



관리자 안내서

AWS Supply Chain



AWS Supply Chain: 관리자 안내서

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

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

Table of Contents

AWS Supply Chain란 무엇인가요?	1
지원되는 브라우저	1
지원되는 언어	1
.....	1
AWS 계정 설정	3
에 가입 AWS 계정	3
관리자 액세스 권한이 있는 사용자 생성	3
사용해야 할 사전 조건 AWS Supply Chain	5
시작하기 AWS Supply Chain	6
1단계: IAM Identity Center 사용자 프로필 할당	6
2단계: 인스턴스 만들기	7
표준 구성 사용	8
고급 구성 사용	10
3단계: AWS Supply Chain 애플리케이션 소유자 선택	16
AWS Supply Chain 웹 애플리케이션에 로그인	18
사용 AWS Supply Chain	19
AWS Supply Chain 콘솔 사용	19
프로필 업데이트	23
계정 프로필 업데이트	23
조직 프로필 업데이트	24
사용자 권한 역할 관리	24
사용자 추가	25
사용자 권한 업데이트	25
사용자 삭제	26
사용자 지정 사용자 권한 역할 생성	26
인스턴스 삭제	27
보안	29
데이터 보호	30
AWS Supply Chain에서 처리된 데이터	31
옵트아웃 기본 설정	31
저장 시 암호화	31
전송 중 암호화	31
키 관리	32
인터넷워크 트래픽 개인 정보 보호	32

에서 권한 부여를 AWS Supply Chain 사용하는 방법 AWS KMS	32
AWS PrivateLink	36
고려 사항	36
인터페이스 엔드포인트 생성	36
엔드포인트 정책을 생성	37
IAM	38
대상	38
ID를 통한 인증	39
정책을 사용하여 액세스 관리	42
가 IAM에서 AWS Supply Chain 작동하는 방식	44
자격 증명 기반 정책 예시	49
문제 해결	50
AWS 관리형 정책	52
AWSSupplyChainFederationAdminAccess	53
정책 업데이트	54
규정 준수 확인	55
복원성	56
AWS 공급망 로깅 및 모니터링	56
AWS Supply Chain CloudTrail의 데이터 이벤트	57
AWS Supply Chain CloudTrail의 관리 이벤트	58
웹 애플리케이션 API	58
를 사용하여 이벤트 관리 EventBridge	64
AWS Supply Chain 이벤트	65
AWS Supply Chain 이벤트 전송	66
이벤트 세부 정보 참조	67
할당량	69
FAQ	71
관리 지원	73
문서 기록	74
.....	lxxvii

AWS Supply Chain란 무엇인가요?

AWS Supply Chain 는 데이터를 통합하고 수요 예측 및 인벤토리 가시성을 개선하기 위한 ML 기반 예측 방법을 제공하는 클라우드 기반 공급망 관리 애플리케이션으로, 실행 가능한 인사이트, 기본 제공 컨텍스트 공동 작업, 수요 계획, 공급 계획, n-계층 공급업체 가시성, 및 지속 가능성 정보 관리.는 기존 엔터프라이즈 리소스 계획(ERP) 및 공급망 관리 시스템에 연결할 AWS Supply Chain 수 있으며 ML 및 생성형 AI를 사용하여 서로 다른 데이터를 변환하고 공급망 데이터 레이크(SCDL)에 통합할 수 있습니다. AWS Supply Chain은 리플랫폼, 선결제 라이선스 요금 또는 장기 약정 없이 공급망 위험 관리를 개선할 수 있습니다.

주제

- [에서 지원하는 브라우저 AWS Supply Chain](#)
- [에서 지원하는 언어 AWS Supply Chain](#)

에서 지원하는 브라우저 AWS Supply Chain

AWS Supply Chain으로 작업하기 전에 다음 표를 사용하여 브라우저가 지원되는지 확인합니다.

브라우저	지원되는 버전
Google Chrome	최신 3개 버전
Mozilla Firefox ESR	버전은 Firefox 수명 종료일 까지 지원됩니다. 자세한 내용은 Firefox ESR release calendar 를 참조하세요.
Mozilla Firefox	최신 3개 버전
Microsoft Edge 및 Edge Chromium	버전 84 이상
Safari	macOS의 Safari 10 이상

에서 지원하는 언어 AWS Supply Chain

AWS Supply Chain 는 다음 언어를 지원합니다.

- 영어(미국)
- 영어(영국)
- 독일어
- 스페인어
- 프랑스어
- 이탈리아어
- 포르투갈어
- 중국어 간체
- 중국어 번체
- 일본어
- 한국어

AWS 계정 설정

이 섹션을 사용하여 AWS 계정을 생성하고 IAM 사용자를 생성합니다. AWS 계정 생성 모범 사례에 대한 자세한 내용은 [모범 사례 AWS 환경 설정을 참조하세요](#).

주제

- [에 가입 AWS 계정](#)
- [관리자 액세스 권한이 있는 사용자 생성](#)

에 가입 AWS 계정

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. <https://portal.aws.amazon.com/billing/signup>을 엽니다.
2. 온라인 지시 사항을 따릅니다.

가입 절차의 일부로는 전화 또는 문자 메시지를 수신하고 전화 키패드에 확인 코드를 입력하는 것이 포함됩니다.

에 가입하면 AWS 계정AWS 계정 루트 사용자인 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 [루트 사용자 액세스 권한이 필요한 작업](#)을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 <https://aws.amazon.com/>으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자 [AWS Management Console](#)로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

루트 사용자를 사용하여 로그인하는 데 도움이 필요하다면 AWS 로그인 User Guide의 [루트 사용자 로 로그인](#)을 참조하세요.

2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

지침은 IAM 사용 설명서의 [AWS 계정 루트 사용자\(콘솔\)에 대한 가상 MFA 디바이스 활성화](#)를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

지침은 AWS IAM Identity Center 사용 설명서의 [AWS IAM Identity Center 설정](#)을 참조하세요.

2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

를 자격 증명 소스 IAM Identity Center 디렉터리로 사용하는 방법에 대한 자습서는 [사용 AWS IAM Identity Center 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조](#)하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하다면 AWS 로그인 사용 설명서의 [AWS 액세스 포털에 로그인](#)을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

지침은 AWS IAM Identity Center 사용 설명서의 [Create a permission set](#)를 참조하세요.

2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

지침은 AWS IAM Identity Center 사용 설명서의 [Add groups](#)를 참조하세요.

사용해야 할 사전 조건 AWS Supply Chain

AWS Supply Chain 인스턴스를 생성하기 전에 다음 단계를 완료해야 합니다.

- 가 있습니다 AWS 계정. 를 생성하려면 섹션을 AWS 계정참조하세요 [AWS 계정 설정](#).
- IAM Identity Center가 활성화되어 있는지 확인합니다. IAM Identity Center를 활성화하려면 [IAM Identity Center 활성화](#)를 참조하세요.
- 필요한 관리 권한이 있습니다. 권한에 대한 자세한 내용은 고급 구성을 참조하세요.
- IAM Identity Center 인스턴스는 인스턴스를 생성하려는 동일한 리전에서 활성화해야 합니다. AWS Supply Chain AWS Supply Chain 는 미국 동부(버지니아 북부), 미국 서부(오레곤), 유럽(프랑크푸르트), 아시아 태평양(시드니) 및 유럽(아일랜드) 리전에서만 지원됩니다.

AWS Supply Chain 인스턴스가 IAM Identity Center 리전과 동일한 리전에 있지 않은 경우 추가 [지원을 위해 문의하세요](#).

- IAM Identity Center 인스턴스에 AWS Supply Chain 관리자로 할당할 사용자가 하나 이상 있어야 합니다. 활성 디렉토리를 IAM Identity Center에 연결할 수 있습니다. 자세한 내용은 [Microsoft AD 디렉토리에 연결을 참조하세요](#).
- IAM Identity Center AWS Supply Chain 에 대한 액세스 권한이 필요한 사용자를 추가합니다.
- 인스턴스를 생성하려면 AWS Key Management Service (AWS KMS)가 필요합니다. 이를 AWS Supply Chain 사용하여 들어오는 모든 데이터를 AWS KMS key 암호화합니다 AWS Supply Chain. AWS KMS 키에 대한 자세한 내용은 [키 생성을 참조하세요](#).

시작하기 AWS Supply Chain

이 섹션에서는 AWS Supply Chain 인스턴스를 생성하고, 사용자 권한 역할을 부여하고, AWS Supply Chain 웹 애플리케이션에 로그인하고, 사용자 지정 사용자 권한 역할을 생성하는 방법을 배울 수 있습니다. 는 AWS 계정 최대 10개의 AWS Supply Chain 인스턴스가 활성 상태이거나 초기화 상태일 수 있습니다.

주제

- [1단계: IAM Identity Center 사용자 프로필 할당](#)
- [2단계: 인스턴스 만들기](#)
- [3단계: AWS Supply Chain 애플리케이션 소유자 선택](#)
- [AWS Supply Chain 웹 애플리케이션에 로그인](#)

1단계: IAM Identity Center 사용자 프로필 할당

인스턴스를 생성하고 AWS Supply Chain 서비스를 사용하려면 기존 IAM Identity Center 사용자 프로필을 연결하거나 새 프로파일을 생성해야 합니다.

1. [AWS Supply Chain 콘솔](#)을 엽니다. 기본에서 "AWS Supply Chain"를 검색할 수도 있습니다 AWS Management Console.
2. 필요한 경우 콘솔 상단에 있는 AWS 리전 선택을 선택하여 리전을 변경합니다. 드롭다운 목록에서 리전을 선택합니다.
3. AWS Supply Chain 인스턴스 생성을 선택합니다. 알림이 나타납니다.

Continue with email



We'll check if you have an existing user and help create one if you don't.

AWS Supply Chain

Email address

Continue

4. 이메일 주소를 입력하고 계속을 선택합니다. IdC는 이메일이 기존 사용자와 일치하는지 확인합니다.
5. 다음 중 하나를 수행합니다.
 - IdC가 이메일 주소와 일치하는 경우 - ID 소스 연결을 선택하고 팀을 온보딩합니다.

 Note

조직에 사용하려는 설정된 IdC 인스턴스가 있는 경우 사용할 수 있습니다 AWS Supply Chain.

- IdC가 기존 사용자와 일치하는 항목을 찾지 못하면 새 사용자 생성 알림이 나타납니다. 다음 단계를 진행합니다.
6. 알림에서 다음을 입력한 후 계속을 선택합니다.
 - 이메일 주소
 - 이름
 - 성

IdC는 사용자를 자동으로 생성하고 AWS Supply Chain 관리자로 추가합니다.

7. 다음 중 하나를 수행합니다.
 - 표준 구성을 사용하여 인스턴스를 생성하려면 생성을 선택합니다. [the section called “표준 구성 사용”](#)을(를) 참조하세요.
 - 사용자 지정 구성을 사용하여 인스턴스를 생성하려면 - 고급 설정에서 편집을 선택합니다. [the section called “고급 구성 사용”](#)을(를) 참조하세요.

2단계: 인스턴스 만들기

에서 인스턴스를 생성하면 공급망 관리 및 분석을 위한 전용 환경이 AWS Supply Chain 설정됩니다. 인스턴스를 설정하려면 기본 세부 정보를 구성하고, 설정을 설정하고, 초기 사용자 액세스 권한을 정의합니다.

 Note

AWS Management Console 관리자만 인스턴스를 생성할 수 있습니다. AWS Supply Chain 인스턴스를 생성하는 AWS Management Console 관리자에는 나열된 모든 권한을 가지고 있어

야 합니다 [사용 AWS Supply Chain](#). 이 관리자는 IAM 사용자를 AWS Supply Chain 관리자로 초대하여를 관리해야 합니다 AWS Supply Chain.

표준 구성 또는 고급 구성의 두 가지 방법 중 하나를 사용하여 인스턴스를 생성합니다. 표준 구성은 사전 설정 파라미터를 사용하여 인스턴스를 빠르게 생성하는 자동화된 프로세스를 사용합니다. 고급 구성을 사용하면 자체 파라미터를 설정하여 인스턴스를 사용자 지정할 수 있습니다.

주제

- [표준 구성 사용](#)
- [고급 구성 사용](#)

표준 구성 사용

표준 구성은 기본 보안 및 암호화 설정을 사용하여 AWS Supply Chain 인스턴스를 생성합니다. 인스턴스는 AWS 지리적 리전에서 작동합니다. 리전에 대한 자세한 내용은 IAM 사용 설명서의 [리전 및 엔드포인트](#)와의 [리전 엔드포인트](#)를 참조하세요 AWS 일반 참조.

사전 설정 파라미터의 표준 구성을 사용하여 AWS Supply Chain 인스턴스를 생성하려면 다음 단계를 따르세요.

1. 생성을 선택합니다.



Create your application

Create your AWS Supply Chain application. We have selected some defaults to get you started.

Create

Edit in advanced setup



Service access and encryption defaults

When you create an AWS Supply Chain application, you grant it [permissions](#) to access some AWS resources on your behalf. Your data at rest will be encrypted using an AWS owned key. To modify these defaults choose **Edit in advanced setup**.

확인 메시지가 나타납니다.



You're all set, please check your email

We sent an email to `user12@amazon.com`. Please check your email to verify your user account and begin using AWS Supply Chain.

