계정이 있는 경우 [AWS Health 대시 보드 시작하기 – 계정 상태](#)을(를) 참조하십시오.

계정이 없는 경우 [AWS Health 대시보드 — 서비스 상태](#)을(를) 참조하십시오.

## AWS Health 대시보드

계정이 AWS 계정있는 경우 AWS Health 대시보드에는 공개 이벤트와 계정별 이벤트가 모두 표시됩니다.

AWS Health 대시보드를 사용하여 특정 지역의 서비스에 대한 향후 유지 관리 문제와 같이 일반적인 인식을 제공하는 이벤트에 대해 알아보는 것이 좋습니다. AWS Health 대시보드를 사용하여 계정에서 더 이상 사용되지 않는 리소스와 같이 본인에게 직접적인 영향을 미칠 수 있는 이벤트에 대해서도 알아볼 수 있습니다.

<https://health.aws.amazon.com/health/home> 에서 [AWS Health 대시보드를 AWS Management Console](#) 보려면 [에 로그인할 수 있습니다](#).

자세한 정보는 [AWS Health 대시 보드 시작하기 – 계정 상태](#)을 참조하세요.

## AWS Health 대시보드 — 서비스 상태

계정이 없는 경우 <https://health.aws.amazon.com/health/status> 의 AWS Health 대시보드 — 서비스 상태를 사용하여 공개 이벤트를 볼 수 있습니다. 공개 이벤트에는 서비스 이용 가능 여부에 대한 정보를

제공하는 AWS 에 대한 서비스 문제가 보고됩니다. 이 웹사이트에는 공개 이벤트만 표시되며, 이는 특정 계정에만 국한되지 않습니다. 이 페이지를 보기 위해 로그인하거나 계정이 있을 필요는 없습니다.

자세한 내용은 [AWS Health 대시보드 — 서비스 상태](#) 섹션을 참조하십시오.

## 이벤트 유형 코드

상태 이벤트에 표시되는 이벤트 유형 코드에는 영향을 받는 서비스와 이벤트 유형이 포함됩니다. 예를 들어, `AWS_EC2_SYSTEM_MAINTENANCE_EVENT` 이벤트 유형 코드가 있는 상태 이벤트를 수신하면 이는 서비스에 사용자에게 영향을 줄 수 있는 유지 관리 이벤트가 예약되어 있음을 의미합니다. 이 정보를 사용하여 미리 계획을 세우거나 계정에 대한 조치를 취하십시오.

## 이벤트 유형 범주

모든 상태 이벤트에는 관련 이벤트 유형 범주가 있습니다. 일부 이벤트의 경우 이벤트 유형 범주가 `AWS_RDS_MAINTENANCE_SCHEDULED` 코드와 같은 이벤트 유형 코드에 나타날 수 있습니다. 이 예시에서는 범주가 예약되어 있습니다. 이 정보를 사용하여 이벤트 범주를 효율적으로 파악할 수 있습니다.

모든 이벤트 유형 범주를 모니터링하는 것이 좋습니다. 각 범주는 서로 다른 유형의 이벤트에 대해 표시된다는 점에 유의하십시오. [DescribeEventTypes](#) API 작업을 사용하여 이벤트 유형 카테고리를 찾을 수도 있습니다.

### 계정 알림

이러한 이벤트는 계정 및 서비스의 관리 또는 보안에 대한 정보를 제공합니다. 이러한 이벤트는 정보를 제공할 수도 있고 긴급 조치가 필요하다는 것을 알릴 수 있습니다. 이러한 유형의 이벤트에 주의를 기울이고 권장되는 조치를 모두 검토하는 것이 좋습니다.

다음은 계정 알림을 위한 이벤트 유형 코드의 예시입니다.

- `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION` – 퍼블릭 액세스를 허용할 수 있는 Amazon S3 버킷이 있습니다.
- `AWS_BILLING_SUSPENSION_NOTICE` – 계정에 미결제 요금이 있어 일시 중지되었거나 계정을 비활성화했습니다.
- `AWS_WORKSPACES_OPERATIONAL_NOTIFICATION`— Amazon의 서비스 문제가 WorkSpaces 있습니다.

## 문제

이러한 이벤트는 AWS 서비스 또는 리소스에 영향을 미치는 예상치 못한 이벤트입니다. 이 범주에 속하는 일반적인 이벤트로는 서비스 성능 저하의 원인이 되는 운영 문제 또는 사용자가 인지해야 하는 현지화된 리소스 수준 문제에 대한 커뮤니케이션이 있습니다.

다음은 문제에 대한 이벤트 유형 코드의 예입니다.

- `AWS_EC2_OPERATIONAL_ISSUE` – 서비스 사용 지연과 같은 서비스 운영 문제
- `AWS_EC2_API_ISSUE` – API 작업의 지연 시간 증가 등의 서비스 API의 운영 문제
- `AWS_EBS_VOLUME_ATTACHMENT_ISSUE` Amazon Elastic Block Store(Amazon EBS) 리소스에 영향을 줄 수 있는 현지화된 리소스 수준 문제
- `AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT` – 이 이벤트는 조치를 취하지 않으면 계정이 일시 중단될 수 있음을 의미합니다.

## 예약된 변경 사항

이러한 이벤트는 서비스 및 리소스의 향후 변경 사항에 대한 정보를 제공합니다. 이러한 이벤트에는 다양한 버전에 대한 end-of-support 알림 및 자동 업그레이드와 같은 계획된 라이프사이클 이벤트가 포함됩니다. 서비스 종단을 방지하기 위한 조치를 취하도록 권장하는 이벤트도 있고, 사용자가 별도의 조치를 취하지 않아도 자동으로 발생하는 이벤트도 있습니다. 예약된 변경 사항 활동 중에는 리소스를 일시적으로 사용할 수 없을 수도 있습니다. 이 범주의 모든 이벤트는 계정별 이벤트입니다.

다음은 예약된 변경 사항에 대한 이벤트 유형 코드 예시입니다.

- `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED` – Amazon EC2 인스턴스를 재부팅해야 합니다.
- `AWS_SAGEMAKER_SCHEDULED_MAINTENANCE`— 서비스 문제 해결과 같은 유지 관리 이벤트가 SageMaker 필요합니다.
- `AWS_RDS_PLANNED_LIFECYCLE_EVENT`— Amazon RDS는 계획된 수명 주기 이벤트 (예: 해당 버전 중 하나에 대한 end-of-support 이벤트) 를 예약하고 있으며, 이 경우 고객 조치가 필요합니다.

### Tip

AWS Health API 또는 AWS Command Line Interface (AWS CLI) 를 사용하여 이벤트 세부 정보를 반환하는 경우, Event 객체에는 값이 있는 `eventScopeCode` 필드가 포함됩니다. ACCOUNT\_SPECIFIC 자세한 내용은 [AWS Health API 참조](#)를 참조하십시오.

## 이벤트 상태

이벤트 상태는 상태 이벤트가 진행 중인지, 마감되었는지 또는 예정된 상태인지를 알려줍니다. AWS Health 대시보드 또는 AWS Health API에서 최대 90일 동안 Health 이벤트를 볼 수 있습니다.

## 영향을 받는 엔터티

영향을 받는 개체는 이벤트의 영향을 받을 수 있는 AWS 리소스입니다. 예를 들어, 계정에서 사용 중인 특정 인스턴스 유형에 대한 Amazon EC2 유지 관리 예약 이벤트를 받은 경우 상태 이벤트를 사용하여 영향을 받는 인스턴스의 ID를 확인할 수 있습니다. 이 정보를 사용하여 리소스 생성 또는 사용 중단과 같은 잠재적인 서비스 문제를 해결할 수 있습니다.

## AWS Health 아마존 이벤트 EventBridge

계정에서 적절한 AWS Health 이벤트를 수신한 후 작업을 자동화하도록 계정에 대한 Amazon EventBridge 규칙을 설정할 수 있습니다. 이는 계획된 모든 수명 주기 이벤트 메시지를 채팅 인터페이스로 보내는 것과 같은 일반적인 작업일 수 있습니다. 또는 IT 서비스 관리 도구에서 워크플로우를 트리거하는 것과 같은 특정 작업일 수도 있습니다.

자세한 정보는 [Amazon을 통한 AWS Health 이벤트 모니터링 EventBridge](#)를 참조하세요.

## AWS Health API

AWS Health API를 사용하여 [AWS Health 대시보드에](#) 나타나는 다음과 같은 정보에 프로그래밍 방식으로 액세스할 수 있습니다.

- AWS 서비스와 리소스에 영향을 줄 수 있는 이벤트에 대한 정보를 얻으세요.
- 조직의 조직 보기 기능을 활성화 또는 비활성화합니다. AWS
- 특정 서비스, 이벤트 유형 범주, 이벤트 유형 코드별로 이벤트를 필터링합니다.

자세한 내용은 [AWS Health API 참조](#)를 참조하십시오.

### Note

API를 [AWS Support](#) 사용하려면 비즈니스, 엔터프라이즈 온램프 또는 엔터프라이즈 지원 플랜이 AWS Health 있어야 합니다. 비즈니스, 엔터프라이즈 온램프 또는 엔터프

라이즈 지원 플랜이 없는 계정에서 AWS Health API를 호출하면 오류가 발생합니다.  
`SubscriptionRequiredException`

## 조직 보기

이 기능을 사용하여 내 AWS 계정의 모든 건강 이벤트를 대시보드의 단일 AWS Organizations 보기로 집계할 수 있습니다. AWS Health 그런 다음 조직의 관리 계정에 로그인하거나 AWS Health API를 사용하여 다양한 계정 및 리소스에 영향을 미칠 수 있는 모든 이벤트를 볼 수 있습니다. AWS Health 콘솔 또는 API에서 이 기능을 활성화할 수 있습니다. 자세한 내용은 [조직 보기를 사용하여 계정 간 AWS Health 이벤트 집계](#)(를) 참조하세요.

# AWS Health 대시보드 — 서비스 상태

AWS Health 대시보드 — 서비스 상태를 사용하여 모든 사람의 상태를 볼 수 AWS 서비스 있습니다. 이 페이지에는 AWS 리전 전반의 서비스에 대해 보고된 서비스 이벤트가 표시됩니다. AWS Health 대시보드 — 서비스 상태 페이지에 AWS 계정 액세스하기 위해 로그인하거나 로그인하지 않아도 됩니다.

## Tip

이 웹사이트는 특정 이벤트에만 국한되지 않는 공개 이벤트만 표시합니다 AWS 계정. 이미 계정이 있는 경우 로그인하여 AWS Health 대시보드를 보고 계정 및 서비스에 영향을 미칠 수 있는 이벤트에 대한 최신 정보를 확인하는 것이 좋습니다. 자세한 설명은 [AWS Health 대시보드 시작하기 - 계정 상태](#) 섹션을 참조하세요.

AWS Health 대시보드를 보려면 — 서비스 상태

1. <https://health.aws.amazon.com/health/status> 페이지로 이동합니다.

## Note

AWS 계정, 페이지에 이미 로그인한 경우 AWS Health 대시보드 — 계정 상태 페이지로 리디렉션됩니다.

2. 서비스 상태에서 미해결 문제 및 최근 문제를 선택하여 최근에 보고된 이벤트를 확인합니다. 이벤트에 대한 다음 정보를 확인할 수 있습니다.
  - 이벤트 이름 및 영향을 받는 리전. 예: 운영 문제 – Amazon Elastic Compute Cloud (버지니아 북부)
  - 서비스 이름
  - 이벤트의 심각도 (예: 정보 또는 성능 저하)
  - 이벤트의 최근 업데이트 타임라인
  - AWS 서비스 해당 목록도 이 이벤트의 영향을 받습니다.

**Note**

이벤트는 현지 시간대 또는 UTC로 볼 수 있습니다. 자세한 내용은 [시간대 설정](#)을 참조하십시오.

- (선택 사항) 이벤트 옆에서 RSS를 선택하여 이 이벤트의 RSS 피드를 구독할 수 있습니다. 지정된 주소로 이 특정 서비스에 대한 알림을 받게 됩니다 AWS 리전.
- 서비스 기록 테이블을 보려면 서비스 기록을 선택합니다. 이 표에는 지난 12개월 동안의 모든 AWS 서비스 중단이 나와 있습니다.

**Tip**

서비스, AWS 리전, 날짜별로 필터링할 수 있습니다.

- 진행 중인 서비스 이벤트 옆의 상태 아이콘



을 선택하면 이벤트에 대한 자세한 정보를 볼 수 있습니다.

- (선택 사항) 이 목록을 과거 이벤트 목록으로 보려면 이벤트 목록 버튼을 선택합니다. 이벤트 옆에서 이벤트를 선택하면 팝업 사이드 패널에서 특정 이벤트에 대한 추가 정보를 볼 수 있습니다.

**Service history**

List of services

List of events

The following table is a running log of AWS service interruptions for the past 12 months. Choose a status icon to see status updates for that service. All dates and times are reported in Pacific Standard Time (PST). To update your time zone, see [Time zone settings](#).

 Add filter
**Note**

2023년 9월 이후에 공개 이벤트를 선택하면 브라우저의 URL이 해당 공개 이벤트로 연결되는 링크로 채워집니다. AWS Health 이 링크를 선택한 후 해당 이벤트 팝업이 있는 이벤트 목록 보기로 이동합니다.



7. (선택 사항) RSS 피드를 구독하려면 RSS를 선택합니다. 그러면 지정된 AWS 리전에서 특정 서비스에 대한 알림을 받게 됩니다.
8. (선택 사항) 현지 시간대 또는 UTC로 이벤트를 볼 수 있습니다. 자세한 내용은 [시간대 설정](#) 섹션을 참조하십시오.
9. (선택 사항) 계정이 있는 경우 계정 상태 열기를 선택하여 로그인합니다. 로그인한 후 계정과 관련된 이벤트를 볼 수 있습니다. 자세한 내용은 [AWS Health 대시 보드 시작하기 - 계정 상태](#) 섹션을 참조하십시오.

# 계획된 라이프사이클 이벤트 AWS Health

의 계획된 라이프사이클 이벤트에 대해 알아보십시오 AWS Health.

## 주제

- [계획된 수명 주기 이벤트란 무엇입니까?](#)
- [계획된 수명 주기 이벤트 알림을 받으면 무엇을 해야 합니까?](#)
- [복원성을 위한 공동 책임 모델](#)
- [계획된 수명 주기 이벤트 액세스](#)

## 계획된 수명 주기 이벤트란 무엇입니까?

AWS Health 애플리케이션의 가용성에 영향을 미칠 수 있는 중요한 변경 사항을 전달합니다. AWS 공동 책임 모델에서는 리소스를 지원하는 기본 하드웨어 및 인프라를 최신으로 유지하고 보안을 유지하기 위한 조치를 AWS 취합니다. 그러나 일부 변경 사항의 경우 애플리케이션에 미치는 영향을 방지하기 위해 고객의 조치 또는 조정이 필요합니다. AWS Health 는 다음과 같은 중요한 변경 사항을 미리 알려 줍니다.

- 오픈소스 소프트웨어 지원 종료 - 일부는 오픈 소스 버전의 소프트웨어를 AWS 서비스 실행합니다. 오픈소스 커뮤니티에서 소프트웨어 버전에 대한 지원을 종료하는 경우 업그레이드를 위한 조치가 필요한 AWS 시점을 알려주고 애플리케이션에 영향을 주지 않도록 합니다.
  - [Amazon RDS for MySQL 엔진 버전 지원 종료](#)
  - [Amazon EKS Kubernetes 버전 지원 종료](#)
- AWS소유한 리소스에 영향을 미치는 변경 사항으로 사용자의 조치가 필요할 수 있습니다.
  - [Amazon RDS 인증 기관 인증서 만료](#)
  - [Amazon WorkDocs Companion은 수명이 다해 더 이상 사용할 수 없습니다.](#)

### Note

이 기준에 맞는 모든 알림은 계획된 라이프사이클 이벤트를 통해 AWS Health 보고됩니다.

- 동적 리소스 소진 및 개선된 메타데이터: 알림을 받은 시점부터 AWS Health 이벤트가 지속되는 동안 영향을 받는 리소스는 특정 개체 상태의 영향을 받는 개체로 AWS Health 이벤트와 연결됩니다. 해당하는 경우 영향을 받는 리소스는 ARN 형식으로 지정됩니다. 영향을 받는 리소스에 고객 조치가

필요한 경우 해당 리소스는 “PENDING” 상태로 나열됩니다. 영향을 받는 리소스에 필요한 조치가 수행되었거나 리소스가 삭제된 경우 상태가 “RESOLVED”로 업데이트됩니다.

#### Note

- 리소스 상태 업데이트는 비동기적으로 주기적으로 수행되며, 드문 경우이긴 하지만 최대 72시간까지 지연될 수 있습니다.
- “PENDING” 또는 “RESOLVED” 상태인 리소스가 아닌 동적 업데이트가 제공되지 않는 예외적인 경우에는 리소스에 상태가 할당되지 않습니다.
- 리소스 상태 업데이트는 AWS GovCloud (US) 및 중국 지역에서 지원되지 않습니다.

## 계획된 수명 주기 이벤트 알림을 받으면 무엇을 해야 합니까?

계획된 라이프사이클 이벤트 AWS Health 경험을 통해 팀은 향후 라이프사이클 변경 사항을 파악하고 조치 완료를 추적할 수 있습니다.

유형 범주: 예약된 변경 사항

이벤트 유형 코드: `AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT`

이벤트 시작 시간: 이벤트 시작 시간은 변경으로 인해 리소스가 영향을 받는 가장 빠른 날짜입니다.

이벤트 종료 시간: 이벤트 종료 시간은 모든 AWS 리소스에서 변경이 완료되는 날짜입니다. 단, 종료 시간이 항상 지정되는 것은 아닙니다. 시작 시간을 변경 날짜로 취급하는 것이 중요합니다.

#### Note

조직은 영향을 받는 리소스가 있는 리전별로 그룹화된 모든 계획된 수명 주기 이벤트에 대해 단일 이벤트 ARN을 받을 것으로 예상할 수 있습니다. 하지만 영향을 받는 OR 리소스가 많은 조직에 있는 경우 ARN이 여러 개 수신될 수 AWS 계정 있습니다.

계획된 수명 주기 이벤트 조기 파악: 계획된 수명 주기 이벤트는 가능한 경우 메이저 버전/변경의 경우 최소 180일, 마이너 버전/변경의 경우 90일의 소요 시간을 갖도록 설계되었습니다.

동적 리소스 소진 및 메타데이터 개선: 알림을 받은 시점부터 AWS Health 이벤트가 지속되는 동안 영향을 받는 리소스는 특정 [개체](#) 상태의 영향을 받는 개체로 AWS Health 이벤트에 연결됩니다. 해당하

는 경우 영향을 받는 리소스는 ARN 형식으로 지정됩니다. 영향을 받는 리소스에 고객 조치가 필요한 경우 해당 리소스는 “PENDING” 상태로 나열됩니다. 영향을 받는 리소스에 필요한 조치가 수행되었거나 리소스가 삭제된 경우 상태가 “RESOLVED”로 업데이트됩니다.

### Note

- AWS Health 알림은 가능한 경우 시간 경과에 따른 상태 업데이트를 제공합니다. 단, 중국 지역은 예외입니다. AWS GovCloud (US)
- 리소스 상태 업데이트는 비동기적으로 주기적으로 수행되며, 드문 경우이긴 하지만 최대 72 시간까지 지연될 수 있습니다.

Open and recent issues
Scheduled changes
Other notifications
Event log

### Scheduled changes

Table Calendar

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

Add filter
< 1 >

Event	Status	Region / Zone	Info	Start time	End time	Affected resources
<a href="#">EKS planned lifecycle event</a>	Upcoming	us-west-2		January 30, 2024 at 6:00:00 PM UTC-8		<a href="#">9 pending</a>
<a href="#">DMS planned lifecycle event</a>	Upcoming	us-east-1		January 29, 2024 at 6:00:00 PM UTC-8		<a href="#">1 pending</a>
<a href="#">DMS planned lifecycle event</a>	Upcoming	eu-west-1		January 29, 2024 at 6:00:00 PM UTC-8		<a href="#">10 pending</a>
<a href="#">EKS planned lifecycle event</a>	Completed	eu-west-1		January 30, 2024 at 6:00:00 PM UTC-8		-

### EKS planned lifecycle event

Resource data is typically refreshed every 24 hours.
 0 Resolved
0%
No actions required

#### Affected resources in account 745485236264 (5)

Add filter
< 1 >

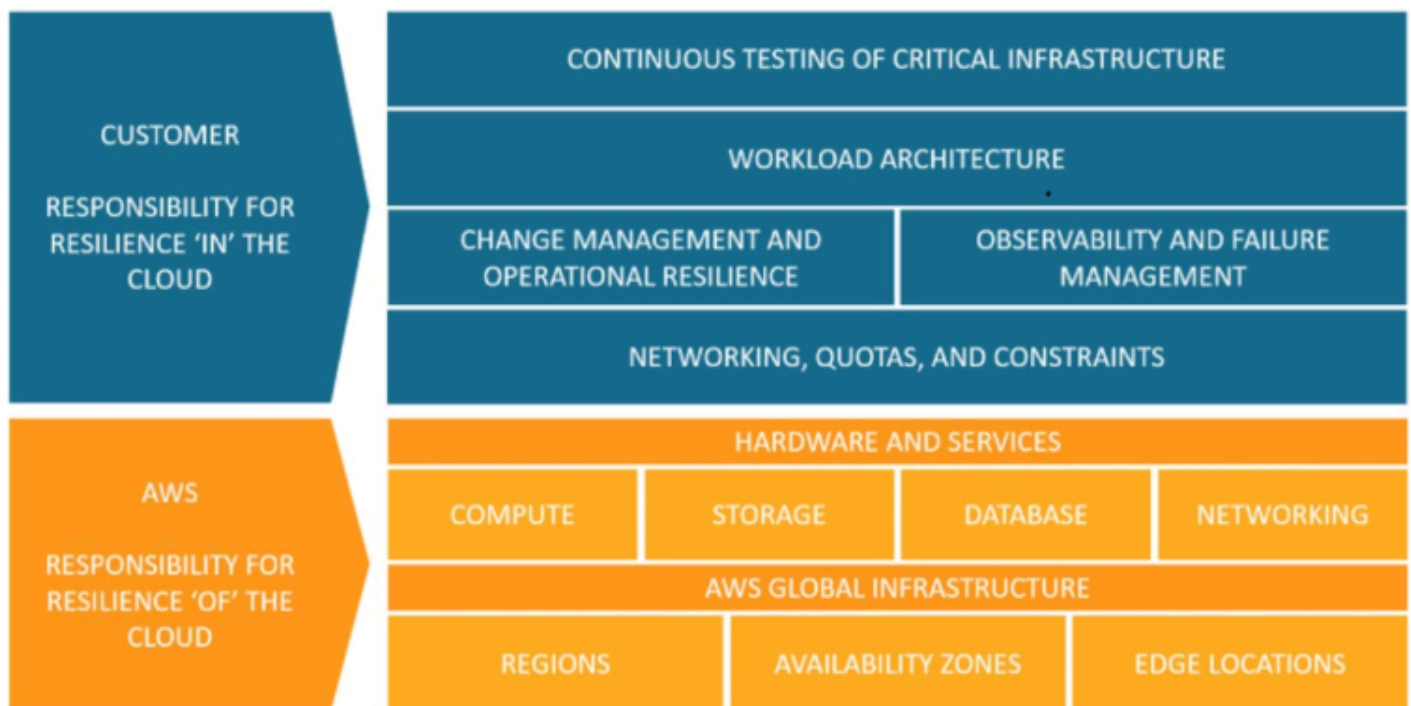
Resource ID / ARN	Resource status	Last update time
arn:aws:eks:us-west-2:745485236264:cluster/prod-ops-cluster	Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/nonprod-dev5	Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/n-preprd-eks	Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/argoworkflows-refactor51	Pending	15 days ago
arn:aws:eks:us-west-1:745485236264:cluster/prod-refactor	Pending	15 days ago

계획된 이벤트 날짜가 지난 후:

1. 해당하는 경우 서비스는 이벤트 시작일 이후 언제든지 리소스에 설명된 변경 사항을 적용할 수 있습니다.
2. 지원 종료일 이전에 모든 리소스를 해결하면 AWS Health 이벤트가 “Closed” 상태로 변경됩니다.
3. 해당 날짜 이후에 미결 리소스가 있지만 해결되지 않은 경우, AWS Health 이벤트는 시작일 또는 종료일로부터 90일 동안 계속 열린 상태로 있습니다. 그 다음 이벤트가 삭제됩니다.

## 복원성을 위한 공동 책임 모델

보안 및 규정 준수는 고객과 공동으로 AWS 책임입니다. 배포된 서비스에 따라 이 공동 모델은 고객의 운영 부담을 완화하는 데 도움이 될 수 있습니다. 이는 호스트 운영 체제 및 가상화 계층부터 서비스가 AWS 운영되는 시설의 물리적 보안에 이르기까지 구성 요소를 운영, 관리 및 제어하기 때문입니다. 고객은 AWS 제공된 보안 그룹 방화벽의 구성 외에도 게스트 운영 체제 (업데이트 및 보안 패치 포함) 및 기타 관련 애플리케이션 소프트웨어에 대한 책임과 관리를 부담합니다. 자세한 내용은 [공동 책임 모델](#)을 참조하십시오.



## 계획된 수명 주기 이벤트 액세스

다음과 같은 여러 채널을 사용하여 계획된 수명 주기 이벤트에 액세스하고 모니터링할 수 있습니다.

- [아마존 사용 EventBridge](#)

- [AWS Health 대시보드 사용](#)
  - [일정 보기](#)
  - [영향을 받는 리소스 보기](#)
- [AWS Health API 사용](#)

# AWS Health 대시보드 시작하기 – 계정 상태

AWS Health 대시보드를 사용하여 AWS Health 이벤트에 대해 알아볼 수 있습니다. 이러한 이벤트는 AWS 서비스 또는 AWS 계정에 영향을 미칠 수 있습니다. 계정에 로그인하면 AWS Health 대시보드에 다음과 같은 방식으로 정보가 표시됩니다.

- [계정 이벤트](#) – 이 페이지에는 계정과 관련된 이벤트가 표시됩니다. 진행 중인 변경 사항, 최근 변경 사항, 예약된 변경을 확인할 수 있습니다. 또한 지난 90일 동안의 모든 이벤트를 보여주는 알림 및 이벤트 로그를 볼 수 있습니다.
- [조직 이벤트](#) – 이 페이지에는 AWS Organizations의 해당 조직과 관련된 특정 이벤트가 표시됩니다. 조직의 진행 중인 변경 사항, 최근 변경 사항, 예약된 변경을 확인할 수 있습니다. 또한 지난 90일 동안의 모든 조직 이벤트를 보여주는 이벤트 로그뿐만 아니라 알림도 확인할 수 있습니다.

## Note

AWS 계정이 없는 경우 [AWS Health 대시보드 — 서비스 상태](#) 항목을 사용하여 일반 서비스 가용성에 대해 알아볼 수 있습니다.

