관리자 안내서

AWS Supply Chain

AWS Supply Chain: 관리자 안내서

Table of Contents

AWS Supply Chain란 무엇인가요? 1
지원되는 브라우저 1
지원되는 언어 1
..... 1
AWS 계정 설정하기 3
가입하여 AWS 계정 3
관리자 액세스 권한이 있는 사용자 생성 3
계정 해지 AWS 5
시작하기: AWS Supply Chain 6
필수 조건 6
콘솔 사용 7
인스턴스 생성 11
IAM Identity Center 활성화 15
IAM Identity Center에서 사용자 추가 15
AWS Supply Chain 애플리케이션 소유자 선택 16
그룹 할당 16
AWS 공급망 웹 애플리케이션에 로그인 17
AWS Supply Chain 처음으로 로그인하기 17
계정 프로필 업데이트 18
조직 프로필 업데이트 18
사용자 권한 역할 18
사용자 추가 20
사용자 권한 업데이트 20
사용자 삭제 21
사용자 지정 사용자 권한 역할 생성 21
인스턴스 삭제 22
보안 23
데이터 보호 23
AWS Supply Chain에서 처리된 데이터 24
옵트아웃 기본 설정 25
저장 중 암호화 25
전송 중 암호화 25
키 관리 25
인터네트워크 트래픽 개인 정보 보호 26

에서 권한 부여를 사용하는 방법 AWS Supply ChainAWS KMS 26
AWS PrivateLink 30
고려 사항 30
인터페이스 엔드포인트 생성 30
엔드포인트 정책을 생성 30
IAM 31
고객 32
ID를 통한 인증 32
정책을 사용한 액세스 관리 35
IAM의 AWS Supply Chain 작동 방식 38
자격 증명 기반 정책 예시 43
문제 해결 44
AWS 관리형 정책 46
AWSSupplyChainFederationAdminAccess 47
정책 업데이트 48
규정 준수 검증 49
복원성 50
로깅 및 모니터링 AWS 공급망 50
AWS Supply Chain 의 데이터 이벤트 CloudTrail 51
AWS Supply Chain 의 관리 이벤트 CloudTrail 52
웹 애플리케이션 API 52
할당량 59
관리 지원 60
사용 설명서 기록 61
..... lxiii

AWS Supply Chain란 무엇인가요?

AWS Supply Chain은 전사적 자원 관리(ERP) 및 공급망 관리 시스템과 같은 기존 솔루션과 함께 작동하는 클라우드 기반 공급망 관리 애플리케이션입니다. AWS Supply Chain을 사용하면 기존 ERP 또는 공급망 시스템의 재고, 공급 및 수요 관련 데이터를 하나의 통합 AWS Supply Chain 데이터 모델에 연결하고 추출할 수 있습니다.

주제

- AWS Supply Chain에서 지원되는 브라우저
- AWS Supply Chain에서 지원하는 언어

AWS Supply Chain에서 지원되는 브라우저

AWS Supply Chain을 사용하기 전에 다음 표를 참조하여 사용 중인 브라우저가 지원되는지 확인합니다.

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

AWS Supply Chain에서 지원하는 언어

AWS Supply Chain은 다음과 같은 언어를 지원합니다.

- 영어(미국)
- 영어(영국)

- 독일어
- 스페인어
- 프랑스어
- 이탈리아어
- 포르투갈어
- 중국어 간체
- 중국어 번체
- 일본어
- 한국어
- 인도네시아어

AWS 계정 설정하기

이 섹션을 사용하여 AWS 계정을 만들고 IAM 사용자를 생성할 수 있습니다. AWS 계정 생성 모범 사례에 대한 자세한 내용은 모범 사례 AWS 환경 구축을 참조하십시오.

주제

- 가입하여 AWS 계정
- 관리자 액세스 권한이 있는 사용자 생성
- 계정 해지 AWS

가입하여 AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 가입 절차가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 가서 내 계정(My Account)을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

등록한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오 AWS 계정 루트 사용자.

보안을 유지하세요 AWS 계정 루트 사용자

1. Root user를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 AWS Management Console소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자 (콘솔) 에 대한 가상 MFA 디바이스 활성화를 참조하십시오.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리 AWS IAM Identity Center

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 필요하면 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.AWS 로그인

추가 사용자에게 액세스 권한 할당

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

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

계정 해지 AWS

계정을 폐쇄하는 방법에 대한 자세한 내용은 AWS 계정 해지를 참조하십시오.

시작하기 AWS Supply Chain

이 섹션에서는 AWS Supply Chain 인스턴스를 만들고, 사용자 권한 역할을 부여하고, AWS Supply Chain 웹 애플리케이션에 로그인하고, 사용자 지정 사용자 권한 역할을 생성하는 방법을 배울 수 있습니다. An은 활성 또는 초기화 중 상태인 AWS Supply Chain 인스턴스를 10개까지 가질 AWS 계정 수 있습니다.

주제

- 필수 조건
- AWS Supply Chain 콘솔 사용
- 인스턴스 생성
- IAM Identity Center 활성화
- AWS Supply Chain 애플리케이션 소유자 선택
- 그룹 할당
- AWS 공급망 웹 애플리케이션에 로그인
- 계정 프로필 업데이트
- 조직 프로필 업데이트
- 사용자 권한 역할
- 사용자 지정 사용자 권한 역할 생성
- 인스턴스 삭제

필수 조건

AWS Supply Chain 인스턴스를 생성하기 전에 다음 단계를 완료해야 합니다.