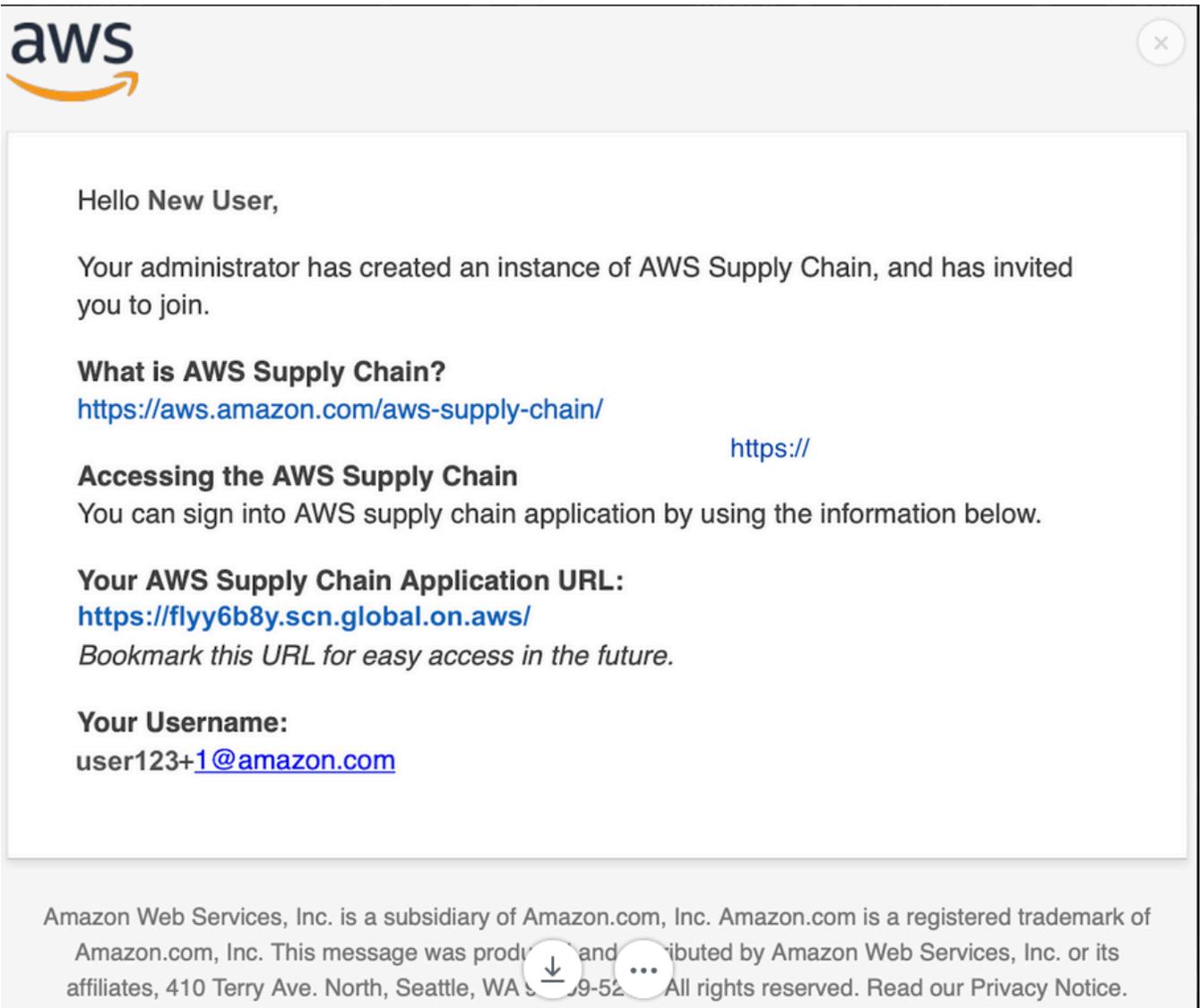
Your new user is stored in IAM Identity Center. Verify your user to active the user account.

Manage application

Sign in to AWS Supply Chain

2. 이메일에서 다음을 확인합니다.

- IdC 팀의 이메일입니다.
- 자격 증명 관리 팀의 이메일입니다.



3. 초대 이메일을 받으면에 로그인합니다 AWS Supply Chain. [the section called “AWS Supply Chain 웹 애플리케이션에 로그인” 단원을 참조하십시오.](#)

고급 구성 사용

고급 구성을 사용하면 자체 파라미터를 설정하여 인스턴스를 사용자 지정할 수 있습니다. 사전 설정 파라미터의 고급 구성을 사용하여 AWS Supply Chain 인스턴스를 생성하려면 다음 단계를 따릅니다.

1. 고급 설정에서 편집을 선택합니다.



Create your application

Create your AWS Supply Chain application. We have selected some defaults to get you started.

Create

Edit in advanced setup



Service access and encryption defaults

When you create an AWS Supply Chain application, you grant it [permissions](#) to access some AWS resources on your behalf. Your data at rest will be encrypted using an AWS owned key. To modify these defaults choose **Edit in advanced setup**.

인스턴스 속성 페이지가 나타납니다.

The screenshot shows the 'Specify instance details' page in the AWS console. It includes the following sections:

- Instance properties**: Includes 'AWS Region' (Europe (Ireland) eu-west-1), a text input for 'Enter an instance name' (1 to 62 characters), and a text area for 'Enter a description - optional' (256 characters max).
- AWS KMS Key - Optional**: Includes a search box for 'Choose an AWS KMS key or enter an ARN' and a 'Create' button.
- Instance tags - optional**: A section for adding tags to the instance.

2. 인스턴스 속성 페이지에 다음을 입력합니다.

- 이름 - 인스턴스 이름을 입력합니다.
- 설명 - AWS Supply Chain 인스턴스에 대한 설명을 입력합니다(예: 프로덕션 인스턴스, 테스트 인스턴스 등).
- AWS KMS 키(선택 사항) - 기본 AWS KMS 키(권장)를 사용하거나 자체 AWS KMS 키를 제공하도록 선택할 수 있습니다. 자세한 정보는 [the section called “사용자 지정 AWS KMS 키 사용”](#)을 참조하세요.
- 인스턴스 태그 - 식별에 사용할 수 있는 태그를 인스턴스에 추가할 수 있습니다. 예를 들어 태그를 추가하여 생성 중인 인스턴스 유형(예: 프로덕션, 테스트, UAT 등)을 정의할 수 있습니다.

Note

S/4 Hana 데이터 연결을 사용하려는 경우 제공한 AWS KMS 키에 연결된 값이 `aws-supply-chain-access` 태그가 있는지 확인합니다 `true`.

3. 인스턴스 생성을 선택합니다.

4. (선택 사항) AWS Supply Chain 인스턴스가 생성되고 AWS KMS 키에서 자체 AWS KMS 키를 사용하도록 선택한 경우가 AWS KMS 키에 AWS Supply Chain 액세스할 수 있도록 KMS 정책을 업데이트합니다.

 Note

YourAccountNumber 및 *YourInstanceID*를 AWS 계정 및 인스턴스 ID로 바꿉니다. AWS Supply Chain 인스턴스입니다.

```
{
  "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-
role-YourInstanceID"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

사용자 지정 AWS KMS 키 사용

인스턴스를 생성할 때 자체 AWS KMS 키를 사용할 수 있습니다. 자체 키를 관리하지만 기존 키를 사용하지 않으려면 새 키를 생성할 수 있습니다.

 Note

AWS 소유 키를 사용하는 것이 AWS Supply Chain 인스턴스에 권장되는 기본 설정입니다.

기존 AWS KMS 키 사용

1. 암호화 설정 사용자 지정을 선택합니다.
2. AWS KMS 키 선택으로 이동합니다.
3. 제공된 필드에 키를 입력합니다.
4. 업데이트를 선택합니다.

AWS KMS 키 생성

1. 생성을 선택합니다.
2. [KMS 키 생성](#)의 단계를 따릅니다.
3. 다음 권한으로 새 키를 업데이트합니다.
 - 키 관리 권한 정의: 선택하지 않은 상태로 둡니다.
 - 키 사용 권한 정의: 선택하지 않은 상태로 둡니다.
 - 키 정책 업데이트: 키 정책을 편집하고를 다음으로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::YourAccountNumber:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow access through SecretManager for all principals in the
account that are authorized to use SecretManager",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
```

```

        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "secretsmanager.Region.amazonaws.com",
            "kms:CallerAccount": "YourAccountNumber"
        }
    }
},
{
    "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
    "Effect": "Allow",
    "Principal": {
        "Service": "scn.Region.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:RetireGrant"
    ],
    "Resource": "*"
}
]
}

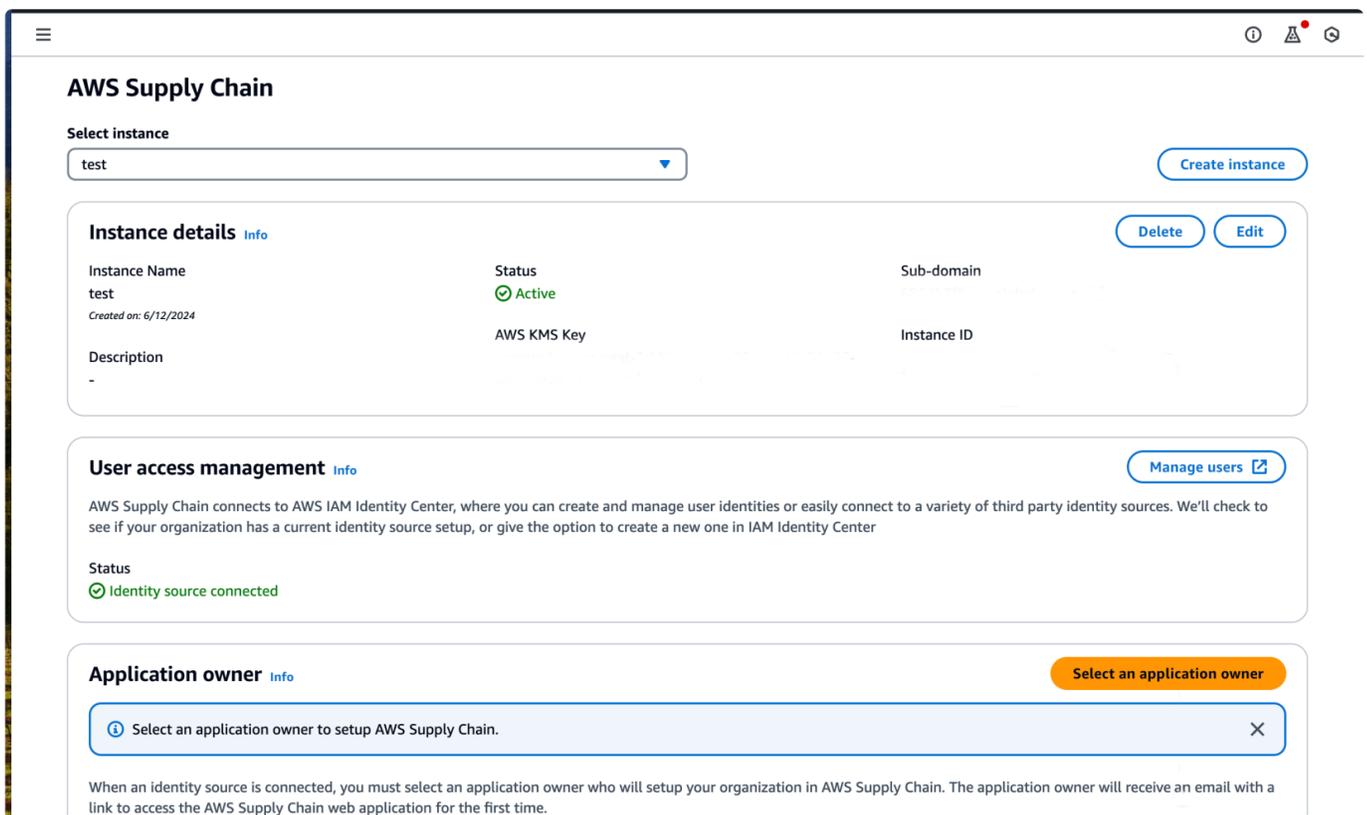
```

3단계: AWS Supply Chain 애플리케이션 소유자 선택

AWS 콘솔 관리자는 AWS Supply Chain 웹 애플리케이션 액세스를 관리할 애플리케이션 소유자를 선택합니다. AWS Supply Chain . AWS Supply Chain 애플리케이션 소유자는 AWS Supply Chain 웹 애플리케이션에 대한 사용자 권한 역할을 추가하거나 제거할 수 있습니다.

인스턴스를 생성하고 자격 증명 소스를 연결한 후 다음 단계에 따라 AWS Supply Chain 애플리케이션 소유자를 선택합니다.

1. AWS Supply Chain 콘솔 대시보드를 엽니다.
2. 애플리케이션 소유자 선택으로 이동하여 AWS Supply Chain 애플리케이션 소유자가 될 사용자를 선택합니다. 검색 결과에는 검색 기준과 일치하는 사용자만 표시됩니다.