계정이 있는 경우 AWS Health 대시보드에 로그인하여 서비스 및 리소스에 영향을 미칠 수 있는 이벤트 및 예정된 변경 사항에 대해 자세히 알아보는 것이 좋습니다.

## 목차

- [AWS Health 대시보드에서 계정 이벤트 보기](#)
  - [미결 및 최근 문제](#)
  - [예약된 변경](#)
  - [기타 알림](#)
  - [이벤트 로그](#)
- [이벤트 세부 정보](#)
- [이벤트 유형](#)
- [일정 보기](#)
- [영향을 받는 리소스 보기](#)
- [시간대 설정](#)
- [조직 상태](#)

- [Amazon EventBridge 설정](#)
- [AWS Health Aware](#)
- [AWS Health 이벤트에 대한 경보](#)

## AWS Health 대시보드에서 계정 이벤트 보기

계정에 로그인하여 맞춤형 이벤트 및 추천을 받을 수 있습니다.

AWS Health 대시보드에서 계정 이벤트를 보려면

1. <https://health.aws.amazon.com/health/home>에서 AWS Health 대시보드를 엽니다.
2. 탐색 창의 계정 상태에서 다음 옵션을 선택할 수 있습니다.
  - a. [미결 및 최근 문제](#) - 진행 중인 이벤트와 종료된 이벤트를 볼 수 있습니다.
  - b. [예약된 변경](#) - 서비스 및 리소스에 영향을 미칠 수 있는 예정된 이벤트를 확인할 수 있습니다.
  - c. [기타 알림](#) - 계정에 영향을 미칠 수 있는 지난 7일간의 기타 알림 및 진행 중인 이벤트를 모두 볼 수 있습니다.
  - d. [이벤트 로그](#) - 지난 90일간의 모든 이벤트를 볼 수 있습니다.

### 미결 및 최근 문제

미결 및 최근 문제 탭을 사용하면 계정에 영향을 미칠 수 있는 지난 7일간의 진행 중인 모든 이벤트를 볼 수 있습니다.

대시보드에서 이벤트를 선택하면 이벤트에 대한 정보와 영향을 받는 리소스 목록이 포함된 세부 정보 창이 나타납니다. 자세한 내용은 [이벤트 세부 정보](#) 섹션을 참조하세요.

필터 목록에서 옵션을 선택하여 모든 탭에 표시되는 이벤트를 필터링할 수 있습니다. 예를 들어, 가용 영역, 리전, 이벤트 종료 시간 또는 마지막 업데이트 시간, AWS 서비스, 서비스 등을 기준으로 결과 범위를 좁힐 수 있습니다.

대시보드에 나타나는 최근 이벤트 대신 모든 이벤트를 보려면 [이벤트 로그](#) 탭을 선택하세요.

#### Note

현재 AWS Health 대시보드에 표시되는 이벤트에 대한 알림은 삭제할 수 없습니다. AWS 서비스에서 이벤트가 해결되면 대시보드 보기에서 알림이 제거됩니다.



## Example : Amazon Elastic Compute Cloud(Amazon EC2)에 대한 운영 문제 이벤트

다음 이미지는 Amazon EC2 인스턴스의 시작 실패 및 연결 문제 이벤트를 보여줍니다.

# Your account health

Stay informed of important events affecting your AWS resources.

[Configure EventBridge](#)

Get notifications for events that might affect your services and resources.

[Go to EventBridge](#)

[Open and recent issues \(16\)](#)
[Scheduled changes \(0\)](#)
[Notifications \(3\)](#)
[Event log](#)

### Open and recent issues (16)

View events that might affect your AWS infrastructure. [35 issues](#) were resolved in the past 24 hours.

Service: Elastic Compute Cloud

Clear filter

< 1 >

#### Event summary

Operational issue - EC2 (Ohio)
Last update: February 20, 2022 at 11:16:34 PM UTC-8
us-east-2

Operational issue - EC2 (Ohio)
Last update: February 17, 2022 at 11:56:09 PM UTC-8
us-east-2

Operational issue - EC2 (N. Virginia)
Last update: February 16, 2022 at 1:36:29 AM UTC-8
us-east-1

### Operational issue - EC2 (Ohio)

[Back to list view](#)

[Details](#)
[Affected resources](#)

#### Event data

Service	Start time
EC2	February 20, 2022 at 11:16:24 PM UTC-8
Status	End time
Open	-
Region / Availability Zone	Category
us-east-1	Issue
Account specific	Affected resources
No	1
<h4>Description</h4> <p>[04:35 AM PST] We are investigating increased EC2 launch failures and networking connectivity issues for some instances in a single Availability Zone (USE1-AZ4) in the US-EAST-1 Region. Other Availability Zones within the US-EAST-1 Region are not affected by this issue.</p>	

## 예약된 변경

예약된 변경 탭을 사용하면 계정에 영향을 미칠 수 있는 예정된 이벤트를 확인할 수 있습니다. 이러한 이벤트에는 서비스에 대한 예약된 유지 관리 활동과 해결을 위해 조치가 필요한 계획된 수명 주기 이벤트가 포함될 수 있습니다. 이러한 활동을 계획하는 데 도움이 되도록 이러한 예약된 변경 사항을 월별 일정에 매핑할 수 있는 일정 보기가 제공됩니다. 필터를 사용할 수 있습니다. 계획된 수명 주기 이벤트에 대한 자세한 내용은 [계획된 라이프사이클 이벤트 AWS Health](#)을(를) 참조하세요.

## 기타 알림

알림 탭을 사용하면 계정에 영향을 미칠 수 있는 지난 7일간의 기타 모든 알림과 진행 중인 이벤트를 볼 수 있습니다. 여기에는 인증서 교체, 결제 알림, 보안 취약성과 같은 이벤트가 포함될 수 있습니다.

## 이벤트 로그

이벤트 로그 탭을 사용하면 모든 AWS Health 이벤트를 볼 수 있습니다. 로그 테이블에는 상태 및 시작 시간을 기준으로 필터링할 수 있는 추가 열이 포함되어 있습니다.

이벤트 로그 테이블에서 이벤트를 선택하면 이벤트에 대한 정보와 영향을 받는 리소스 목록이 포함된 세부 정보 창이 나타납니다. 자세한 내용은 [이벤트 세부 정보](#) 섹션을 참조하세요.

다음 필터 옵션을 선택하여 검색 결과의 범위를 좁힐 수 있습니다:.

- 가용 영역
- 종료 시간
- 이벤트
- 이벤트 ARN
- 이벤트 범주
- 최종 업데이트 시간
- 리전
- 리소스 ID/ARN
- 서비스
- 시작 시간
- 상태

Example : 이벤트 로그

다음 이미지는 미국 동부(버지니아 북부) 및 미국 동부(오하이오) 리전의 최근 이벤트를 보여줍니다.

IAM-user ▼ Global ▼ Support ▼

Last refreshed less than 1 min ago ↻

### Event log

< 1 >

Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2) ✕
Clear filter

Event ▼	Status	Event category ▼	Region / Zone <a href="#">Info</a>	Start time ▼	Last update time ▼	Affected resources
<a href="#">Lambda operational issue</a>	Closed	Issue	us-east-1	October 9, 2020 at 2:03:48 AM UTC-7	October 9, 2020 at 3:11:09 AM UTC-7	-
<a href="#">EC2 operational issue</a>	Closed	Issue	us-east-1	October 9, 2020 at 1:48:51 AM UTC-7	October 9, 2020 at 11:54:16 AM UTC-7	-
<a href="#">SNS operational issue</a>	Closed	Issue	us-east-1	September 30, 2020 at 8:28:18 AM UTC-7	September 30, 2020 at 11:42:54 AM UTC-7	-
<a href="#">EC2 operational issue</a>	Closed	Issue	us-east-1	September 16, 2020 at 7:30:41 AM UTC-7	September 16, 2020 at 7:45:03 AM UTC-7	-
<a href="#">Storagegateway operational issue</a>	Closed	Issue	us-east-1	September 13, 2020 at 12:46:47 PM UTC-7	September 13, 2020 at 6:32:24 PM UTC-7	-
<a href="#">Deepracer operational issue</a>	Closed	Issue	us-east-1	August 31, 2020 at 6:32:39 PM UTC-7	August 31, 2020 at 9:10:12 PM UTC-7	-

## 이벤트 세부 정보

이벤트를 선택하면 이벤트에 대한 두 개의 탭이 나타납니다. 세부 정보 탭에는 다음 정보가 표시됩니다.

- 서비스
- 상태
- 리전 / 가용 영역
- 이벤트가 계정별 이벤트인지 여부
- 시작 및 종료 시간
- 범주
- 영향을 받는 리소스 수
- 이벤트에 대한 설명 및 업데이트 일정

영향을 받는 리소스 탭에는 이벤트의 영향을 받는 모든 AWS 리소스에 대한 다음 정보가 표시됩니다.

- 사용 가능하거나 관련성이 있는 경우 리소스 ID(예: vol-a1b2c34f)와 같은 Amazon EBS 볼륨 ID 또는 Amazon 리소스 이름(ARN)입니다.
- 계획된 수명 주기 이벤트의 경우 영향을 받는 이 리소스 목록에는 리소스의 최신 상태(보류 중, 알 수 없음 또는 해결됨)도 포함됩니다. 이 목록은 보통 24시간마다 새로 고침됩니다.

리소스에 나타나는 항목을 필터링할 수 있습니다. 리소스 ID 또는 ARN으로 결과 범위를 좁힐 수 있습니다.

Example : AWS Lambda에 대한 AWS Health 이벤트

다음 스크린샷은 Lambda의 이벤트 예시를 보여줍니다.

The screenshot displays the AWS Health console interface. On the left, the 'Event log' section shows a list of events filtered by region (US East N. Virginia and US East Ohio). The 'Event summary' section lists several operational issues, with the 'Lambda operational issue' selected. On the right, the 'Lambda operational issue' details are shown, including the event name, status (Closed), region (us-east-1), category (Issue), and a detailed description of the problem and its resolution.

**Event log**

Search: Add filter

Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2) X

Clear filter

< 1 >

**Event summary**

- Lambda operational issue**  
Last update: October 9, 2020 at 3:11:09 AM UTC-7 us-east-1
- EC2 operational issue**  
Last update: October 9, 2020 at 11:54:16 AM UTC-7 us-east-1
- SNS operational issue**  
Last update: September 30, 2020 at 11:42:54 AM UTC-7 us-east-1
- EC2 operational issue**  
Last update: September 16, 2020 at 7:45:03 AM UTC-7 us-east-1
- Storagegateway operational issue**  
Last update: September 13, 2020 at 6:32:24 PM UTC-7 us-east-1
- Deepracer operational issue**  
Last update: August 31, 2020 at 9:10:12 PM UTC-7 us-east-1
- Sagemaker operational issue**  
Last update: August 31, 2020 at 9:04:39 PM UTC-7 us-east-1
- Batch operational issue**

**Lambda operational issue** [Back to list view](#)

Details | Affected resources

**Event data**

Event	Start time
Lambda operational issue	October 9, 2020 at 2:03:48 AM UTC-7
Status	End time
Closed	October 9, 2020 at 3:11:08 AM UTC-7
Region / Availability Zone	Affected resources
us-east-1	-
Category	
Issue	

**Description**

[RESOLVED] Increased Invoke Error Rate

[02:03 AM PDT] We have identified an increase in invoke error rates in the US-EAST-1 Region and are working towards resolution.

[03:11 AM PDT] Between October 8 10:35 PM and October 9 2:25 AM PDT we experienced increased Lambda invoke error rates in the US-EAST-1 Region. The issue has been resolved and the service is operating normally.

## 이벤트 유형

다음과 같은 두 가지 유형의 AWS Health 이벤트가 있습니다.

- 공개 이벤트는 계정에 국한되지 않는 서비스 이벤트입니다. 예를 들어, AWS 리전에 Amazon EC2에 문제가 있는 경우 해당 리전에서 서비스나 리소스를 사용하지 않더라도 AWS Health에서 이벤트에 대한 정보를 제공합니다.
- 계정별 이벤트는 내 계정 또는 조직의 계정에만 해당됩니다. 예를 들어, 사용 중인 리전에서 Amazon EC2 인스턴스에 문제가 있는 경우 AWS Health은(는) 이벤트에 대한 정보와 영향을 받는 Amazon EC2 인스턴스 목록을 제공합니다.

다음 옵션을 사용하여 이벤트가 공개 이벤트인지 계정별 이벤트인지 식별할 수 있습니다.

- AWS Health 대시보드에서 이벤트의 영향을 받는 리소스 탭을 선택합니다. 리소스가 있는 이벤트는 계정에 따라 다릅니다. 리소스가 없는 이벤트는 공개되며 계정에 한정되지 않습니다. 자세한 내용은 [AWS Health 대시 보드 시작하기 - 계정 상태](#) 섹션을 참조하세요.
- AWS Health API를 사용하여 eventScopeCode 파라미터를 반환합니다. 이벤트는 PUBLIC, ACCOUNT\_SPECIFIC 또는 NONE 값을 가질 수 있습니다. 자세한 내용은 AWS Health API 참조에서 [DescribeEventDetails](#) 작업을 참조하세요.

## 일정 보기

일정 보기는 예약된 변경 탭에서 AWS Health 이벤트를 월간 일정으로 계획하는데 사용할 수 있습니다. 이 보기에서는 최대 과거 3개월과 1년 후의 예약된 변경 사항을 확인할 수 있습니다.

AWS Health 이벤트는 날짜별로 표시됩니다. 날짜를 선택하면 AWS Health 이벤트에 대한 추가 세부 정보가 포함된 사이드 패널이 표시됩니다. 예정된 이벤트와 진행 중인 이벤트는 검은색으로 표시됩니다. 완료된 이벤트는 회색으로 표시됩니다. 한 날짜에 이벤트가 두 개 이상 있는 경우 검은색 및 회색 이벤트의 수만 표시됩니다. 날짜를 선택하면 사이드 패널에 AWS Health 이벤트 목록이 표시됩니다. 사이드 패널에서 이벤트를 선택하여 이벤트에 대한 정보를 표시할 수 있습니다. 사이드 패널에는 이전 보기로 이동할 수 있는 브레드크럼이 있습니다.

### Scheduled changes

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

Any event ▼

<

February 2024

>

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday
28	29 2 Upcoming	30 2 Upcoming 1 Completed	31	1	2

☰

⚙️

✕

30 January 2024

Scheduled events starting on 30 January 2024 (Showing 3 of 3) [View all on the table view](#)

EKS planned lifecycle event (us-west-2)

Event status: Upcoming

EKS planned lifecycle event (us-east-1)

Event status: Upcoming

EKS planned lifecycle event (eu-west-1)

Event status: Completed

## 영향을 받는 리소스 보기

계획된 수명 주기 이벤트의 경우 AWS Health 이벤트는 일반적으로 영향을 받는 리소스의 상태를 매일 업데이트합니다. 상태를 보려면 AWS Health 이벤트를 선택하세요. 상태는 사이드 패널의 영향을 받는 리소스 탭에 표시됩니다.

계정 수준 AWS Health 이벤트는 영향을 받는 리소스 탭 상단에 영향을 받는 리소스 상태의 요약 표시합니다. 영향을 받는 리소스 목록이 해당 상태와 함께 표에 표시됩니다. 계획된 수명 주기 이벤트는 리소스 상태 필드를 사용하는 이벤트 유형의 예입니다. 계획된 수명 주기 이벤트에 대한 자세한 내용은 [계획된 라이프사이클 이벤트 AWS Health](#) 항목을 참조하세요.

조직 보기에 액세스하는 경우 AWS Health 이벤트에는 포함된 모든 계정의 영향을 받는 모든 리소스의 상태 요약이 표시됩니다. 다음 요약에는 영향을 받는 계정 목록과 해당 계정에 대해 보류 중인 리소스 수가 나와 있습니다. 계정 번호 또는 보류 중인 리소스 수를 선택하여 계정 보기 요약을 표시합니다. 계정 보기 요약에는 영향을 받는 계정의 조직 목록으로 돌아갈 수 있는 브레드크럼이 있습니다. 영향을 받는 리소스 상태 요약은 분할 패널 상단에 표시됩니다.

## DMS planned lifecycle event



Details

Affected accounts

[Affected accounts](#) > Account 586464445636

## ▼ Summary of affected resources

3

## Affected resources

Resource data is typically refreshed every 24 hours.

<span style="color: red;">■</span> <b>3 Pending</b> May require action	100%
<span style="color: orange;">■</span> <b>0 Unknown</b> Not able to verify status	0%
<span style="color: green;">■</span> <b>0 Resolved</b> No actions required	0%

## Affected resources in account 586464445636 (3)

 Add filter

&lt; 1 &gt;

Resource ID / ARN	Resource status	Last update time
arn:aws:dms:eu-west-1:586464445636:cluster/prod-financedb2	<span style="color: red;">⌚</span> Pending	1 day ago
arn:aws:dms:eu-west-1:586464445636:cluster/prod-financedb	<span style="color: red;">⌚</span> Pending	1 day ago
arn:aws:dms:eu-west-1:586464445636:cluster/prod-2main-db	<span style="color: red;">⌚</span> Pending	1 day ago

## 시간대 설정

AWS Health 대시보드에서 현지 시간대 또는 UTC 시간대로 이벤트를 확인할 수 있습니다. AWS Health 대시보드에서 시간대를 변경하면 대시보드의 모든 타임스탬프와 공개 이벤트가 지정한 시간대로 업데이트됩니다.

시간대 설정을 업데이트하려면

1. <https://health.aws.amazon.com/health/home>에서 AWS Health 대시보드를 엽니다.
2. 페이지 하단에서 쿠키 환경설정을 선택합니다.
3. 기능성 쿠키에 대해 허용을 선택합니다. 그런 다음 기본 설정 저장을 선택합니다.
4. AWS Health 대시보드의 탐색 창에서 시간대 설정을 선택합니다.

5. AWS Health 대시보드 세션의 시간대를 선택합니다. 변경 사항 저장(Save changes)을 선택합니다.


## 조직 상태

AWS Health은(는) AWS Organizations와(과) 통합되어 조직에 속한 모든 계정의 이벤트를 볼 수 있습니다. 조직에 표시되는 이벤트에 대한 중앙 집중식 보기가 제공됩니다. 이러한 이벤트를 사용하여 리소스, 서비스 및 애플리케이션의 변경 사항을 모니터링할 수 있습니다.

자세한 내용은 [조직 보기를 사용하여 계정 간 AWS Health 이벤트 집계](#) 섹션을 참조하세요.


### Enable organizational view

#### Key benefits




**Organization-wide visibility**

Aggregate your Health events from all member AWS accounts in your AWS organization. This provides a centralized view for all events, such as operational issues, scheduled maintenance, and account notifications.



**API access**

If you have a Business or Enterprise Support plan, you can integrate with the AWS Health API to programmatically use organizational view and look up details for events that occur in your organization. [Learn more](#)



**Chat integration**

Using the AWS Health API, you can ingest events into your Amazon Chime or Slack channel to get notified when an event occurs. Filter events to get the ones that matter most to your organization. [Learn more](#)

#### Get started

**1. Set up AWS Organizations**

You must have an AWS organization with all features enabled.

✓ Success

[Manage AWS Organizations](#)
[View documentation](#)

**2. Enable organizational view for AWS Health**

After you set up AWS Organizations and sign in to the management account, you can enable AWS Health to aggregate all events. These events appear in the Personal Health Dashboard.

[Enable organizational view](#)
[View documentation](#)

## Amazon EventBridge 설정

AWS Health 이벤트에 대한 변경 사항을 감지하고 이에 대응하려면 EventBridge를 사용하세요. 계정에서 발생하는 특정 AWS Health 이벤트를 모니터링한 다음 이벤트가 변경되면 AWS Health에서 알림을 받거나 조치를 취하도록 규칙을 설정할 수 있습니다.

### AWS Health와 함께 EventBridge 사용하기

1. <https://health.aws.amazon.com/health/home>에서 AWS Health 대시보드를 엽니다.
2. EventBridge 콘솔로 이동하여 규칙을 생성하려면 다음 중 하나를 수행합니다.
  - 탐색 창의 Health Integrations에서 Amazon EventBridge를 선택합니다.
  - EventBridge 구성에서 EventBridge로 이동을 선택합니다.
3. 규칙을 만들고 이벤트를 모니터링하려면 다음 절차를 따르세요. [Amazon을 통한 AWS Health 이벤트 모니터링 EventBridge](#) 섹션을 참조하세요.



# AWS Health Aware

Slack, JIRA, ServiceNow 등에 상태 이벤트를 전송하는 데 사용할 수 있는 저렴한 비용의 애플리케이션인 [AWS HealthAware](#)를 사용하여 AWS Health API를 시작할 수 있습니다. 현재 무료 라이브 [웨비나](#)에 참가하실 수 있습니다.

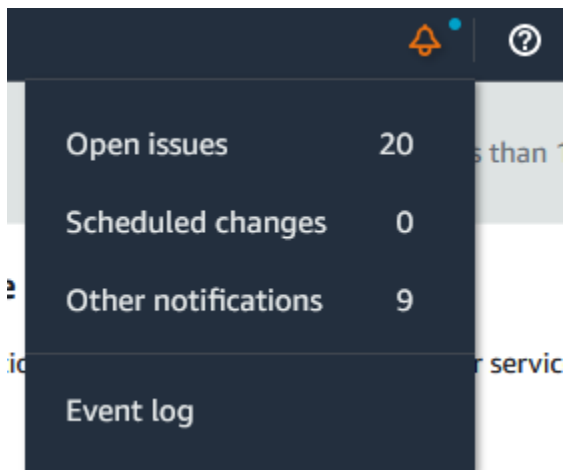
## AWS Health 이벤트에 대한 경보

AWS Health 대시보드의 콘솔 탐색 모음에는 알림 메뉴와 함께 종 모양 아이콘이 있습니다. 이 기능은 각 범주의 대시보드에 나타나는 최근 AWS Health 이벤트 수를 표시합니다. 이 종 모양의 아이콘은 Amazon EC2, Amazon Relational Database Service(RDS), AWS Identity and Access Management(IAM), AWS Trusted Advisor 등 여러 AWS 콘솔에 표시됩니다.

종 아이콘을 선택하여 최근 이벤트가 계정에 영향을 미치는지 확인합니다. 그런 다음 이벤트를 선택하고 AWS Health 대시보드로 이동하여 자세한 정보를 확인할 수 있습니다.

Example : 미결 이벤트

다음 이미지는 계정의 미결 이벤트와 알림 이벤트를 보여줍니다.



# AWS Health에 대한 AWS 사용자 알림 구성

AWS Health는 운영 문제, 계획된 유지 관리, 계획된 소프트웨어 수명 주기 이벤트 등 서비스 운영에 대한 정보를 제공합니다. 영향을 받는 리소스 ID, 현재 상태 (미결 또는 마감), 리소스 상태와 같은 AWS Health 이벤트 세부 정보를 포괄적으로 파악하려면 AWS Health API, Amazon EventBridge의 aws.health 소스, AWS Health 대시보드와 같은 AWS Health 엔드포인트를 사용하는 것이 가장 좋습니다. 이러한 엔드포인트는 워크로드에 영향을 미칠 수 있는 미결 이벤트와 변경 사항에 대한 가장 상세한 실시간 정보를 제공합니다.

[AWS 사용자 알림](#)을 통해 추가 UX 채널(이메일, 채팅 또는 AWS 콘솔 모바일 애플리케이션에 대한 푸시 알림)으로 알림을 받을 수 있습니다. AWS Health 이벤트 알림에는 위에 나열된 엔드포인트만큼 자세한 데이터가 포함되어 있지는 않지만, 이해관계자에게 문제 및 변경 사항을 알릴 수 있는 간단하고 효과적인 방법을 제공합니다. 사용자가 만든 규칙에 따라 사용자 알림은 이벤트가 사용자가 규칙에서 지정된 값과 일치하면 알림을 생성하고 전송합니다. 알림을 전송할 UX 전송 채널을 선택하고, 특정 이벤트에 대해 생성되는 알림 수를 줄이도록 집계를 설정할 수 있습니다. 알림은 콘솔 알림 센터에서도 볼 수 있습니다. 예를 들어, Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스처럼 AWS 계정에 업데이트 예정이 리소스가 있는 경우 채팅 알림을 받을 수 있습니다.

AWS 사용자 알림 설정에 대한 자세한 내용은 [AWS사용자 알림 시작하기](#)를 참조하세요.

# AWS Health API에 액세스

AWS Health은(는) HTTPS를 전송으로, JSON을 메시지 직렬화 형식으로 사용하는 RESTful 웹 서비스입니다. 애플리케이션 코드는 AWS Health API로 직접 요청할 수 있습니다. REST API를 직접 사용하는 경우 요청에 서명하고 이를 인증하기 위해 필요한 코드를 작성해야 합니다. AWS Health 연산 및 매개변수에 대한 자세한 내용은 [AWS Health API Reference](#)를 참조하세요.

## Note

AWS Health API를 사용하려면 [AWS Support](#)의 Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 있어야 합니다. Business, Enterprise On-Ramp, 또는 Enterprise Support 플랜을 보유하지 않은 AWS 계정에서 AWS Health API를 호출하면 `SubscriptionRequiredException` 오류가 발생합니다.

AWS SDK를 사용하여 AWS Health REST API 호출을 래핑할 수 있으므로 애플리케이션 개발을 간소화할 수 있습니다. AWS 자격 증명을 입력하면 이러한 라이브러리에서 인증 및 서명 요청을 처리합니다.

AWS Health은(는) 또한 AWS Management Console에서 이벤트 및 영향을 받는 엔티티를 보고 검색하는 데 사용할 수 있는 AWS Health 대시보드도 제공합니다. [AWS Health 대시보드 시작하기 - 계정 상태](#) 섹션을 참조하세요.

## 엔드포인트

AWS Health API는 [다중 리전 애플리케이션 아키텍처](#)를 따르며 액티브-패시브 구성에 두 개의 리전 엔드포인트가 있습니다. 액티브-패시브 DNS 장애 조치를 지원하기 위해 AWS Health 각 단일 글로벌 엔드포인트를 제공합니다. 글로벌 엔드포인트에서 DNS 검색을 수행하여 액티브 엔드포인트와 해당 서명 AWS 리전을 확인할 수 있습니다. 이렇게 하면 코드에 사용할 엔드포인트를 알 수 있어 AWS Health에서 최신 정보를 파악할 수 있습니다.

글로벌 엔드포인트에 요청할 때는 대상 리전 엔드포인트에 AWS 액세스 보안 인증 정보를 지정하고 해당 리전의 서명을 구성해야 합니다. 그렇지 않으면 인증이 실패할 수 있습니다. 자세한 내용은 [AWS Health API 요청에 서명](#) 섹션을 참조하세요.

다음 표는 기본 구성을 나타낸 것입니다.