- 를 생성했습니다 AWS 계정. 자세한 정보는 AWS 계정 설정하기을 참조하세요.

  > **Note**
  >
  > 아직 AWS IAM Identity Center활성화하지 않았다면 AWS 조직을 만들고 IAM ID 센터를 활성화하십시오. 조직 생성에 대한 자세한 내용은 AWS 조직 생성을 참조하십시오.

- AWS Supply Chain 인스턴스를 생성하려는 AWS 리전 위치와 동일한 위치에서 IAM Identity Center를 켜십시오. AWS Supply Chain 미국 동부 (버지니아 북부), 미국 서부 (오레곤), 유럽 (프랑크푸르

트) 및 유럽 (아일랜드) 지역에서만 지원됩니다. 자세한 정보는 IAM Identity Center 활성화 을 참조하세요.

> **Note**
>
> AWS Supply Chain 수요 계획 및 공급 계획은 유럽 (아일랜드) 지역에서 지원되지 않습니다.

> **Note**
>
> 여기에 나열된 지역 이외의 지역에서 IAM Identity Center를 활성화하지 않은 경우 AWS Supply Chain 인스턴스를 생성할 수 없습니다.

- AWS Identity and Access Management (IAM) 콘솔에서 IAM 사용자를 생성할 수 있습니다. 자세한 정보는 AWS 계정 설정하기을 참조하세요.
- IAM ID 센터에 액세스해야 AWS Supply Chain 하는 사용자를 추가합니다. 자세한 정보는 IAM Identity Center에서 사용자 추가을 참조하세요. 또한 Active Directory를 IAM Identity Center에 연결할 수도 있습니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 Connect to a Microsoft AD directory 단원을 참조하세요.
- Microsoft Active Directory를 사용하는 경우 Active Directory 동기화가 활성화되어 있는지 확인합니다.
- 인스턴스를 생성하려면 AWS Key Management Service (AWS KMS) 가 필요합니다. AWS Supply Chain 이를 AWS KMS key 사용하여 들어오는 AWS Supply Chain모든 데이터를 암호화합니다.

AWS Supply Chain 콘솔 사용

> **Note**
>
> 계정이 AWS 조직의 구성원 AWS 계정이고 서비스 제어 정책 (SCP) 이 포함된 경우 조직의 SCP가 구성원 계정에 다음 권한을 부여하는지 확인하세요. 다음 권한이 조직의 SCP 정책에 포함되어 있지 않으면 AWS Supply Chain 인스턴스 생성이 실패합니다.

AWS Supply Chain 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 AWS Supply Chain 리소스의 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보

다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

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

사용자와 역할이 AWS Supply Chain 콘솔을 계속 사용할 수 있도록 하려면 엔티티에 AWS Supply Chain `ConsoleAccess` 또는 `ReadOnly` AWS 관리형 정책도 연결하세요. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

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:DescribeOrganization",
```

```
                "organizations:CreateOrganization",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:CreateGrant",
                "kms:RetireGrant",
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "sso:StartPeregrine",
                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetPeregrineStatus",
                "sso:GetSSOStatus",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:AssociateProfile",
                "sso:AssociateDirectory",
                "sso:RegisterRegion",
                "sso:StartSSO",
                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:GetManagedApplicationInstance",
```

```
                "sso-directory:SearchUsers"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

인스턴스 생성

> **Note**
>
> AWS 계정내에서 인스턴스를 최대 10개까지 생성할 수 있습니다. 10개의 인스턴스에는 활성 인스턴스와 초기화 중인 인스턴스가 포함됩니다. IAM Identity Center (Single AWS Sign-On의 후속) 를 이미 활성화한 경우, IAM Identity Center를 활성화한 AWS 리전 곳과 동일한 곳에 AWS Supply Chain 인스턴스를 생성해야 합니다. AWS Supply Chain 지역 간 IAM ID 센터 호출을 지원하지 않습니다.

AWS Supply Chain 인스턴스를 생성하려면 다음 단계를 따르십시오.

> **Note**
>
> AWS Management Console 관리자만 인스턴스를 만들 수 있습니다. AWS Supply Chain 인스턴스를 생성하는 AWS Management Console 관리자는 아래에 나열된 모든 권한을 가져야 AWS Supply Chain 콘솔 사용 합니다. 이 관리자는 IAM 사용자를 관리할 AWS Supply Chain AWS Supply Chain관리자로 초대해야 합니다.

1. 에서 AWS Supply Chain https://console.aws.amazon.com/scn/home 콘솔을 엽니다.
2. 필요한 경우 AWS 리전을 변경합니다. 콘솔 창 상단의 표시줄에서 리전 선택 목록을 열고 리전을 선택합니다. 리전에 관한 자세한 내용은 IAM 사용 설명서의 Regions and endpoints 단원을 참조하세요. 또한 Amazon Web Services 일반 참조의 리전 및 엔드포인트도 참조하세요.