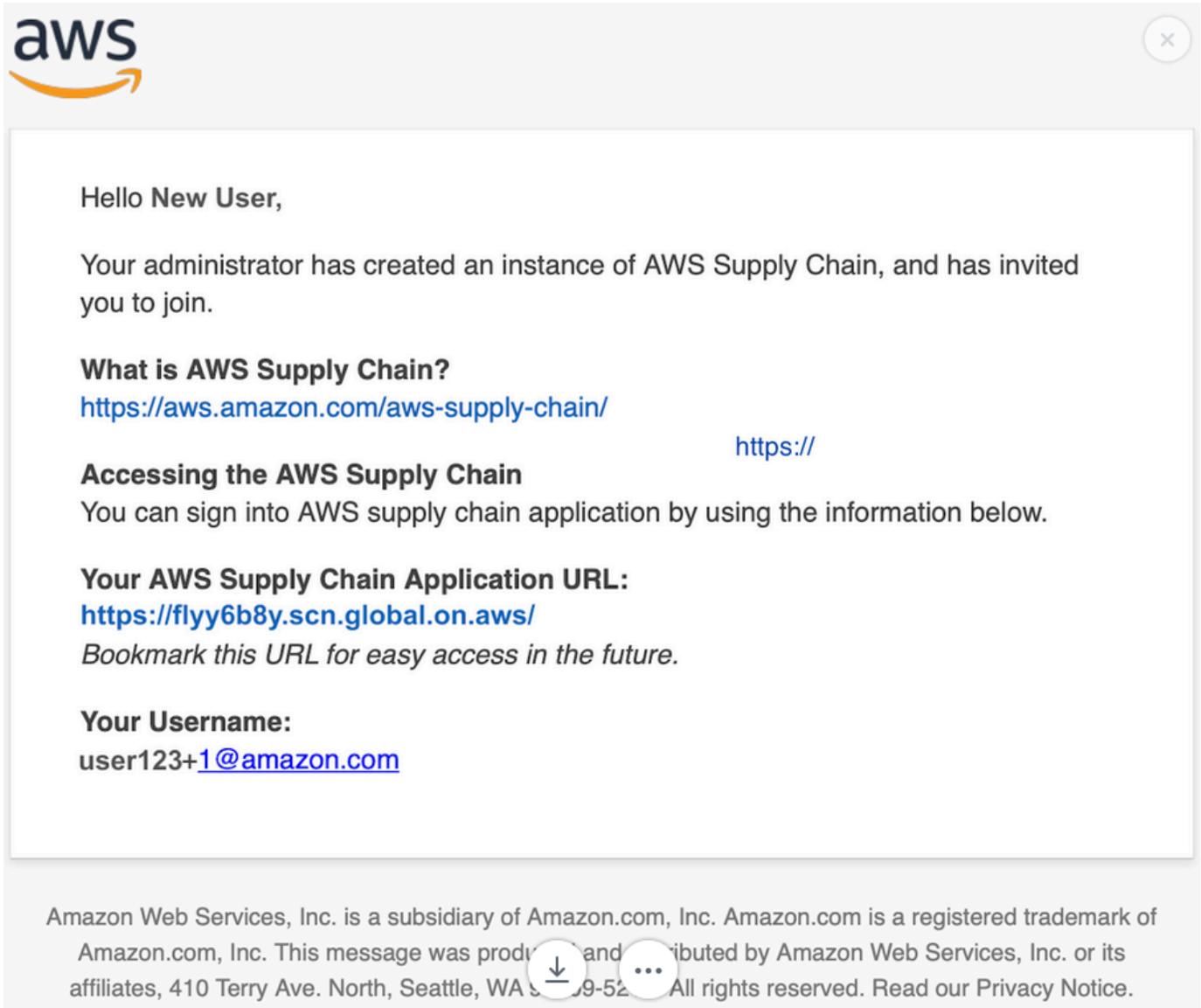


3. (선택 사항) IAM Identity Center로 이동을 선택하여 사용자를 더 추가합니다. 사용자 추가에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 ID [소스 관리를 참조하고 사용자 권한 역할에 대한 자세한 내용은 사용자 권한 역할을 참조하세요](https://docs.aws.amazon.com/aws-supply-chain/latest/adminguide/adding-users-groups.html). <https://docs.aws.amazon.com/aws-supply-chain/latest/adminguide/adding-users-groups.html>

Note

AWS Supply Chain 콘솔에서는 한 번에 한 명의 사용자만 추가할 수 있습니다. AWS Supply Chain에서는 그룹을 애플리케이션 소유자로 추가할 수 없습니다.

- 초대 전송을 선택합니다. 웹 애플리케이션 관리자에게 이메일이 전송됩니다. 웹 애플리케이션 관리자가 초대 이메일을 받으면 애플리케이션 URL을 선택하고에 로그인할 수 있습니다 AWS Supply Chain.



AWS Supply Chain 콘솔 대시보드에서 애플리케이션 소유자 아래에 나열된 사용자가 표시됩니다.

AWS Supply Chain에서 관리를 선택하여 AWS Supply Chain 웹 애플리케이션에서 사용자를 추가 및 제거합니다.

AWS Supply Chain 웹 애플리케이션에 로그인

AWS Supply Chain 관리자는 AWS Supply Chain 웹 애플리케이션에 대한 이메일 초대를 받아야 합니다.

1. 이메일에 있는 링크를 선택하거나 AWS Supply Chain 콘솔 대시보드의 하위 도메인에서 웹 URL을 선택할 수 있습니다.

AWS Supply Chain 웹 애플리케이션 로그인 페이지가 나타납니다.

2. AWS IAM Identity Center 사용자 자격 증명을 입력하고 로그인을 선택합니다.

Note

처음 로그인할 때만 계정 및 조직에 대한 프로필을 작성하라는 메시지가 표시됩니다.

3. 프로필 작성 페이지에서 직책 및 시간대를 입력합니다. 다음을 선택합니다.
4. 조직 정보 추가 페이지에서 조직 이름을 입력하고 본사 위치를 선택합니다. 필요에 따라 회사 로고를 추가할 수 있습니다. 다음을 선택합니다.
5. AWS Supply Chain의 팀원 설정 페이지에서 AWS Supply Chain 웹 애플리케이션에 액세스할 수 있게 할 사용자를 선택합니다. [Invite Users]를 선택합니다. AWS Supply Chain 사용자 권한 역할에 대한 자세한 내용은 섹션을 참조하세요 [사용자 권한 역할 관리](#).
6. 나중에 사용자를 추가하려는 경우 지금은 건너뛰기를 선택할 수 있습니다.

온보딩 완료 페이지가 나타납니다.

7. 추가한 각 사용자는 링크가 포함된 이메일 메시지를 수신하거나 링크 복사를 선택하여 사용자에게 링크를 보낼 AWS Supply Chain 수 있습니다.
8. AWS Supply Chain 대시보드를 보려면 홈페이지로 이동을 선택합니다.

사용 AWS Supply Chain

AWS Supply Chain 는 공급망 네트워크에 대한 가시성을 확보하고, 정보에 입각한 결정을 신속하게 내리고, 공급망 복원력을 개선하는 데 도움이 되는 클라우드 기반 애플리케이션입니다. AWS Supply Chain를 사용하면 서로 다른 데이터 소스를 연결하고, 기계 학습을 사용하여 인사이트를 생성하고, 내부 팀 및 외부 파트너와 협업할 수 있습니다. 이 섹션에서는 몇 가지 AWS Supply Chain 기본 함수를 안내합니다.

주제

- [AWS Supply Chain 콘솔 사용](#)
- [프로필 업데이트](#)
- [사용자 권한 역할 관리](#)
- [인스턴스 삭제](#)

AWS Supply Chain 콘솔 사용

콘솔을 사용하는 것이 서비스 리소스와 구성을 관리하는 가장 쉬운 방법입니다. 콘솔은 리소스를 보고, 생성하고, 수정하고, 모니터링할 수 있는 직관적인 웹 기반 인터페이스를 제공합니다. 이 섹션에서는 콘솔에 액세스하고 탐색하여 일반적인 관리 작업을 수행하는 방법을 보여줍니다.

Note

AWS 계정이 AWS 조직의 멤버 계정이고 서비스 제어 정책(SCP)이 포함된 경우 조직의 SCP가 멤버 계정에 다음 권한을 부여해야 합니다. 조직의 SCP 정책에 다음 권한이 포함되지 않으면 AWS Supply Chain 인스턴스 생성이 실패합니다.

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

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

콘솔 관리자가 AWS Supply Chain 인스턴스를 성공적으로 생성하고 업데이트하려면 다음 권한이 필요합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "scn:*",
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3>DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutBucketOwnershipControls",
        "s3:PutBucketNotification",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging"
      ],
      "Resource": "arn:aws:s3:::aws-supply-chain-*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "cloudtrail:CreateTrail",
        "cloudtrail:PutEventSelectors",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:StartLogging"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
```

```
"events:DescribeRule",
"events:PutRule",
"events:PutTargets"
],
"Resource": "*",
"Effect": "Allow"
},
{
  "Action": [
    "chime:CreateAppInstance",
    "chime>DeleteAppInstance",
    "chime:PutAppInstanceRetentionSettings",
    "chime:TagResource"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "cloudwatch:PutMetricData",
    "cloudwatch:Describe*",
    "cloudwatch:Get*",
    "cloudwatch:List*"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "organizations:CreateOrganization",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:EnableAWSServiceAccess",
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "kms:CreateGrant",
    "kms:RetireGrant",
    "kms:DescribeKey"
  ],
  ],
```

```
"Resource": key_arn,
"Effect": "Allow"
},
{
  "Action": [
    "kms:ListAliases"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "iam:CreateRole",
    "iam:CreatePolicy",
    "iam:GetRole",
    "iam:PutRolePolicy",
    "iam:AttachRolePolicy",
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "sso:AssociateDirectory",
    "sso:AssociateProfile",
    "sso:CreateApplication",
    "sso:CreateApplicationAssignment",
    "sso:CreateInstance",
    "sso:CreateManagedApplicationInstance",
    "sso>DeleteApplication",
    "sso>DeleteApplicationAssignment",
    "sso>DeleteManagedApplicationInstance",
    "sso:DescribeApplication",
    "sso:DescribeDirectories",
    "sso:DescribeInstance",
    "sso:DescribeRegisteredRegions",
    "sso:DescribeTrusts",
    "sso:DisassociateProfile",
    "sso:GetManagedApplicationInstance",
    "sso:GetPeregrineStatus",
    "sso:GetProfile",
    "sso:GetSharedSsoConfiguration",
    "sso:GetSsoConfiguration",
```