설명	서명 리전	Endpoint	프로토콜
액티브	us-east-1	health.us-east-1.amazonaws.com	HTTPS
패시브	us-east-2	health.us-east-2.amazonaws.com	HTTPS
전 세계	us-east-1	global.health.amazonaws.com	HTTPS

**Note**

현재 액티브 엔드포인트의 서명 리전입니다.

엔드포인트가 액티브 엔드포인트인지 확인하려면 글로벌 엔드포인트 CNAME에서 DNS 검색을 수행한 다음 확인된 이름에서 AWS 리전을 추출합니다.

Example : 글로벌 엔드포인트에서 DNS 검색

다음 명령은 global.health.amazonaws.com 엔드포인트에서 DNS 검색을 완료합니다. 그러면 이 명령은 us-east-1 리전 엔드포인트를 반환합니다. 이 출력은 AWS Health에 어느 엔드포인트를 사용해야 하는지 알려줍니다.

```
dig global.health.amazonaws.com | grep CNAME
```

```
global.health.amazonaws.com. 10 IN CNAME health.us-east-1.amazonaws.com
```

#### **Tip**

액티브 엔드포인트와 패시브 엔드포인트 모두 AWS Health 데이터를 반환합니다. 하지만 최신 AWS Health 데이터는 액티브 엔드포인트에서만 사용할 수 있습니다. 패시브 엔드포인트의 데이터는 결국 액티브 엔드포인트와 일치하게 됩니다. 액티브 엔드포인트가 변경되면 모든 워크플로우를 다시 시작하는 것이 좋습니다.

## 고가용성 엔드포인트 데모 사용

다음 코드 예제에서는 AWS Health가 글로벌 엔드포인트에 대한 DNS 검색을 사용하여 액티브 리전 엔드포인트와 서명 리전을 결정합니다. 그런 다음 액티브 엔드포인트가 변경되면 코드가 워크플로우를 다시 시작합니다.

주제

- [Java 데모 사용](#)
- [Python 데모 사용](#)

### Java 데모 사용

전제 조건

[Gradle](#)을 설치해야 합니다.

Java 예제를 사용하려면

1. GitHub에서 [AWS Health 고가용성 엔드포인트 데모](#)를 다운로드하세요.
2. 데모 프로젝트 high-availability-endpoint/java 디렉터리로 이동합니다.
3. 명령줄 창에 다음 명령을 입력합니다.

```
gradle build
```

4. 다음 명령을 입력하여 AWS 보안 인증 정보를 지정합니다.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"  
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY"  
export AWS_SESSION_TOKEN="your-aws-token"
```

5. 다음 명령을 입력하여 데모를 실행합니다.

```
gradle run
```

Example : AWS Health 이벤트 출력

코드 예제는 AWS 계정에서 지난 7일간의 최근 AWS Health 이벤트를 반환합니다. 다음 예제의 출력에는 AWS Config 서비스에 대한 AWS Health 이벤트가 포함됩니다.

```
> Task :run
[main] INFO aws.health.high.availability.endpoint.demo.HighAvailabilityV2Workflow
- EventDetails(Event=Event(Arn=arn:aws:health:global::event/CONFIG/
AWS_CONFIG_OPERATIONAL_NOTIFICATION/AWS_CONFIG_OPERATIONAL_NOTIFICATION_88a43e8a-
e419-4ca7-9baa-56bcde4dba3,
Service=CONFIG, EventTypeCode=AWS_CONFIG_OPERATIONAL_NOTIFICATION,
EventTypeCategory=accountNotification, Region=global,
StartTime=2020-09-11T02:55:49.899Z, LastUpdatedTime=2020-09-11T03:46:31.764Z,
StatusCode=open, EventScopeCode=ACCOUNT_SPECIFIC),
EventDescription=EventDescription(LatestDescription=As part of our ongoing efforts
to optimize costs associated with recording changes related to certain ephemeral
workloads,
AWS Config is scheduled to release an update to relationships modeled within
ConfigurationItems (CI) for 7 EC2 resource types on August 1, 2021.
Examples of ephemeral workloads include changes to Amazon Elastic Compute Cloud
(Amazon EC2) Spot Instances, Amazon Elastic MapReduce jobs, and Amazon EC2
Autoscaling.
This update will optimize CI models for EC2 Instance, SecurityGroup, Network
Interface, Subnet, VPC, VPN Gateway, and Customer Gateway resource types to record
direct relationships and deprecate indirect relationships.
```

A direct relationship is defined as a one-way relationship (A->B) between a resource (A) and another resource (B), and is typically derived from the Describe API response of resource (A).

An indirect relationship, on the other hand, is a relationship that AWS Config infers (B->A), in order to create a bidirectional relationship.

For example, EC2 instance -> Security Group is a direct relationship, since security groups are returned as part of the describe API response for an EC2 instance.

But Security Group -> EC2 instance is an indirect relationship, since EC2 instances are not returned when describing an EC2 Security group.

Until now, AWS Config has recorded both direct and indirect relationships. With the launch of Advanced queries in March 2019, indirect relationships can easily be answered by running Structured Query Language (SQL) queries such as:

```
SELECT
  resourceId,
  resourceType
WHERE
  resourceType = 'AWS::EC2::Instance'
AND
  relationships.resourceId = 'sg-234213'
```

By deprecating indirect relationships, we can optimize the information contained within a Configuration Item while reducing AWS Config costs related to relationship changes.

This is especially useful in case of ephemeral workloads where there is a high volume of configuration changes for EC2 resource types.

Which resource relationships are being removed?

Resource Type: Related Resource Type

- 1 AWS::EC2::CustomerGateway: AWS::VPN::Connection
- 2 AWS::EC2::Instance: AWS::EC2::EIP, AWS::EC2::RouteTable
- 3 AWS::EC2::NetworkInterface: AWS::EC2::EIP, AWS::EC2::RouteTable
- 4 AWS::EC2::SecurityGroup: AWS::EC2::Instance, AWS::EC2::NetworkInterface
- 5 AWS::EC2::Subnet: AWS::EC2::Instance, AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable
- 6 AWS::EC2::VPC: AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::Subnet, AWS::EC2::VPNGateway, AWS::EC2::SecurityGroup
- 7 AWS::EC2::VPNGateway: AWS::EC2::RouteTable, AWS::EC2::VPNConnection

Alternate mechanism to retrieve this relationship information:

The `SelectResourceConfig` API accepts a SQL `SELECT` command, performs the corresponding search, and returns resource configurations matching the properties. You can use this API to retrieve the same relationship information.

For example, to retrieve the list of all EC2 Instances related to a particular VPC `vpc-1234abc`, you can use the following query:

```
SELECT
  resourceId,
  resourceType
WHERE
  resourceType = 'AWS::EC2::Instance'
AND
  relationships.resourceId = 'vpc-1234abc'
```

If you have any questions regarding this deprecation plan, please contact AWS Support [1]. Additional sample queries to retrieve the relationship information for the resources listed above is provided in [2].

[1] <https://aws.amazon.com/support>

[2] <https://docs.aws.amazon.com/config/latest/developerguide/examplerelationshipqueries.html>),

```
EventMetadata={})
```

## Java 리소스

- 자세한 내용은 AWS SDK for Java API 참조의 [Interface HealthClient](#) 및 [소스 코드](#)를 참조하세요.
- 이 데모에서 DNS 검색에 사용되는 라이브러리에 대한 자세한 내용은 GitHub의 [dnsjava](#)를 참조하세요.

## Python 데모 사용

### 전제 조건

[Python 3](#)을 설치해야 합니다.

Python 예제를 사용하려면

1. GitHub에서 [AWS Health 고가용성 엔드포인트 데모](#)를 다운로드하세요.
2. 데모 프로젝트 high-availability-endpoint/python 디렉터리로 이동합니다.
3. 명령줄 창에 다음 명령을 입력합니다.

```
pip3 install virtualenv
virtualenv -p python3 v-aws-health-env
```

#### Note

Python 3.3 이상의 경우 virtualenv를 설치하는 대신 내장 venv 모듈을 사용하여 가상 환경을 만들 수 있습니다. 자세한 내용은 Python 웹 사이트의 [venv - Creation of virtual environments](#)를 참조하세요.

```
python3 -m venv v-aws-health-env
```

4. 다음 명령을 입력하여 가상 환경을 활성화합니다.

```
source v-aws-health-env/bin/activate
```

5. 다음 명령을 입력하여 존속성을 설치합니다.



```
pip install -r requirements.txt
```

6. 다음 명령을 입력하여 AWS 보안 인증 정보를 지정합니다.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

7. 다음 명령을 입력하여 데모를 실행합니다.

```
python3 main.py
```

Example : AWS Health 이벤트 출력

코드 예제는 AWS 계정에서 지난 7일간의 최근 AWS Health 이벤트를 반환합니다. 다음 출력은 AWS 보안 알림에 대한 AWS Health 이벤트를 반환합니다.

```
INFO:botocore.credentials:Found credentials in environment variables.
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-
a9a5-876544042721',
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',
'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':
datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9,
547000, tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'},
description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
endpoints.\n\nWe
are in the process of updating all AWS Federal Information Processing Standard
(FIPS) endpoints across all AWS regions
to Transport Layer Security (TLS) version 1.2 by March 31, 2021 . In order to avoid
an interruption in service, we encourage you to act now, by ensuring that you
connect to AWS FIPS endpoints at a TLS version of 1.2.
If your client applications fail to support TLS 1.2 it will result in connection
failures when TLS versions below 1.2 are no longer supported.\n\nBetween now and
March 31, 2021 AWS will remove TLS 1.0 and TLS 1.1 support from each FIPS endpoint
where no connections below TLS 1.2 are detected over a 30-day period.
After March 31, 2021 we may deploy this change to all AWS FIPS endpoints, even if
there continue
```

to be customer connections detected at TLS versions below 1.2. \n\nWe will provide additional updates and reminders on the AWS Security Blog, with a 'TLS' tag [1]. If you need further guidance or assistance, please contact AWS Support [2] or your Technical Account Manager (TAM).

Additional information is below.\n\nHow can I identify clients that are connecting with TLS

1.0/1.1?\n\nFor customers using S3 [3], Cloudfront [4] or Application Load Balancer [5] you can use your access logs to view the TLS connection information for these services, and identify client connections that are not at TLS 1.2. If you are using the AWS Developer Tools on your clients, you can find information on how to properly configure your client's TLS versions by visiting Tools to Build on AWS [7] or our associated AWS Security Blog has a link for each unique code language [7].\n\nWhat is Transport Layer Security (TLS)? \n\nTransport Layer Security (TLS Protocols) are cryptographic protocols designed to provide secure communication across a computer network [6].\n\nWhat are AWS FIPS endpoints? \n\nAll AWS services offer Transport Layer Security (TLS) 1.2 encrypted endpoints that can be used for all API calls. Some AWS services also offer FIPS 140-2 endpoints [9] for customers that require use of FIPS validated cryptographic libraries. \n\n[1] <https://aws.amazon.com/blogs/security/tag/tls/>\n[2] <https://aws.amazon.com/support>\n[3] <https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html>\n[4] <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html>\n[5] <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>\n[6] <https://aws.amazon.com/tools>\n[7] <https://aws.amazon.com/blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints>\n[8] [https://en.wikipedia.org/wiki/Transport\\_Layer\\_Security](https://en.wikipedia.org/wiki/Transport_Layer_Security)\n[9] <https://aws.amazon.com/compliance/fips>}

8. 완료한 후 다음 명령을 입력하여 가상 컴퓨터를 비활성화합니다.

```
deactivate
```

## Python 리소스

- Health. Client에 대한 자세한 내용은 [Python\(Boto3\)용 AWS SDK API 참조](#)를 참조하세요.
- 이 데모에서 DNS 검색에 사용되는 라이브러리에 대한 자세한 내용은 [dnspython](#) 툴킷 및 GitHub의 [소스 코드](#)를 참조하세요.

# AWS Health API 요청에 서명

AWS SDK 또는 AWS Command Line Interface(AWS CLI)을(를) 사용하여 AWS에 요청을 하면 이러한 도구는 도구를 구성할 때 지정한 액세스 키로 요청에 자동으로 서명합니다. 예를 들어 이전고가용성 엔드포인트 데모에 AWS SDK for Java를 사용하는 경우 요청에 서명할 필요가 없습니다.

## Java 코드 예

AWS SDK for Java로 AWS Health API를 사용하는 방법에 대한 추가 예제는 이 [예제 코드](#)를 참조하세요.

요청할 때 AWS Health에 정기적으로 액세스하기 위해 AWS 루트 계정 자격 증명을 사용하지 않는 것이 좋습니다. 그 대신 IAM 사용자의 자격 증명을 사용하면 됩니다. 자세한 내용은 IAM 사용 설명서에서 [AWS 계정 루트 사용자 액세스 키 잠그기](#)를 참조하세요.

AWS SDK 또는 AWS CLI을(를) 사용하지 않는 경우 요청에 직접 서명해야 합니다. AWS 시그니처 버전 4를 사용하는 것이 좋습니다. 자세한 내용은 AWS 일반 참조의 [AWS API 요청 서명](#)을 참조하세요.

# AWS Health에서 지원되는 작업

AWS Health에서 AWS 계정에 영향을 주는 이벤트 관련 정보를 얻을 수 있는 작업은 다음과 같습니다.

- AWS Health에서 지원되는 이벤트 유형
- 지정된 필터 기준에 맞는 하나 이상의 이벤트에 대한 정보
- 하나 이상의 이벤트가 영향을 미치는 엔터티에 대한 정보
- 지정된 필터 기준에 맞는 범주별 이벤트 또는 엔터티 수

모든 작업은 변경을 허용하지 않습니다. 즉 데이터를 검색하나 수정하지는 않습니다. 다음 단원에서는 AWS Health 작업에 대해서 간략하게 살펴보겠습니다.

## 이벤트 유형

[DescribeEventTypes](#) 작업은 필요에 따라 지정한 필터에 맞는 이벤트 유형을 검색합니다. 이벤트 유형은 이벤트의 AWS 서비스, 이벤트 유형 코드 및 범주 등을 정의해 놓은 템플릿입니다. 이벤트 유형과 이벤트는 객체 지향 프로그래밍의 클래스 및 객체와 유사합니다. AWS Health에서 지원하는 이벤트 유형 수는 앞으로 계속 늘어납니다.

## 이벤트

[DescribeEvents](#) 작업은 AWS 계정과 관련된 이벤트의 요약 정보를 검색합니다. 이 이벤트는 AWS 운영 문제, AWS 인프라의 예약된 변경 또는 보안 및 결제 알림과 관련될 수 있습니다.

[DescribeEventDetails](#) 작업은 AWS 서비스, 리전, 가용 영역, 이벤트 시작 및 종료 시간, 텍스트 설명 등 하나 이상의 이벤트에 대한 세부 정보를 검색합니다.

영향을 받는 엔터티

[DescribeAffectedEntities](#) 작업은 하나 이상의 이벤트가 해당되는 엔터티에 대한 정보를 검색합니다. AWS 리소스에 할당된 상태 등 추가 기준으로 결과를 필터링할 수 있습니다.

집계

[DescribeEventAggregates](#) 작업은 각 이벤트 유형 범주의 이벤트 수를 검색하며, 필요에 따라 여러 기준으로 필터링할 수 있습니다. [DescribeEntityAggregates](#) 작업은 하나 이상의 지정된 이벤트에 의해 영향을 받는 엔터티(리소스) 수를 검색합니다.

AWS Organizations 및 조직 보기

DescribeEventsForOrganization

[DescribeEventsForOrganization](#)은 지정된 필터 기준을 충족하는 AWS Organizations의 이벤트에 대한 요약 정보를 반환합니다.

DescribeAffectedAccountsForOrganization

[DescribeAffectedAccountsForOrganization](#)은 제공된 이벤트의 영향을 받은 AWS Organizations조직 내 AWS 계정 목록을 반환합니다.

DescribeEventDetailsForOrganization

[DescribeEventDetailsForOrganization](#)은 AWS Organizations에 있는 하나 이상의 계정에 대해 지정된 하나 이상의 이벤트에 대한 자세한 정보를 반환합니다.

DescribeAffectedEntitiesForOrganization

[DescribeAffectedEntitiesForOrganization](#)은 필터 기준에 따라 조직 내 하나 이상의 계정에 대해 하나 이상의 이벤트에 의해 영향을 받은 엔터티 목록을 반환합니다.

EnableHealthServiceAccessForOrganization

[EnableHealthServiceAccessForOrganization](#)은 고객을 대신하여 AWS Organizations와(과) 상호 작용할 수 있는 AWS Health 서비스 권한을 부여하고 조직의 관리 계정에 서비스 연결 역할을 적용합니다.

## DisableHealthServiceAccessForOrganization

[DisableHealthServiceAccessForOrganization](#) 작업은 고객을 대신하여 AWS Health 서비스가 AWS Organizations와(과) 상호 작용할 수 있는 권한을 취소합니다.

## DescribeHealthServiceStatusForOrganization

[DescribeHealthServiceStatusForOrganization](#) 작업은 조직과의 작업인 AWS Health를 활성화 또는 비활성화에 대한 상태 정보를 제공합니다.

이러한 작업에 대한 자세한 내용은 [AWS Health API 참조](#)를 참조하세요.

# AWS Health API용 샘플 Java 코드

다음 Java 코드 예제에서는 AWS Health 클라이언트를 시작하고 이벤트 및 엔터티에 대한 정보를 검색하는 방법을 보여줍니다.

## 1단계: 자격 증명 초기화

AWS Health API와 통신하려면 유효한 자격 증명이 필요합니다. AWS 계정과 연결된 모든 IAM 사용자의 키 페어를 사용할 수 있습니다.

[AWSCredentials](#) 인스턴스를 만들고 초기화합니다.

```
AWSCredentials credentials = null;
try {
    credentials = new ProfileCredentialsProvider("default").getCredentials();
} catch (Exception e) {
    throw new AmazonClientException(
        "Cannot load the credentials from the credential profiles file. "
        + "Please make sure that your credentials file is at the correct "
        + "location (/home/username/.aws/credentials), and is in valid format.", e);
}
```

## 2단계: AWS Health API 클라이언트 초기화

이전 단계에서 초기화한 자격 증명 객체를 사용하여 AWS Health 클라이언트를 만듭니다.

```
import com.amazonaws.services.health.AWSHealthClient;

AWSHealth awsHealthClient = new AWSHealthClient(credentials);
```

## 3단계: AWS Health API 작업을 사용하여 이벤트 정보 가져오기

### DescribeEvents

```
import com.amazonaws.services.health.model.DescribeEventsRequest;
import com.amazonaws.services.health.model.DescribeEventsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventsRequest request = new DescribeEventsRequest();

EventFilter filter = new EventFilter();
// Filter on any field from the supported AWS Health EventFilter model.
// Here is an example for Region us-east-1 events from the EC2 service.
filter.setServices(singletonList("EC2"));
filter.setRegions(singletonList("us-east-1"));
request.setFilter(filter);

DescribeEventsResult response = awsHealthClient.describeEvents(request);
List<Event> resultEvents = response.getEvents();

Event currentEvent = null;
for (Event event : resultEvents) {
    // Display result event data; here is a subset.
    System.out.println(event.getArn());
    System.out.println(event.getService());
    System.out.println(event.getRegion());
    System.out.println(event.getAvailabilityZone());
    System.out.println(event.getStartTime());
    System.out.println(event.getEndTime());
}
```

### DescribeEventAggregates

```
import com.amazonaws.services.health.model.DescribeEventAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEventAggregatesResult;
import com.amazonaws.services.health.model.EventAggregate;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventAggregatesRequest request = new DescribeEventAggregatesRequest();
// set the aggregation field
request.setAggregateField("eventTypeCategory");
```

```
// filter more on result if needed
EventFilter filter = new EventFilter();
filter.setRegions(singleton("us-east-1"));
request.setFilter(filter);

DescribeEventAggregatesResult response =
    awsHealthClient.describeEventAggregates(request);

// print event count for each eventTypeCategory
for (EventAggregate aggregate: response.getEventAggregates()) {
    System.out.println("Event Category:" + aggregate.getAggregateValue());
    System.out.println("Event Count:" + aggregate.getCount());
}
```

## DescribeEventDetails

```
import com.amazonaws.services.health.model.DescribeEventDetailsRequest;
import com.amazonaws.services.health.model.DescribeEventDetailsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventDetails;

DescribeEventDetailsRequest describeEventDetailsRequest = new
    DescribeEventDetailsRequest();
// set event ARN and local value

describeEventDetailsRequest.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));
describeEventDetailsRequest.setLocale("en-US");
filter.setEventArns
DescribeEventDetailsResult describeEventDetailsResult =
    awsHealthClient.describeEventDetails(request);
EventDetails eventDetail = describeEventDetailsResult.getSuccessfulSet().get(0);

// check event-related fields
Event event = eventDetail.getEvent();
System.out.println(event.getService());
System.out.println(event.getRegion());
System.out.println(event.getAvailabilityZone());
System.out.println(event.getStartTime());
System.out.println(event.getEndTime());

// print out event description
```

```
System.out.println(eventDetail.getEventDescription().getLatestDescription());
```

## DescribeAffectedEntities

```
import com.amazonaws.services.health.model.AffectedEntity;
import com.amazonaws.services.health.model.DateTimeRange;
import com.amazonaws.services.health.model.DescribeAffectedEntitiesRequest;
import
    com.amazonaws.services.health.model.DescribeAffectedEntitiesResult;

DescribeAffectedEntitiesRequest request = new DescribeAffectedEntitiesRequest();
EntityFilter filter = new EntityFilter();

filter.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeAffectedEntitiesResult response =
    awsHealthClient.describeAffectedEntities(request);

for (AffectedEntity affectedEntity: response.getEntities()) {
    System.out.println(affectedEntity.getEntityValue());
    System.out.println(affectedEntity.getAwsAccountId());
    System.out.println(affectedEntity.getEntityArn());
}
```

## DescribeEntityAggregates

```
import com.amazonaws.services.health.model.DescribeEntityAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEntityAggregatesResult;
import com.amazonaws.services.health.model.EntityAggregate;

DescribeEntityAggregatesRequest request = new DescribeEntityAggregatesRequest();

request.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeEntityAggregatesResult response =
    awsHealthClient.describeEntityAggregates(request);

for (EntityAggregate entityAggregate : response.getEntityAggregates()) {
    System.out.println(entityAggregate.getEventArn());
    System.out.println(entityAggregate.getCount());
}
```



```
}
```

# 보안 입력 AWS Health

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

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 [프로그램별 범위 내 AWS 서비스 규정 준수](#) 참조하십시오. AWS Health
- 클라우드에서의 보안 - 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 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 Health됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 AWS Health 충족하도록 구성하는 방법을 보여줍니다. 또한 AWS Health 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

## 주제

- [데이터 보호: AWS Health](#)
- [AWS Health의 Identity and Access Management\(IAM\)](#)
- [로그인 및 모니터링 AWS Health](#)
- [규정 준수 검증: AWS Health](#)
- [의 탄력성 AWS Health](#)
- [AWS Health에서 인프라 보안](#)
- [의 구성 및 취약성 분석 AWS Health](#)
- [AWS Health의 보안 모범 사례](#)

## 데이터 보호: AWS Health

AWS [공동 책임 모델](#) 의 데이터 보호에 적용됩니다 AWS Health. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 사용자는 인프라에서 호

스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시 FAQ](#)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 [AWS 공동 책임 모델 및 GDPR](#) 블로그 게시물을 참조하세요.

데이터 보호를 위해 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(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\(Federal Information Processing Standard\) 140-2](#)를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API AWS Health 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.

## 데이터 암호화

데이터를 AWS Health 암호화하는 방법에 대한 다음 정보를 참조하십시오.

데이터 암호화란 전송 중 (서비스에서 사용자 AWS 계정으로 이동하는 동안) 및 유휴 상태 (서비스에 저장되는 동안) 를 보호하는 것을 말합니다. AWS 전송 계층 보안(TLS)을 사용하여 전송 중인 데이터를 보호하거나 클라이언트 측 암호화를 사용하여 유휴 상태인 데이터를 보호할 수 있습니다.

AWS Health 이벤트 발생 시 이메일 주소나 고객 이름과 같은 개인 식별 정보 (PII) 를 기록하지 않습니다.

## 저장 중 암호화

에 AWS Health 저장된 모든 데이터는 저장 시 암호화됩니다.

## 전송 중 암호화

주고 받는 AWS Health 모든 데이터는 전송 중에 암호화됩니다.

## 키 관리

AWS Health 클라우드에서 암호화된 데이터에 대한 고객 관리 암호화 키는 지원하지 않습니다. AWS

# AWS Health의 Identity and Access Management(IAM)

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. AWS Health IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

### 주제

- [고객](#)
- [ID를 통한 인증](#)
- [정책을 사용한 액세스 관리](#)
- [IAM의 AWS Health 작동 방식](#)
- [AWS Health ID 기반 정책 예제](#)
- [AWS Health ID 및 액세스 문제 해결](#)
- [AWS Health의 서비스 링크 역할 사용](#)
- [AWS 관리형 정책은 다음과 같습니다. AWS Health](#)

## 고객

사용하는 방식 AWS Identity and Access Management (IAM) 은 수행하는 작업에 따라 다릅니다. AWS Health

서비스 사용자 - AWS Health 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS Health 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할

수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AWS Health의 기능에 액세스할 수 없는 경우 [AWS Health ID 및 액세스 문제 해결](#)을 참조하세요.

서비스 관리자 — 회사에서 AWS Health 리소스를 담당하는 경우 전체 액세스 권한이 있을 수 AWS Health 있습니다. 서비스 사용자가 액세스해야 하는 AWS Health 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 Health알아보려면 [IAM의 AWS Health 작동 방식](#)을 참조하십시오.

IAM 관리자 - IAM 관리자라면 AWS Health에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 AWS Health ID 기반 정책의 예를 보려면 [AWS Health ID 기반 정책 예제](#)를 참조하십시오.

## ID를 통한 인증

인증은 자격 증명 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 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 방법](#)을 참조하십시오. 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 서명](#)을 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\(MFA\) 사용](#)을 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 이

메일 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 태스크](#)를 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 증명에 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명에 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체](#)를 참조하세요.

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

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 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 역할](#)은 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 사용](#)을 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 증명에 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 [타사 자격 증명 공급자의 역할 만들기](#)를 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 세트](#)를 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 서비스 경우에는 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 차이](#)를 참조하세요.
- **서비스 간 액세스** — 일부는 다른 AWS 서비스 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 서비스 서비스에 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 세션](#)을 참조하세요.
- **서비스 역할** - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 [IAM 역할](#)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [AWS 서비스에 대한 권한을 위임할 역할 생성](#)을 참조하세요.
- **서비스 연결 역할** — 서비스 연결 역할은 연결된 서비스 역할의 한 유형입니다. AWS 서비스 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 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 프로파일을 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 부여](#)를 참조하세요.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 [IAM 사용 설명서](#)의 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 거부되는지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 [JSON 정책 개요](#)를 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 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성](#)을 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 선택](#)을 참조하세요.

### 리소스 기반 정책

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



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

AWS Health 리소스 기반 조건을 지원합니다. 사용자가 볼 수 있는 AWS Health 이벤트를 지정할 수 있습니다. 예를 들어, AWS Health Dashboard에서 IAM 사용자에게만 특정 Amazon EC2 이벤트에 대한 액세스를 허용하는 정책을 만들 수 있습니다.

자세한 정보는 [리소스](#)를 참조하세요.

## 액세스 제어 목록

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

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 [액세스 제어 목록\(ACL\) 개요](#)를 참조하세요.

AWS Health ACL은 지원하지 않습니다.

## 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 엔티티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔티티의 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 엔티티에 대한 권한 경계](#)를 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 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 [SCP 작동 방식](#)을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할 자

격 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 정책](#)을 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 로직](#)을 참조하십시오.

## IAM의 AWS Health 작동 방식

IAM을 사용하여 액세스를 관리하려면 먼저 어떤 IAM 기능과 함께 사용할 수 있는지 이해해야 합니다. AWS Health AWS Health기타 AWS 서비스가 AWS Health IAM과 연동되는 방식을 자세히 알아보려면 IAM 사용 설명서의 [IAM과 연동되는AWS 서비스를](#) 참조하십시오.

### 주제

- [AWS Health 보안 인증 기반 정책](#)
- [AWS Health 리소스 기반 정책](#)
- [AWS Health 태그 기반 인증](#)
- [AWS Health IAM 역할](#)

## AWS Health 보안 인증 기반 정책

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스 및 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. AWS Health 는 특정 작업, 리소스 및 조건 키를 지원합니다. JSON 정책에서 사용하는 모든 요소에 대해 알고 싶다면 IAM 사용 설명서의 [IAM JSON 정책 요소 참조](#)를 참조하십시오.

### 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 Action요소는 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 Health 사용합니다. health: 예를 들어, [DescribeEventDetails API 작업을 통해 특정 이벤트에 대한 세부](#) 정보를 볼 수 있는 권한을 다른 사람에게 부여하려면 해당 작업을 정책에 포함해야 합니다. health:DescribeEventDetails

정책 설명에는 Action OR NotAction 요소가 포함되어야 합니다. AWS Health 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 집합을 정의합니다.

명령문 하나에 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
    "health:action1",
    "health:action2"
```

와일드카드(\*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, Describe라는 단어로 시작하는 모든 작업을 지정하려면 다음 작업을 포함합니다.

```
"Action": "health:Describe*"
```

AWS Health 작업 목록을 보려면 IAM 사용 설명서의 [정의된 AWS Health작업](#)을 참조하십시오.