> **Note**
>
> AWS Supply Chain 미국 동부 (버지니아 북부), 미국 서부 (오레곤), 유럽 (프랑크푸르트) 아시아 태평양 (시드니) 지역 및 유럽 (아일랜드) 지역에서만 지원됩니다.
> AWS Supply Chain 수요 계획 및 공급 계획은 유럽 (아일랜드) 지역에서 지원되지 않습니다.

3. AWS Supply Chain 대시보드에서 인스턴스 생성을 선택합니다.
4. 인스턴스 속성 페이지에 다음 정보를 입력합니다.
   - AWS 지역 - IAM ID 센터를 활성화한 지역을 선택합니다. 리전을 변경하려면 오른쪽 상단의 드롭다운 메뉴에서 리전 선택을 선택합니다. 인스턴스를 생성한 후에는 리전을 변경할 수 없습니다.
   - 이름 – 인스턴스 이름을 입력합니다.
   - (선택 사항) 설명 - 인스턴스에 대한 설명을 입력합니다.
5. AWS KMS 키에서 KMS 키를 입력하고 다음과 같이 KMS 키 정책을 업데이트합니다.

> **Note**
>
> 애플리케이션 관리자가 AWS Supply Chain 인스턴스에 사용자를 추가하면 해당 사용자는 AWS KMS key에 액세스할 수 있습니다. 사용자 권한을 관리하여 사용자를 추가하거나 제거할 수 있습니다. 사용자 권한에 대한 자세한 내용은 사용자 권한 역할 단원을 참조하세요.

> **Note**
>
> *## YourAccountNumber*, *YourInstanceID#* 사용자, AWS 지역 AWS 계정, AWS Supply Chain 인스턴스 ID 및 AWS KMS 키로 바꾸십시오. *YourKmsKeyArn*

```
{
"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"
                }

            }
        }
    ]
}
```

KMS 키가 없으면 생성을 선택하여 이 키를 생성할 수 있는 AWS KMS 콘솔로 이동합니다. 이전 KMS 키 정책을 사용합니다. KMS 키 생성 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 생성 단원을 참조하세요.

S/4 Hana 데이터 연결을 사용하려는 경우 제공한 KMS 키에 관련 값이 true인 aws-supply-chain-access태그가 있는지 확인하십시오.

6. (선택 사항) 인스턴스 태그에서 새 태그 추가를 선택하여 인스턴스에 태그를 할당합니다. 이 태그를 사용하여 인스턴스를 식별할 수 있습니다. 태그에 대한 자세한 내용은 Creating tags 단원을 참조하세요.
7. 인스턴스 생성을 선택합니다.

   AWS Supply Chain 인스턴스를 생성하는 데 약 2~3분이 소요됩니다. 인스턴스가 생성되면 AWS Supply Chain 대시보드의 Status 필드가 Active로 표시됩니다.
8. AWS Supply Chain 인스턴스가 생성되면 AWS KMS 키에 액세스할 수 AWS Supply Chain 있도록 KMS 정책을 업데이트하십시오.

> **Note**
>
> *YourInstanceID# AWS Supply Chain #### ID#* 바꾸십시오. AWS Supply Chain 콘솔 대시보드에서 인스턴스 ID를 찾을 수 있습니다.

```
        {
    "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": "*"
},
{
    "Sid": "Enable ASC to backfill KMS permissions",
    "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":"YourKmsKeyArn"
}
```

IAM Identity Center 활성화

사용을 AWS Supply Chain시작하기 전에 ID 소스에 연결해야 합니다. 자세한 내용은 IAM 사용 설명서의 IAM 시작하기 단원을 참조하세요.

IAM Identity Center에서 사용자 추가

IAM ID 센터 서비스를 AWS Supply Chain 사용하기 위한 사용자를 관리할 수 있습니다. IAM Identity Center는 클라우드 기반 IAM ID 센터 서비스로, 모든 애플리케이션 및 클라우드 애플리케이션에 대한 IAM Identity Center 액세스를 중앙에서 편리하게 관리할 수 AWS 계정 있습니다. IAM 사용자를 추가하려면 IAM 사용 설명서의 AWS 계정에서 IAM 사용자 생성 단원을 참조하세요.

IAM 사용자 그룹 생성에 대한 자세한 내용은 IAM 사용 설명서의 IAM 사용자 그룹 생성 단원을 참조하세요.

> **Note**
>
> 사용자를 추가하려면 사용자는 IAM AWS Supply Chain ID 센터 그룹에 속해야 합니다.

AWS Supply Chain 애플리케이션 소유자 선택

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

인스턴스가 생성되고 ID 소스가 연결되면 다음 단계에 따라 AWS Supply Chain 애플리케이션 소유자를 선택합니다.

1. AWS Supply Chain 콘솔 대시보드의 애플리케이션 소유자 아래에서 애플리케이션 소유자 할당을 선택합니다.
2. 애플리케이션 소유자 선택에서 AWS Supply Chain 애플리케이션 소유자로 활동할 사용자를 선택합니다. 사용자 이름만 검색할 수 있으며, 검색 기준과 일치하는 사용자가 표시됩니다.

   더 많은 사용자를 추가하려면 IAM Identity Center로 이동을 선택합니다. 사용자 추가에 대한 자세한 내용은 IAM Identity Center에서 사용자 추가 단원을 참조하고, 사용자 권한 역할에 대한 자세한 내용은 사용자 권한 역할 단원을 참조하세요.