```

    "sso:GetSSOStatus",
    "sso:ListApplicationAssignments",
    "sso:ListApplicationTemplates",
    "sso:ListDirectoryAssociations",
    "sso:ListInstances",
    "sso:ListProfileAssociations",
    "sso:ListProfiles",
    "sso:PutApplicationAuthenticationMethod",
    "sso:PutApplicationGrant",
    "sso:RegisterRegion",
    "sso:SearchDirectoryGroups",
    "sso:SearchDirectoryUsers",
    "sso:SearchGroups",
    "sso:SearchUsers",
    "sso:StartPeregrine",
    "sso:StartSSO",
    "sso:UpdateSsoConfiguration",
    "sso-directory:SearchUsers"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
]
}

```

*key_arn*은 AWS Supply Chain 인스턴스에 사용할 키를 지정합니다. 모범 사례를 알아보고 사용하려는 키로만 액세스를 제한하려면 IAM 정책 설명에서 KMS 키 지정을 AWS Supply Chain 참조하세요. <https://docs.aws.amazon.com/kms/latest/developerguide/cmks-in-iam-policies.html> 모든 KMS 키를 나타내려면 와일드카드 문자만 사용합니다("*").

프로필 업데이트

AWS Supply Chain 웹 애플리케이션에서 언제든지 계정 및 조직 프로필을 업데이트할 수 있습니다.

계정 프로필 업데이트

계정 프로필을 업데이트하려면 다음 단계를 따르세요.

1. AWS Supply Chain 웹 애플리케이션 대시보드의 왼쪽 탐색 창에서 설정 아이콘을 선택합니다.
2. 계정 프로필을 선택합니다.

계정 프로필 페이지가 나타납니다.

3. 계정 정보를 업데이트하고 저장을 선택합니다.

조직 프로필 업데이트

조직 프로필을 업데이트하려면 다음 단계를 따르세요.

1. AWS Supply Chain 웹 애플리케이션 대시보드의 왼쪽 탐색 창에서 설정 아이콘을 선택합니다.
2. 조직을 선택한 다음, 조직 프로필을 선택합니다.

조직 프로필 페이지가 나타납니다.

3. 조직 로고 또는 본사 위치를 업데이트한 다음, 저장을 선택합니다.

사용자 권한 역할 관리

AWS Supply Chain 관리자는 기본 사용자 권한 역할을 사용하거나 사용자 지정 권한 역할을 생성할 수 있습니다. AWS Supply Chain에는 다음과 같은 기본 사용자 권한 역할이 있습니다.

- Administrator - 모든 데이터와 사용자 권한을 생성, 확인, 관리할 수 있는 액세스 권한입니다.
- Data Analyst - 모든 데이터 연결을 생성, 확인, 관리할 수 있는 액세스 권한입니다.
- Inventory Manager - 인사이트를 생성, 확인, 관리할 수 있는 액세스 권한입니다.
- Demand Planner - 수요 계획을 생성, 확인 및 관리할 수 있는 액세스 권한입니다.
- Partner Data Manager - 파트너를 관리 및 확인하고, 데이터 요청을 관리 및 확인하며, 지속 가능성 데이터를 확인할 수 있는 액세스 권한입니다.
- Supply Planner - 공급 계획을 관리하고 확인할 수 있는 액세스 권한입니다.

Note

AWS Supply Chain 관리자는 사용자를 추가하기 전에 다음 사항에 유의하세요.

- 각 기본 사용자 권한 역할은 권한 집합으로 정의됩니다. 기본 사용자 권한 역할에 사용자를 추가하거나 사용자 정의 권한 역할을 생성할 수 있습니다.
- 한 사용자에게 하나의 사용자 권한 역할만 할당할 수 있습니다.
- 기본 사용자 권한 역할은 편집하거나 삭제할 수 없습니다.

- 생성한 사용자 지정 권한 역할을 편집하면 해당 사용자 지정 권한 역할에 속한 모든 사용자의 권한이 업데이트됩니다.
- 생성한 사용자 지정 권한 역할을 삭제하면 사용자 지정 권한 역할의 모든 사용자가 액세스 권한을 잃게 됩니다 AWS Supply Chain.
- 에서는 그룹 추가가 지원되지 않습니다 AWS Supply Chain.

주제

- [사용자 추가](#)
- [사용자 권한 업데이트](#)
- [사용자 삭제](#)
- [사용자 지정 사용자 권한 역할 생성](#)

사용자 추가

AWS Supply Chain 관리자는 AWS Supply Chain 웹 애플리케이션에 액세스할 사용자를 추가할 수 있습니다. 먼저 사용자를 IAM Identity Center(IdC)에 추가한 다음에 추가할 수 있습니다 AWS Supply Chain. IdC에 사용자를 추가하는 방법에 대한 자세한 내용은 [사용자 액세스 할당](#)을 참조하세요.

사용자가 IdC에 추가되면 다음 단계에 따라 사용자를 추가합니다.

1. AWS Supply Chain 대시보드에서 설정 아이콘을 선택합니다.
2. 사용자 및 권한을 선택합니다.
3. 사용자, 사용자를 선택합니다. 사용자 관리 페이지가 나타납니다.
4. 새 사용자 추가를 선택합니다. 사용자 추가 페이지가 나타납니다.
5. 사용자 추가(Add user) 드롭다운 메뉴에서 사용자를 선택합니다.
6. 역할 선택 드롭다운 메뉴에서 사용자의 역할을 선택합니다.
7. 추가를 선택합니다.

사용자 권한 업데이트

현재 사용자의 사용자 권한 역할을 업데이트하려면 다음 단계를 AWS Supply Chain 따릅니다.

1. AWS Supply Chain 대시보드의 왼쪽 탐색 창에서 설정 아이콘을 선택합니다.

2. 권한을 선택한 다음, 사용자를 선택합니다.

사용자 관리 페이지가 나타납니다.

3. 사용자 관리 페이지에서 사용자 권한 역할을 업데이트할 사용자 또는 그룹을 선택하고 권한 역할 드롭다운 메뉴에서 권한 역할 중 하나를 선택합니다.

Note

할당한 역할 권한에 따라 AWS Supply Chain 대시보드가 사용자 지정됩니다. 자세한 내용은 [사용자 지정 사용자 권한 역할 생성](#) 단원을 참조하십시오.

4. 저장(Save)을 선택합니다.

사용자 삭제

AWS Supply Chain 관리자는 AWS Supply Chain 웹 애플리케이션에서 사용자를 삭제할 수 있습니다. 다음 단계에 따라 사용자를 삭제합니다.

1. AWS Supply Chain 대시보드의 왼쪽 탐색 창에서 설정 아이콘을 선택합니다.
2. 권한을 선택한 다음, 사용자를 선택합니다.

사용자 관리 페이지가 나타납니다.

3. 사용자 관리 페이지에서 삭제하려는 사용자를 선택하고 삭제 아이콘을 선택합니다.

사용자 지정 사용자 권한 역할 생성

기본 사용자 권한 역할 외에도 사용자 지정 사용자 권한 역할을 생성하여 여러 권한 역할을 포함하고 특정 위치 및 제품을 추가할 수 있습니다. 다음 단계에 따라 새 권한 역할을 생성합니다.

1. AWS Supply Chain 대시보드의 왼쪽 탐색 창에서 설정 아이콘을 선택합니다. 권한을 선택한 다음, 권한 역할을 선택합니다.

권한 역할 페이지가 나타납니다.

2. 새 역할 생성을 선택합니다.
3. 권한 역할 관리 페이지의 역할 이름 아래에 이름을 입력합니다.
4. 슬라이더를 움직여 사용자 권한 역할을 선택합니다.

- 관리 - 사용자에게 관리 권한을 할당하면 정보를 추가, 편집, 관리할 수 있습니다.
- 보기 - 사용자에게 보기 권한을 할당하면 현재 정보만 볼 수 있습니다.

5.

Note

인스턴스가 데이터 소스에 연결된 경우 위치 액세스 및 제품 액세스에서 제품 및 위치만 선택할 수 있습니다. 예를 들어 시애틀 위치에서 아보카도만 관리하기 위한 사용자 지정 관리자 사용자를 생성하거나 시애틀 위치에서 아보카도에 대한 인사이트만 관리하기 위한 인사이트 사용자를 생성할 수 있습니다.

위치 액세스에서 검색 창에 입력하는 대로 리전을 검색하고 리전을 선택합니다.

6. 제품 액세스에서 검색 창에 입력하는 대로 제품을 검색하고 제품을 선택합니다.
7. 저장(Save)을 선택합니다.

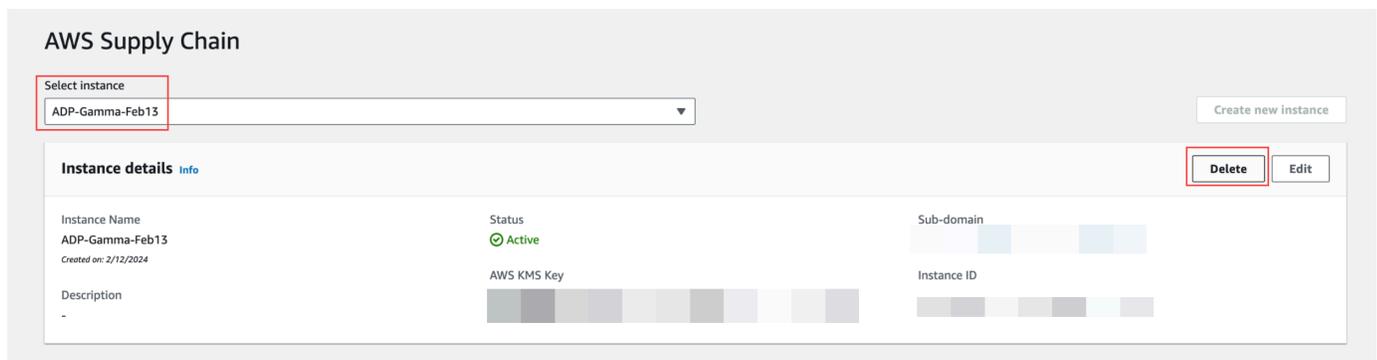
인스턴스 삭제

인스턴스를 삭제하려면 다음 단계를 따릅니다.

Note

인스턴스를 삭제할 때 Amazon S3 버킷의 정보는 자동으로 삭제되지 않습니다.

1. 에서 AWS Supply Chain 콘솔을 엽니다 <https://console.aws.amazon.com/scn/home>.
2. AWS Supply Chain 콘솔 대시보드의 드롭다운에서 삭제할 인스턴스를 선택합니다.



3. Delete(삭제)를 선택합니다.

4. AWS Supply Chain 인스턴스 삭제 페이지의 확인에 **delete**를 입력하여 인스턴스를 삭제할지 확인합니다.
5. Delete(삭제)를 선택합니다. 인스턴스 삭제가 시작되고 인스턴스가 삭제되면 확인 메시지가 표시됩니다.

 Note

인스턴스가 삭제되면의 Amazon Q와 관련된 정보가 AWS Supply Chain 자동으로 삭제됩니다.

의 보안 AWS Supply Chain

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

보안은 AWS와 사용자의 공동 책임입니다. [공동 책임 모델](#)에서는 이를 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS 서비스 에서 실행되는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 [AWS 규정 준수 프로그램](#)의 일환으로 보안 효과를 테스트하고 검증합니다. 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 [AWS 제공 범위 내 서비스규정 준수 프로그램](#) 제공 범위 내 서비스를 AWS Supply Chain참조하세요.
- 클라우드의 보안 - 사용하는 AWS 서비스 에 따라 책임이 결정됩니다. 또한 사용자는 데이터의 민감도, 요구 사항, 관련 법률 및 규정을 비롯한 다른 요인에 대해서도 책임이 있습니다.

이 설명서는 AWS Supply Chain사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표에 맞게 AWS Supply Chain 를 구성하는 방법을 보여줍니다. 또한 AWS Supply Chain 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스 되는 다른를 사용하는 방법도 알아봅니다.

주제

- [의 데이터 보호 AWS Supply Chain](#)
- [인터페이스 엔드포인트를 AWS Supply Chain 사용한 액세스\(AWS PrivateLink\)](#)
- [에 대한 IAM AWS Supply Chain](#)
- [AWS 에 대한 관리형 정책 AWS Supply Chain](#)
- [에 대한 규정 준수 검증 AWS Supply Chain](#)
- [의 복원력 AWS Supply Chain](#)
- [로깅 및 모니터링 AWS Supply Chain](#)
- [를 사용하여 AWS Supply Chain 이벤트 관리 Amazon EventBridge](#)

의 데이터 보호 AWS Supply Chain

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

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

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

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API AWS CLI또는 AWS SDKs를 사용하여 AWS Supply Chain 또는 다른 AWS 서비스 로 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

AWS Supply Chain에서 처리된 데이터

특정 AWS Supply Chain 인스턴스의 권한 있는 사용자가 액세스할 수 있는 데이터를 제한하기 위해 AWS Supply Chain에 보관된 데이터는 AWS 계정 ID와 AWS Supply Chain 인스턴스 ID로 구분됩니다.

AWS Supply Chain은 사용자 정보, 데이터 커넥터에서 추출한 정보, 인벤토리 세부 정보와 같은 다양한 공급망 데이터를 처리합니다.

옵트아웃 기본 설정

당사는 [AWS 서비스 약관에](#) 명시된 AWS Supply Chain대로에서 처리하는 귀하의 콘텐츠를 사용하고 저장할 수 있습니다. 옵트아웃 AWS Supply Chain 하여 콘텐츠를 사용하거나 저장하려면 AWS Organizations에서 옵트아웃 정책을 생성할 수 있습니다. 옵트아웃 정책 생성에 대한 자세한 내용은 [AI 서비스 옵트아웃 정책 구문 및 예제를](#) 참조하세요.

저장 시 암호화

PII로 분류된 고객 응대 데이터 또는 Amazon Q에서에 의해 저장 AWS Supply Chain 되는 데 사용되는 콘텐츠를 포함한 고객 콘텐츠를 나타내는 데이터는 저장 시(즉 AWS Supply Chain, 디스크에 저장, 저장 또는 저장되기 전) AWS Supply Chain 인스턴스에 한정된 키로 암호화됩니다.

Amazon S3 서버 측 암호화를 사용하면 각 고객 계정에 고유한 AWS Key Management Service 데이터 키를 사용하여 모든 콘솔 및 웹 애플리케이션 데이터를 암호화할 수 있습니다. 에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 [란 무엇입니까 AWS Key Management Service?](#)를 AWS KMS keys참조하세요.

Note

AWS Supply Chain 의 기능 Supply Planning 및 N-Tier Visibility는 제공된 KMS-CMK로 data-at-rest 암호화를 지원하지 않습니다.

전송 중 암호화

AWS Supply Chain과 AWS Supply Chain 교환하여 Amazon Q에 사용되는 콘텐츠를 포함한 데이터는 업계 표준 TLS 암호화를 사용하여 사용자의 웹 브라우저와 AWS Supply Chain 간에 전송 중에 보호됩니다.

키 관리

AWS Supply Chain 는 KMS-CMK를 부분적으로 지원합니다.

에서 AWS KMS 키를 업데이트하는 방법에 대한 자세한 내용은 섹션을 AWS Supply Chain참조하세요
[요2단계: 인스턴스 만들기](#).

인터넷워크 트래픽 개인 정보 보호

Note

AWS Supply Chain 는 PrivateLink를 지원하지 않습니다.

에 대한 Virtual Private Cloud(VPC) 엔드포인트 AWS Supply Chain 는 VPC 내의 논리적 엔터티로,에 대한 연결만 허용합니다 AWS Supply Chain. VPC는 요청을 로 라우팅 AWS Supply Chain 하고 응답을 VPC로 다시 라우팅합니다. 자세한 내용은 [VPC 사용 설명서의 VPC 엔드포인트](#)를 참조하세요.

에서 권한 부여를 AWS Supply Chain 사용하는 방법 AWS KMS

AWS Supply Chain 는 고객 관리형 키를 사용하기 위한 [권한 부여](#)를 필요로 합니다.

AWS Supply Chain 는 CreateInstance 작업 중에 전달되는 AWS KMS 키를 사용하여 여러 권한 부여를 생성합니다.는 [CreateGrant](#) 요청을에 전송하여 사용자를 대신하여 권한 부여를 AWS Supply Chain 생성합니다 AWS KMS. 의 권한 부여 AWS KMS 는 고객 계정의 AWS KMS 키에 대한 AWS Supply Chain 액세스 권한을 부여하는 데 사용됩니다.

Note

AWS Supply Chain 는 자체 권한 부여 메커니즘을 사용합니다. 사용자가에 추가되면 AWS KMS 정책을 사용하여 동일한 사용자 나열을 거부할 수 AWS Supply Chain없습니다.

AWS Supply Chain 는 다음에 대한 권한 부여를 사용합니다.

- 인스턴스에 저장된 데이터를 [암호화](#)하도록 GenerateDataKey 요청을 AWS KMS 에 보냅니다.
- 인스턴스와 연결된 암호화된 데이터를 읽기 위해 AWS KMS 에 Decrypt 요청을 보냅니다.
- Amazon Forecast와 같은 다른 AWS 서비스로 데이터를 전송할 때 데이터를 안전하게 유지하기 위해 DescribeKey, CreateGrant 및 RetireGrant 권한을 추가하려면

언제든지 권한 부여에 대한 액세스 권한을 취소하거나 고객 관리형 키에 대한 서비스 액세스를 제거할 수 있습니다. 이렇게 하면 고객 관리형 키로 암호화된 데이터에 액세스할 수 AWS Supply Chain 없어 해당 데이터에 의존하는 작업에 영향을 미칩니다.

에 대한 암호화 모니터링 AWS Supply Chain

다음 예제는 Encrypt, GenerateDataKey 및 고객 관리형 키로 암호화된 데이터에 액세스 Decrypt하기 AWS Supply Chain 위해 호출한 KMS 작업을 모니터링하는 AWS CloudTrail 이벤트입니다.

Encrypt