## 리소스

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

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 Resource 또는 NotResource 요소가 반드시 추가되어야 합니다. 모범 사례에 따라 [Amazon 리소스 이름\(ARN\)](#)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

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

```
"Resource": "*"

```

AWS Health 이벤트는 다음과 같은 Amazon 리소스 이름 (ARN) 형식을 가집니다.

```
arn:${Partition}:health:*::event/service/event-type-code/event-ID
```

예를 들어, EC2\_INSTANCE\_RETIREMENT\_SCHEDULED\_ABC123-DEF456 이벤트를 문에 지정하려면 다음 ARN을 사용합니다.

```
"Resource": "arn:aws:health:*::event/EC2/EC2_INSTANCE_RETIREMENT_SCHEDULED/EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456"
```

특정 계정에 속하는 Amazon EC2 AWS Health 이벤트를 모두 지정하려면 와일드카드 (\*) 를 사용합니다.

```
"Resource": "arn:aws:health:*::event/EC2/*/*"
```

ARN 형식에 대한 자세한 내용은 [Amazon 리소스 이름 \(ARN\) 및 AWS 서비스](#) 네임스페이스를 참조하십시오.

일부 AWS Health 작업은 특정 리소스에서 수행할 수 없습니다. 이러한 경우, 와일드카드(\*)를 사용해야 합니다.

```
"Resource": ""
```

AWS Health API 작업에는 여러 리소스가 포함될 수 있습니다. 예를 들어 [DescribeEvents](#) 작업은 지정된 필터 기준을 충족하는 이벤트에 대한 정보를 반환합니다. 즉, IAM 사용자에게 이 이벤트를 볼 수 있는 권한이 있어야 합니다.

단일 문에서 여러 리소스를 지정하려면 ARN을 쉼표로 구분합니다.

```
"Resource": [
    "resource1",
    "resource2"
```

AWS Health 상태 이벤트에 대한 리소스 수준 권한과 [DescribeAffectedEntities](#) 및 [DescribeEventDetails](#) API 작업에 대한 리소스 수준 권한만 지원합니다. 자세한 정보는 [리소스 및 작업 기반 조건](#)을 참조하세요.

AWS Health 리소스 유형 및 해당 ARN 목록을 보려면 IAM 사용 설명서의 [리소스 정의 AWS Health](#) 기준을 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 [AWS Health가 정의한 작업](#)을 참조하세요.

## 조건 키

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

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

한 문에서 여러 Condition요소를 지정하거나 단일 Condition요소에서 여러 키를 지정하는 경우 AWS 는 논리적 AND태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 OR 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

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

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 [AWS 설명서의 글로벌 조건 컨텍스트 키](#)를 참조하십시오.

AWS Health 자체 조건 키 세트를 정의하며 일부 글로벌 조건 키 사용도 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 설명서의 [AWS 글로벌 조건 컨텍스트 키](#)를 참조하십시오.

[DescribeAffected개체](#) 및 [DescribeEvent세부 정보](#) API 작업은 health:eventTypeCode 및 health:service 조건 키를 지원합니다.

AWS Health 조건 키 목록을 보려면 IAM 사용 설명서의 [조건 키를 참조하십시오 AWS Health](#). 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 [작업 정의 기준](#)을 참조하십시오. AWS Health

## 예제

AWS Health ID 기반 정책의 예를 보려면 을 참조하십시오. [AWS Health ID 기반 정책 예제](#)

## AWS Health 리소스 기반 정책

리소스 기반 정책은 지정된 보안 주체가 리소스에서 수행할 수 있는 작업과 조건을 지정하는 JSON 정책 문서입니다. AWS Health AWS Health 상태 이벤트에 대한 리소스 기반 권한 정책을 지원합니다. 리

소스 기반 정책을 사용하여 리소스별로 다른 계정에 사용 권한을 부여할 수 있습니다. 또한 리소스 기반 정책을 사용하여 AWS 서비스가 이벤트에 액세스하도록 허용할 수 있습니다. AWS Health

크로스 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 엔티티를 [리소스 기반 정책의 보안 주체](#)로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 서로 다른 AWS 계정에 있는 경우 보안 주체에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔티티에 보안 인증 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용자 설명서의 [IAM 역할과 리소스 기반 정책의 차이](#)를 참조합니다.

AWS Health [DescribeAffected엔티티](#) 및 [DescribeEvent디테일](#) API 작업에 대한 리소스 기반 정책만 지원합니다. 정책에서 이러한 작업을 지정하여 이벤트에 대한 작업을 수행할 수 있는 보안 주체 (계정, 사용자, 역할 및 연동 사용자) 를 정의할 수 있습니다. AWS Health

예제

AWS Health 리소스 기반 정책의 예를 보려면 을 참조하십시오. [리소스 및 작업 기반 조건](#)

## AWS Health 태그 기반 인증

AWS Health 리소스에 태그를 지정하거나 태그를 기반으로 액세스를 제어하는 기능은 지원하지 않습니다.

## AWS Health IAM 역할

[IAM 역할](#)은 AWS 계정 내에서 특정 권한을 가진 엔티티입니다.

임시 자격 증명 사용: AWS Health

임시 보안 인증을 사용하여 페더레이션을 통해 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. [AssumeRole](#) 또는 [GetFederationToken](#) 과 같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 얻습니다.

AWS Health 임시 자격 증명 사용을 지원합니다.

## 서비스 연결 역할

[서비스 연결 역할](#)을 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 Health 서비스 연결 역할을 통합할 수 있도록 지원합니다. AWS Organizations이 서비스 연결 역할의 이름은 `AWSServiceRoleForHealth_Organizations`입니다. 이 역할에는 [Health OrganizationsService RolePolicy](#) AWS 관리형 정책이 첨부되어 있습니다. AWS 관리형 정책을 사용하면 AWS Health 조직 내 다른 AWS 계정의 건강 이벤트에 액세스할 수 있습니다.

[EnableHealthServiceAccessForOrganization](#) 작업을 사용하여 계정에 서비스 연결 역할을 만들 수 있습니다. 하지만 이 기능을 사용하지 않도록 설정하려면 먼저 작업을 호출해야 합니다. [DisableHealthServiceAccessForOrganization](#) 그런 다음 IAM 콘솔, IAM API 또는 AWS Command Line Interface ()AWS CLI를 통해 역할을 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 사용](#)을 참조하십시오.

자세한 내용은 [조직 보기를 사용하여 계정 간 AWS Health 이벤트 집계](#) 섹션을 참조하십시오.

## 서비스 역할

이 기능을 사용하면 서비스가 사용자를 대신하여 [서비스 역할](#)을 수입할 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 Health 서비스 역할을 지원하지 않습니다.

## AWS Health ID 기반 정책 예제

기본적으로 IAM 사용자 및 역할은 AWS Health 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 생성](#)을 참조하세요.

## 주제

- [정책 모범 사례](#)
- [AWS Health 콘솔 사용](#)
- [사용자가 자신의 고유한 권한을 볼 수 있도록 허용](#)
- [AWS Health Dashboard 및 API에 액세스 AWS Health](#)
- [리소스 및 작업 기반 조건](#)



## 정책 모범 사례

ID 기반 정책은 누군가가 계정에서 AWS Health 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르십시오.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 [AWS 관리형 정책](#) 또는 [AWS 직무에 대한 관리형 정책](#)을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 [IAM의 정책 및 권한](#)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 [IAM Access Analyzer 정책 검증](#)을 참조하세요.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하다면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 [MFA 보호 API 액세스 구성](#)을 참조하세요.

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

## AWS Health 콘솔 사용

AWS Health 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 AWS 계정의 AWS Health 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다. 최소 필수 권한보다 더 제한적



인 보안 인증 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(IAM 사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

해당 엔티티가 AWS Health 콘솔을 계속 사용할 수 있도록 다음 AWS 관리형 정책을 연결할 수 [AWSHealthFullAccess](#) 있습니다.

AWSHealthFullAccess 정책은 엔티티에 다음에 대한 모든 액세스 권한을 부여합니다.

- 조직 내 모든 계정에 대해 AWS Health 조직 보기 기능을 활성화하거나 비활성화합니다. AWS
- AWS Health Dashboard AWS Health 콘솔에서
- AWS Health API 작업 및 알림
- AWS 조직에 속한 계정에 대한 정보 보기
- 관리 계정의 조직 단위(OU) 보기

Example : AWSHealthFullAccess

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": "health.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "health:*",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListParents"
      ],
    }
  ]
}
```

```

        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "health.amazonaws.com"
            }
        }
    }
]
}

```

#### Note

또한 Health\_OrganizationsServiceRolePolicy AWS 관리형 정책을 사용하여 조직의 다른 계정에 대한 이벤트를 볼 AWS Health 수 있습니다. 자세한 정보는 [AWS Health의 서비스 링크 역할 사용](#)을 참조하세요.

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

자세한 내용은 IAM 사용 설명서의 [사용자에게 권한 추가](#)를 참조하십시오.

## 사용자가 자신의 고유한 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": "*"
}
]
}

```

## AWS Health Dashboard 및 API에 액세스 AWS Health

모든 AWS 계정에서 AWS Health Dashboard 사용할 수 있습니다. AWS Health API는 비즈니스, 엔터프라이즈 온램프 또는 엔터프라이즈 지원 플랜을 보유한 계정에서만 사용할 수 있습니다. 자세한 정보는 [AWS Support](#)를 참조하세요.

IAM을 사용하여 엔티티(사용자, 그룹 또는 역할)를 생성한 다음 해당 엔티티에 및 API에 액세스할 수 있는 권한을 부여할 수 있습니다. AWS Health Dashboard AWS Health

기본적으로 IAM 사용자는 AWS Health Dashboard 또는 API에 액세스할 수 없습니다. AWS Health 단일 사용자, 사용자 그룹 또는 역할에 IAM 정책을 추가하여 사용자에게 계정 AWS Health 정보에 대한 액세스 권한을 부여합니다. 자세한 내용은 [자격 증명\(사용자, 그룹 및 역할\)](#) 및 [IAM 정책 개요](#)를 참조하십시오.

IAM 사용자를 만든 후 그 사용자에게 개별 암호를 부여할 수 있습니다. 그러면 사용자는 계정별 로그인 페이지를 사용하여 계정에 로그인하고 AWS Health 정보를 볼 수 있습니다. 자세한 내용은 [사용자의 계정 로그인 방법](#) 단원을 참조하십시오.

**Note**

조회 AWS Health Dashboard 권한이 있는 IAM 사용자는 계정의 모든 AWS 서비스에서 상태 정보에 읽기 전용으로 액세스할 수 있으며, 여기에는 Amazon EC2 인스턴스 ID, EC2 인스턴스 IP 주소, 일반 보안 알림과 같은 AWS 리소스 ID가 포함될 수 있지만 이에 국한되지 않습니다. 예를 들어 IAM 정책이 AWS Health API에 대한 액세스만 허용하는 경우 정책이 적용되는 사용자 또는 역할은 다른 IAM 정책에서 액세스를 허용하지 않더라도 AWS 서비스 및 관련 리소스에 대해 게시된 모든 정보에 액세스할 수 있습니다. AWS Health Dashboard

두 개의 API 그룹을 사용할 수 있습니다. AWS Health

- 개별 계정 — [DescribeEvents](#) 및 [DescribeEvent세부](#) 정보와 같은 작업을 사용하여 계정의 AWS Health 이벤트에 대한 정보를 가져올 수 있습니다.
- 조직 계정 — [DescribeEventsForOrganization](#) 및 조직과 같은 작업을 사용하여 [DescribeEventDetailsFor조직에 속한](#) 계정의 AWS Health 이벤트에 대한 정보를 가져올 수 있습니다.

사용 가능한 API 작업에 대한 자세한 내용은 [AWS Health API 참조](#)를 참조하십시오.

**개별 작업**

IAM 정책의 Action 요소를 `health:Describe*`(으)로 설정할 수 있습니다. 이렇게 하면 AWS Health Dashboard 및 에 액세스할 수 AWS Health있습니다. AWS Health eventTypeCode및 서비스를 기반으로 이벤트에 대한 액세스 제어를 지원합니다.

**액세스 설명**

이 정책문은 모든 Describe\* AWS Health API 작업에 AWS Health Dashboard 대한 액세스 권한을 부여합니다. 예를 들어, 이 정책을 사용하는 IAM 사용자는 AWS Health Dashboard in에 액세스하여 AWS Health DescribeEvents API 작업을 호출할 수 있습니다. AWS Management Console

**Example : 액세스 설명**

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

```

    "health:Describe*"
  ],
  "Resource": "*"
}]
}

```

## 액세스 거부

이 정책 설명문은 API에 AWS Health Dashboard 대한 액세스를 거부합니다 AWS Health . 이 정책을 사용하는 IAM 사용자는 API를 확인할 수 없으며 AWS Health API 작업을 호출할 수 없습니다. AWS Health Dashboard AWS Management Console

Example : 액세스 거부

```

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

```

## 조직 보기

에 대한 조직 보기를 활성화하려면 AWS Health 및 AWS Organizations 작업에 대한 AWS Health 액세스를 허용해야 합니다.

IAM 정책의 Action 요소에는 다음 권한이 포함되어야 합니다.

- iam:CreateServiceLinkedRole
- organizations:EnableAWSServiceAccess
- organizations:DescribeAccount
- organizations:DisableAWSServiceAccess
- organizations:ListAccounts
- organizations:ListDelegatedAdministrators
- organizations:ListParents

각 API에 필요한 정확한 권한을 이해하려면 IAM 사용 설명서의 [AWS Health API로 정의된 작업 및 알림](#)을 참조하십시오.

#### Note

조직이 API에 액세스하려면 관리 계정의 자격 증명을 사용해야 합니다 AWS Health . AWS Organizations 자세한 정보는 [조직 보기를 사용하여 계정 간 AWS Health 이벤트 집계](#)을 참조하십시오.

### AWS Health 조직 보기에 대한 모든 액세스 권한 허용

이 정책 설명문은 조직 보기 기능에 필요한 모든 AWS Organizations 작업 AWS Health 및 작업에 대한 액세스 권한을 부여합니다.

#### Example : AWS Health 조직 보기 액세스 허용

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": "health.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "health:*",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListParents"
      ],
    }
  ]
}
```

```

        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
    }
]
}

```

## AWS Health 조직 보기에 대한 모든 액세스 권한 거부

이 정책 설명문은 AWS Organizations 작업에 대한 액세스를 거부하지만 개별 계정의 AWS Health 작업에 대한 액세스는 허용합니다.

### Example : AWS Health 조직 보기 액세스 거부

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "health:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [

```

```

        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListParents"
    ],
    "Resource": "*"
},
{
    "Effect": "Deny",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/AWSServiceRoleForHealth*"
}
]
}

```

#### Note

권한을 부여하려는 사용자 또는 그룹에 이미 IAM 정책이 있는 경우 해당 정책에 AWS Health-specific policy 설명을 추가할 수 있습니다.

## 리소스 및 작업 기반 조건

AWS Health [DescribeAffectedEntities](#) 및 [DescribeEvent세부](#) API 작업에 대한 [IAM 조건을](#) 지원합니다. 리소스 및 작업 기반 조건을 사용하여 AWS Health API가 사용자, 그룹 또는 역할에 보내는 이벤트를 제한할 수 있습니다.

이렇게 하려면 IAM 정책의 Condition 블록을 업데이트하거나 Resource 요소를 설정합니다. [문자열 조건을](#) 사용하여 특정 AWS Health 이벤트 필드를 기반으로 액세스를 제한할 수 있습니다.

정책에서 AWS Health 이벤트를 지정할 때 다음 필드를 사용할 수 있습니다.

- eventTypeCode
- service

#### 참고

- [DescribeAffectedEntities](#) 및 [DescribeEventDetails](#) API 작업은 리소스 수준 권한을 지원합니다. 예를 들어, 특정 AWS Health 이벤트를 허용하거나 거부하는 정책을 생성할 수 있습니다.



- [DescribeAffectedEntitiesForOrganization](#) 및 [DescribeEventDetailsFor조직](#) API 작업은 리소스 수준 권한을 지원하지 않습니다.
- 자세한 내용은 서비스 권한 부여 참조의 [AWS Health API 및 알림에 대한 작업, 리소스, 조건 키](#)를 참조하십시오.

#### Example : 작업 기반 조건

이 정책문은 AWS Health Describe\* API 작업에 대한 액세스는 허용하지만 Amazon AWS Health Dashboard EC2와 관련된 모든 AWS Health 이벤트에 대한 액세스는 거부합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "health:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "health:DescribeAffectedEntities",
        "health:DescribeEventDetails"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "health:service": "EC2"
        }
      }
    }
  ]
}
```

#### Example : 리소스 기반 조건

다음 정책은 효과는 동일하지만 Resource 요소를 대신 사용합니다.

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

```

"Statement": [
{
  "Effect": "Allow",
  "Action": [
    "health:Describe*"
  ],
  "Resource": "*"
},
{
  "Effect": "Deny",
  "Action": [
    "health:DescribeEventDetails",
    "health:DescribeAffectedEntities"
  ],
  "Resource": "arn:aws:health:*::event/EC2/*/*"
}]
}

```

#### Example : 조건 eventTypeCode

이 정책 설명문은 AWS Health Describe\* API 작업에 대한 액세스 권한을 AWS Health Dashboard 부여하지만, eventTypeCode 일치하는 AWS\_EC2\_\* 모든 AWS Health 이벤트에 대한 액세스는 거부합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "health:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "health:DescribeAffectedEntities",
        "health:DescribeEventDetails"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "health:eventTypeCode": "AWS_EC2_*"
        }
      }
    }
  ]
}

```

```

    }
  }
]
}

```

### Important

[DescribeAffectedEntities](#) 및 [DescribeEventDetails](#) 작업을 호출하고 AWS Health 이벤트에 액세스할 권한이 없는 경우 `AccessDeniedException` 오류가 나타납니다. 자세한 정보는 [AWS Health ID 및 액세스 문제 해결](#)을 참조하세요.

## AWS Health ID 및 액세스 문제 해결

다음 정보를 사용하여 IAM을 사용할 때 발생할 수 있는 일반적인 문제를 AWS Health 진단하고 수정하십시오.

### 주제

- [저는 다음과 같은 작업을 수행할 권한이 없습니다. AWS Health](#)
- [저는 IAM을 수행할 권한이 없습니다. PassRole](#)
- [액세스 키를 보아야 합니다.](#)
- [저는 관리자이며 다른 사람들이 액세스할 수 있도록 허용하고 싶습니다. AWS Health](#)
- [내 AWS 계정 외부의 사용자가 내 리소스에 액세스할 수 있도록 허용하고 싶습니다. AWS Health](#)

### 저는 다음과 같은 작업을 수행할 권한이 없습니다. AWS Health

작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 사용자 이름과 비밀번호를 제공한 사람입니다.

이 `AccessDeniedException` 오류는 사용자에게 사용 권한 AWS Health Dashboard 또는 AWS Health API 작업이 없는 경우 나타납니다.

이 경우 사용자의 관리자는 사용자에게 액세스를 허용하도록 정책을 업데이트해야 합니다.

AWS Health API에는 비즈니스, 엔터프라이즈 온램프 또는 엔터프라이즈 지원 플랜이 필요합니다. [AWS Support](#) Business, Enterprise On-Ramp 또는 Enterprise Support 플랜이 없는 계정에서 AWS Health API를 호출하면 다음 오류 코드가 반환됩니다: `SubscriptionRequiredException`

## 저는 IAM을 수행할 권한이 없습니다. PassRole

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AWS Health에 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 marymajor라는 IAM 사용자가 콘솔을 사용하여 AWS Health에서 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 Health

다른 사람이 액세스할 수 있도록 하려면 액세스가 AWS Health필요한 개인 또는 애플리케이션을 위한 IAM 엔티티 (사용자 또는 역할) 를 생성해야 합니다. 다른 사용자들은 해당 엔티티에 대한 보안 인증을 사용해 AWS에 액세스합니다. 그런 다음 AWS Health에 대한 올바른 권한을 부여하는 정책을 엔티티에 연결해야 합니다.

바로 시작하려면 IAM 사용 설명서의 [첫 번째 IAM 위임 사용자 및 그룹 생성](#)을 참조하십시오.

내 AWS 계정 외부의 사용자가 내 리소스에 액세스할 수 있도록 허용하고 싶습니다.

AWS Health

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 Health 지원 여부를 알아보려면 을 참조하십시오 [IAM의 AWS Health 작동 방식](#).
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 [설명서에서 자신이 소유한 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공](#)을 참조하십시오.
- [제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공](#)을 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 차이](#)를 참조하십시오.

## AWS Health의 서비스 링크 역할 사용

AWS Health AWS Identity and Access Management ([IAM](#)) [서비스 연결 역할을 사용합니다](#). 서비스 연결 역할은 직접 연결되는 고유한 유형의 IAM 역할입니다. AWS Health서비스 연결 역할은 AWS Health에서 사전 정의하며 서비스에서 다른 AWS 서비스 을(를) 호출하기 위해 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가하지 않도록 서비스 연결 역할을 AWS Health 사용하여 설정할 수 있습니다. AWS Health 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 해당 역할만 AWS Health 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

## AWS Health에 대한 서비스 링크 역할 권한

AWS Health 다음과 같은 두 가지 서비스 연결 역할이 있습니다.

- [AWSServiceRoleForHealth\\_Organizations](#)— 이 역할은 AWS Health (health.amazonaws.com)가 사용자 대신 액세스할 AWS 서비스 수 있는 역할을 맡을 것으로 신뢰합니다. 이 역할에는 Health\_OrganizationsServiceRolePolicy AWS 관리형 정책이 첨부되어 있습니다.
- [AWSServiceRoleForHealth\\_EventProcessor](#)— 이 역할은 AWS Health 서비스 주체 (event-processor.health.amazonaws.com)가 대신 역할을 맡을 것으로 신뢰합니다. 이 역할에는 AWSHealth\_EventProcessorServiceRolePolicy AWS 관리형 정책이 첨부되어 있습니다. 서비스 주체는 이 역할을 사용하여 AWS 사고 탐지 및 대응을 위한 Amazon EventBridge 관리형 규칙을 생성합니다. 이 규칙은 계정에서 경보 상태 변경 정보를 계정으로 전달하는 AWS 계정 데 필요한 AWS Health인프라입니다.

AWS 관리형 정책에 대한 자세한 내용은 을 참조하십시오 [AWS 관리형 정책은 다음과 같습니다. AWS Health](#).

## AWS Health에 대한 서비스 링크 역할 생성

AWSServiceRoleForHealth\_Organizations 서비스 연결 역할은 생성할 필요가 없습니다.

[EnableHealthServiceAccessForOrganization](#) 오퍼레이션을 호출하면 계정에 이 서비스 연결 역할이 자동으로 AWS Health 생성됩니다.

계정에서 AWSServiceRoleForHealth\_EventProcessor 서비스 연결 역할을 수동으로 만들어야 합니다. 자세한 정보는 IAM 사용 설명서의 [서비스 연결 역할 생성](#) 섹션을 참조하십시오.

## AWS Health에 대한 서비스 링크 역할 편집

AWS Health 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 편집](#)을 참조하세요.

## AWS Health에 대한 서비스 링크 역할 삭제

AWSServiceRoleForHealth\_Organizations 역할을 삭제하려면 먼저 작업을 호출해야 합니다.

[DisableHealthServiceAccessForOrganization](#) 그런 다음 IAM 콘솔, IAM API 또는 AWS Command Line Interface ()AWS CLI를 통해 역할을 삭제할 수 있습니다.

AWSServiceRoleForHealth\_EventProcessor 역할을 삭제하려면 AWS 인시던트 탐지 AWS Support 및 대응에 문의하여 워크로드를 오프보딩하도록 요청하세요. 이 프로세스가 완료되면 IAM 콘솔, IAM API 또는 AWS CLI을(를) 통해 역할 중 하나를 삭제할 수 있습니다.

### 관련 정보

자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 사용](#)을 참조하십시오.

## AWS 관리형 정책은 다음과 같습니다. AWS Health

AWS 관리형 정책은 에서 생성하고 관리하는 독립형 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 정책](#)을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트 하는 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 정책](#)을 참조하세요.

AWS Health 에는 다음과 같은 관리형 정책이 있습니다.