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

3. 초대 전송을 선택합니다.

   AWS Supply Chain 콘솔 대시보드에서 애플리케이션 소유자 아래에 사용자가 나열되어 있는 것을 볼 수 있습니다.
4. AWS Supply Chain 웹 애플리케이션에서 AWS Supply Chain사용자를 추가 및 제거하려면 [Manage in] 을 선택합니다.

그룹 할당

애플리케이션 소유자 또는 AWS Supply Chain 관리자는 IAM Identity Center 그룹에 속한 사용자만 추가할 수 있습니다. AWS Supply Chain

1. AWS Supply Chain 콘솔 대시보드의 그룹에서 그룹 할당을 선택합니다.

   그룹 페이지가 나타납니다.
2. 그룹 이름에서 액세스할 수 있는 사용자가 있는 그룹을 선택하고 AWS Supply Chain 할당을 선택합니다.

   AWS Supply Chain 대시보드의 그룹 아래에 나열한 그룹이 표시됩니다.
3. 그룹 관리를 선택하여 IAM Identity Center에 새 그룹을 추가할 수 있습니다. IAM Identity Center에 그룹을 추가하면 해당 그룹은 AWS Supply Chain의 그룹 이름 아래에 나열됩니다.

AWS 공급망 웹 애플리케이션에 로그인

AWS Supply Chain 관리자는 AWS Supply Chain 웹 애플리케이션에 대한 이메일 초대를 받았어야 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.

AWS Supply Chain 처음으로 로그인하기

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

AWS Supply Chain 관리자로 AWS Supply Chain 웹 애플리케이션에 로그인한 후 다음 단계에 따라 설정을 완료하십시오.

1. 프로필 작성 페이지에서 직책 및 시간대를 입력합니다. 다음을 선택합니다.
2. 조직 정보 추가 페이지에서 조직 이름을 입력하고 본사 위치를 선택합니다. 필요에 따라 회사 로고를 추가할 수 있습니다. 다음을 선택합니다.
3. AWS Supply Chain의 팀원 설정 페이지에서 AWS Supply Chain 웹 애플리케이션에 액세스할 수 있게 할 사용자를 선택합니다. [Invite Users]를 선택합니다. IAM Identity Center에 사용자를 추가

하는 방법에 대한 자세한 내용은 IAM Identity Center에서 사용자 추가 단원을 참조하세요. AWS Supply Chain 사용자 권한 역할에 대한 자세한 내용은 을 참조하십시오사용자 권한 역할.

4. 나중에 사용자를 추가하려는 경우 지금은 건너뛰기를 선택할 수 있습니다.

   온보딩 완료 페이지가 나타납니다.

5. 추가한 각 사용자는 다음으로 이동하는 링크가 포함된 이메일 메시지를 받거나 AWS Supply Chain, 링크 복사를 선택하여 사용자에게 링크를 보낼 수 있습니다.
6. AWS Supply Chain 대시보드를 보려면 홈페이지로 이동을 선택합니다.

계정 프로필 업데이트

AWS Supply Chain 웹 애플리케이션에서 언제든지 계정 프로필을 업데이트할 수 있습니다. 다음 단계에 따라 계정을 업데이트합니다.

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

AWS Supply Chain 웹 애플리케이션에서 언제든지 조직 프로필을 업데이트할 수 있습니다. 다음 단계에 따라 조직 프로필을 업데이트합니다.

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

AWS Supply Chain 관리자는 기본 사용자 권한 역할을 사용하거나 사용자 지정 권한 역할을 만들 수 있습니다. AWS Supply Chain 에는 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.
- Planner - 예측, 재정의를 생성, 확인, 관리하고 수요 계획을 게시할 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 사항을 참고하십시오.
>
> - 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 역할 아래의 모든 사용자는 액세스 권한을 잃게 AWS Supply Chain됩니다.
> - 에서는 그룹 추가가 지원되지 않습니다 AWS Supply Chain.

주제

- 사용자 추가
- 사용자 권한 업데이트
- 사용자 삭제

사용자 추가

> **Note**
>
> 사용자를 추가하기 전에 사용자가 IAM Identity Center 그룹에 속해 있고 그룹이 할당되었는지 확인하십시오. AWS Supply Chain

AWS Supply Chain 관리자는 AWS Supply Chain 웹 애플리케이션에 액세스할 사용자를 추가할 수 있습니다. 다음 단계에 따라 사용자를 추가합니다.

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

   사용자 관리 페이지가 나타납니다.
3. 새 사용자 추가를 선택합니다.

   사용자 추가 페이지가 나타납니다.
4. 사용자 추가 드롭다운 메뉴에서 사용자를 선택하고 역할 선택에서 사용자의 역할을 선택합니다.
5. 추가를 선택합니다.

사용자 권한 업데이트

현재 AWS Supply Chain 사용자의 사용자 권한 역할을 업데이트할 수 있습니다. 다음 단계에 따라 사용자 권한 역할을 업데이트합니다.

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 업데이트하려는 사용자 또는 그룹을 선택하고 권한 역할 드롭다운 메뉴에서 아래 권한 역할 중 하나를 선택합니다.