```

    {
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
      },
      "eventTime": "2024-03-06T22:39:32Z",
      "eventSource": "kms.amazonaws.com",
      "eventName": "Encrypt",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "172.12.34.56",
      "userAgent": "Example/Desktop/1.0 (V1; OS)",
      "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
      },
      "responseElements": null,
      "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
      "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
      "readOnly": true,
      "resources": [
        {
          "accountId": account ID,
          "type": "AWS::KMS::Key",
          "ARN": "arn:aws:kms:us-east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
      ],
      "eventType": "AwsApiCall",

```

```

"managementEvent": true,
"recipientAccountId": "112233445566",
"sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
"eventCategory": "Management"
}

```

GenerateDataKey

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "scn.amazonaws.com"
  },
  "eventTime": "2024-03-06T22:39:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "172.12.34.56",
  "userAgent": "Example/Desktop/1.0 (V1; OS)",
  "requestParameters": {
    "encryptionContext": {
      "aws:s3:arn": "arn:aws:s3:::test/rawEvent/bf6666c1-111-48aaca-b6b0-dsadsadsa3432423/noFlowName/scn.data.inboundorder/20240306_223934_536"
    },
    "keyId": "arn:aws:kms:us-east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
    "keySpec": "AES_222"
  },
  "responseElements": null,
  "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
  "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
  "readOnly": true,
  "resources": [
    {
      "accountId": account ID,
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
    }
  ],
}

```

```

"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "112233445566",
"sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
"eventCategory": "Management"
}

```

Decrypt

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "scn.amazonaws.com"
  },
  "eventTime": "2024-03-06T22:39:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "172.12.34.56"
  "userAgent": "Example/Desktop/1.0 (V1; OS)",
  "requestParameters": {
    "keyId": "arn:aws:kms:us-east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
  },
  "responseElements": null,
  "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
  "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
  "readOnly": true,
  "resources": [
    {
      "accountId": account ID,
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "112233445566",

```

```

    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}

```

인터페이스 엔드포인트를 AWS Supply Chain 사용한 액세스(AWS PrivateLink)

AWS PrivateLink 를 사용하여 VPC와 간에 프라이빗 연결을 생성할 수 있습니다 AWS Supply Chain. 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결을 사용하지 않고 VPC 에 있는 AWS Supply Chain 것처럼 액세스할 수 있습니다. VPC의 인스턴스에서 AWS Supply Chain API에 액세스하는 데는 퍼블릭 IP 주소가 필요하지 않습니다.

AWS PrivateLink에서 제공되는 인터페이스 엔드포인트를 생성하여 이 프라이빗 연결을 설정합니다. 인터페이스 엔드포인트에 대해 사용 설정하는 각 서브넷에서 엔드포인트 네트워크 인터페이스를 생성합니다. 이는 AWS Supply Chain로 향하는 트래픽의 진입점 역할을 하는 요청자 관리형 네트워크 인터페이스입니다.

자세한 내용은 AWS PrivateLink 가이드의 [AWS 서비스 통한 액세스를 AWS PrivateLink](#) 참조하세요.

에 대한 고려 사항 AWS Supply Chain

에 대한 인터페이스 엔드포인트를 설정하기 전에 AWS PrivateLink 가이드의 [고려 사항을](#) AWS Supply Chain 검토하세요.

AWS Supply Chain 는 인터페이스 엔드포인트를 통해 모든 API 작업을 호출할 수 있도록 지원합니다.

에 대한 인터페이스 엔드포인트 생성 AWS Supply Chain

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 AWS Supply Chain 사용하기 위한 인터페이스 엔드포인트를 생성할 수 있습니다 AWS CLI. 자세한 내용은 AWS PrivateLink 설명서의 [인터페이스 엔드포인트 생성](#)을 참조하세요.

다음 서비스 이름을 AWS Supply Chain 사용하여 용 인터페이스 엔드포인트를 생성합니다.

```
com.amazonaws.region.scn
```

인터페이스 엔드포인트에 프라이빗 DNS를 사용하도록 설정하는 경우, 리전에 대한 기본 DNS 이름(예: AWS Supply Chain)을 사용하여 API 요청을 할 수 있습니다. 예: `scn.region.amazonaws.com`.

엔드포인트의 엔드포인트 정책 생성

엔드포인트 정책은 인터페이스 엔드포인트에 연결할 수 있는 IAM 리소스입니다. 기본 엔드포인트 정책은 인터페이스 엔드포인트를 AWS Supply Chain 통해에 대한 전체 액세스를 허용합니다. VPC AWS Supply Chain 에서에 허용되는 액세스를 제어하려면 인터페이스 엔드포인트에 사용자 지정 엔드포인트 정책을 연결합니다.

엔드포인트 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 보안 주체(AWS 계정, IAM 사용자 및 IAM 역할)
- 수행할 수 있는 작업
- 작업을 수행할 수 있는 리소스

자세한 내용은 AWS PrivateLink 가이드의 [엔드포인트 정책을 사용하여 서비스에 대한 액세스 제어를 참조](#)하세요.

예: AWS Supply Chain 작업에 대한 VPC 엔드포인트 정책

다음은 사용자 지정 엔드포인트 정책의 예입니다. 이 정책은 인터페이스 엔드포인트에 연결될 때 모든 리소스의 모든 보안 주체에 대한 액세스 권한을 나열된 AWS Supply Chain 작업에 부여합니다.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "scn:action-1",
        "scn:action-2",
        "scn:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

}

에 대한 IAM AWS Supply Chain

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

주제

- [대상](#)
- [ID를 통한 인증](#)
- [정책을 사용하여 액세스 관리](#)
- [가 IAM에서 AWS Supply Chain 작동하는 방식](#)
- [AWS Supply Chain에 대한 자격 증명 기반 정책 예시](#)
- [AWS Supply Chain 자격 증명 및 액세스 문제 해결](#)

대상

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

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

서비스 관리자 - 회사에서 AWS Supply Chain 리소스를 책임지고 있는 경우에 대한 전체 액세스 권한이 있을 수 있습니다 AWS Supply Chain. 서비스 사용자가 액세스해야 하는 AWS Supply Chain 기능과 리소스를 결정하는 것은 사용자의 작업입니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가에서 IAM을 사용하는 방법에 대한 자세한 내용은 섹션을 AWS Supply Chain참조하세요 [가 IAM에서 AWS Supply Chain 작동하는 방식](#).

IAM 관리자 - IAM 관리자라면 AWS Supply Chain에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 자격 AWS Supply Chain 증명 기반 정책 예제를 보려면 [섹션을 참조하세요](#) [AWS Supply Chain에 대한 자격 증명 기반 정책 예시](#).

ID를 통한 인증

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

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

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

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

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

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 테루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 [루트 사용자 보안 인증이 필요한 작업](#)을 참조하세요.

페더레이션 자격 증명

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

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

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

IAM 사용자 및 그룹

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

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

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

IAM 역할

[IAM 역할](#)은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수입하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS

CLI 사용하여 역할을 수입할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 [역할 수입 방법](#)을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

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

- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여](#)를 참조하세요.

정책을 사용하여 액세스 관리

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

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

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

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

ID 기반 정책

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

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

리소스 기반 정책

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

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

액세스 제어 목록(ACL)

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

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

기타 정책 타입

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

- 권한 경계 - 권한 경계는 ID 기반 정책에 따라 IAM 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 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. Principal 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 [IAM 엔티티에 대한 권한 경계](#)를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유한 여러 AWS 계정 를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔티티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 [Service control policies](#)을 참조하세요.

- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이 포함 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [리소스 제어 정책\(RCPs\)](#)을 참조하세요.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 [세션 정책](#)을 참조하세요.

여러 정책 유형

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

가 IAM에서 AWS Supply Chain 작동하는 방식

IAM을 사용하여에 대한 액세스를 관리하기 전에 사용할 수 있는 IAM 기능에 대해 AWS Supply Chain 알아봅니다 AWS Supply Chain.

에서 사용할 수 있는 IAM 기능 AWS Supply Chain

IAM 기능	AWS Supply Chain 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
임시 보안 인증	예

IAM 기능	AWS Supply Chain 지원
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	아니요

AWS Supply Chain 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방식을 개괄적으로 알아보려면 IAM 사용 설명서의 [AWS IAM으로 작업하는 서비스를](#) 참조하세요.

예 대한 자격 증명 기반 정책 AWS Supply Chain

ID 기반 정책 지원: 예

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

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

예 대한 자격 증명 기반 정책 예제 AWS Supply Chain

AWS Supply Chain 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS Supply Chain에 대한 자격 증명 기반 정책 예시](#).

내의 리소스 기반 정책 AWS Supply Chain

리소스 기반 정책 지원: 아니요

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

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

에 대한 정책 작업 AWS Supply Chain

정책 작업 지원: 예

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

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

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

의 정책 작업은 작업 앞에 다음 접두사를 AWS Supply Chain 사용합니다.

```
scn
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

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

AWS Supply Chain 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS Supply Chain에 대한 자격 증명 기반 정책 예시](#).

에 대한 정책 리소스 AWS Supply Chain

정책 리소스 지원: 예

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

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

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

```
"Resource": "*"

```

AWS Supply Chain 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS Supply Chain에 대한 자격 증명 기반 정책 예시](#).

에 대한 정책 조건 키 AWS Supply Chain

서비스별 정책 조건 키 지원: 예

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

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

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

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

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

AWS Supply Chain 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요 [AWS Supply Chain에 대한 자격 증명 기반 정책 예시](#).

에서 임시 자격 증명 사용 AWS Supply Chain

임시 자격 증명 지원: 예

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

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

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

에 대한 액세스 세션 전달 AWS Supply Chain

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [전달 액세스 세션](#)을 참조하세요.

AWS Supply Chain의 서비스 역할

서비스 역할 지원: 예

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

⚠ Warning

서비스 역할에 대한 권한을 변경하면 AWS Supply Chain 기능이 중단될 수 있습니다. 에서 관련 지침을 AWS Supply Chain 제공하는 경우에만 서비스 역할을 편집합니다.

에 대한 서비스 연결 역할 AWS Supply Chain

서비스 링크 역할 지원: 아니요

서비스 연결 역할은 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 [IAM으로 작업하는AWS 서비스](#) 섹션을 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AWS Supply Chain에 대한 자격 증명 기반 정책 예시

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

이러한 JSON 정책 예시 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성](#) 단원을 참조하세요.

주제

- [정책 모범 사례](#)

정책 모범 사례

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

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

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

AWS Supply Chain 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단 AWS Supply Chain 하고 수정할 수 있습니다.

주제

- [에서 작업을 수행할 권한이 없음 AWS Supply Chain](#)
- [iam:PassRole을 수행하도록 인증되지 않음](#)
- [내 외부의 사람이 내 AWS Supply Chain 리소스에 액세스 AWS 계정 하도록 허용하고 싶습니다.](#)

에서 작업을 수행할 권한이 없음 AWS Supply Chain

AWS Management Console 에서 작업을 수행할 권한이 없는 경우 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 사용자 이름과 비밀번호를 제공한 사람입니다.