### 목차

- [AWS 관리형 정책: AWSHealth\\_EventProcessorServiceRolePolicy](#)
- [AWS 관리형 정책: Health\\_OrganizationsServiceRolePolicy](#)

- [AWS 관리형 정책: AWSHealthFullAccess](#)
- [AWS HealthAWS 관리형 정책 업데이트](#)

## AWS 관리형 정책: AWSHealth\_EventProcessorServiceRolePolicy

AWS Health [AWSHealth\\_EventProcessorServiceRolePolicy](#) AWS 관리형 정책을 사용합니다. 이 관리형 정책은 AWSServiceRoleForHealth\_EventProcessor 서비스 연결 역할에 연결됩니다. 이 정책을 통해 서비스 연결 역할이 사용자를 대신하여 작업을 완료할 수 있습니다. IAM 엔터티에 이 정책을 연결할 수 없습니다. 자세한 정보는 [AWS Health의 서비스 링크 역할 사용](#)을 참조하세요.

관리형 정책에는 AWS 사고 탐지 및 대응을 위한 Amazon EventBridge 규칙에 액세스할 수 AWS Health 있는 다음과 같은 권한이 있습니다.

### 권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `events`— EventBridge 규칙을 설명 및 삭제하고 해당 규칙의 대상을 설명 및 업데이트합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Condition": {
        "StringEquals": {"events:ManagedBy": "event-processor.health.amazonaws.com"}
      },
      "Action": [
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
```



```

        "Action": [
            "events:ListTargetsByRule",
            "events:DescribeRule"
        ],
        "Resource": "*",
        "Effect": "Allow"
    }
}

```

정책 변경 사항 목록은 [AWS HealthAWS 관리형 정책 업데이트](#)을(를) 참조하십시오.

## AWS 관리형 정책: Health\_OrganizationsServiceRolePolicy

AWS Health [Health\\_OrganizationsServiceRolePolicy](#) AWS 관리형 정책을 사용합니다. 이 관리형 정책은 AWSServiceRoleForHealth\_Organizations 서비스 연결 역할에 연결됩니다. 이 정책을 통해 서비스 연결 역할이 사용자를 대신하여 작업을 완료할 수 있습니다. IAM 엔터티에 이 정책을 연결할 수 없습니다. 자세한 정보는 [AWS Health의 서비스 링크 역할 사용](#)을 참조하세요.

이 정책은 건강 조직 보기에 필요한 AWS Organizations 세부 정보에 액세스할 수 AWS Health 있는 권한을 부여합니다.

### 권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- organizations— Organizations의 AWS Organizations 계정과 함께 사용할 수 AWS 서비스 있는 계정을 설명합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",

```

```

        "organizations:DescribeAccount"
      ],
      "Resource": "*"
    }
  ]
}

```

정책 변경 사항 목록은 [AWS HealthAWS 관리형 정책 업데이트](#)을(를) 참조하십시오.

## AWS 관리형 정책: AWSHealthFullAccess

AWS Health [AWSHealthFullAccess](#) AWS 관리형 정책을 사용합니다. 정책은 개체 (IAM 사용자 또는 역할) 에게 AWS Health 콘솔 액세스 권한을 부여합니다. 자세한 정보는 [AWS Health 콘솔 사용](#)을 참조하세요.

### 권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- **organizations**— 조직의 모든 계정에 대해 AWS Health 조직 보기 기능을 활성화 또는 비활성화 하고 관리 계정의 조직 단위 (OU) 를 볼 수 있습니다. AWS
- **health**— AWS Health API 작업 및 알림에 대한 액세스
- **iam**— 서비스에 연결된 IAM 역할을 생성합니다. AWS Health

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationWriteAccess",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": "health.amazonaws.com"
        }
      }
    }
  ]
}

```

```

    }
  },
  {
    "Sid": "HealthFullAccess",
    "Effect": "Allow",
    "Action": [
      "health:*",
      "organizations:DescribeAccount",
      "organizations:ListAccounts",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListParents"
    ],
    "Resource": "*"
  },
  {
    "Sid": "ServiceLinkAccess",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": "health.amazonaws.com"
      }
    }
  }
]
}

```

정책 변경 사항 목록은 [AWS HealthAWS 관리형 정책 업데이트](#)을(를) 참조하십시오.

## AWS HealthAWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Health 이후의 AWS 관리형 정책 업데이트에 대한 세부 정보를 볼 수 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 [에 대한 문서 기록 AWS Health](#) 페이지에서 RSS 피드를 구독하십시오.

다음 표에는 2022년 1월 13일 이후 AWS Health 관리형 정책에 대한 중요 업데이트가 설명되어 있습니다.

## AWS Health

변경 사항	설명	날짜
<a href="#">AWS 관리형 정책: AWSHealthFullAccess</a> - 기존 정책에 대한 업데이트	AWS Health AWSHealth FullAccess 정책을 AWS GovCloud (US) Regions 및 중국 지역으로 확대했습니다.	2023년 10월 16일
<a href="#">AWS 관리형 정책: Health_OrganizationsServiceRolePolicy</a> - 기존 정책에 대한 업데이트	AWS Health 서비스 연결 역할이 함께 사용할 수 있는 계정 및 AWS 서비스를 설명할 수 있도록 하는 새 AWS Organizations 동작을 추가했습니다. AWS Organizations	2023년 7월 19일
변경 로그 게시	AWS Health 관리형 정책의 변경 로그.	2023년 1월 13일

## 로그인 및 모니터링 AWS Health

모니터링은 및 기타 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. AWS Health AWS 문제를 관찰하고, 문제 발생 시 보고하고 AWS Health, 적절한 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 추적하고 필요할 때 새 인스턴스를 자동으로 시작할 수 있습니다. 자세한 내용은 [Amazon CloudWatch 사용 설명서를](#) 참조하십시오.
- EventBridgeAmazon은 AWS 리소스 변경을 설명하는 시스템 이벤트 near-real-time 스트림을 제공합니다. EventBridge 자동화된 이벤트 기반 컴퓨팅을 지원합니다. 특정 이벤트를 감시하고 이러한 이벤트가 발생하면 다른 AWS 서비스에서 자동화된 작업을 트리거하는 규칙을 작성할 수 있습니다. 자세한 정보는 [Amazon을 통한 AWS Health 이벤트 모니터링 EventBridge](#)를 참조하세요.
- 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 사

용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 전화를 걸었는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하십시오.

자세한 정보는 [모니터링 AWS Health](#)을 참조하세요.

## 규정 준수 검증: AWS Health

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면 AWS 서비스 규정 준수 [프로그램의 AWS 서비스 범위별, 규정](#) 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 [AWS 규정 준수 프로그램 AWS 보증 프로그램 규정 AWS](#) 참조하십시오.

를 사용하여 AWS Artifact 타사 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 킷 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 참조](#)를 참조하십시오.

- [AWS 규정 준수 리소스 AWS](#) — 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 참조](#)를 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 위협을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

## 의 탄력성 AWS Health

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 Health 이벤트는 여러 가용 영역에 저장되고 복제됩니다. 이 접근 방식을 사용하면 AWS Health Dashboard 또는 AWS Health API 작업에서 액세스할 수 있습니다. AWS Health 이벤트가 발생한 날로부터 최대 90일 동안 이벤트를 볼 수 있습니다.

AWS 지역 및 가용 영역에 대한 자세한 내용은 [AWS 글로벌 인프라](#)를 참조하십시오.

## AWS Health에서 인프라 보안

관리형 서비스로서 [Amazon Web Services: 보안 프로세스 개요](#) 백서에 설명된 [AWS 글로벌 네트워크 보안 절차에 따라](#) 보호됩니다. AWS Health

AWS 게시된 API 호출을 사용하여 네트워크를 AWS Health 통해 액세스할 수 있습니다. 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 Health

구성 및 IT 제어는 귀하와 당사 고객 간의 AWS 공동 책임입니다. 자세한 내용은 AWS [공동 책임 모델](#)을 참조하십시오.

## AWS Health의 보안 모범 사례

다음과 같은 작업 모범 사례를 참조하십시오 AWS Health.

### AWS Health 사용자에게 가능한 최소 권한 부여

사용자 및 그룹에 대해 최소한의 액세스 정책 권한 집합을 사용하여 최소 권한의 원칙을 준수합니다. 예를 들어, AWS Identity and Access Management (IAM) 사용자에게 에 대한 액세스를 허용할 수 있습니다. AWS Health Dashboard 동일한 사용자가 AWS Organizations에 대한 액세스를 활성화 또는 비활성화하는 것은 허용하지 않을 수 있습니다.

자세한 정보는 [AWS Health ID 기반 정책 예제](#)을 참조하세요.

## 보기 AWS Health Dashboard

AWS Health Dashboard 자주 확인하여 계정이나 애플리케이션에 영향을 미칠 수 있는 이벤트를 찾아보십시오. 예를 들어 업데이트해야 하는 Amazon EC2(Amazon Elastic Compute Cloud) 인스턴스와 같은 리소스에 대한 이벤트 알림을 받을 수 있습니다.

자세한 정보는 [AWS Health 대시 보드 시작하기 - 계정 상태](#)을 참조하세요.

## Amazon Chime 또는 AWS Health 슬랙과 통합

채팅 AWS Health 도구와 통합할 수 있습니다. 이 통합을 통해 여러분과 팀은 AWS Health 이벤트에 대한 알림을 실시간으로 받을 수 있습니다. 자세한 내용은 의 [AWS Health 도구](#)를 참조하십시오 GitHub.

## AWS Health 이벤트 모니터링

Amazon AWS Health Events와 통합하여 특정 CloudWatch 이벤트에 대한 규칙을 생성할 수 있습니다. Events에서 규칙과 일치하는 CloudWatch 이벤트를 감지하면 알림을 받고 조치를 취할 수 있습니다.

CloudWatch 이벤트 이벤트는 지역별로 다르므로 애플리케이션 또는 인프라가 있는 지역에서 이 서비스를 구성해야 합니다.

경우에 따라 AWS Health 이벤트 지역을 결정할 수 없습니다. 이러한 상황이 발생하면 기본적으로 미국 동부(버지니아 북부)에 이벤트가 표시됩니다. 이 지역에서 CloudWatch 이벤트를 설정하여 이러한 이벤트를 모니터링할 수 있습니다.

자세한 정보는 [Amazon을 통한 AWS Health 이벤트 모니터링 EventBridge](#)을 참조하세요.



## 조직 보기를 사용하여 계정 간 AWS Health 이벤트 집계

기본적으로 AWS Health을(를) 사용하면 단일 AWS 계정의 AWS Health 이벤트를 볼 수 있습니다. AWS Organizations를 사용하는 경우, 조직 전체에서 AWS Health 이벤트를 중앙 집중식으로 볼 수도 있습니다. 이 기능을 사용하면 단일 계정 작업과 동일한 정보에 액세스할 수 있습니다. 필터를 사용하여 특정 AWS 리전, 계정 및 서비스의 이벤트를 볼 수 있습니다.

이벤트를 집계하여 운영 이벤트의 영향을 받는 조직의 계정을 식별하거나 보안 취약성에 대한 알림을 받을 수 있습니다. 그런 다음 이 정보를 사용하여 조직 전체의 리소스 유지 관리 이벤트를 사전 예방적으로 관리하고 자동화할 수 있습니다. 이 기능을 사용하여 코드 변경 또는 업데이트가 필요한 AWS 서비스의 예정된 변경 사항에 대한 최신 정보를 얻을 수 있습니다.

[위임된 관리자](#) 기능을 사용하여 AWS Health 조직 보기에 대한 액세스 권한을 멤버 계정에 위임하는 것이 좋습니다. 이렇게 하면 운영팀이 조직의 AWS Health 이벤트에 더 쉽게 액세스할 수 있습니다. 위임된 관리자 기능을 사용하면 관리 계정을 제한하는 동시에 팀이 AWS Health 이벤트에 대한 조치를 취하는 데 필요한 가시성을 확보할 수 있습니다.

### Important

- AWS Health는 조직 보기를 사용하도록 설정하기 전에 조직에서 발생한 이벤트를 기록하지 않습니다. 예를 들어, 이 기능을 활성화하기 전에 조직의 멤버 계정(111122223333)이 Amazon Elastic Compute Cloud(Amazon EC2)에 대한 이벤트를 수신한 경우 이 이벤트는 조직 보기에 표시되지 않습니다.
- 조직의 계정에 대해 전송된 AWS Health 이벤트는 이벤트가 사용 가능한 한 조직 보기에 표시되며, 해당 계정 중 하나 이상이 조직을 떠나는 경우에도 이벤트가 사용 가능한 한 최대 90일 동안 표시됩니다.
- 조직 이벤트는 삭제되기 전 90일 동안 사용할 수 있습니다. 이 할당량은 늘릴 수 없습니다.

## 필수 조건

조직 보기를 사용하기 전에 다음을 수행해야 합니다.

- [모든 기능](#)이 활성화된 조직의 구성원이어야 합니다.
- 관리 계정에 AWS Identity and Access Management(IAM) 사용자로 로그인하거나 IAM 역할을 맡습니다.

조직의 관리 계정에서 루트 사용자로 로그인할 수도 있습니다(권장되지 않음). 자세한 내용은 IAM 사용 설명서에서 [AWS 계정 루트 사용자 액세스 키 잡그기](#)를 참조하세요.

- IAM 사용자로 로그인하는 경우 [AWSHealthFullAccess](#) 정책과 같은 AWS Health 및 Organizations 작업에 대한 액세스 권한을 부여하는 IAM 정책을 사용하세요. 자세한 내용은 [AWS Health ID 기반 정책 예제](#) 섹션을 참조하세요.

## 주제

- [조직 보기\(콘솔\)](#)
- [조직 보기\(CLI\)](#)
- [위임된 관리자 조직 보기](#)

## 조직 보기(콘솔)

AWS Health 콘솔을 사용하여 AWS 조직의 상태 이벤트를 중앙 집중식으로 볼 수 있습니다.

추가 비용 없이 모든 AWS Support 플랜에 대해 AWS Health 콘솔에서 조직 보기를 사용할 수 있습니다.

### Note

관리 계정에서 사용자가 이 기능에 액세스할 수 있도록 허용하려면 해당 사용자에게 [AWSHealthFullAccess](#) 정책과 같은 권한이 있어야 합니다. 자세한 내용은 [AWS Health ID 기반 정책 예제](#) 섹션을 참조하세요.

## 목차

- [조직 보기 활성화\(콘솔\)](#)
- [조직 보기 이벤트 보기\(콘솔\)](#)
  - [미결 및 최근 문제](#)
  - [예약된 변경](#)
  - [기타 알림](#)
  - [이벤트 로그](#)
- [영향을 받는 계정 및 리소스 보기\(콘솔\)](#)

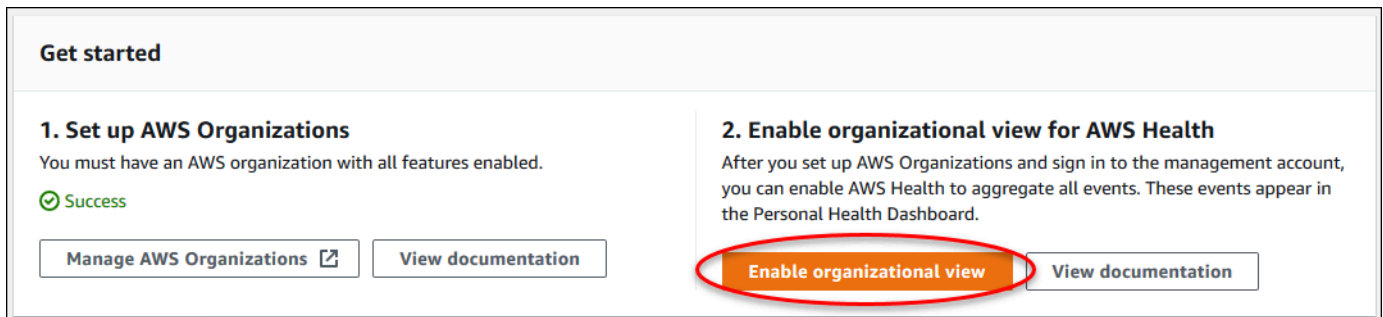
## • [조직 보기 사용 안 함\(콘솔\)](#)

### 조직 보기 활성화(콘솔)

AWS Health 콘솔에서 조직 보기를 사용 설정할 수 있습니다. AWS 조직의 관리 계정으로 로그인해야 합니다.

조직의 AWS Health 대시보드를 보려면

1. <https://health.aws.amazon.com/health/home>에서 AWS Health 대시보드를 엽니다.
2. 탐색 창의 조직 상태에서 구성을 선택합니다.
3. 조직 보기 사용 페이지에서 조직 보기 사용을 선택합니다.



4. (선택 사항) 조직 단위(OU) 생성 등 AWS 조직을 변경하려면 AWS Organizations 관리를 선택합니다.

자세한 내용은 AWS Organizations 사용 설명서의 [AWS Organizations 시작하기](#)를 참조하세요.

#### 주의

- 이 기능을 활성화하는 작업은 비동기 프로세스이며 완료하는 데 시간이 걸립니다. 조직에 포함된 계정 수에 따라 계정을 로드하는 데 몇 분이 걸릴 수 있습니다. 나중에 나가서 AWS Health 콘솔을 확인할 수 있습니다.
- Business, Enterprise On-Ramp 또는 Enterprise Support 플랜을 보유한 경우, [DescribeHealthServiceStatusForOrganization](#) API 작업을 호출하여 프로세스 상태를 확인할 수 있습니다.
- 이 기능을 사용 설정하면 관리되는 정책과 함께 `AWSServiceRoleForHealth_Organizations` 서비스 연결 역할이 조직의

Health\_OrganizationsServiceRolePolicy AWS 관리 계정에 적용됩니다. 자세한 내용은 [AWS Health의 서비스 링크 역할 사용](#) 섹션을 참조하세요.

## 조직 보기 이벤트 보기(콘솔)

조직 보기 기능을 사용 설정하면 AWS Health에서 조직의 모든 계정에 대한 상태 이벤트를 표시합니다.

계정이 조직에 가입하면 AWS Health에서 계정을 기관 보기에 자동으로 추가합니다. 계정이 조직에서 벗어나면 해당 계정의 새 이벤트가 더 이상 조직 보기에 로깅되지 않습니다. 그러나 기존 이벤트는 그대로 유지되며 최대 90일 제한까지 쿼리할 수 있습니다.

AWS는 관리자 계정 해지 유효 날짜부터 90일 동안 계정에 대한 정책 데이터를 유지합니다. 90일의 기간이 종료되는 시점에 AWS는 계정의 모든 정책 데이터를 영구적으로 삭제합니다.

- 정책을 보관하면 결과를 90일 넘게 유지할 수 있습니다. 또한 EventBridge 규칙에 사용자 지정 작업을 사용하여 결과를 S3 버킷에 저장할 수 있습니다.
- AWS가 정책 데이터를 유지하는 한 해지된 계정을 다시 열 때 AWS가 계정을 서비스 관리자로 재할당하고 계정의 서비스 정책 데이터를 복구합니다.
- 자세한 내용은 [계정 해지](#)를 참조하세요.

### Important

AWS GovCloud (US) 리전의 고객인 경우:

- 계정을 해지하기 전에 계정 리소스를 백업한 다음 삭제합니다. 계정을 해지한 뒤에는 더 이상 해당 계정에 액세스할 수 없습니다.

### Note

이 기능을 활성화하면 AWS Health 콘솔에 [AWS Health 대시보드 - 서비스 상태](#)의 최근 7일간의 공개 이벤트를 표시할 수 있습니다. 이러한 공개 이벤트는 조직의 계정에만 국한되지 않습니다. AWS Health 대시보드의 이벤트 - 서비스 상태는 지역별 AWS 서비스 가용성에 대한 공개 정보를 제공합니다.

다음 페이지에서 조직 보기 이벤트를 확인할 수 있습니다.

## 주제

- [미결 및 최근 문제](#)
- [예약된 변경](#)
- [기타 알림](#)
- [이벤트 로그](#)

## 미결 및 최근 문제

미결 및 최근 문제 탭을 사용하면 조직에 영향을 미치는 AWS 서비스에 대한 변경 사항 및 리소스 등 AWS 인프라에 영향을 미칠 수 있는 이벤트를 볼 수 있습니다.

### 조직 보기 이벤트를 보려면

1. <https://health.aws.amazon.com/health/home>에서 AWS Health 대시보드를 엽니다.
2. 탐색 창의 조직 상태에서 미결 및 최근 문제를 선택하여 최근에 보고된 이벤트를 확인합니다.
3. 이벤트를 선택합니다. 세부 정보 탭에서 이벤트에 대한 다음 정보를 검토할 수 있습니다:
  - 이벤트 이름
  - 상태
  - 리전 / 가용 영역
  - 영향을 받는 계정
  - 시작 시간
  - 종료 시간
  - 범주
  - 설명

### Example : 조직 보기에 대한 미해결 문제

다음 Amazon Relational Database Service(RDS) 이벤트는 조직 보기의 미결 및 최근 문제 탭에 나타나며 조직의 한 계정에 영향을 줍니다.

**Open issues**

View event log

View events that might affect your AWS infrastructure, such as changes to AWS services and resources.

Add filter

< 1 >

**Event summary**

**EC2 operational issue**  
Last update: November 18, 2020 at 7:50:35 AM UTC-8 us-east-1

**S3 operational issue**  
Last update: November 18, 2020 at 7:50:35 AM UTC-8 us-east-1

**RDS storage issue**  
Last update: November 18, 2020 at 7:50:35 AM UTC-8 us-east-1

**RDS storage issue**  
Last update: November 18, 2020 at 7:50:35 AM UTC-8 us-east-1

**EC2 operational issue**  
Last update: November 18, 2020 at 1:51:23 AM UTC-8 us-east-1

**CloudFront operational issue**  
Last update: November 18, 2020 at 2:10:46 AM UTC-8 us-east-1

**EC2 scheduled maintenance issue**  
Last update: November 18, 2020 at 7:50:26 AM UTC-8 us-east-1

**RDS storage issue**

Back to list view

Details
Affected accounts

**Event data**

Event	RDS storage issue	Start time	November 18, 2020 at 7:50:10 AM UTC-8
Status	Open	End time	-
Region / Availability Zone	us-east-1a	Category	Issue
Affected accounts	1		

**Description**

Unfortunately, there was an unrecoverable storage failure on your Amazon RDS instance associated with this event. As a result, your instance has been put in a storage failed state.

You can recover your database instance at your earliest convenience by using one of the following methods:

1) Using your latest snapshot - you can view the available backups on the AWS Management Console under the "Snapshots" tab. More information on restoring from a DB snapshot can be found here: [http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ShareSnapshot.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ShareSnapshot.html)

## 예약된 변경

예약된 변경 탭을 사용하면 조직에 영향을 미칠 수 있는 예정된 이벤트를 볼 수 있습니다. 이러한 이벤트에는 서비스에 대해 예약된 유지 관리 활동이 포함될 수 있습니다.

## 기타 알림

알림 탭을 사용하면 조직에 영향을 미칠 수 있는 지난 7일간의 기타 모든 알림과 진행 중인 이벤트를 볼 수 있습니다. 여기에는 인증서 교체, 결제 알림, 보안 취약성과 같은 이벤트가 포함될 수 있습니다.

## 이벤트 로그

이벤트 로그 탭을 사용하면 조직 보기에 대한 AWS Health 이벤트를 볼 수도 있습니다. 열 레이아웃 및 동작은 이벤트 로그 탭에 이벤트 범주, 상태, 시작 시간과 같은 추가 열과 필터 옵션이 포함되어 있다는 점을 제외하면 미결 및 최근 문제 탭과 비슷합니다.

이벤트 로그 탭에서 조직 보기 이벤트를 보려면

1. <https://health.aws.amazon.com/health/home>에서 AWS Health 대시보드를 엽니다.
2. 탐색 창의 조직 상태 아래에서 이벤트 로그를 선택합니다.
3. 이벤트 로그에서 이벤트 이름을 선택합니다. 이벤트에 대한 다음 정보를 확인할 수 있습니다.

- 이벤트 이름

- 상태
- 리전 / 가용 영역
- 영향을 받는 계정
- 시작 시간
- 종료 시간
- 범주
- 설명

Example : 조직 보기에 대한 이벤트 로그 탭

다음 예인 Amazon DynamoDB(DynamoDB) 이벤트는 이벤트 로그 탭에 표시되며 조직의 두 계정에 영향을 줍니다.

### Event log

<
1
...
>

#### Event summary

VPN emergency maintenance scheduled

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

VPN emergency maintenance scheduled

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

ElastiCache redis maintenance scheduled

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

ElastiCache redis maintenance scheduled

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

EC2 instance network maintenance scheduled

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

EC2 instance network maintenance scheduled

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

Direct Connect maintenance scheduled

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

Direct Connect maintenance scheduled

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

Lambda operational issue

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

API Gateway maintenance scheduled

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

RDS storage failure MAZ

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

RDS storage maintenance scheduled

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

CloudFront operational issue

Last update: November 27, 2020 at 8:38:41 AM UTC-8

us-east-1

### EC2 instance network maintenance scheduled

[Back to list view](#)

Details

Affected accounts

#### Event data

Event	EC2 instance network maintenance scheduled	Start time	November 28, 2020 at 8:38:20 AM UTC-8
Status	Upcoming	End time	November 29, 2020 at 8:38:20 AM UTC-8
Region / Availability Zone	us-east-1a	Category	Scheduled change
Affected accounts	2		

#### Description

One or more of your Amazon EC2 instances is scheduled for maintenance on for hours starting at UTC. During this time, the instances associated with this event in the us-east-1 region will continue to run but will experience a loss of network connectivity.

Normal network connectivity to your instances will be restored after the maintenance is complete. You can maintain normal network connectivity during this time by migrating the instances listed above to replacement instances. Replacement instances will not be affected by this scheduled maintenance. Otherwise, no action is required on your part.

You can see more information on this maintenance in the AWS Management Console at </ec2/home?region=us-east-1#s=Events>

Additional information about maintenance events, including how to migrate to replacement instances, can be found at [http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/monitoring-instances-status-check\\_sched.html](http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/monitoring-instances-status-check_sched.html)

We perform maintenance regularly to ensure that the EC2 service continues uninterrupted for our customers. In most cases, maintenance can be performed without service interruption. When maintenance cannot be performed without service interruption, we work hard to keep any impact as brief as possible.

If you have any questions or concerns, you can contact the AWS Support Team on the community forums and via AWS Premium Support at: <http://aws.amazon.com/support>

## 영향을 받는 계정 및 리소스 보기(콘솔)

조직 상태에서는 이벤트의 영향을 받는 조직 내 계정과 관련 리소스를 확인할 수 있습니다. 예를 들어 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 유지 관리 이벤트가 예정된 경우, Amazon EC2 인스턴스가 포함된 조직 내 계정이 세부 정보 탭에 표시될 수 있습니다. 특정 리소스를 파악한 다음 계정 소유자에게 문의할 수 있습니다.

영향을 받는 계정 및 리소스를 보려면

1. <https://health.aws.amazon.com/health/home>에서 AWS Health 대시보드를 엽니다.
2. 탐색 창의 조직 상태에서 탭 중 하나를 선택합니다.
3. 영향을 받는 계정에 대한 값이 있는 이벤트를 선택합니다.
4. 영향을 받는 계정 탭을 선택합니다.
5. 계정에 대한 다음 정보를 보려면 계정 세부 정보 표시를 선택합니다.
  - 계정 ID
  - 계정 이름
  - 기본 이메일
  - 조직 단위(OU)

EC2 instance network maintenance scheduled

Back to list view

Details

Affected accounts

Affected accounts (1)

Show account details

Q Add filter

< 1 >

Account ID	Account name	Primary email	Organizational unit
▼ 123456789012	Jane Doe AWS account	janedoe@example.com	r-abcd

6. 계정을 확장하여 영향을 받는 리소스를 확인합니다.



EC2 instance network maintenance scheduled

Back to list view

Details

Affected accounts

Affected accounts (1)

Show account details

< 1 >

Account ID	Account name	Primary email	Organizational unit
▼ 123456789012	Jane Doe AWS account	janedoe@example.com	r-abcd
arn:aws:ec2:us-east-1:123456789012:instance/i-01cdfc3fc1example			
arn:aws:ec2:us-east-1:123456789012:instance/example-entity-name-2			

7. 리소스가 10개 이상인 경우 모든 리소스 보기를 선택하여 확인할 수 있습니다.
8. 이 특정 이벤트의 계정 ID 기준으로 필터링하려면 다음을 수행합니다.
  - a. 영향을 받는 계정 탭에서 필터 추가를 선택하고 계정 ID를 선택한 다음 계정 ID를 입력합니다. 한 번에 하나의 계정 ID만 입력할 수 있습니다.
  - b. Apply(적용)를 선택합니다. 입력한 계정이 목록에 나타납니다.

## 조직 보기 사용 안 함(콘솔)

조직의 이벤트를 집계하지 않으려면 관리 계정에서 이 기능을 끌 수 있습니다.

AWS Health에서는 조직의 다른 모든 계정에 대한 이벤트 집계를 중지합니다. 조직의 이전 이벤트는 삭제될 때까지 계속 볼 수 있습니다.

조직 보기를 비활성화하려면

1. <https://health.aws.amazon.com/health/home>에서 AWS Health 대시보드를 엽니다.
2. 탐색 창의 조직 상태에서 구성을 선택합니다.
3. 조직 보기 활성화 페이지에서 조직 보기 비활성화를 선택합니다.

## 2. Enable organizational view for AWS Health

After you set up AWS Organizations and sign in to the management account, you can enable AWS Health to aggregate all events. These events appear in the Personal Health Dashboard.

✓ Success

Disable organizational view

View documentation

이 기능을 비활성화하면 AWS Health에서 더 이상 조직의 이벤트가 집계되지 않습니다. 그러나 서비스 연결 역할은 AWS Identity and Access Management (IAM) 콘솔, IAM API 또는 AWS Command Line Interface(AWS CLI)을(를) 통해 삭제할 때까지 관리 계정에 남아 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스에 연결 역할 삭제](#)를 참조하세요.

## 조직 보기(CLI)

AWS Health 콘솔 대신 AWS Command Line Interface(AWS CLI)에서 조직 보기 기능을 활성화할 수도 있습니다. 콘솔을 사용하려면 [조직 보기 활성화\(콘솔\)](#)을 참조하세요.

### Note

사용자가 조직 보기 기능을 위해 관리 계정에 액세스할 수 있도록 허용하려면 해당 사용자에게 [AWSHealthFullAccess](#) 정책과 같은 권한이 있어야 합니다. 자세한 내용은 [AWS Health ID 기반 정책 예제](#) 섹션을 참조하세요.

### 목차

- [조직 보기 활성화\(CLI\)](#)
- [조직 보기 이벤트 보기\(CLI\)](#)
- [조직 보기 사용 안 함\(CLI\)](#)
- [AWS Health 조직 보기 API 작업](#)

## 조직 보기 활성화(CLI)

조직 보기를 사용 설정하려면 [EnableHealthServiceAccessForOrganization](#) API 작업을 사용하면 됩니다.

AWS Command Line Interface(AWS CLI) 또는 자체 코드를 사용하여 이 작업을 호출할 수 있습니다.

#### Note

- AWS Health API를 사용하려면 [Business](#), [Enterprise On-Ramp](#), 또는 [Enterprise](#) 지원 플랜이 있어야 합니다.
- 미국 동부(버지니아 북부) 리전 엔드포인트를 사용해야 합니다.

## Example

다음 AWS CLI 명령을 사용하면 AWS 계정에서 이 기능을 사용할 수 있습니다. 이 명령은 관리 계정 또는 필요한 권한이 있는 역할을 맡을 수 있는 계정에서 사용할 수 있습니다.