   > **Note**
   >
   > 할당한 역할 권한에 따라 AWS Supply Chain 대시보드가 사용자 지정됩니다. 자세한 정보는 사용자 지정 사용자 권한 역할 생성을 참조하세요.

- 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.
- Planner - 예측, 재정의를 생성, 확인, 관리하고 수요 계획을 게시할 수 있는 액세스 권한입니다.

4. 저장을 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.

> **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.

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.

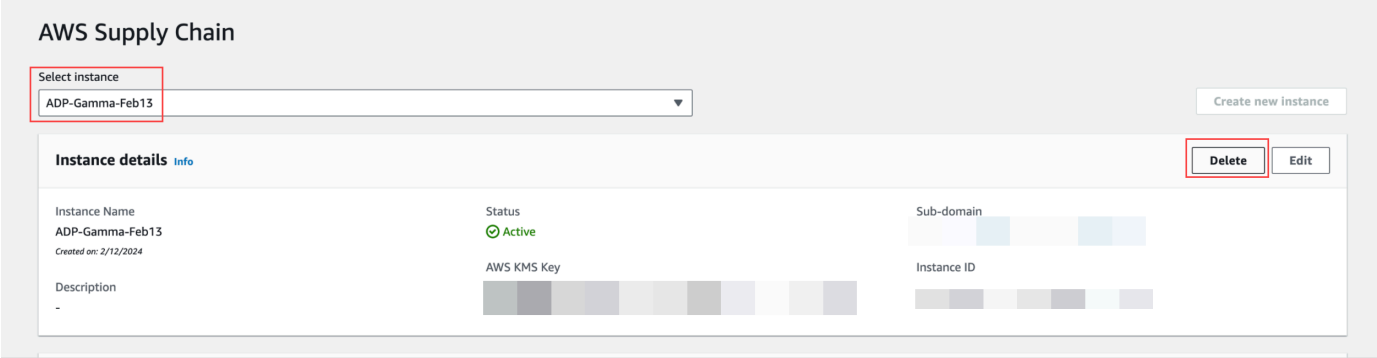
3. 권한 역할 관리 페이지의 역할 이름 아래에 이름을 입력합니다.
4. 슬라이더를 움직여 사용자 권한 역할을 선택합니다.
   - 관리 - 사용자에게 관리 권한을 할당하면 정보를 추가, 편집, 관리할 수 있습니다.
   - 보기 - 사용자에게 보기 권한을 할당하면 현재 정보만 볼 수 있습니다.
5. 위치 액세스에서 검색 창에 입력하는 대로 리전을 검색하고 리전을 선택합니다.
6. 제품 액세스에서 검색 창에 입력하는 대로 제품을 검색하고 제품을 선택합니다.
7. 저장을 선택합니다.

인스턴스 삭제

인스턴스를 삭제하려면 다음 단계를 사용하십시오.

> **Note**
>
> 인스턴스를 삭제할 때 Amazon S3 버킷의 정보는 자동으로 삭제되지 않습니다.

1. 에서 AWS Supply Chain 콘솔을 엽니다https://console.aws.amazon.com/scn/home.
2. AWS Supply Chain 콘솔 대시보드의 드롭다운에서 삭제하려는 인스턴스를 선택합니다.



3. 삭제를 선택합니다.
4. AWS Supply Chain 인스턴스 삭제 페이지의 확인에서 인스턴스를 **`delete`** 삭제할지 여부를 입력하여 확인합니다.
5. 삭제를 선택합니다. 인스턴스 삭제가 시작되고 인스턴스가 삭제되면 확인 메시지가 표시됩니다.

보안 내부 AWS Supply Chain

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 AWS 구축된 데이터 센터 및 네트워크 아키텍처를 활용할 수 있습니다.

보안은 AWS와 사용자의 공동 책임입니다. 공동 책임 모델에서는 이를 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 AWS 보안은 클라우드 내에서 실행되는 인프라를 보호하는 역할을 합니다. AWS 서비스 AWS 클라우드 AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 준수 프로그램별 범위 내 AWS 서비스 규정 준수 프로그램별 참조하십시오. AWS Supply Chain
- 클라우드에서의 보안 — AWS 서비스 사용하는 방식에 따라 책임이 결정됩니다. 또한 사용자는 데이터의 민감도, 요구 사항, 관련 법률 및 규정을 비롯한 다른 요인에 대해서도 책임이 있습니다.

이 설명서는 AWS Supply Chain 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 AWS Supply Chain 충족하도록 구성하는 방법을 보여줍니다. 또한 AWS Supply Chain 리소스를 모니터링하고 보호하는 데 도움이 AWS 서비스 되는 기타 도구를 사용하는 방법도 알아봅니다.

주제

- 의 데이터 보호 AWS Supply Chain
- 인터페이스 엔드포인트를 AWS Supply Chain 사용한 액세스 (AWS PrivateLink)
- IAM에 대한 AWS Supply Chain
- AWS Supply Chain의 AWS 관리형 정책
- AWS Supply Chain의 규정 준수 검증
- AWS Supply Chain의 복원성
- 로깅 및 모니터링 AWS Supply Chain

의 데이터 보호 AWS Supply Chain

AWS 공동 책임 모델 의 데이터 보호에 적용됩니다 AWS Supply Chain. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 이 인프라에서 호

스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 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. 이 방식을 사용하면 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 리소스와 통신할 수 있습니다. AWS TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하여 Amazon S3에 저장된 민감한 데이터를 검색하고 보호합니다.
- 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 Federal Information Processing Standard(FIPS) 140-2를 참조하십시오.