다음의 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 `scn:GetWidget` 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
scn:GetWidget on resource: my-example-widget
```

이 경우 Mateo는 *my-example-widget* 태스크를 사용하여 `scn:GetWidget` 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AWS Supply Chain에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 AWS Supply Chain에서 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 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 AWS Supply Chain 리소스에 액세스 AWS 계정 하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제

어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 에서 이러한 기능을 AWS Supply Chain 지원하는지 여부를 알아보려면 [섹션을 참조하세요](#)가 [IAM에서 AWS Supply Chain 작동하는 방식](#).
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 [IAM 사용 설명서의 소유 AWS 계정 한 다른의 IAM 사용자에게 액세스 권한 제공을 참조하세요](#).
- 리소스에 대한 액세스 권한을 타사에 제공하는 방법을 알아보려면 IAM 사용 설명서의 [타사 AWS 계정 소유에 대한 액세스 권한 제공을](#) AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [외부에서 인증된 사용자에게 액세스 권한 제공\(ID 페더레이션\)](#)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 [IAM의 크로스 계정 리소스 액세스](#)를 참조하세요.

AWS 에 대한 관리형 정책 AWS Supply Chain

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 [고객 관리형 정책](#)을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 AWS 관리형 정책에 정의된 권한을 AWS 업데이트하면 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS 는 새 AWS 서비스 가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 [AWS 관리형 정책](#)을 참조하세요.

AWS 관리형 정책: AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess는 AWS Supply Chain 애플리케이션 내에서 작업을 수행하는 데 필요한 권한을 포함하여 AWS Supply Chain 페더레이션 사용자에게 AWS Supply Chain 애플리케이션에 대한 액세스 권한을 제공합니다. 이 정책은 IAM Identity Center 사용자 및 그룹에 대한 관리 권한을 제공하며 AWS Supply Chain 에서 생성한 역할에 연결됩니다. AWSSupplyChainFederationAdminAccess 정책을 다른 어떤 IAM 엔터티에도 연결해서는 안 됩니다.

이 정책은 scn:* 권한을 AWS Supply Chain 통해에 대한 모든 액세스를 제공하지만 AWS Supply Chain 역할에 따라 권한이 결정됩니다. AWS Supply Chain 역할에는 필요한 권한만 포함되며 관리자 APIs에 대한 권한은 없습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- Chime - Amazon Chime AppInstance에서 사용자를 생성하거나 삭제할 수 있는 액세스 권한을 제공합니다. 채널, 채널 멤버, 진행자를 관리할 수 있는 액세스 권한을 제공합니다. 채널에 메시지를 보낼 수 있는 액세스 권한을 제공합니다. Chime 작업 범위는 "SCNInstanceId" 태그가 지정된 앱 인스턴스로 제한됩니다.
- AWS IAM Identity Center (AWS SSO) - IAM Identity Center에서 사용자 프로필을 연결 및 연결 해제하고, 프로필 연결을 나열하고, 애플리케이션 할당을 나열하고, 애플리케이션을 설명하고, 인스턴스를 설명하고, 애플리케이션 할당 구성을 가져오는 데 필요한 권한을 제공합니다.
- AppFlow - 연결 프로필을 생성, 업데이트, 삭제할 수 있는 액세스 권한을 제공합니다. 흐름을 생성, 업데이트, 삭제, 시작, 중지할 수 있는 액세스 권한을 제공합니다. 흐름을 태그 지정 및 태그 해제하고 흐름 레코드를 설명할 수 있는 액세스 권한을 제공합니다.
- Amazon S3 - 모든 버킷을 나열할 수 있는 액세스 권한을 제공합니다. arn:aws:s3::aws-supply-chain-data-* 리소스 ARN이 있는 버킷에 대한 GetBucketLocation, GetBucketPolicy, PutObject, GetObject 및 ListBucket 액세스 권한을 제공합니다.
- SecretsManager - 보안 암호 생성 및 보안 암호 정책 업데이트에 대한 액세스 권한을 제공합니다.
- KMS - Amazon AppFlow 서비스에 키 및 키 별칭을 나열할 수 있는 액세스 권한을 제공합니다. key-value aws-supply-chain-access : true 태그가 지정된 KMS 키에 대한 DescribeKey, CreateGrant 및 ListGrants 권한을 제공합니다. 보안 암호를 생성하고 보안 암호 정책을 업데이트할 수 있는 액세스 권한을 제공합니다.

권한(kms:ListKeys, kms:ListAliases, kms:GenerateDataKey 및 kms:Decrypt)은 Amazon AppFlow로 제한되지 않으며 계정의 모든 AWS KMS 키에 이러한 권한을 부여할 수 있습니다.

이 정책의 권한을 보려면 AWS Management Console에서 [AWSSupplyChainFederationAdminAccess](#)를 확인하세요.

AWS Supply Chain AWS 관리형 정책에 대한 업데이트

다음 표에는 이 서비스가 이러한 변경 사항을 추적하기 시작한 이후의 AWS 관리형 정책 업데이트에 대한 AWS Supply Chain 세부 정보가 나열되어 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS Supply Chain 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWSSupplyChainFederationAdminAccess - 정책 업데이트	AWS Supply Chain 는 IAM Identity Center에서 연합된 사용자가 ListApplicationAssignments, DescribeApplication, DescribeInstance 및 GetApplicationAssignmentConfiguration 작업에 액세스할 수 있도록 관리형 정책을 업데이트했습니다.	2024년 12월 10일
AWSSupplyChainFederationAdminAccess - 정책 업데이트	AWS Supply Chain 는 IAM Identity Center의 ListProfileAssociations 작업에 페더레이션 사용자가 액세스할 수 있도록 관리형 정책을 업데이트했습니다.	2023년 11월 1일
AWSSupplyChainFederationAdminAccess - 정책 업데이트	AWS Supply Chain 는 리소스 arn:aws:s3::aws-supply-chain-data-*를 사용하여 전용 S3 버킷의 PutObject 및	2023년 9월 21일

변경 사항	설명	날짜
	GetObject 작업에 페더레이션 사용자가 액세스할 수 있도록 관리형 정책을 업데이트했습니다.	
AWSSupplyChainFederationAdminAccess – 새 정책	AWS Supply Chain 는 연합된 사용자가 AWS Supply Chain 애플리케이션에 액세스할 수 있도록 허용하는 새 정책을 추가했습니다. 여기에는 AWS Supply Chain 애플리케이션 내에서 작업을 수행하는 데 필요한 권한이 포함됩니다.	2023년 3월 1일
AWS Supply Chain 변경 사항 추적 시작	AWS Supply Chain 는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2023년 3월 1일

에 대한 규정 준수 검증 AWS Supply Chain

타사 감사자는 여러 규정 준수 프로그램의 AWS Supply Chain 일환으로의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

특정 규정 준수 프로그램의 범위에 AWS 서비스 속하는 목록은 규정 준수 프로그램 [AWS 제공 범위 내 서비스 규정 준수 프로그램](#) . 일반 정보는 [AWS 규정 준수 프로그램](#) .

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 [Downloading Reports in Downloading AWS Artifact](#) 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS Supply Chain 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- [보안 및 규정 준수 빠른 시작 안내서](#) – 이 배포 안내서에서는 아키텍처 고려 사항에 관해 설명하고 보안 및 규정 준수에 중점을 둔 기본 AWS 환경을 배포할 때 취해야 할 단계를 제공합니다.
- [HIPAA 보안 및 규정 준수 백서 설계](#) -이 백서에서는 기업이 AWS 를 사용하여 HIPAA 준수 애플리케이션을 생성하는 방법을 설명합니다.

- [AWS 규정 준수 리소스](#) - 이 워크북 및 가이드 모음은 업계 및 위치에 적용될 수 있습니다.
- AWS Config 개발자 안내서의 [Evaluating Resources with Rules](#) - 이 안내서에서는 리소스 구성이 내부 사례, 업계 지침, 규정을 얼마나 잘 준수하는지 평가합니다.
- [AWS Security Hub](#) - 보안 업계 표준 및 모범 사례 준수 여부를 확인하는 AWS 데 도움이 되도록 내 보안 상태를 포괄적 AWS 서비스 으로 볼 수 있습니다.

의 복원력 AWS Supply Chain

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 기반으로 구축됩니다.는 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공합니다. 이러한 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 [AWS 글로벌 인프라를](#) 참조하세요.

AWS 글로벌 인프라 외에도 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 몇 가지 기능을 AWS Supply Chain 제공합니다.

로깅 및 모니터링 AWS Supply Chain

로깅 및 모니터링은 AWS Supply Chain 및 기타 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 중요한 부분입니다.는 AWS CloudTrail 모니터링 도구를 AWS 제공하여 AWS Supply Chain을 모니터링하고, 문제가 있을 때 보고하고, 적절한 경우 자동 조치를 취합니다.

Note

AWS Supply Chain 콘솔에서만 호출되는 APIs 캡처됩니다 AWS CloudTrail.

AWS CloudTrail은 직접 수행하거나 AWS 계정을 대신하여 수행한 API 직접 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 호출했는지 어떤 소스 IP 주소에 호출이 이루어졌는지 언제 호출이 발생했는지 확인할 수 있습니다. scn.amazonaws.com AWS Supply Chain 이벤트를 볼 수 있습니다. 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하십시오.

Note

AWS Supply Chain 다음 사항에 유의하세요.

- 예 액세스할 수 없는 사용자를 초대하면 AWS Supply Chain 이러한 사용자는 웹 애플리케이션에서 수신하는 알림에 정보를 받지 못합니다. 초대된 사용자는 웹 애플리케이션 링크가 포함된 이메일 알림을 받으며, 필수 사용자 권한이 있는 경우에만 로그인하여 알림의 내용을 확인할 수 있습니다.
- 특정 인사이트에 대한 사용자 권한이 있거나 없는 모든 사용자는 인사이트 채팅 메시지를 볼 수 있습니다.
- 애플리케이션 관리자는 AWS Supply Chain 인스턴스에 사용자를 추가할 때에 액세스할 수 있습니다 AWS KMS key. 사용자 권한을 관리하여 사용자를 추가하거나 제거할 수 있습니다. 사용자 권한에 대한 자세한 내용은 [사용자 권한 역할 관리](#) 단원을 참조하세요.

AWS Supply Chain CloudTrail의 데이터 이벤트

Note

아래에 나열된 웹 애플리케이션 APIs는 CloudTrail의 데이터 이벤트에 나열 [AWS Supply Chain 웹 애플리케이션 APIs](#) 됩니다.

[데이터 이벤트](#)는 리소스 기반 또는 리소스에서 수행된 리소스 작업에 대한 정보를 제공합니다(예: Amazon S3 객체 읽기 또는 쓰기). 이를 데이터 영역 작업이라고도 합니다. 데이터 이벤트가 대량 활동인 경우도 있습니다. 기본적으로 CloudTrail은 데이터 이벤트를 로깅하지 않습니다. CloudTrail 이벤트 기록은 데이터 이벤트를 기록하지 않습니다.

데이터 이벤트에는 추가 요금이 적용됩니다. CloudTrail 요금에 대한 자세한 내용은 [AWS CloudTrail 요금](#)을 참조하세요.

CloudTrail 콘솔 AWS CLI 또는 CloudTrail API 작업을 사용하여 AWS Supply Chain 리소스 유형에 대한 데이터 이벤트를 로깅할 수 있습니다.

- CloudTrail 콘솔을 사용하여 데이터 이벤트를 로깅하려면 [추적](#) 또는 [이벤트 데이터 스토어](#)를 생성하여 데이터 이벤트를 기록하거나 [기존 추적 또는 이벤트 데이터 스토어를 업데이트](#)하여 데이터 이벤트를 기록합니다.

1. 데이터 이벤트를 로깅하려면 데이터 이벤트를 선택합니다.
 2. 데이터 이벤트 유형에서 데이터 이벤트를 로깅할 리소스 유형을 선택합니다.
 3. 사용할 템플릿에서 로그 선택기를 선택합니다. 리소스 유형에 대한 모든 데이터 이벤트를 로그하거나, 모든 `readOnly` 이벤트를 로그하거나, 모든 `writeOnly` 이벤트를 로그하거나, 사용자 지정 로그 선택기 템플릿을 생성하여 `readOnly`, `eventName` 및 `resources.ARN` 필드를 필터링할 수 있습니다.
- 를 사용하여 데이터 이벤트를 로깅하려면 `eventCategory` 필드를 `Data` 로 AWS CLI 설정하고 `resources.type` 필드를 리소스 유형 값 로 설정하도록 `--advanced-event-selectors` 파라미터를 구성합니다. 조건을 추가하여 `readOnly`, `eventName` 및 `resources.ARN` 필드의 값을 필터링할 수 있습니다.
 - 데이터 이벤트를 로깅하도록 추적을 구성하려면 [put-event-selectors](#) 명령을 실행합니다. 자세한 내용은 [AWS CLI로 추적에 대한 데이터 이벤트 로깅](#)을 참조하세요.
 - 데이터 이벤트를 로깅하도록 이벤트 데이터 스토어를 구성하려면 [create-event-data-store](#) 명령을 실행하여 데이터 이벤트를 로깅할 새 이벤트 데이터 스토어를 생성하거나 [update-event-data-store](#) 명령을 실행하여 기존 이벤트 데이터 스토어를 업데이트합니다. 자세한 내용은 [AWS CLI로 데이터 이벤트 스토어에 대한 데이터 이벤트 로깅](#)을 참조하세요.

*`eventName`, `readOnly` 및 `resources.ARN` 필드를 필터링하여 중요한 이벤트만 로깅하도록 고급 이벤트 선택기를 구성할 수 있습니다. 필드에 대한 자세한 내용은 [AdvancedFieldSelector](#) 섹션을 참조하세요.

AWS Supply Chain CloudTrail의 관리 이벤트

[관리 이벤트](#)는 AWS 계정의 리소스에서 수행되는 관리 작업에 대한 정보를 제공합니다. 이를 컨트롤 플레인 작업이라고도 합니다. 기본적으로 CloudTrail은 관리 이벤트를 로깅합니다.

AWS Supply Chain은 모든 컨트롤 플레인 작업을 CloudTrail에 관리 이벤트로 기록합니다.

AWS Supply Chain 웹 애플리케이션 APIs

이 섹션에 나열된 APIs는 페더레이션 사용자를 대신하여 AWS Supply Chain 애플리케이션에서 호출합니다. 이러한 API는 CloudTrail 로그에 표시되지 않으며 서비스 권한 부여 참조 문서에 캡처되지 않습니다. [AWS Supply Chain](#) 단원을 참조하세요. 이러한 APIs에 대한 액세스는 페더레이션 사용자 역할 권한을 기반으로 AWS Supply Chain 애플리케이션에 의해 제어됩니다. AWS Supply Chain 애플리케이션 중단을 방지하기 위해 이러한 APIs에 대한 액세스를 제어하려고 하서는 안 됩니다.

사용자 역할

다음 APIs는 사용자, 사용자 역할, 사용자 알림 및 채팅 메시지를 관리하는 데 사용됩니다 AWS Supply Chain.