```
aws health enable-health-service-access-for-organization --region us-east-1
```

다음 코드 예제에서는 [EnableHealthServiceAccessForOrganization](#) API 작업을 호출합니다.

## Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

## Java

다음 예제에서는 버전 Java 2.0용 AWS SDK를 사용할 수 있습니다.

```
import software.amazon.awssdk.services.health.HealthClient;
import software.amazon.awssdk.services.health.HealthClientBuilder;

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
import
    software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRequest;
import
    software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationResponse;
```

```
import
software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequest;
import
software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResponse;

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

import software.amazon.awssdk.regions.Region;

public class EnableHealthServiceAccessDemo {
    public static void main(String[] args) {
        HealthClient client = HealthClient.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(
                DefaultCredentialsProvider.builder().build()
            )
            .build();

        try {
            DescribeHealthServiceStatusForOrganizationResponse statusResponse =
client.describeHealthServiceStatusForOrganization(
                DescribeHealthServiceStatusForOrganizationRequest.builder().build()
            );

            String status =
statusResponse.healthServiceAccessStatusForOrganization();
            if ("ENABLED".equals(status)) {
                System.out.println("EnableHealthServiceAccessForOrganization already
enabled!");
                return;
            }

            client.enableHealthServiceAccessForOrganization(
                EnableHealthServiceAccessForOrganizationRequest.builder().build()
            );

            System.out.println("EnableHealthServiceAccessForOrganization is in
progress");
        } catch (ConcurrentModificationException cme) {
            System.out.println("EnableHealthServiceAccessForOrganization is already
in progress. Wait for the action to complete before trying again.");
        } catch (Exception e) {
            System.out.println("EnableHealthServiceAccessForOrganization FAILED: " +
e);
        }
    }
}
```

```

    }
  }
}
```

자세한 내용은 [Java 2.0용 AWS SDK 개발자 안내서](#)를 참조하세요.

이 기능을 사용 설정하면 관리되는 정책과 함께 `AWSServiceRoleForHealth_Organizations` [서비스 연결 역할](#)이 조직의 `Health_OrganizationsServiceRolePolicy` AWS 관리 계정에 적용됩니다.

#### Note

이 기능을 활성화하는 작업은 비동기 프로세스이며 완료하는 데 시간이 걸립니다. [DescribeHealthServiceStatusForOrganization](#) 작업을 호출하여 프로세스의 상태를 확인할 수 있습니다.

## 조직 보기 이벤트 보기(CLI)

이 기능을 사용하면 AWS Health에서 조직의 계정에 영향을 주는 이벤트를 기록하기 시작합니다. 계정이 조직에 가입하면 AWS Health에서 계정을 기관 보기에 자동으로 추가합니다.

#### Note

AWS Health는 조직 보기를 사용하도록 설정하기 전에 조직에서 발생한 이벤트를 기록하지 않습니다.

계정이 조직에서 벗어나면 해당 계정의 새 이벤트가 더 이상 조직 보기에 로깅되지 않습니다. 그러나 기존 이벤트는 그대로 유지되며 최대 90일 제한까지 쿼리할 수 있습니다.

AWS는 관리자 계정 해지 유효 날짜부터 90일 동안 계정에 대한 정책 데이터를 유지합니다. 90일의 기간이 종료되는 시점에 AWS는 계정의 모든 정책 데이터를 영구적으로 삭제합니다.

- 정책을 보관하면 결과를 90일 넘게 유지할 수 있습니다. 또한 EventBridge 규칙에 사용자 지정 작업을 사용하여 결과를 S3 버킷에 저장할 수 있습니다.
- AWS가 정책 데이터를 유지하는 한 해지된 계정을 다시 열 때 AWS가 계정을 서비스 관리자로 재할당하고 계정의 서비스 정책 데이터를 복구합니다.

- 자세한 내용은 [계정 해지](#)를 참조하세요.

#### Important

AWS GovCloud (US) 리전의 고객인 경우:

- 계정을 해지하기 전에 계정 리소스를 백업한 다음 삭제합니다. 계정을 해지한 뒤에는 더 이상 해당 계정에 액세스할 수 없습니다.

AWS Health API 작업을 사용하여 조직 보기에서 이벤트를 반환할 수 있습니다.

Example : 조직 보기 이벤트 설명

다음 AWS CLI 명령은 조직의 AWS 계정에 대한 상태 이벤트를 반환합니다.

```
aws health describe-events-for-organization --region us-east-1
```

다른 AWS Health API 작업에 대한 내용은 다음 섹션을 참조하세요.

## 조직 보기 사용 안 함(CLI)

조직 보기를 비활성화하려면 [DisableHealthServiceAccessForOrganization](#) API 작업을 사용하여 비활성화할 수 있습니다.

Example

다음 AWS CLI 명령을 사용하면 계정에서 이 기능을 비활성화할 수 있습니다.

```
aws health disable-health-service-access-for-organization --region us-east-1
```

#### Note

조직 [DisableAWSServiceAccess](#) API 작업을 사용하여 조직 기능을 비활성화할 수도 있습니다. 이 작업을 호출한 후 AWS Health에서는 조직의 다른 모든 계정에 대한 이벤트 집계를 중지합니다. 조직 보기에 대한 AWS Health API 작업을 호출하면 AWS Health에서 오류를 반환합니다. AWS Health는 AWS 계정의 상태 이벤트를 계속 집계합니다.

이 기능을 비활성화하면 AWS Health에서 더 이상 조직의 이벤트를 집계하지 않습니다. 그러나 서비스 연결 역할은 AWS Identity and Access Management (IAM) 콘솔, IAM API 또는 AWS CLI(를) 통해 삭제할 때까지 관리 계정에 남아 있습니다. 자세한 내용은 IAM 사용 설명서에서 [서비스 연결 역할 삭제하기](#)를 참조하세요.

## AWS Health 조직 보기 API 작업

다음 AWS Health API 작업을 사용하여 조직 보기를 활성화할 수 있습니다.

- [DescribeEventsForOrganization](#) - 조직 전체의 이벤트에 대한 요약 정보를 반환합니다.
- [DescribeAffectedAccountsForOrganization](#) - 지정된 이벤트의 영향을 받은 조직 내 AWS 계정 목록을 반환합니다.
- [DescribeEventDetailsForOrganization](#) - 조직에서 하나 이상의 계정에 대해 지정된 이벤트에 대한 자세한 정보를 반환합니다.
- [DescribeAffectedEntitiesForOrganization](#) - 조직에서 하나 이상의 계정에 대해 하나 이상의 이벤트의 영향을 받은 엔터티의 목록을 반환합니다.

다음 작업을 사용하여 AWS Health(를) 조직 작업에서 사용 설정하거나 사용 중지할 수 있습니다.

- [EnableHealthServiceAccessForOrganization](#) - 조직과 상호 작용할 수 있는 AWS Health 권한을 부여하고 조직의 관리 계정에 SLR을 적용합니다.
- [DisableHealthServiceAccessForOrganization](#) - 조직과 상호 작용할 수 있는 AWS Health 권한을 취소합니다.
- [DescribeHealthServiceStatusForOrganization](#) - 조직에 대한 AWS Health 활성화 여부에 대한 상태 정보를 반환합니다.

이러한 API 작업을 호출하려면 Business, Enterprise On-Ramp, 또는 Enterprise 지원 플랜이 있어야 합니다. 최소 Business 지원 플랜을 보유한 계정에서 `DescribeEventForOrganization` 및 `DescribeAffectedAccountsForOrganization` 작업을 호출하면, 개별 계정의 지원 수준에 관계없이 조직의 모든 계정에 대한 정보를 반환할 수 있습니다. 다음 예시를 참조하세요.

Example 예시: Business 및 Developer 지원 플랜이 있는 계정이 있는 조직

- 조직에 세 개의 계정이 있습니다. 관리 계정에는 Business 지원 플랜이 있고 다른 두 계정에는 Developer 지원 플랜이 있습니다.
- 관리 계정 또는 필요한 권한으로 역할을 맡을 수 있는 계정에서 `DescribeEventForOrganization` API 작업을 호출합니다.

- AWS Health는 세 계정의 정보를 반환합니다.

최소 Business 지원 플랜이 있는 계정에서 `DescribeEventDetailsForOrganization` 및 `DescribeAffectedEntitiesForOrganization` API 작업을 호출하는 경우에는 Business, Enterprise On-Ramp 또는 Enterprise 지원 플랜이 있는 조직의 계정에 대한 정보만 반환할 수 있습니다.

Example 예: Enterprise, Business 및 Developer Support 플랜이 있는 계정이 있는 조직

- 조직에 다섯 개의 계정이 있습니다. 관리 계정에는 Enterprise 지원 플랜이 있고, 두 개의 계정에는 Business 지원 플랜이 있으며, 두 개의 계정에는 Developer 지원 플랜이 있습니다.
- 관리 계정에서 `DescribeEventDetailsForOrganization` API 작업을 호출합니다.
- AWS Health은(는) Enterprise 또는 Business 지원 플랜이 있는 계정에 대한 정보만 반환합니다. 개발자 지원 플랜이 있는 계정은 응답의 `failedSet`에 표시됩니다.

## 위임된 관리자 조직 보기

AWS Organizations를 통해 AWS Health의 위임된 관리자 기능을 활용하여 관리 계정 이외의 계정으로 [AWS Health Dashboard](#) 또는 [AWS Health API](#)를 통해 프로그래밍 방식으로 집계된 AWS Health 이벤트를 볼 수 있습니다. 위임된 관리자 기능을 사용하면 여러 팀이 조직 전체의 상태 이벤트를 확인하고 관리할 수 있는 유연성을 확보할 수 있습니다. 가능한 경우 관리 계정 외부로 책임을 위임하는 것이 AWS 보안 모범 사례입니다.

### 목차

- [조직 보기에 대한 위임된 관리자 등록](#)
- [조직 보기에서 위임된 관리자 제거](#)

## 조직 보기에 대한 위임된 관리자 등록

조직의 조직 보기를 활성화한 후에는 조직의 멤버 계정을 최대 5개까지 위임 관리자로 등록할 수 있습니다. 이 작업을 수행하려면 [RegisterDelegatedAdministrator](#) API 작업을 호출합니다. 멤버 계정을 등록하면 해당 계정은 관리자 계정을 위임받게 되며 AWS Health Dashboard에서 AWS Health 조직 보기에 액세스할 수 있습니다. 계정에 [Business](#), [Enterprise On-Ramp](#) 또는 [Enterprise](#) Support 플랜이 있는 경우, 위임된 관리자는 AWS Health API를 사용하여 AWS Health조직 보기에 액세스할 수 있습니다.



위임된 관리자를 설정하려면 조직의 관리 계정에서 다음 AWS Command Line Interface(AWS CLI) 명령을 호출합니다. 이 명령은 관리 계정 또는 필요한 AWS Identity and Access Management 권한이 있는 역할을 맡을 수 있는 계정에서 사용할 수 있습니다. 다음 예시의 명령에서 ACCOUNT\_ID를 등록하려는 멤버 계정 ID와 함께 AWS Health 서비스 주체 “health.amazonaws.com”으로 바꿉니다.

```
aws organizations register-delegated-administrator --account-id ACCOUNT_ID --service-principal health.amazonaws.com
```

위임된 관리자를 등록하면 조직 전체의 계정에 영향을 미치는 모든 AWS Health 이벤트에 대한 가시성을 확보할 수 있습니다. 지난 90일 동안 또는 조직 보기 기능이 처음 활성화된 이후 중에서 더 최근 날짜의 과거 이벤트를 볼 수 있습니다. 위임된 관리자 기능을 활성화하는 작업은 비동기식 프로세스이므로 완료하는 데 최대 1분이 소요됩니다.

## 조직 보기에서 위임된 관리자 제거

위임된 관리자에 대한 액세스 권한을 제거하려면 [DeregisterDelegatedAdministrator](#) API 작업을 호출하세요.

조직의 관리 계정에서 다음 AWS CLI 명령을 호출하여 위임된 관리자 멤버 계정을 제거합니다. 다음 예시 명령에서는 ACCOUNT\_ID를 제거하고자하는 멤버 계정 ID로 바꿉니다.

```
aws organizations deregister-delegated-administrator --account-id ACCOUNT_ID --service-principal health.amazonaws.com
```

# Amazon을 통한 AWS Health 이벤트 모니터링 EventBridge

EventBridge Amazon을 사용하여 AWS Health 이벤트를 감지하고 이에 대응할 수 있습니다. 그런 다음, 생성한 규칙에 따라 이벤트가 규칙에 지정한 값과 일치할 때 하나 이상의 대상 작업을 EventBridge 호출합니다. 이벤트 유형에 따라 이벤트 정보를 캡처하거나, 추가 이벤트를 시작하거나, 알림을 보내거나, 수정 조치를 취하거나, 기타 작업을 수행할 수 있습니다. 예를 들어 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스와 같이 업데이트가 예정된 AWS 리소스가 AWS 계정 있는 경우를 사용하여 AWS Health 이메일 알림을 받을 수 있습니다.

## 참고

- AWS Health 최선을 다해 이벤트를 전송합니다. 이벤트 전달이 항상 보장되는 것은 아닙니다 EventBridge.
- 생성한 모든 EventBridge 규칙은 해당 규칙에 대한 알림만 받을 수 있습니다 AWS 계정. 내 계정의 다른 계정에 대한 조직 이벤트를 수신하려면 [조직 보기 및 위임된 관리자 AWS Health 액세스를 사용한 이벤트 집계를](#) 참조하십시오. AWS Organizations

AWS Health 워크플로의 EventBridge 일부로 다음을 포함하여 여러 대상 유형 중에서 선택할 수 있습니다.

- AWS Lambda 함수
- Amazon Kinesis Data Streams
- Amazon Simple Queue Service(Amazon SQS) 대기열
- 내장 타겟 (예: CloudWatch 알람 액션)
- Amazon Simple Notification Service(SNS) 주제

예를 들어 AWS Health 이벤트가 발생하면 Lambda 함수를 사용하여 Slack 채널에 알림을 전달할 수 있습니다. 또는 이벤트 발생 시 EventBridge AWS Health Lambda를 사용하여 Amazon SNS로 사용자 지정 텍스트 또는 SMS 알림을 보낼 수 있습니다.

AWS Health 이벤트에 대한 응답으로 생성할 수 있는 자동화 및 사용자 지정 알림의 샘플은 의 [AWS Health 도구](#)를 참조하십시오. GitHub

주제

- [에 AWS 리전 대한 정보 AWS Health](#)
- [공개 이벤트 정보 AWS Health](#)
- [에 대한 이벤트 프로세서 AWS Health](#)
- [에 대한 EventBridge 규칙 생성 AWS Health](#)
- [AWS Health 이벤트 스키마 Amazon EventBridge](#)
- [이벤트 페이지 매김 AWS Health EventBridge](#)
- [조직 보기 및 위임된 관리자 액세스를 사용하여 이벤트를 집계합니다 AWS Health .](#)
- [다음과 같은 이벤트 수신 AWS HealthAWS Chatbot](#)
- [Amazon EC2 인스턴스에 대한 작업 자동화](#)
- [SMC 커넥터를 다음과 같이 구성하십시오. AWS Health](#)

## 에 AWS 리전 대한 정보 AWS Health

AWS Health 이벤트를 수신하려는 각 지역에 대한 EventBridge 규칙을 생성해야 합니다. 규칙을 생성하지 않으면 이벤트를 수신할 수 없습니다. 예를 들어, 미국 서부(오레곤) 리전에서 이벤트를 수신하려면 이 리전에 대한 규칙을 생성해야 합니다.

백업 리전에 추가 규칙을 설정하면 진행 중인 이벤트로 인해 기본 규칙이 영향을 받는 경우에 대비하여 워크플로우의 복원력을 한층 강화할 수 있습니다. 에 대한 AWS Health 공개 이벤트는 영향을 받는 지역과 백업 지역 모두에 동시에 전송됩니다. 자세한 내용은 [AWS Health의 공개 이벤트 정보](#)를 참조하십시오. 표준 AWS 파티션의 모든 리전에 대해 미국 서부(오레곤)에 규칙을 백업으로 설정하면 기본 리전이 진행 중인 문제의 영향을 받더라도 이벤트를 계속 수신할 수 있습니다. 미국 서부(오레곤) 리전의 백업 리전은 미국 동부(버지니아 북부) 리전입니다.

예를 들어 유럽 (프랑크푸르트) 지역의 이벤트를 모니터링하고 있는데 해당 지역을 일시적으로 사용할 수 없는 경우 해당 이벤트를 미국 서부 (오레곤) 지역에도 전송합니다. AWS Health 그런 다음, 백업 EventBridge 규칙이 지정한 대상으로 이벤트를 전송합니다. 백업 규칙을 만들려면 아래의 [에 대한 EventBridge 규칙 생성 AWS Health](#)에 대한 절차를 따르고 미국 서부(오레곤) 리전을 사용합니다.

일부 AWS Health 이벤트는 지역별로 다르지 않습니다. 특정 리전에 국한되지 않는 이벤트를 글로벌 이벤트라고 합니다. 여기에는 AWS Identity and Access Management (IAM)을 위해 전송된 이벤트가 포함됩니다. 글로벌 이벤트를 수신하려면 미국 동부(버지니아 북부) 리전을 기본 지역으로, 미국 서부(오레곤) 지역을 백업 지역으로 지정하는 규칙을 만들어야 합니다.

에서 글로벌 이벤트를 수신하려면 AWS GovCloud (미국 서부) 지역에 규칙을 생성해야 합니다. AWS GovCloud (US)

## 공개 이벤트 정보 AWS Health

에서 AWS Health 이벤트를 모니터링하는 EventBridge 규칙을 만들면 규칙은 계정별 이벤트와 공개 이벤트를 모두 제공합니다.

- 계정별 이벤트는 계정 및 리소스에 영향을 줍니다. 예를 들어, Amazon EC2 인스턴스에 대한 필수 업데이트 또는 기타 예약된 변경 사항 이벤트에 대해 알려주는 이벤트가 이에 해당합니다.
- 공개 이벤트는 [AWS Health Dashboard – Service health](#)에 표시됩니다. 공개 이벤트는 AWS 계정에만 국한된 것이 아니며, 서비스의 리전별 가용성에 대한 공개 정보를 제공합니다.

### Important

두 이벤트 유형을 모두 수신하려면 규칙에서 "source": [ "aws.health"] 값을 사용해야 합니다. "source": [ "aws.health\*"]와 같은 와일드카드는 모든 이벤트 모니터링 패턴과 일치하지 않습니다.

에서 공개 이벤트를 모니터링하는 경우 백업 규칙을 만드는 것이 좋습니다. AWS 리전에 대한 AWS Health 공개 이벤트는 영향을 받는 지역과 백업 지역 모두에 동시에 전송됩니다. EventARN 및 CommunicationID를 사용하여 AWS Health 이벤트의 중복을 제거하는 것이 좋습니다. 백업 지역으로 전송된 AWS Health 메시지와 동일하게 유지되기 때문입니다.

매개 변수를 사용하여 이벤트가 공개 이벤트인지 계정별 이벤트인지 식별할 수 있습니다. EventBridge eventScopeCode 이벤트에는 OR가 PUBLIC 포함될 수 있습니다. ACCOUNT\_SPECIFIC 이 파라미터를 기준으로 규칙을 필터링할 수도 있습니다.

예: Amazon Elastic Compute Cloud용 관리형 정책

다음 이벤트는 미국 동부(버지니아 북부)의 Amazon EC2에 대한 운영 문제를 보여줍니다.