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

AWS Supply Chain에서 처리된 데이터

특정 AWS 공급망 인스턴스의 승인된 사용자가 액세스할 수 있는 데이터를 제한하기 위해 공급망 내에 보관되는 데이터는 AWS 계정 ID와 AWS 공급망 인스턴스 ID로 분리됩니다. AWS

AWS 공급망은 사용자 정보, 데이터 커넥터에서 추출한 정보, 재고 세부 정보 등 다양한 공급망 데이터를 처리합니다.

옵트아웃 기본 설정

AWS는 AWS 서비스 약관에 명시된 대로 처리하는 사용자 콘텐츠를 사용하고 저장할 수 있습니다. AWS Supply Chain콘텐츠 사용 또는 저장을 AWS Supply Chain 거부하려면 AWS Organizations에서 옵트아웃 정책을 생성할 수 있습니다. 옵트아웃 정책 생성에 대한 자세한 내용은 AI 서비스 옵트아웃 정책 구문 및 예를 참조하십시오.

저장 중 암호화

PII로 분류된 연락처 데이터 또는 저장되는 고객 콘텐츠를 나타내는 데이터는 저장 시 (즉, 디스크에 저장, 저장 또는 저장되기 전) 시간 제한이 있고 해당 인스턴스에만 적용되는 키를 사용하여 암호화됩니다. AWS Supply Chain AWS Supply Chain

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 KMS keys무엇입니까를 참조하십시오. AWS Key Management Service AWS Key Management Service 개발자 안내서에서

> **Note**
>
> AWS Supply Chain 기능 공급 계획 및 N-Tier 가시성은 제공된 KMS-CMK를 data-at-rest 사용한 암호화를 지원하지 않습니다.

전송 중 암호화

AWS 공급망과 교환되는 데이터는 업계 표준 TLS 암호화를 사용하여 사용자의 웹 브라우저와 AWS 공급망 간에 전송되는 동안 보호됩니다.

키 관리

AWS Supply Chain KMS-CMK를 부분적으로 지원합니다.

AWS KMS 키 업데이트에 대한 자세한 내용은 을 참조하십시오. AWS Supply Chain인스턴스 생성

인터네트워크 트래픽 개인 정보 보호

> **Note**
>
> AWS Supply Chain 지원하지 PrivateLink 않습니다.

의 가상 사설 클라우드 (VPC) 엔드포인트는 AWS Supply Chain 연결만 허용하는 VPC 내의 논리적 개체입니다. AWS Supply Chain VPC는 요청을 VPC로 AWS Supply Chain 라우팅하고 응답을 VPC로 다시 라우팅합니다. 자세한 내용은 VPC 사용 설명서의 VPC 엔드포인트를 참조하십시오.

에서 권한 부여를 사용하는 방법 AWS Supply ChainAWS KMS

AWS Supply Chain 고객 관리 키를 사용하려면 허가가 필요합니다.

AWS Supply Chain CreateInstance작업 중에 전달된 AWS KMS 키를 사용하여 여러 권한 부여를 생성합니다. AWS Supply Chain 에 CreateGrant요청을 보내 사용자를 대신하여 권한 부여를 생성합니다 AWS KMS. 권한 AWS KMS 부여는 고객 계정의 AWS KMS 키에 AWS Supply Chain 대한 액세스 권한을 부여하는 데 사용됩니다.

> **Note**
>
> AWS Supply Chain 자체 인증 메커니즘을 사용합니다. 사용자를 추가한 후에는 AWS KMS 정책을 사용하여 동일한 사용자 등록을 거부할 수 없습니다. AWS Supply Chain

AWS Supply Chain 부여를 사용하는 용도는 다음과 같습니다.

- 인스턴스에 저장된 데이터를 GenerateDataKey AWS KMS 암호화하라는 요청을 전송하기 위함입니다.
- 인스턴스와 연결된 암호화된 데이터를 읽기 위해 Decrypt 요청을 로 전송합니다. AWS KMS
- Amazon Forecast와 같은 다른 AWS 서비스로 데이터를 전송할 때 데이터를 안전하게 유지하기 위해 DescribeKeyCreateGrant, 및 RetireGrant권한을 추가합니다.

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

암호화 모니터링 대상 AWS Supply Chain

다음은 고객 관리 키로 암호화된 데이터에 `Decrypt` AWS Supply Chain 액세스하기 위해 호출한 `EncryptGenerateDataKey`, KMS 작업 모니터링 AWS CloudTrail 이벤트의 예입니다.

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)

를 AWS PrivateLink 사용하여 VPC와 간에 프라이빗 연결을 생성할 수 있습니다. AWS Supply Chain 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 연결을 사용하지 않고도 VPC에 있는 AWS Supply Chain 것처럼 액세스할 수 있습니다. AWS Direct Connect 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 서비스AWS PrivateLink 액세스를 참조하십시오.