```
scn:AddMembersToResourceBasedChat
scn:AssignGalaxyRoleToUser
scn:AssociateUser
scn:BatchGetUsers
scn:BatchMarkNotificationAsDelivered
scn:CreateRole
scn>DeleteRole
scn:DescribeChatForUser
scn:GetAccessDetailConfig
scn:GetChatPreferencesForUser
scn:GetMessagingSessionConnectionDetails
scn:GetNotificationsPreference
scn:GetOrCreateChimeUser
scn:GetOrCreateResourceBasedChat
scn:GetOrCreateUserBasedChat
scn:GetOrganizationInfo
scn:GetResourceBasedChatArn
scn:GetUserDetails
scn:ListChatMembers
scn:ListChatMessages
scn:ListChatModerators
scn:ListChats
scn:ListRoles
scn:ListUserNotifications
scn:ListUsersWithRole
scn:MarkNotificationAsDelivered
scn:MarkNotificationAsRead
scn:RemoveMemberFromResourceBasedChat
scn:RemoveUser
scn:SearchChimeUsers
scn:SearchUsers
scn:SendChatMessage
scn:SetNotificationsPreference
scn:UpdateChatPreferencesForUser
scn:UpdateChatReadMarker
scn:UpdateOrganizationInfo
```

```
scn:UpdateRole  
scn:UpdateUser
```

데이터 레이크

다음 API는 데이터 레이크에서 데이터 흐름과 연결을 생성하고 관리하는 데 사용됩니다.

```
scn:CreateConnection  
scn:CreateDataflow  
scn:CreateDeleteDataByPartitionJob  
scn:CreateExtractFlows  
scn:CreatePresignedUrl  
scn:CreateSampleParsingJob  
scn:CreateSap0DataConnection  
scn:CreateUpdateDatasetSchemaJob  
scn>DeleteConnection  
scn>DeleteDataflow  
scn>DeleteExtractFlows  
scn>DeleteSap0DataConnection  
scn:describeDatasetGroup  
scn:DescribeDataset  
scn:DescribeJob  
scn:GetConnection  
scn:GetCreateExtractFlowsStatus  
scn:GetDataflow  
scn:ListConnections  
scn:ListCustomerFiles  
scn:ListDataflows  
scn:ListDataflowStats  
scn:ListDatasets  
scn:UpdateConnection  
scn:UpdateDataflow  
scn:UpdateExtractFlow
```

인사이트

다음 API는 인사이트 애플리케이션에서 필터, 감시 목록을 관리하고 인벤토리 변경 사항을 확인하는데 사용됩니다.

```
scn:AddModeratorToResourceBasedChat
scn:ComputePostRebalancedQuantities
scn:ComputePostRebalancedQuantitiesV1
scn:CreateInsightFilter
scn:CreateInsightSubscription
scn>DeleteInsightFilter
scn>DeleteInsightSubscription
scn:GetInsightLineItem
scn:GetInsightSubscription
scn:GetInstanceAttribute
scn:GetInstanceRequiredDatasetAvailabilityStatus
scn:GetKpiData
scn:GetModelEndpointStatus
scn:GetPIVForProduct
scn:GetPIVForSite
scn:GetPIVForSiteAndProduct
scn:GetPIVForSitesAndProducts
scn:GetProducts
scn:GetProductSummaryAggregates
scn:GetSites
scn:GetSiteSummaryAggregates
scn:IsUserAuthorizedForInsightLineItem
scn:ListCustomAttributeValue
scn:ListGeographiesAsGalaxyAdmin
scn:ListInsightFilters
scn:ListInsightLineItems
scn:ListInsightSubscriptions
scn:ListInventoryQuantityAggregates
scn:ListInventoryRisksBySiteAndProduct
scn:ListInventorySummariesBySite
scn:ListPIVProductsBySite
scn:ListProductHierarchiesAsGalaxyAdmin
scn:ListProducts
scn:ListProductsAsGalaxyAdmin
scn:ListSites
scn:ListUsers
```

```
scn:PotentiallyComputeThenListRebalancingOptionsForInsightLineItem
scn:RegisterInstanceAttribute
scn:UpdateInsightFilter
scn:UpdateInsightLineItemStatus
scn:UpdateInsightSubscription
scn:UpdateRebalancingOptionStatus
scn:UpdateRebalancingOptionStatusV1
```

Demand Planning

다음 APIs는에서 예측, 수요 계획 또는 통합 문서를 생성하고 관리하는 AWS Supply Chain 데 사용됩니다.

```
scn:AssociateDatasetWithWorkbook
scn:CreateBaselineForecast
scn:CreateDemandPlan
scn:CreateDemandPlanningCycle
scn:CreateDemandPlanningDatasetExportJob
scn:CreateDerivedForecast
scn:CreateWorkbook
scn>DeleteDemandForecastConfig
scn>DeleteDemandPlanningCycle
scn>DeleteDerivedForecast
scn>DeleteWorkbook
scn:DescribeBaselineForecast
scn:DescribeDemandPlanningCycleAccuracyJob
scn:DescribeDerivedForecast
scn:DescribePlanningCycle
scn:DescribeWorkbook
scn:DisassociatePlanningCycle
scn:GetDemandForecastConfig
scn:GetDemandPlan
scn:GetDemandPlanningCycle
scn:GetDemandPlanningCycleAccuracy
scn:GetDemandPlanningDatasetJob
scn:ListDemandPlans
scn:ListDerivedForecasts
scn:ListForecastingJobs
scn:ListPlanningCycles
```

```
scn:ListWorkbooks
scn:PublishDemandPlan
scn:PutDemandForecastConfig
scn:StartDemandPlanningCycleAccuracyJob
scn:StartForecastingJob
scn:UpdateDemandPlan
scn:UpdateDemandPlanningCycleMetadata
scn:UpdateWorkbook
```

공급 계획

다음 APIs는에서 공급 계획을 생성하고 관리하는 AWS Supply Chain 데 사용됩니다.

```
scn:CreateReplenishmentPipeline
scn:GetReplenishmentPipeline
scn:UpdateReplenishmentPipeline
scn:ListReplenishmentPipelinesByInstance
scn:GetInstanceReplenishmentConfig
scn:CreateBacktest
scn:CreateReplenishmentReviewInstanceConfig
scn:GetReplenishmentReviewInstanceConfig
scn:ListReplenishmentVendors
scn:GetExceptionsSupplyInsightsStatistics
scn:GetPorSupplyInsightsStatistics
scn:GetPlanToPOConversionAnalytics
scn:GetPurchasePlanStatistics
scn:ListPlanExceptions
scn:ListPurchaseOrderRequestLines
scn:UpdatePurchaseOrderRequestLines
scn:ListBomPurchasePlans
scn:ListBomProductionPlans
scn:ListBomTransferPlans
scn:ListBomInsights
scn:ListBomProcesses
scn:ExportBomPlans
scn:GetBomPlanSummary
scn:GetDashboardAnalytics
scn:GetPurchaseOrderRequestExplanation
scn:ListBomSupplyPlan
```

```
scn:GetBomPlanRecordDetails
scn:GetBomPlanSummaryAnalytics
scn:ListBomPurchaseOrders
scn:ListBomTransferOrders
scn:ListBomProductionOrders
scn:ExportAllExplodedBoms
scn:ExportBillOfMaterials
scn:ExportInventoryPolicy
scn:ExportProductionProcess
scn:ExportSourcingRule
scn:ExportTransportationLane
scn:ExportVendorLeadTime
scn:ImportBillOfMaterials
scn:ImportInventoryPolicy
scn:ImportProductionProcess
scn:ImportSourcingRule
scn:ImportTransportationLane
scn:ImportVendorLeadTime
```

의 Amazon Q AWS Supply Chain

다음 APIs는 Amazon Q in에서 사용됩니다 AWS Supply Chain.

```
scn:GetQMessage
scn:ListQMessages
scn:PutQMessageFeedback
scn:SendQMessage
scn:GetQEnablementStatus
scn:UpdateQEnablementStatus
```

를 사용하여 AWS Supply Chain 이벤트 관리 Amazon EventBridge

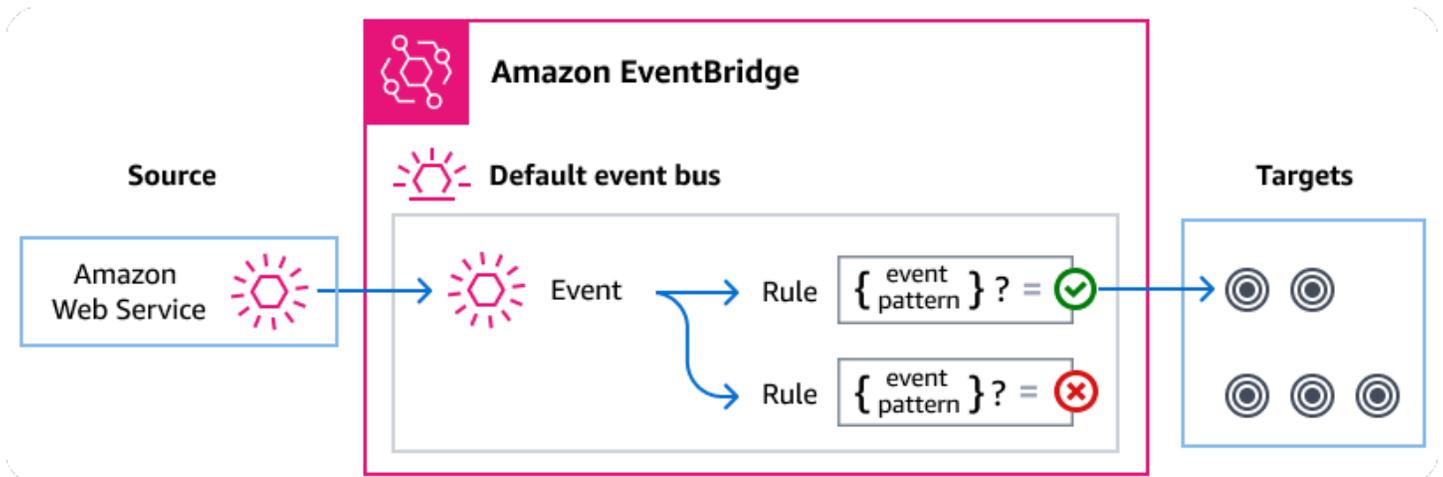
를 사용하면 다른 서비스를 자동화하여 Step Functions 표준 워크플로의 실행 상태 변경에 대응할 EventBridge수 있습니다.

Amazon EventBridge 는 이벤트를 사용하여 애플리케이션 구성 요소를 함께 연결하는 서버리스 서비스이므로 확장 가능한 이벤트 기반 애플리케이션을 더 쉽게 구축할 수 있습니다. 이벤트 기반 아키텍처

는 이벤트를 내보내고 이에 응답하여 함께 작동하는 느슨하게 결합된 소프트웨어 시스템을 구축하는 스타일입니다. 이벤트는 리소스나 환경의 변화를 나타냅니다.

운영 방식은 다음과 같습니다.

많은 AWS 서비스와 마찬가지로 이벤트는 AWS Supply Chain 생성하고 EventBridge 기본 이벤트 버스로 전송합니다. (기본 이벤트 버스는 모든 AWS 계정에 자동으로 프로비저닝됩니다.) 이벤트 버스는 이벤트를 수신하여 0개 이상의 목적지 또는 대상에 전달하는 라우터입니다. 이벤트 버스에 대해 지정된 규칙은 이벤트가 도착할 때 이벤트를 평가합니다. 각 규칙은 이벤트가 규칙의 이벤트 패턴과 일치하는지 여부를 확인합니다. 이벤트가 일치하면 이벤트 버스는 이벤트를 지정된 대상에게 전송합니다.



주제

- [AWS Supply Chain 이벤트](#)
- [EventBridge 규칙을 사용하여 AWS Supply Chain 이벤트 전송](#)
- [AWS Supply Chain 이벤트 세부 정보 참조](#)

AWS Supply Chain 이벤트

AWS Supply Chain 는 다음 이벤트를 기본 EventBridge 이벤트 버스로 자동으로 전송합니다. 규칙의 이벤트 패턴과 일치하는 이벤트는 지정된 대상으로 [기본](#) 제공됩니다. 이벤트는 비순차적으로 전달될 수 있습니다.

자세한 내용을 알아보려면 Amazon EventBridge 사용 설명서의 [EventBridge 이벤트](#)를 참조하세요.

이벤트 세부 정보 유형	설명
AWS 공급망 데이터 통합 상태 변경	수집된 각 파일의 상태를 표시합니다 AWS Supply Chain.

EventBridge 규칙을 사용하여 AWS Supply Chain 이벤트 전송

EventBridge 기본 이벤트 버스가 이벤트를 대상으로 전송 AWS Supply Chain 하도록 하려면 규칙을 생성해야 합니다. 각 규칙에는 이벤트 버스에서 수신된 각 이벤트와 EventBridge 일치하는 이벤트 패턴이 포함되어 있습니다. 이벤트 데이터가 지정된 이벤트 패턴과 일치하면는 해당 이벤트를 규칙의 대상(들)로 EventBridge 전달합니다.

이벤트 버스 규칙 생성에 대해 자세히 알아보려면 EventBridge 사용 설명서의 [이벤트에 대응하는 규칙 생성](#)을 참조하세요.

이벤트와 일치하는 AWS Supply Chain 이벤트 패턴 생성

각 이벤트 패턴은 다음을 포함하는 JSON 객체입니다.

- 이벤트를 전송하는 서비스를 식별하는 `source` 속성입니다. AWS Supply Chain 이벤트의 경우 소스는 `aws.supplychain`입니다.
- (선택 사항): 일치시킬 이벤트 유형의 배열을 포함하는 `detail-type` 속성입니다.
- (선택 사항): 일치시킬 다른 이벤트 데이터를 포함하는 `detail` 속성입니다.

예를 들어 다음 이벤트 패턴은의 모든 AWS Supply Chain Data Integration Status Change 이벤트와 일치합니다 AWS Supply Chain.