```
{
  "version": "0",
  "id": "fd9d4512-1eb0-50f6-0491-d016ae56aef0",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2023-02-15T10:07:10Z",
  "region": "us-east-1",
  "resources": [],
```

```

    "detail": {
      "eventArn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE",
      "service": "EC2",
      "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
      "eventTypeCategory": "issue",
      "eventScopeCode": "PUBLIC",
      "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
      "startTime": "Wed, 15 Feb 2023 22:07:07 GMT",
      "lastUpdatedTime": "Wed, 15 Feb 2023 22:07:07 GMT",
      "statusCode": "open",
      "eventRegion": "us-east-1",
      "eventDescription": [
        {
          "latestDescription": "We are investigating increased API Error rates and Latencies for Amazon Elastic Compute Cloud in the US-EAST-1 Region.",
          "language": "en_US"
        }
      ],
      "page": "1",
      "totalPages": "1",
      "affectedAccount": "123456789012",
    }
  }
}

```

## 에 대한 이벤트 프로세서 AWS Health

계정에 AWS 사고 탐지 및 대응을 사용하는 경우 계정에

[AWSServiceRoleForHealth\\_EventProcessor](#) 서비스 연결 역할을 설치해야 합니다.

이 역할은 역할을 수임하기 위해 `event-processor.health.amazonaws.com` 서비스 보안 주체를 신뢰합니다. 이 역할에는 `AWSHealth_EventProcessorServiceRolePolicy` AWS 관리형 정책이 첨부되어 있습니다. 이 정책에는 역할이 수행할 수 있는 권한 (예: 다른 AWS 서비스 사람에게 전화 걸기) 이 나열됩니다.

그러면 이 역할을 통해 계정에 Amazon EventBridge 관리형 규칙이 생성됩니다. 이 규칙의 이름은 `AWSHealthEventProcessor-DO-NOT-DELETE`입니다. 이 규칙은 계정의 경보 상태 변경 정보를 계정으로 전달할 EventBridge 수 있는 계정의 필수 AWS Health인프라입니다.

## 관련 정보

자세한 내용은 다음 주제를 참조하십시오.

- [AWS Health의 서비스 링크 역할 사용](#)
- [AWS 관리형 정책: AWSHealth\\_EventProcessorServiceRolePolicy](#)

## 에 대한 EventBridge 규칙 생성 AWS Health

계정 내 AWS Health 이벤트에 대한 알림을 받는 EventBridge 규칙을 만들 수 있습니다. 에 대한 AWS Health이벤트 규칙을 생성하기 전에 다음을 수행하십시오.

- 에서 이벤트, 규칙, 대상을 숙지하세요. EventBridge 자세한 내용은 [Amazon이란 무엇입니까 EventBridge?](#) 를 참조하십시오. Amazon EventBridge 사용 설명서와 [새로운 기능 EventBridge — AWS 리소스 변경 사항 추적 및 대응에 대해 알아보십시오.](#)
- 이벤트 규칙에 사용할 대상을 만듭니다.

에 대한 EventBridge 규칙을 만들려면 AWS Health

1. <https://console.aws.amazon.com/events/> 에서 아마존 EventBridge 콘솔을 엽니다.
2. 변경하려면 AWS 리전페이지 오른쪽 상단의 지역 선택기를 사용하십시오. AWS Health 이벤트를 추적할 리전을 선택합니다.
3. 탐색 창에서 [Rules]를 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 작성 페이지에서 이벤트 소스로 이벤트 및 EventBridge 파트너AWS 이벤트를 선택합니다.
8. 이벤트 패턴 아래의 이벤트 소스에서 AWS 서비스(를) 선택합니다.
9. 이벤트 패턴의 AWS 서비스에서 건강을 선택합니다.
10. 이벤트 유형에서 다음 옵션 중 하나를 선택합니다.
  - 특정 Health Abuse 이벤트 – 이벤트 유형 이름에 단어 Abuse가 포함된 AWS Health 이벤트에 대한 규칙을 생성합니다.
  - 특정 건강 이벤트 — Amazon EC2와 같은 특정 AWS 서비스이벤트에 대한 규칙을 생성합니다.
11. 모든 서비스 또는 특정 서비스를 선택할 수 있습니다. 특정 서비스를 선택한 경우 다음 옵션 중 하나를 선택합니다.

- 모든 이벤트 유형 카테고리를 선택하면 모든 이벤트 유형 카테고리에 적용되는 규칙을 만들 수 있습니다.
- 특정 이벤트 유형 범주를 선택한 다음 목록에서 `issue`, `accountNotification` 또는 `scheduledChange`와 같은 값을 선택합니다.

#### Tip

- 특정 서비스에 대한 모든 AWS Health 이벤트를 모니터링하려면 모든 이벤트 유형 범주와 모든 리소스를 선택하는 것이 좋습니다. 이렇게 하면 규칙이 새 이벤트 유형 코드를 포함하여 지정된 서비스에 대한 모든 AWS Health 이벤트를 모니터링할 수 있습니다. 예시의 규칙은 [모든 Amazon EC2 이벤트](#)를 참조하십시오.
- 규칙을 생성하여 두 개 이상의 서비스 또는 이벤트 유형 범주를 모니터링할 수 있습니다. 그러려면 해당 규칙에 대한 이벤트 패턴을 수동으로 업데이트해야 합니다. 자세한 내용은 [여러 서비스 및 범주에 대한 규칙 생성](#) 섹션을 참조하십시오.

12. 특정 서비스 및 이벤트 유형 범주를 선택한 경우 다음 이벤트 유형 코드 옵션 중 하나를 선택하십시오.

- 모든 이벤트 유형 코드를 선택하여 모든 이벤트 유형 코드에 적용되는 규칙을 만듭니다.
- 특정 이벤트 유형 코드를 선택한 다음 목록에서 하나 이상의 값을 선택합니다. 이렇게 하면 특정 이벤트 유형 코드에만 적용되는 규칙이 생성됩니다. 예를 들어 **AWS\_EC2\_INSTANCE\_STOP\_SCHEDULED** 및 **AWS\_EC2\_INSTANCE\_RETIREMENT\_SCHEDULED**를 선택하면 해당 이벤트가 계정에서 발생하는 경우에만 규칙이 적용됩니다.

13. 영향을 받는 리소스에 대해 다음 옵션 중 하나를 선택합니다.

- 모든 리소스를 선택하여 모든 리소스에 적용되는 규칙을 만듭니다.
- 특정 리소스를 선택하고 하나 이상의 리소스 ID를 입력합니다. 예를 들어, **i-EXAMPLEa1b2c3de4**와 같은 Amazon EC2 인스턴스 ID를 지정하여 이 리소스에만 영향을 미치는 이벤트를 모니터링할 수 있습니다.

14. 규칙 설정이 이벤트 모니터링 요건을 충족하는지 검토합니다.

15. 다음을 선택합니다.

16. 대상 선택 페이지에서 이 규칙에 대해 만든 대상 유형을 선택한 후 해당 유형에 필요한 모든 추가 옵션을 구성합니다. 예를 들어 이벤트를 Amazon SQS 대기열 또는 Amazon SNS 주제로 보낼 수 있습니다.

17. 다음을 선택합니다.

18. (선택 사항) 태그 구성(Configure tags) 페이지에서 태그를 추가하고 다음(Next)을 선택합니다.
  - 참고: 현재 aws.health 소스에서는 태그를 전송하지 않습니다. EventBridge
19. 검토 및 생성(Review and create) 페이지에서 규칙 설정을 검토하여 이벤트 모니터링 요구 사항을 충족하는지 확인합니다.
20. Create rule을 선택합니다.

Example : 모든 Amazon EC2 이벤트에 대한 규칙

다음 예제는 이벤트 유형 카테고리, 이벤트 코드, 리소스를 비롯한 모든 Amazon EC2 이벤트를 EventBridge 모니터링하는 규칙을 생성합니다.

The screenshot shows the 'Event pattern' configuration page in the AWS EventBridge console. The page has two tabs: 'Event pattern form' (selected) and 'Custom patterns (JSON editor)'. On the left, under 'AWS service', the 'Health' dropdown is selected. Under 'Event type', the 'Specific Health events' dropdown is selected. A blue information box states: 'This builder helps to build an event pattern to get events from AWS Health regarding health status of other AWS services.' Below this, there are radio button options for 'Any service' and 'Specific service(s)' (selected), with 'EC2' selected in the dropdown. Further down, there are radio button options for 'Any event type category' (selected), 'Specific event type category(s)', 'Any resource' (selected), and 'Specific resource(s)'. On the right, the 'Event pattern' section shows a JSON filter: 

```
1 {
2   "source": ["aws.health"],
3   "detail-type": ["AWS Health Event"],
4   "detail": {
5     "service": ["EC2"]
6   }
7 }
```

 At the bottom right, there are buttons for 'Copy', 'Test pattern', and 'Edit pattern'.



## Example : 특정 Amazon EC2 이벤트에 대한 규칙

다음 예제는 다음을 EventBridge 모니터링하는 규칙을 생성합니다.

- Amazon EC2 서비스
- scheduledChange 이벤트 유형 범주
- AWS\_EC2\_INSTANCE\_TERMINATION\_SCHEDULED 및  
AWS\_EC2\_INSTANCE\_RETIREMENT\_SCHEDULED의 이벤트 유형 코드
- ID i-EXAMPLEa1b2c3de4가 있는 인스턴스

**AWS service**  
The name of the AWS service as the event source

Health ▼

**Event type**  
The type of events as the source of the matching pattern

Specific Health events ▼

**i** This builder helps to build an event pattern to get events from AWS Health regarding health status of other AWS services.

☐ Any service

☒ Specific service(s)

EC2 ▼

☐ Any event type category

☒ Specific event type category(s)

scheduledChange ▼

☐ Any event type code

☒ Specific event type code(s)

▼

AWS\_EC2\_INSTANCE\_TERMINATION\_SC X  
HEDULED

AWS\_EC2\_INSTANCE\_RETIREMENT\_SCH X  
EDULED

☐ Any resource

☒ Specific resource(s)

i-EXAMPLEa1b2c3de4

## 여러 서비스 및 범주에 대한 규칙 생성

이전 절차의 예시는 단일 서비스 및 이벤트 유형 범주에 대한 규칙을 만드는 방법을 보여줍니다. 여러 서비스 및 이벤트 유형 범주에 대한 규칙을 만들 수도 있습니다. 즉, 모니터링하려는 각 서비스 및 범주에 대해 별도의 규칙을 만들 필요가 없습니다. 그러려면 이벤트 패턴을 편집한 다음 변경 사항을 수동으로 입력해야 합니다.

다음 옵션 중 하나를 사용할 수 있습니다.

기존 규칙에 서비스 및 범주를 추가하려면

1. EventBridge 콘솔의 규칙 페이지에서 규칙 이름을 선택합니다.
2. 오른쪽 상단 모서리에서 편집을 선택합니다.
3. 다음을 선택합니다.
4. 이벤트 패턴의 경우 패턴 편집을 선택한 다음 텍스트 필드에 변경 사항을 입력합니다.
5. 검토 및 업데이트 페이지가 표시될 때까지 다음을 선택합니다.
6. 규칙 업데이트를 선택하여 변경 사항을 저장합니다.

새 규칙에 서비스 및 범주를 추가하려면

1. 이 작업을 수행하려면 [9단계의 에 대한 EventBridge 규칙 생성 AWS Health](#) 절차를 수행합니다.
2. 목록에서 단일 서비스나 범주를 선택하는 대신 이벤트 패턴에서 패턴 편집을 선택합니다.
3. 텍스트 필드에 변경 내용을 입력합니다. 고유한 이벤트 패턴을 만들기 위한 모델로 다음 [예시 패턴](#)을 참조하십시오.
4. 이벤트 패턴을 검토한 다음 [에 대한 EventBridge 규칙 생성 AWS Health](#)의 나머지 절차에 따라 규칙을 생성하십시오.

API 또는 AWS Command Line Interface (AWS CLI) 를 사용하십시오.

새 규칙이나 기존 규칙의 경우 [PutRule](#) API 작업 또는 `aws events put-rule` 명령을 사용하여 이벤트 패턴을 업데이트하십시오. 예제 AWS CLI 명령은 명령 참조의 [put-rule](#)을 AWS CLI 참조하십시오.

Example 예: 여러 서비스 및 이벤트 유형 범주

다음 이벤트 패턴은 세 가지 AWS 서비스, 즉 Amazon EC2 `issueaccountNotification`, Amazon EC2 Auto Scaling 및 Amazon VPC의, 및 `scheduledChange` 이벤트 유형 카테고리에 대한 이벤트를 모니터링하는 규칙을 생성합니다.

```
{
  "detail": {
    "eventTypeCategory": [
      "issue",
      "accountNotification",
      "scheduledChange"
    ],
  },
}
```

```

    "service": [
      "AUTOSCALING",
      "VPC",
      "EC2"
    ],
    "detail-type": [
      "AWS Health Event"
    ],
    "source": [
      "aws.health"
    ]
  }

```

## AWS Health 이벤트 스키마 Amazon EventBridge

다음은 AWS Health 이벤트 스키마입니다. 이전 버전의 스키마에 대한 변경 또는 추가 사항은 “New”로 강조 표시됩니다. 샘플 페이로드를 스키마 다음에 제공합니다.

### AWS Health 이벤트 스키마


#### AWS Health 이벤트 스키마

파라미터	설명	필수
version	EventBridge 버전, 현재 “0”	예
id	이벤트 uniqueEventBridge 식별자	예
detail-type	세부 유형을 설명합니다. AWS Health 이벤트의 경우 이는 다음과 같습니다&AWS	예


파라미터	설명	필수
	Health Event. AWS Health Abuse Event	
source	이벤트 버스 소스. AWS Health 이벤트의 경우 다음과 같습니다. aws.health	예


파라미터	설명	필수
account	<p>이벤트가 전송된 대상 계정 AWS Health ID입니다.</p> <div>  <b>Note</b>  조직 보기의 경우, 관리 또는 위임된 관리자 계정에 수신된 경우 이는 affectedAccount와 다릅니다. </div>	예

파라미터	설명	필수
time	알림이 전송된 시간. EventBridge 형식: yyyy-mm-ddThh:mm:ssZ	예

파라미터	설명	필수
region	<p>알림이 전달된 대상을 식별합니다. AWS 리전</p> <div> <b>Note</b> 이 필드는 이 이벤트의 영향을 받는 지역을 나타내지 않습니다. AWS Health 이 정보는 “detail.eventRegion”으로 제공됩니다.</div>	예



파라미터	설명	필수
resources	<p>영향을 받는 리소스가 있는 경우 계정 내에서 영향을 받는 리소스의 목록을 설명합니다.</p> <div>  <b>Note</b>  참조된 리소스가 없는 경우 이 필드는 비어 있을 수 있습니다. </div>	아니요
세부 정보	이 섹션에는 아래와 같이 AWS Health 이벤트의 모든 세부 정보가 포함되어 있습니다.	예


파라미터	설명	필수
eventArn	<p>특정 지역의 AWS Health 이벤트 고유 식별자에는 지역 및 이벤트 ID가 포함됩니다.</p> <div data-bbox="1068 590 1273 1241"> <p> <b>Note</b></p> <p>eventArn은 특정 고객 계정이 나리 전에 고유하지 않습니다.</p> </div>	예

파라미터	설명	필수
서비스	AWS Health 이벤트의 AWS 서비스 영향을 받는 사람. 예를 들어, Amazon EC2, Amazon Simple Storage Service, Amazon Redshift, 또는 Amazon Relational Database Service	예

파라미터	설명	필수
	<p>이벤트 TypeCode</p> <p>이벤트 유형의 고유 식별자입니다. 예를 들면 AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED 및 AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED 등입니다. MAINTENANCE_SCHEDULED 이 포함된 이벤트는 일반적으로 startTime 약 2주 전에 푸시됩니다.</p> <div data-bbox="1068 1409 1271 1881"> <p> <b>Note</b></p> <p>새로 계획된 모든 수명 주기 이벤트에는</p> </div>	예


파라미터		설명	필수
		<div><div>AWS_{SEI ICE}_PL/ NED_LIFI YCLE_EVI T 이 벤트 유형 이 있 습니 다.</div></div>	
	이벤트 TypeCategory	이벤트의 범 주 코드입니 다. 가능한 값 은 issue, accountNo tificatio n , investiga tion 및 scheduled Change 입니 다.	예


파라미터		설명	필수
	이벤트 ScopeCode	이벤트가 계 정별 AWS Health 이벤 트인지 공개 이벤트인지를 나타냅니다. 가능한 값은 ACCOUNT_S PECIFIC 또 는 PUBLIC입 니다.	예

파라미터	설명	필수
	<p>communicationId (New)</p> <p>이벤트에 대한 이 커뮤니케이션의 고유 식별자입니다. AWS Health CommunicationID가 동일한 메시지는 가능한 백업 메시지 또는 단일 AWS Health 이벤트의 페이지입니다. 이 식별자를 accountId와 함께 사용하면 메시지 중복을 제거하는 데 도움이 됩니다.</p> <div data-bbox="1068 1339 1273 1852"> <p> <b>Note</b></p> <p>페이지 매김 기능이 출시됨에 따라 communicationId</p> </div>	예

파라미터	설명	필수
	<p>에 페 이지 번호 가 포 함되 어 있 어 여 러 페 이지 에서 communic tionId 를 고 유하 게 유 지할 수 있 습니 다(예: 12345678 10-1). 자세 한 내 용은 <a href="#">이벤 트 페 이지 매김 AWS Health EventBrid ge</a> 섹 션을 참조</p>	





파라미터	설명	필수
	하십 시오.	
	<div> <div>startTime</div> <div> AWS Health 이벤트 시 작 시간.. DoW, DD, MMM, YYYY, HH:MM:SS TZ </div> <div>  Note 예약 된 이 벤트 의 시 작 시 간은 미래 일 수 있습 니다. </div> </div>	예

파라미터	설명	필수
endTime	<p>AWS Health 이벤트 종료 시간 형식은 다음과 같습니다. DoW, DD MMM YYYY HH:MM:SS TZ.</p> <div data-bbox="1068 638 1273 1381"> <p> <b>Note</b></p> <p>미래에 설정되는 이벤트에는 EndTime이 제공되지 않을 수 있습니다.</p> </div>	아니요
	마지막으로 UpdatedTime	예

파라미터	설명	필수
<div>statusCode</div>	<p>AWS Health 이벤트 상태. 유형 범주에는 다양한 상태가 있습니다.</p> <p>Issue이벤트 카테고리에 사용할 수 있는 open 값은 closed 또는 upcoming 입니다.</p> <p>scheduled Changes 이벤트 범주는 Upcoming, Ongoing, 또는 Completed 과 같이 상태가 다릅니다.</p> <p>AccountNotifications 이벤트 범주에는 상태가 없으며 "-"로 설정되어 있습니다.</p>	<div>예</div>

파라미터		설명	필수
	eventRegion	이 AWS Health 이벤트에서 설명하는 영향을 받는 지역.	예
	eventDescription	AWS Health 이벤트를 설명하는 섹션. 여기에는 이벤트를 설명하는 언어 및 텍스트 필드가 포함됩니다.	예
	language	AWS Health 이벤트에 사용된 언어. 이는 일반적으로 이벤트가 게시되는 리전에 따라 결정됩니다. us-east-1 리전의 경우, 일반적으로 "en_US"입니다.	예

파라미터	설명	필수
	<p>latestDescription</p> <p>AWS Health API에서 렌더링되고 일반적으로 AWS Health 대시보드에 나타나는 AWS Health 이벤트를 설명합니다.</p> <div data-bbox="1068 730 1269 1810"> <p> <b>Note</b></p> <p>공개 이벤트의 경우 여기에는 최신 업데이트만 포함되며 이벤트의 전체 기록은 포함되지 않습니다.</p> </div>	예

파라미터		설명	필수
	eventMetadata	AWS Health 이벤트에 제공할 수 있는 추가 이벤트 메타데이터	아니요
	<metadata key 1>	메타데이터 키, 값 문자열 "keystring1": "keyvalue1" <div>  <b>Note</b>              이벤트를 메타데이터 키-값 쌍은 이벤트를 전송한 서비스에 의해 결정됩니다. AWS Health           </div>	아니요


파라미터		설명	필수
	affectedEntities	이 AWS Health 이벤트 내에서 영향을 받는 리소스의 리소스 값과 상태를 설명하는 배열입니다.	아니요
	entityValue	리소스/엔터티 ID	아니요
	lastUpdatedtime (New)	다음 형식의 이 리소스/엔터티 상태가 다음 형식으로 마지막으로 업데이트된 시간: DoW, DD MMM YYYY HH:MM:SS TZ	아니요

파라미터		설명	필수
	status (new)	영향을 받 는 리소스/엔 터티의 상태 입니다. 가 능한 값은 IMPAIRED, UNIMPAIRE D , PENDING, RESOLVED, UNKNOWN입니 다.	아니요




파라미터	설명	필수
<div>page (New)</div>	<p>이 메시지가 나타내는 페이지입니다. 자세한 내용은 <a href="#">이벤트 페이지 매김 AWS Health EventBridge</a> 섹션을 참조하십시오.</p> <div>  <b>Note</b>        페이지 매김은 리소스에 서만 발생합니다. 256KB 크기 제한 위반의 다른 원인으로 인해 통신이 실패할 수     </div>	예

파라미터		설명	필수
		있습니다.	

파라미터	설명	필수
	<p>totalPages (New)</p> <p>이 상태 이벤트의 총 페이지 수입니다. 자세한 내용은 <a href="#">이벤트 페이지 매김 AWS Health EventBridge</a> 섹션을 참조하십시오.</p> <div data-bbox="1068 730 1271 1818"> <p> <b>Note</b></p> <p>이 정보를 사용하여 계정에 대해 여러 페이지로 구성된 통신의 모든 페이지를 수신했는지 확인할 수 있습니다.</p> </div>	예

파라미터		설명	필수
		습니다.	

파라미터	설명	필수
<p>affectedAccount (New)</p>	<p>영향을 받는 계정의 accountId입니다.</p> <div data-bbox="1068 445 1273 1869"> <p> <b>Note</b></p> <p>이 상 태 이 벤트 가 의 일 부 인 계 정 으 로 전 송 되 고 관 리 또 는 위 임된 관 리 자 계 정 으 로 수 신 되 는 경 우 이 는 “계 정” AWS Organizations 필드 와 다 를 수</p> </div>	<p>예</p>

파라미터	설명	필수
	있습니다.	

## 공개 상태 이벤트 - Amazon EC2 운영 문제

```
{
  "version": "0",
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2023-01-27T09:01:22Z",
  "region": "af-south-1",
  "resources": [],
  "detail": {
    "eventArn": "arn:aws:health:af-south-1::event/EC2/
AWS_EC2_OPERATIONAL_ISSUE/AWS_EC2_OPERATIONAL_ISSUE_7f35c8ae-af1f-54e6-a526-
d0179ed6d68f",
    "service": "EC2",
    "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
    "eventTypeCategory": "issue",
    "eventScopeCode": "PUBLIC",
    "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
    "startTime": "Fri, 27 Jan 2023 06:02:51 GMT",
    "endTime": "Fri, 27 Jan 2023 09:01:22 GMT",
    "lastUpdatedTime": "Fri, 27 Jan 2023 09:01:22 GMT",
    "statusCode": "open",
    "eventRegion": "af-south-1",
    "eventDescription":
    [{
      "language": "en_US",
      "latestDescription": "Current severity level: Operating normally\n
\n[RESOLVED] \n\n [03:15 PM PST] We continue see recovery \n\nThe following AWS
services were previously impacted but are now operating normally: APPSYNC, BACKUP,
EVENTS."
    }],
    "affectedEntities": [],
    "page": "1",
  }
}
```

```

    "totalPages": "1",
    "affectedAccount": "123456789012",
  }
}

```

## 계정별 AWS Health 이벤트 - Elastic Load Balancing API 문제

```

{
  "version": "0",
  "id": "121345678-1234-1234-1234-123456789012",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2022-06-10T06:27:57Z",
  "region": "ap-southeast-2",
  "resources": [],
  "detail": {
    "eventArn": "arn:aws:health:ap-southeast-2::event/
AWS_ELASTICLOADBALANCING_API_ISSUE_90353408594353980",
    "service": "ELASTICLOADBALANCING",
    "eventTypeCode": "AWS_ELASTICLOADBALANCING_API_ISSUE",
    "eventTypeCategory": "issue",
    "eventScopeCode": "ACCOUNT_SPECIFIC",
    "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
    "startTime": "Fri, 10 Jun 2022 05:01:10 GMT",
    "endTime": "Fri, 10 Jun 2022 05:30:57 GMT",
    "statusCode": "open",
    "eventRegion": "ap-southeast-2",
    "eventDescription": [{
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }],
    "page": "1",
    "totalPages": "1",
    "affectedAccount": "123456789012",
  }
}

```

## 계정별 AWS Health 이벤트 - Amazon EC2 인스턴스 스토어 드라이브 성능 저하

```
{
  "version": "0",
  "id": "121345678-1234-1234-1234-123456789012",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2022-06-03T06:27:57Z",
  "region": "us-west-2",
  "resources": [
    "i-abcd1111"
  ],
  "detail": {
    "eventArn": "arn:aws:health:us-west-2::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
    "service": "EC2",
    "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
    "eventTypeCategory": "issue",
    "eventScopeCode": "ACCOUNT_SPECIFIC",
    "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
    "startTime": "Fri, 3 Jun 2022 05:01:10 GMT",
    "endTime": "Fri, 3 Jun 2022 05:30:57 GMT",
    "statusCode": "open",
    "eventRegion": "us-west-2",
    "eventDescription": [{
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }],
    "affectedEntities": [{
      "entityValue": "i-abcd1111",
    }],
    "page": "1",
    "totalPages": "1",
    "affectedAccount": "123456789012",
  }
}
```



## 이벤트 페이지 매김 AWS Health EventBridge

AWS Health “리소스” 또는 “AffectedEntities” 목록으로 인해 메시지 크기가 256KB 메시지 크기 제한을 초과하는 EventBridge 경우 AWS Health 이벤트 페이지 매김을 지원합니다. 이전에는 이 한도를 초과했을 때 이벤트와 함께 전체 리소스 목록을 전달하지 AWS Health 애플리케이션이었습니다.

AWS Health 이제 메시지에 모든 “리소스”와 “Detail.AffectedEntities”가 포함됩니다. 이 “리소스” 및 “Detail.AffectedEntities” 목록이 256KB를 초과하는 경우 상태 이벤트를 여러 페이지로 분할하고 해당 AWS Health 페이지를 개별 메시지로 게시합니다. EventBridge 각 페이지에는 동일한 eventARN과 communicationId가 유지되므로 모든 페이지가 수신된 후 “resources” 또는 “detail.affectedEntities” 목록을 재조합하는 데 도움이 됩니다.

이러한 추가 메시지로 인해 불필요한 메시지가 발생할 수 있습니다. 예를 들어, EventBridge 규칙이 이메일이나 채팅과 같이 사람이 읽을 수 있는 인터페이스로 전달되는 경우). 사람이 읽을 수 있는 알림을 받은 고객은 “detail.page” 필드에 필터를 추가하여 첫 페이지만 처리할 수 있습니다. 이렇게 하면 후속 페이지에서 생성되는 불필요한 메시지를 제거할 수 있습니다.

페이지 매김 실행을 지원하기 위한 몇 가지 스키마 변경 사항이 포함되어 있습니다. 각 communicationId에는 이제 페이지가 1개뿐인 경우에도 communicationId 뒤에 하이픈으로 연결된 페이지 번호가 포함됩니다. 또한 이벤트의 현재 페이지 번호와 총 페이지 수를 설명하는 detail.page와 detail.totalPages라는 두 개의 새 필드도 있습니다. AWS Health 페이지로 구분된 각 메시지에 포함된 정보는 “detail.affectedEntities” 또는 “resources” 목록을 제외하고는 동일합니다. 이러한 목록은 모든 페이지를 수신한 후에 다시 구성할 수 있습니다. 영향을 받는 리소스 및 엔터티의 페이지는 순서에 구애받지 않습니다.

## 조직 보기 및 위임된 관리자 액세스를 사용하여 이벤트를 집계합니다 AWS Health .

AWS Health EventBridgeAmazon에 게시된 AWS Health 이벤트에 대한 조직 보기 및 위임된 관리자 액세스를 지원합니다. 조직 보기가 켜져 있으면 관리 계정 또는 위임된 관리자 계정이 내 조직 내 모든 계정으로부터 단일 AWS Health 이벤트 피드를 수신합니다. AWS Health AWS Organizations

이 기능은 조직 전체의 AWS Health 이벤트를 관리하는 데 도움이 되는 중앙 집중식 보기를 제공하도록 설계되었습니다. 관리 계정에서 조직 보기 및 EventBridge 규칙을 설정해도 조직의 다른 계정에 대한 규칙은 비활성화되지 않습니다. EventBridge

에서 조직 보기 및 위임된 관리자 액세스를 활성화하는 방법에 대한 AWS Health 자세한 내용은 이벤트 [집계를 AWS Health](#) 참조하십시오.

## 다음과 같은 이벤트 수신 AWS HealthAWS Chatbot

Slack 및 Amazon Chime과 같은 채팅 클라이언트에서 직접 AWS Health 이벤트를 수신할 수 있습니다. 이 이벤트를 사용하여 AWS 애플리케이션과 인프라에 영향을 미칠 수 있는 최근 AWS 서비스 문제를 식별할 수 있습니다. 그런 다음 [AWS Health Dashboard](#) 로그인하여 업데이트에 대해 자세히 알아볼 수 있습니다. 예를 들어 AWS 계정에서 AWS\_EC2\_INSTANCE\_STOP\_SCHEDULED 이벤트 유형을 모니터링하는 경우 이벤트가 Slack 채널에 직접 표시될 수 있습니다. AWS Health

### 필수 조건

시작하기 전에 다음 사항이 필요합니다.

- 로 AWS Chatbot구성된 채팅 클라이언트. Amazon Chime 및 Slack을 구성할 수 있습니다. 자세한 내용은 [AWS Chatbot 관리자 가이드에서 AWS Chatbot](#)(으)로 시작하기를 참조하십시오.
- 생성하고 구독 중인 Amazon SNS 주제입니다. 이미 SNS 주제가 있으면 그 역할을 사용하면 됩니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 [Amazon SNS 시작하기](#)를 참조하십시오.

를 사용하여 AWS Health 이벤트를 수신하려면 AWS Chatbot

- 그런 다음 13단계의 [에 대한 EventBridge 규칙 생성 AWS Health](#) 절차를 따릅니다.
  - 13단계에서 이벤트 패턴 설정을 마치면 패턴의 마지막 줄에 심표를 추가하고 다음 줄을 추가하여 페이지징된 AWS Health 이벤트에서 불필요한 채팅 메시지를 제거합니다. [이벤트 페이지 매김 AWS Health EventBridge](#) 섹션을 참조하십시오.
 