고려 사항 AWS Supply Chain

에 대한 AWS Supply Chain 인터페이스 엔드포인트를 설정하기 전에 AWS PrivateLink 가이드의 고려 사항을 검토하십시오.

AWS Supply Chain 인터페이스 엔드포인트를 통해 모든 API 작업에 대한 호출을 지원합니다.

에 대한 인터페이스 엔드포인트를 생성합니다. AWS Supply Chain

Amazon VPC 콘솔 또는 AWS Command Line Interface () AWS Supply Chain AWS CLI 를 사용하기 위한 인터페이스 엔드포인트를 생성할 수 있습니다. 자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트 생성을 참조하십시오.

다음 서비스 이름을 AWS Supply Chain 사용하기 위한 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 에 API 요청을 할 수 있습니다. 예를 들어 *scn*.*region*.amazonaws.com입니다.

인터페이스 엔드포인트에 엔드포인트 정책 생성

엔드포인트 정책은 인터페이스 인터페이스 엔드포인트에 연결할 수 있는 IAM 리소스입니다. 기본 엔드포인트 정책은 인터페이스 엔드포인트를 AWS Supply Chain 통한 전체 액세스를 허용합니다. AWS

Supply Chain VPC에서 허용된 액세스를 제어하려면 인터페이스 엔드포인트에 사용자 지정 엔드포인트 정책을 연결하십시오.

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 참조하세요.

예: 작업에 대한 VPC 엔드포인트 정책 AWS Supply Chain

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":"*"
      }
   ]
}
```

IAM에 대한 AWS Supply Chain

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 Supply Chain IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- IAM의 AWS Supply Chain 작동 방식
- AWS Supply Chain에 대한 자격 증명 기반 정책 예시
- ID 및 액세스 문제 해결 AWS Supply Chain

고객

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

서비스 사용자 - AWS Supply Chain 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS Supply Chain 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AWS Supply Chain의 기능에 액세스할 수 없는 경우 ID 및 액세스 문제 해결 AWS Supply Chain을 참조하세요.

서비스 관리자 — 회사에서 AWS Supply Chain 리소스를 담당하는 경우 전체 액세스 권한이 있을 수 AWS Supply Chain있습니다. 서비스 사용자가 액세스해야 하는 AWS Supply Chain 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 Supply Chain알아보려면 을 참조하십시오IAM의 AWS Supply Chain 작동 방식.

IAM 관리자 - IAM 관리자라면 AWS Supply Chain에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 AWS Supply Chain ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Supply Chain에 대한 자격 증명 기반 정책 예시

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 AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더

레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하십시오.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하십시오.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 보안 인증이 있는 IAM 사용자를 생성하는 대신 임시 보안 인증을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

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

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

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 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 생성 단원을 참조하십시오. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 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 방법입

니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 계정 간 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

- 서비스 간 액세스 — 일부는 다른 기능을 사용합니다. AWS 서비스 AWS 서비스예를 들어 서비스에서 직접적 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자

또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

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` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

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 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 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.

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. 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 가이드의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 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 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하십시오.

여러 정책 타입

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

IAM의 AWS Supply Chain 작동 방식

IAM을 사용하여 액세스를 AWS Supply Chain관리하기 전에 어떤 IAM 기능과 함께 사용할 수 있는지 알아보세요. AWS Supply Chain

함께 사용할 수 있는 IAM 기능 AWS Supply Chain

IAM 특성	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
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	아니요

AWS Supply Chain 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

아이덴티티 기반 정책은 다음과 같습니다. AWS Supply Chain

보안 인증 기반 정책 지원	예

자격 증명 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 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

다음에 대한 ID 기반 정책 예제 AWS Supply Chain

AWS Supply Chain ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Supply Chain에 대한 자격 증명 기반 정책 예시

내 리소스 기반 정책 AWS Supply Chain

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 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 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 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 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

에 대한 정책 조치 AWS Supply Chain

정책 작업 지원	예

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 Supply Chain 사용합니다.

```
scn
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

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

AWS Supply Chain ID 기반 정책의 예를 보려면 을 참조하십시오. 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 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 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 ID 기반 정책의 예를 보려면 을 참조하십시오. 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 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 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` 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예컨대, 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 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

AWS Supply Chain 자격 증명 기반 정책의 예를 보려면 을 참조하십시오. AWS Supply Chain에 대한 자격 증명 기반 정책 예시

다음과 같은 임시 자격 증명 사용 AWS Supply Chain

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 일부 자격 증명이 AWS 서비스 작동하지 않습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하십시오.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하십시오.

전달 액세스 세션 대상 AWS Supply Chain

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하기 위한 요청과 함께 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AWS Supply Chain의 서비스 역할

서비스 역할 지원	예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.

> **Warning**
>
> 서비스 역할의 권한을 변경하면 AWS Supply Chain 기능이 중단될 수 있습니다. 서비스 역할을 편집하기 위한 지침이 AWS Supply Chain 제공되는 경우에만 서비스 역할을 편집하십시오.

서비스 연결 역할은 다음과 같습니다. AWS Supply Chain

서비스 연결 역할 지원	아니요

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

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 Yes(네) 링크를 선택합니다.