```
{
  "source": ["aws.supplychain"],
  "detail-type": ["AWS Supply Chain Data Integration Status Change"]
}
```

자세한 내용은 EventBridge 사용 설명서의 [이벤트 패턴](#)을 참조하세요.

AWS Supply Chain 이벤트 세부 정보 참조

AWS 서비스의 모든 이벤트에는 이벤트의 소스인 AWS 서비스, 이벤트가 생성된 시간, 이벤트가 발생한 계정 및 리전 등 이벤트에 대한 메타데이터가 포함된 공통 필드 세트가 있습니다. 이러한 일반 필드에 대한 정의는 Amazon EventBridge 사용 설명서의 [이벤트 구조 참조](#)를 참조하세요.

또한 각 이벤트에는 해당 특정 이벤트와 관련된 데이터를 포함하는 detail 필드가 있습니다. 다음 참조는 다양한 AWS Supply Chain 이벤트에 대한 세부 정보 필드를 정의합니다.

EventBridge 를 사용하여 AWS Supply Chain 이벤트를 선택하고 관리할 때는 다음 사항에 유의하는 것이 좋습니다.

- 의 모든 이벤트에 대한 source 필드는 로 AWS Supply Chain 설정됩니다aws.supplychain.
- detail-type 필드는 이벤트 유형을 지정합니다.

예: AWS Supply Chain Data Integration Status Change.

- detail 필드는 해당 특정 이벤트와 관련된 데이터를 포함합니다.

AWS Supply Chain 이벤트와 일치하는 규칙을 활성화하는 이벤트 패턴을 구성하는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 안내서의 [이벤트 패턴](#)을 참조하세요.

이벤트 및 이벤트 EventBridge 처리 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 [Amazon EventBridge 이벤트를](#) 참조하세요.

AWS 공급망 데이터 통합 상태 변경

다음은 AWS Supply Chain Data Integration Status Change event 이벤트의 예입니다.

```
{
  "version": "0",
  "id": "instanceID",
  "detail-type": "AWS Supply Chain Data Integration Status Change",
  "source": "aws.supplychain",
  "account": "accountID",
  "time": "2024-03-30T12:26:13Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "version": "1.0",
```

```
    "instanceId": "instanceID",
    "flowArn": "arn:aws:scn:region:accountID:instance/instanceID/data-integration-
flows/flowname",
    "flowExecutionId": "flowExecutionId",
    "status": "IN_PROGRESS",
    "startTime": "2024-03-30T12:26:13Z",
    "endTime": "",
    "message": "",
    "sourceType": "S3",
    "sourceInfo": {
      "s3Source": {
        "bucketName": "aws-supply-chain-data-instanceID",
        "key": "flowname"
      }
    }
  }
}
```

endTime는 상태가 실패 또는 성공인 경우에만 사용할 수 있습니다.

에 대한 할당량 AWS Supply Chain

AWS 계정에는 각에 대해 이전에 제한이라고 하는 기본 할당량이 있습니다 AWS 서비스. 다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다. 계정 수준으로 설정된 리소스에 대한 할당량 증가를 요청할 수 있습니다. 계정 수준 할당량에 대한 자세한 내용은 아래 표를 참조하세요.

할당량을 보려면 [Service Quotas 콘솔](#)을 AWS Supply Chain 엽니다. 탐색 창에서 AWS 서비스를 선택하고 AWS Supply Chain을 선택합니다.

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 [할당량 증가 요청](#)을 참조하세요. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 [한도 증가 양식](#)을 사용합니다.

AWS 계정에는 다음과 관련된 할당량이 있습니다 AWS Supply Chain.

리소스	Default	조정 가능
인스턴스 개수	10	아니요
<div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-bottom: 10px;"> <p> Note AWS 계정 내에서 최대 10개의 인스턴스를 생성할 수 있습니다.</p> </div>		
Amazon S3 버킷 수	100	아니요
AWS 계정 내 활성화 및 보류 중인 초대	30	예
AWS 계정 내 데이터 요청	4,000	예
감시 목록당 인사이트 행 항목	1,000	아니요
AWS 계정 내 인스턴스당 Insights 감시 목록	1,000	예
AWS 계정 내 사용자당 Insights 감시 목록	100	예

리소스	Default	조정 가능
AWS 계정 내 인스턴스당 데이터 통합 흐름	100	아니요
AWS 계정 내 인스턴스당 사용자 지정 데이터 세트 네임스페이스	20	예
AWS 계정 내 인스턴스당 사용자 지정 데이터 세트 네임스페이스당 데이터 세트	250	예
AWS 계정 내 인스턴스당 기본 데이터 세트 네임스페이스의 데이터 세트	1,000	아니요

FAQ

다음 정보는 IAM Identity Center를 활성화할 때 발생하는 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

질문	Answer
IAM Identity Center 통합이 필요한 이유는 무엇입니까?	IAM Identity Center는 자격 증명 소스의 동기화를 관리하는 IAM 내의 기능입니다. IAM Identity Center는 AWS Supply Chain 인스턴스의 자격 증명 소스입니다. AWS 콘솔과 AWS Supply Chain 웹 애플리케이션을 설정하도록 IAM Identity Center를 구성해야 합니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서 의 AWS IAM Identity Center 활성화 를 참조하세요.
에 IAM Identity Center 조직 인스턴스를 사용하는 이유는 무엇입니까 AWS Supply Chain?	조직 인스턴스를 생성하면 AWS 계정 간에 IAM Identity Center 액세스를 활성화할 수 있습니다. 예를 들어 IAM Identity Center가 AWS Supply Chain 인스턴스 AWS 계정과 동일한 계정에서 활성화되지 않은 경우 조직 IAM Identity Center 인스턴스 생성의 이점에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서 의 IAM Identity Center의 조직 인스턴스 를 참조하세요.
에 위임된 관리자 권한이 필요한 이유는 무엇입니까 AWS Supply Chain?	<p>위임된 관리자가 있어야 하는 것은 AWS Supply Chain 아니지만 AWS 조직의 관리 계정에 대한 액세스를 제한하고 IAM Identity Center를 관리하는 것이 조직 설정의 모범 사례입니다. 자세한 내용은 AWS 조직 위임 관리자를 참조하세요.</p> <p>조직 인스턴스를 생성하는 동안 AWS Supply Chain 인스턴스를 생성하는 데 사용할 계정이 IAM Identity Center 계정과 동일한 조직의 일부인지 확인합니다. 인스턴스를 생성하는 데 필요한 권한이 활성화되어 있고 IAM Identity Center</p>

질문	Answer
	<p>계정과 동일한 리전에 AWS Supply Chain 인스턴스를 생성할 수 있는지 확인합니다. AWS Supply Chain 인스턴스를 생성하는 데 필요한 권한에 대한 자세한 내용은 섹션을 참조하세요 요시작하기 AWS Supply Chain.</p>

AWS 지원

관리자로서에 대한 지원 센터에 문의해야 하는 경우 다음 옵션 중 하나를 AWS Supply Chain 선택합니다.

- 지원 계정이 있는 경우 [지원 센터로](#) 이동하여 티켓을 제출합니다.
- [AWS Management Console](#)을 열고 AWS Supply Chain, 지원, 사례 생성을 선택합니다.

다음 정보를 제공하면 도움이 됩니다.

- AWS Supply Chain 인스턴스 ID/ARN.
- AWS 리전.
- 문제에 대한 자세한 설명

AWS Supply Chain 관리자 안내서의 문서 기록

다음 표에서는에 대한 설명서 릴리스를 설명합니다 AWS Supply Chain.

변경 사항	설명	날짜
업데이트된 할당 AWS Supply Chain 량	관련 AWS 계정의 할당량을 업데이트했습니다 AWS Supply Chain.	2025년 5월 12일
AWS 관리형 정책 업데이트	AWS Supply Chain 는 IAM Identity Center에서 페더레이션 사용자가 ListApplicationAssignments, DescribeApplication, DescribeInstance 및 GetApplicationAssignmentConfiguration 작업에 액세스할 수 있도록 관리형 정책을 업데이트했습니다.	2024년 12월 10일
KMS 정책 업데이트	가 AWS KMS 키에 AWS Supply Chain 액세스할 수 있도록 KMS 정책을 업데이트했습니다.	2024년 3월 18일
PrivateLink 지원	인터페이스 엔드포인트(AWS PrivateLink)를 AWS Supply Chain 사용하여 액세스할 수 있습니다.	2024년 2월 26일
그룹 추가	사용자가 AWS Supply Chain 에 액세스하려면 IAM Identity Center 그룹에 속해야 합니다.	2023년 11월 14일
AWS 관리형 정책 업데이트	AWS Supply Chain 는 연합된 사용자가 IAM Identity Center 의 ListProfileAssociations 작업	2023년 11월 1일

에 액세스할 수 있도록 관리형 정책을 업데이트했습니다.

[AWS 관리형 정책 업데이트](#)

AWS Supply Chain 는 리소스 `arn:aws:s3::aws-supply-chain-data-*`를 사용하여 전용 Amazon S3 버킷의 PutObject 및 GetObject 작업에 페더레이션 사용자가 액세스할 수 있도록 관리형 정책을 업데이트했습니다.

2023년 9월 21일

[리전 지원에 대한 정보 업데이트](#)

AWS Supply Chain 이제 아시아 태평양(시드니) 리전에서도 Demand Planning이 지원됩니다.

2023년 9월 12일

[AWS 콘솔을 사용하여 옵트인 및 옵트아웃 AWS Supply Chain](#)

AWS Supply Chain 이제 사용자는 AWS 콘솔을 사용하여 AWS Organizations에서 콘텐츠를 사용하거나 저장하도록 옵트인 및 옵트아웃 AWS Supply Chain 할 수 있습니다.

2023년 9월 7일

[리전 지원에 대한 정보 업데이트](#)

AWS Supply Chain 는 이제 아시아 태평양(시드니) 리전과 유럽(아일랜드) 리전에서도 지원됩니다.

2023년 7월 19일

[AWS Support에 문의하고 인스턴스를 생성하는 방법에 대한 정보 업데이트](#)

AWS Supply Chain 이제 사용자는 AWS Support에 문의하여 도움을 받고 인스턴스 생성 방법에 대한 콘텐츠를 업데이트 할 수 있습니다.

2023년 4월 3일

AWS 관리형 정책 추가

AWS Supply Chain은 AWS Supply Chain 애플리케이션 내에서 작업을 수행하는 데 필요한 권한을 포함하여 연합된 사용자가 AWS Supply Chain 애플리케이션에 액세스할 수 있도록 허용하는 새 정책을 추가했습니다.

2023년 3월 1일

최초 릴리스

AWS Supply Chain 관리자 안내서의 최초 릴리스입니다.

2022년 11월 29일

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