```
"detail.page": ["1"]
```
  - [14단계](#)에서 대상을 선택할 때는 SNS 주제를 선택합니다. 콘솔에서도 이와 동일한 SNS 주제를 사용하게 됩니다. AWS Chatbot
  - 나머지 단계를 완료하여 규칙을 생성합니다.
- [AWS Chatbot 콘솔](#)로 이동합니다.
- Slack 채널 이름과 같은 채팅 클라이언트를 선택한 다음 편집을 선택합니다.
- 알림 - 옵션 섹션의 주제에서 1단계에서 지정한 것과 동일한 SNS 주제를 선택합니다.
- 저장을 선택합니다.

규칙에 EventBridge 맞는 이벤트를 AWS Health 보내면 채팅 클라이언트에 AWS Health 이벤트가 표시됩니다.

6. AWS Health 대시보드에서 자세한 정보를 보려면 이벤트 이름을 선택하세요.


### Example : Slack으로 전송된 AWS Health 이벤트

다음은 미국 동부 (버지니아 북부) 지역의 Amazon EC2와 아마존 심플 스토리지 서비스 (Amazon S3)에서 Slack 채널에 나타나는 두 가지 AWS Health 이벤트의 예입니다.



**AWS**

APP 11:46 AM



**AWS Health Event | us-east-1 | Account: 123456789012 | open**

Event type code: AWS\_EC2\_PERSISTENT\_INSTANCE\_RETIREMENT\_SCHEDULED

EC2 has detected degradation of the underlying hardware hosting your Amazon EC2 instance associated with this event in the us-east-1 region. Due to this degradation your instance could already be unreachable. We will stop your instance after 2021-03-19 18:36:40 PST. Please take appropriate action before this time.

You can find more information about retirement events scheduled for your EC2 instances in the AWS Management Console <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Events>


What will happen to my instance?

Your instance will be stopped after the specified retirement date. You can start it again.

[Show more](#)


Start time: Sat, 20 Mar 2021 01:35:40 GMT

End time: Sat, 20 Mar 2021 01:36:40 GMT



**AWS**

APP 12:08 PM



**AWS Health Event | us-east-1 | Account: 123456789012 | open**

Event type code: AWS\_S3\_OPEN\_ACCESS\_BUCKET\_NOTIFICATION

We are writing to notify you that you may have exposed your S3 bucket/s to a larger audience than you intended. AWS recommends that you review your bucket permissions and ACLs to determine whether the access is appropriate. S3 bucket permissions should never contain `Principal::*` unless you intend to grant public access to your data. Additionally, S3 bucket ACLs should be appropriately scoped to prevent unintended access to `Authenticated Users` or `Everyone` unless your use case requires it.

The list of buckets with this configuration is associated with this event.

The following links provide an overview...

[Show more](#)

Start time: Sat, 20 Mar 2021 01:35:40 GMT

End time: Sat, 20 Mar 2021 01:36:40 GMT

# Amazon EC2 인스턴스에 대한 작업 자동화

Amazon EC2 인스턴스에 대해 예약된 이벤트에 응답하는 작업을 자동화할 수 있습니다. AWS 계정으로 이벤트를 AWS Health 보내면 EventBridge 규칙이 AWS Systems Manager 자동화 문서와 같은 대상을 호출하여 사용자를 대신하여 작업을 자동화할 수 있습니다.

예를 들어, Amazon Elastic Block Store (Amazon EBS) 지원 EC2 인스턴스에 대해 Amazon EC2 인스턴스 사용 중지 이벤트가 예정된 경우 해당 이벤트 유형이 대시보드로 AWS Health 전송됩니다. `AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED` AWS Health 규칙에서 이 이벤트 유형을 감지하면 인스턴스의 중지 및 시작을 자동화할 수 있습니다. 이렇게 하면 이러한 작업을 수동으로 수행할 필요가 없습니다.

## Note

Amazon EC2 인스턴스에 대한 작업을 자동화하려면 Systems Manager에서 인스턴스를 관리해야 합니다.

자세한 내용은 Amazon EC2 사용 [설명서의 Amazon EC2 EventBridge 자동화를](#) 참조하십시오.

## 필수 조건

규칙을 생성하려면 먼저 AWS Identity and Access Management (IAM) 정책을 생성하고, IAM 역할을 생성하고, 역할의 신뢰 정책을 업데이트해야 합니다.

### IAM 정책 생성

다음 절차에 따라 역할에 맞는 고객 관리형 정책을 생성합니다. 이 정책은 사용자를 대신하여 작업을 수행할 수 있는 권한을 역할에 부여합니다. 이 절차에서는 IAM 콘솔에서 JSON 정책 편집기를 사용합니다.

### IAM 정책을 만들려면

1. [에 AWS Management Console 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.](#)
2. 탐색 창에서 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. JSON 탭을 선택합니다.
5. 다음 JSON을 복사한 다음 편집기에서 기본 JSON과 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/AutomationEVRole"
    }
  ]
}
```

- a. Resource파라미터에서 Amazon 리소스 이름 (ARN) 의 경우 AWS 계정 ID를 입력합니다.
- b. 역할 이름을 바꾸거나 기본값을 사용할 수도 있습니다. 이 예시에서는 **AutomationEVRole**을 사용합니다.
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. 정책 검토 페이지에서 이름 (예: **AutomationEV**) RolePolicy 및 설명 (선택 사항) 을 입력합니다.
10. 요약 페이지를 검토하여 정책에서 허용하는 권한을 확인합니다. 정책에 만족하면 정책 생성을 선택합니다.

이 정책은 이 역할이 수행할 수 있는 작업을 정의합니다. 자세한 내용은 IAM 사용 설명서의 [IAM 정책 생성\(콘솔\)](#)을 참조하십시오.

## IAM 역할 생성

정책을 생성한 후 IAM 역할을 생성한 다음 이 정책을 해당 역할에 연결해야 합니다.

## 서비스의 역할을 만들려면 AWS

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/iam/> 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 유형 선택(Select type of trusted entity)에서 AWS 서비스(service)를 선택합니다.
4. 이 역할을 말도록 허용할 서비스에 대해 EC2를 선택합니다.
5. 다음: 권한을 선택합니다.
6. 생성한 정책 이름 (예: **AutomationEV RolePolicy**) 을 입력한 다음 정책 옆의 확인란을 선택합니다.
7. 다음: 태그를 선택합니다.
8. (선택 사항) 태그를 키 값 페어로 사용하여 메타데이터를 역할에 추가할 수 있습니다.
9. 다음: 검토를 선택합니다.
10. 역할 이름에 **AutomationEVRole**을 입력합니다. 이 이름은 사용자가 생성한 IAM 정책의 ARN에 표시되는 이름과 동일해야 합니다.

11. (선택 사항) Role description(역할 설명)에 역할에 대한 설명을 입력합니다.
12. 역할을 검토한 다음 Create role을 선택합니다.

자세한 내용은 IAM [사용 설명서의 AWS 서비스 역할 생성](#)을 참조하십시오.

## 신뢰 정책 업데이트

마지막으로 생성한 역할에 대한 신뢰 정책을 업데이트할 수 있습니다. EventBridge 콘솔에서 이 역할을 선택할 수 있으려면 이 절차를 완료해야 합니다.

### 역할에 대한 신뢰 정책 업데이트

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/iam/> 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택합니다.
3. AWS 계정의 역할 목록에서 생성한 역할의 이름 (예: *AutomationVrole*) 을 선택합니다.
4. 신뢰 관계 탭을 선택한 후 신뢰 관계 편집을 선택합니다.
5. 정책 문서의 경우 다음 JSON을 복사하고 기본 정책을 제거한 다음 복사한 JSON을 그 자리에 붙여넣습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com",
          "events.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. 신뢰 정책 업데이트를 선택합니다.

자세한 내용은 IAM 사용 설명서에서 역할 [신뢰 정책 수정하기\(콘솔\)](#)를 참조하십시오.

## 에 대한 규칙을 생성하세요. EventBridge

이 절차에 따라 EventBridge 콘솔에서 규칙을 생성하면 사용 중지될 예정인 EC2 인스턴스의 중지 및 시작을 자동화할 수 있습니다.

Systems Manager의 자동 EventBridge 동작에 대한 규칙을 만들려면

1. <https://console.aws.amazon.com/events/> 에서 아마존 EventBridge 콘솔을 엽니다.
2. 탐색 창의 이벤트 아래에서 규칙을 선택합니다.
3. 규칙 생성 페이지에서 규칙의 이름과 설명을 입력합니다.
4. 패턴 정의(Define pattern)에서 이벤트 패턴(Event pattern)을 선택한 다음 서비스별 사전 정의된 패턴(Pre-defined pattern by service)을 선택합니다.
5. 서비스 제공업체에서 AWS를 선택합니다.
6. 서비스 이름에서 상태를 선택합니다.
7. 이벤트 유형에서 특정 상태 이벤트를 선택합니다.
8. 특정 서비스를 선택한 다음 EC2를 선택합니다.
9. 특정 이벤트 유형 범주를 선택한 다음 scheduledChange를 선택합니다.
10. 특정 이벤트 유형 코드를 선택한 다음 이벤트 유형 코드를 선택합니다.

예를 들어 Amazon EC2 EBS 지원 인스턴스의 경우

**AWS\_EC2\_PERSISTENT\_INSTANCE\_RETIREMENT\_SCHEDULED**를 선택합니다. Amazon EC2 인스턴스 스토어 지원 인스턴스의 경우 **AWS\_EC2\_INSTANCE\_RETIREMENT\_SCHEDULED**를 선택합니다.

11. [모든 리소스(Any resource)]를 선택합니다.

이벤트 패턴은 다음 예와 유사합니다.

### Example

```
{
  "source": [
    "aws.health"
  ],
  "detail-type": [
    "AWS Health Event"
  ],
  "detail": {
    "service": [
```



```

    "EC2"
  ],
  "eventTypeCategory": [
    "scheduledChange"
  ],
  "eventTypeCode": [
    "AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED"
  ]
}
}

```

12. 시스템 관리자 자동화 문서 대상을 추가합니다. 대상 선택의 대상에서 SSM 자동화를 선택합니다.
13. [문서(Document)]에서 [AWS-RestartEC2Instance]를 선택합니다.
14. 자동화 파라미터 구성을 펼친 다음 입력 변환기를 선택합니다.
15. 입력 경로 필드에 **{"Instances": "\$.resources"}**를 입력합니다.
16. 두 번째 필드에 **{"InstanceId": <Instances>}**을(를) 입력합니다.
17. 기존 역할 사용을 선택한 다음, 생성한 IAM 역할(예: *AutomationvRole*)을 선택합니다.

대상은 다음 예시와 같은 형식이어야 합니다.

Target

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

Remove

SSM Automation

Document

AWS-RestartEC2Instance

► Configure document version

▼ Configure automation parameter(s)

☐ No Parameter(s)
 ☐ Constant
 ☒ Input Transformer

```
{"Instances": "$.resources"}
```

```
{"InstanceId": <Instances>}
```

EventBridge needs permission to call SSM Start Automation Execution with your supplied Automation document and parameters. By continuing, you are allowing us to do so.

☐ Create a new role for this specific resource
 ☒ Use existing role

AutomationEVRole

### Note

필수 EC2 및 Systems Manager 권한과 신뢰 관계를 갖춘 기존 IAM 역할이 없는 경우 해당 역할은 목록에 표시되지 않습니다. 자세한 내용은 [필수 조건](#) 섹션을 참조하십시오.

## 18. 생성을 선택합니다.

계정에서 규칙과 일치하는 이벤트가 발생하면 지정된 대상으로 이벤트를 전송합니다.  
EventBridge

## SMC 커넥터를 다음과 같이 구성하십시오. AWS Health

AWS Health 이벤트를 JIRA와 통합하고 ServiceNow , 서비스 관리 커넥터 (SMC) 를 사용하여 운영 및 계정 정보를 수신하고, 예정된 변경에 대비하고, 건강 이벤트를 관리할 수 있습니다. SMC 통합은 전송된 Health 이벤트를 사용하여 JIRA 티켓 및 인시던트를 자동으로 생성, 매핑 및 업데이트할 AWS Health 수 있습니다. EventBridge ServiceNow

조직 보기 및 위임된 관리자 액세스 권한을 사용하여 JIRA 내에서 조직 전체의 건강 이벤트를 쉽게 관리하고 AWS Health 정보를 팀의 워크플로에 직접 통합할 수 있습니다. ServiceNow

[SMC를 사용한 ServiceNow 통합에 대한 자세한 내용은 통합을 참조하십시오. AWS Health ServiceNow](#)

[SMC를 사용한 JIRA Management Cloud 통합에 대한 자세한 내용은 JIRA를 참조하십시오.AWS Health](#)

# 모니터링 AWS Health

모니터링은 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 AWS Health 있어 중요한 부분입니다. AWS 문제를 관찰하고, 문제 발생 시 보고하고 AWS Health, 적절한 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. 자세한 내용은 [Amazon CloudWatch 사용 설명서](#)를 참조하십시오.

EventBridge Amazon을 사용하면 서비스와 리소스에 영향을 줄 수 있는 AWS Health 이벤트에 대한 알림을 받을 수 있습니다. 예를 들어 Amazon EC2 인스턴스에 대한 이벤트를 AWS Health 게시하는 경우 이러한 알림을 사용하여 조치를 취하고 필요에 따라 리소스를 업데이트하거나 교체할 수 있습니다. 자세한 정보는 [Amazon을 통한 AWS Health 이벤트 모니터링 EventBridge](#)을 참조하세요.

- AWS CloudTrail 계정에서 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 설명서](#)를 참조하세요.

## 주제

- [를 AWS Health 사용하여 API 호출을 로깅합니다. AWS CloudTrail](#)

## 를 AWS Health 사용하여 API 호출을 로깅합니다. AWS CloudTrail

AWS Health 에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합됩니다 AWS Health. CloudTrail API 호출을 AWS Health 이벤트로 캡처합니다. 캡처된 호출에는 AWS Health 콘솔에서의 호출 및 AWS Health API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 에 대한 이벤트를 포함하여 Amazon S3 버킷으로 CloudTrail 이벤트를 지속적으로 전송할 수 AWS Health있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람 AWS Health, 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 설명서](#)를 참조하십시오.

## AWS Health 자세한 내용은 CloudTrail

CloudTrail 계정을 만들 때 AWS 계정에서 활성화됩니다. 에서 AWS Health지원되는 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 AWS Health트레일을 생성하세요. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로 콘솔에서 트레일을 생성하면 트레일이 모든 AWS 지역에 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 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 Health API 작업은 API 참조에 의해 CloudTrail 기록되며 [AWS Health API 참조에](#) 문서화됩니다. 예를 들어, DescribeEventsDescribeEventDetails, 및 DescribeAffectedEntities 작업에 대한 호출은 CloudTrail 로그 파일에 항목을 생성합니다.

AWS Health 는 다음 작업을 CloudTrail 로그 파일에 이벤트로 기록할 수 있습니다.

- 요청을 루트로 했는지 IAM 보안 인증 정보로 했는지 여부
- 역할 또는 페더레이션 사용자에게 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 다른 AWS 서비스에서 요청했는지 여부

자세한 내용은 [CloudTrail 사용자 ID 요소를 참조하십시오.](#)

원하는 만큼 오래 Amazon S3 버킷에 로그 파일을 저장할 수 있습니다. 또한 Amazon S3 수명 주기 규칙을 정의하여 로그 파일을 자동으로 보관하거나 삭제할 수도 있습니다. 기본적으로 로그 파일은 Amazon S3 서버 측 암호화(SSE)를 사용하여 암호화합니다.

로그 파일 전송 시 알림을 받으려면 새 로그 파일이 전송될 때 Amazon SNS 알림을 CloudTrail 게시하도록 구성할 수 있습니다. 자세한 내용은 [Amazon SNS 알림 구성을 참조하십시오 CloudTrail.](#)

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

자세한 내용은 [여러 지역에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 수신](#)을 참조하십시오.

## 예: AWS Health 로그 파일 항목

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 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.

다음 예제는 [DescribeEntityAggregates](#) 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/JaneDoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JaneDoe",
        "sessionContext": {"attributes": {
          "mfaAuthenticated": "false",
          "creationDate": "2016-11-21T07:06:15Z"
        }},
        "invokedBy": "AWS Internal"
      },
      "eventTime": "2016-11-21T07:06:28Z",
      "eventSource": "health.amazonaws.com",
      "eventName": "DescribeEntityAggregates",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "AWS Internal",
      "requestParameters": {"eventArns": ["arn:aws:health:us-east-1::event/EBS/EBS_LOST_VOLUME/EBS_LOST_VOLUME_123"]},
      "responseElements": null,
      "requestID": "05b299bc-afb9-11e6-8ef4-c34387f40bd4",
      "eventID": "e4deb9dc-dbc2-4bdb-8515-73e8abcbcb29b",
    }
  ]
}
```

```
"eventType": "AwsApiCall",  
"recipientAccountId": "123456789012"  
}  
],  
...  
}
```

# 에 대한 문서 기록 AWS Health

다음 표에서는 이번 릴리스의 AWS Health 설명서를 설명합니다.

- API 버전: 2016-08-04

다음 표에서는 2020년 8월 28일부터 시작되는 AWS Health 설명서의 중요 업데이트에 대해 설명합니다. 이제 RSS 피드를 구독하여 업데이트에 관한 알림을 받을 수 있습니다.

변경 사항	설명	날짜
<a href="#">보안 섹션 AWS Health 설명서에서 인터넷워크 트래픽 개인 정보 보호를 제거했습니다.</a>	자세한 내용은 <a href="#">보안을</a> 참조하십시오. AWS Health	2024년 3월 27일
<a href="#">AWS Health 설명서를 위해 AWS Health 대시보드 — 서비스 상태 및 계획된 라이프사이클 이벤트가 업데이트되었습니다.</a>	자세한 내용은 <a href="#">AWS Health 대시보드 — 서비스 상태 및 계획된 라이프사이클 이벤트를 참조하십시오 AWS Health.</a>	2024년 2월 15일
<a href="#">규칙 만들기에서 중복된 bullet 포인트를 제거했습니다. EventBridge AWS Health</a>	<a href="#">EventBridge 규칙 만들기에서 중복된 bullet point를 제거했습니다.</a> AWS Health	2023년 12월 4일
<a href="#">계획된 수명 주기 이벤트에 대한 문서 추가</a>	자세한 내용은 <a href="#">Planned Lifecycle Events for AWS Health</a> 항목을 참조하십시오.	2023년 10월 31일
<a href="#">AWSHealthFullAccess 에 대한 설명서 업데이트</a>	이제 AWS GovCloud (US) Regions에서 AWSHealth FullAccess 관리형 정책을 사용할 수 있습니다. <a href="#">에 대한 AWS 관리형 정책을</a> 참조하십시오 AWS Health.	2023년 10월 16일



<a href="#">에 AWS 사용자 알림 구성에 대한 설명서가 추가되었습니다 AWS Health.</a>	이제 에서 AWS 사용자 알림을 구성할 수 AWS Health있습니다. 자세한 내용은 <a href="#">AWS 사용자 알림 구성을 참조하십시오 AWS Health.</a>	2023년 8월 30일
<a href="#">위임된 관리자 기능에 대한 설명서가 이벤트 집계 섹션에 AWS Health 추가되었습니다.</a>	자세한 내용은 <a href="#">위임된 관리자 조직 보기</a> 를 참조하십시오.	2023년 7월 27일
<a href="#">SLR 정책 업데이트</a>	AWS 관리형 정책 업데이트: Health_. OrganizationsServiceRolePolicy 자세한 내용은 <a href="#">AWS Health에 대한AWS 관리형 정책</a> 을 참조하십시오.	2023년 7월 19일
<a href="#">AWS Health 이제 스키마가 이벤트 메타데이터를 지원합니다.</a>	이제 이벤트에서 이벤트 메타데이터를 받을 수 있습니다. AWS Health 자세한 내용은 <a href="#">Amazon을 통한 AWS Health 이벤트 모니터링</a> 을 참조하십시오 EventBridge.	2023년 6월 20일
<a href="#">Amazon용 설명서 업데이트 EventBridge</a>	이제 Amazon EventBridge 규칙을 사용하여 계정별 이벤트와 공개 이벤트를 모두 모니터링할 수 있습니다. 자세한 내용은 <a href="#">Amazon을 통한 AWS Health 이벤트 모니터링</a> 을 참조하십시오 EventBridge.	2023년 5월 2일
<a href="#">AWS 관리형 정책에 대한 설명서가 추가되었습니다.</a>	<a href="#">AWS HealthAWS 관리형 정책 및 AWS Health서비스 연결 역할 사용</a> 설명서가 추가되었습니다.	2023년 1월 18일

### [시간대 설정 설명서가 추가되었습니다.](#)

새 시간대 기능을 사용하여 현지 시간대 또는 UTC로 AWS Health 대시보드를 볼 수 있습니다. 자세한 내용은 대시보드 [시작하기 — 계정 상태 및 AWS HealthAWS Health 대시보드 — 서비스 상태를](#) 참조하십시오.

2022년 9월 21일

### [업데이트된 설명서](#)

AWS Health Aware에 대한 설명서가 추가되었습니다. 자세한 내용은 [AWS Health 인식](#)을 참조하십시오.

2022년 5월 25일

### [업데이트된 설명서](#)

Service Health Dashboard와 AWS Personal Health Dashboard가 대시보드로 리브랜딩되었습니다. AWS Health

2022년 2월 28일

자세한 내용은 대시보드 [시작하기 — 계정 상태 및 AWS Health 대시보드 — 서비스 상태를](#) 참조하십시오. AWS Health

### [Amazon용 설명서 업데이트 EventBridge](#)

AWS Health Amazon을 사용하여 Health 이벤트를 EventBridge 모니터링하기 위한 새 주제입니다. 자세한 내용은 [Amazon을 통한 AWS Health 이벤트 모니터링을](#) 참조하십시오 EventBridge.

2022년 2월 3일

### [업데이트된 설명서](#)

[엔터프라이즈 온램프 지원](#) 폴란이 있는 경우 API를 사용할 수 있습니다. AWS Health

2021년 11월 24일

<a href="#">추가된 설명서</a>	개념에 대한 새 주제. AWS Health 자세한 내용은 <a href="#">AWS Health개념</a> 을 참조하십시오.	2021년 7월 29일
<a href="#">CloudWatch 이벤트 설명서가 업데이트되었습니다.</a>	여러 서비스 및 이벤트 유형 범주에 대한 규칙을 생성하는 방법에 대한 섹션이 추가되었습니다. 자세한 내용은 <a href="#">여러 서비스 및 카테고리에 대한 규칙 만들기</a> 항목을 참조하십시오.	2021년 5월 7일
<a href="#">CloudWatch 이벤트 설명서 업데이트</a>	Amazon CloudWatch Events 규칙에 대한 AWS Systems Manager 작업을 자동화하도록 섹션을 업데이트했습니다. 자세한 내용은 <a href="#">Amazon EC2 인스턴스에 대한 작업 자동화</a> 를 참조하십시오.	2021년 4월 28일
<a href="#">CloudWatch 이벤트 설명서가 업데이트되었습니다.</a>	채팅 AWS Health 클라이언트에서 이벤트를 수신하는 섹션을 추가했습니다. 자세한 내용은 <a href="#">AWS Health 이벤트 수신</a> 을 참조하십시오 AWS Chatbot.	2021년 3월 16일
<a href="#">업데이트된 설명서</a>	<p>다음 주제가 업데이트되었습니다.</p> <ul style="list-style-type: none"> <li>• <a href="#">AWS Health 이벤트 집계</a> 주제가 업데이트되었습니다.</li> <li>• <a href="#">Amazon CloudWatch Events 주제를 통한 AWS Health 이벤트 모니터</a> 재구성 및 업데이트</li> <li>• <a href="#">리소스 및 작업 기반 조건</a> 섹션이 업데이트되었습니다.</li> </ul>	2021년 1월 29일

### [콘솔에 조직 보기를 위한 AWS Health 대시보드가 추가되었습니다. AWS Health](#)

AWS Health 콘솔을 사용하여 조직 보기 기능을 활성화할 수 있습니다. 그러면 AWS 조직의 멤버 계정에 대한 상태 이벤트를 볼 수 있습니다.

2020년 12월 14일

### [고가용성 엔드포인트 데모](#)

예제 코드를 사용하여 활성 지역 엔드포인트와 서명 AWS 지역을 결정할 수 AWS Health 있습니다.

2020년 10월 22일

### [AWS Health 사용 설명서 업데이트](#)

AWS Health 문서에 대한 최신 업데이트를 구독할 수 있도록 조직 업데이트 및 RSS 피드를 추가했습니다.

2020년 8월 28일

## 이전 업데이트

변경 사항	설명	날짜
예제를 포함하도록 조직 보기 항목이 업데이트되었습니다.	<a href="#">조직 보기를 사용하여 계정 간 AWS Health 이벤트 집계</a> 섹션을 참조하십시오.	2020년 6월 3일
보안 및 AWS Health	AWS Health 사용 시 보안 고려 사항에 대한 정보를 추가했습니다. <a href="#">보안 입력 AWS Health</a> 섹션을 참조하십시오.	2020년 5월 5일
AWS Organizations의 모든 계정에서 집계된 이벤트의 조직 보기를 사용하는 방법을 설명하는 새 단원이 추가되었습니다.	<a href="#">조직 보기를 사용하여 계정 간 AWS Health 이벤트 집계</a> 섹션을 참조하십시오.	2019년 12월 18일

변경 사항	설명	날짜
API에서 제공하는 이벤트 제한을 설명하는 “리소스 및 작업 기반 조건” 섹션이 AWS Health 새로 추가되었습니다.	<a href="#">AWS Health의 Identity and Access Management(IAM)</a> 섹션을 참조하십시오.	2018년 8월 2일
정보 가시성에 AWS Health 대한 메모를 추가했습니다.	<a href="#">AWS Health의 Identity and Access Management(IAM)</a> 섹션을 참조하십시오.	2017년 8월 16일
서비스 릴리스.	AWS Health 출시.	2016년 1월 12일

# AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 [AWS 용어집](#)을 참조하세요.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.