AWS Supply Chain에 대한 자격 증명 기반 정책 예시

기본적으로 사용자와 역할에는 리소스를 만들거나 수정할 AWS Supply Chain 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

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

- 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 줄이

는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 대한AWS 관리형 정책을 참조하십시오.

- 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 설명서의 IAM의 정책 및 권한을 참조하십시오.
- 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 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 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 Analyzer 정책 검증을 참조하십시오.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하십시오.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하십시오.

ID 및 액세스 문제 해결 AWS Supply Chain

다음 정보를 사용하면 및 IAM을 사용할 때 발생할 수 있는 일반적인 문제를 AWS Supply Chain 진단하고 해결하는 데 도움이 됩니다.

주제

- 저는 다음과 같은 작업을 수행할 권한이 없습니다. AWS Supply Chain
- 저는 iam을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 내 AWS Supply Chain 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

저는 다음과 같은 작업을 수행할 권한이 없습니다. AWS Supply Chain

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

다음 예제 오류는 mateojacksonIAM 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* 작업을 사용하여 scn:*GetWidget* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

저는 iam을 수행할 권한이 없습니다. PassRole

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AWS Supply Chain에 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 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 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 AWS Supply Chain 리소스에 액세스할 수 있도록 AWS 계정 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 참조하십시오.

- 이러한 기능의 AWS Supply Chain 지원 여부를 알아보려면 을 참조하십시오IAM의 AWS Supply Chain 작동 방식.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서에서 자신이 소유한 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 페더레이션)을 참조하십시오.
- 교차 계정 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

AWS Supply Chain의 AWS 관리형 정책

AWS 관리형 정책은 AWS에 의해 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있기 때문에 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에서 정의한 권한은 변경할 수 없습니다. AWS에서 AWS 관리형 정책에 정의된 권한을 업데이트할 경우 정책이 연결되어 있는 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에도 업데이트가 적용됩니다. 새로운 AWS 서비스를 시작하거나 새로운 API 작업을 기존 서비스에 이용하는 경우 AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSSupplyChainFederationAdminAccess

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

이 정책은 scn:* 권한을 통해 AWS Supply Chain에 대한 모든 액세스 권한을 제공하지만, AWS Supply Chain 역할에 따라 권한이 결정됩니다. AWS Supply Chain 역할에는 필수 권한만 포함되며 관리 API에 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 Center 애플리케이션 인스턴스와 연결된 사용자 프로필 및 목록 프로필을 연결하고 연결 해제하는 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-suply-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, kms:Decrypt)은 Amazon AppFlow로 제한되지 않으며 이러한 권한은 계정의 AWS KMS 키에 부여될 수 있습니다.

이 정책의 권한을 보려면 AWS Management Console에서 AWSSupplyChainFederationAdminAccess를 확인하세요.

AWS 관리형 정책으로 AWS Supply Chain 업데이트

다음 표에는 이 서비스가 해당 변경 사항을 추적하기 시작한 이후 AWS Supply Chain에 대한 AWS 관리형 정책 업데이트와 관련한 세부 정보가 나와 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 Chain은 페더레이션 사용자가 IAM Identity Center의 ListProfileAssociations 작업에 액세스할 수 있도록 관리형 정책을 업데이트했습니다.	2023년 11월 1일
AWSSupplyChainFederationAdminAccess – 정책 업데이트	AWS Supply Chain은 페더레이션 사용자가 arn:aws:s3:::aws-supply- chain-data-* 리소스 ARN을 사용하여 전용 S3 버킷의 PutObject 및 GetObject 작업에 액세스할 수 있도록 관리형 정책을 업데이트했습니다.	2023년 9월 21일
AWSSupplyChainFederationAdminAccess – 새 정책	AWS Supply Chain은 페더레이션 사용자가 AWS Supply Chain 애플리케이션에 액세스할 수 있도록 새 정책을 추가했	2023년 3월 1일

변경 사항	설명	날짜
	습니다. 여기에는 AWS Supply Chain 애플리케이션 내에서 작업을 수행하는 데 필요한 권한이 포함됩니다.	
AWS Supply Chain에서 변경 사항 추적 시작	AWS Supply Chain가 AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2023년 3월 1일

AWS Supply Chain의 규정 준수 검증

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

특정 규정 준수 프로그램의 범위에 속하는 AWS 서비스 목록은 규정 준수 프로그램 제공 AWS 범위 내 서비스를 참조하세요. 일반적인 정보는 AWS 규정 준수 프로그램을 참조하세요.

AWS Artifact를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact에서 보고서 다운로드를 참조하세요.

AWS Supply Chain 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 결정됩니다. AWS에서는 규정 준수를 지원할 다음과 같은 리소스를 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 기술 백서 아키텍팅 - 이 백서는 기업에서 AWS를 사용하여 HIPAA를 준수하는 애플리케이션을 생성하는 방법을 설명합니다.
- AWS 규정 준수 리소스 - 고객 조직이 속한 산업 및 위치에 적용될 수 있는 워크북 및 가이드 콜렉션입니다.
- AWS Config 개발자 안내서의 Evaluating Resources with Rules - 이 안내서에서는 리소스 구성이 내부 사례, 업계 지침, 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - 이 AWS 서비스는 보안 산업 표준 및 모범 사례 규정 준수 여부를 확인하는 데 도움이 되도록 AWS 내 보안 상태를 종합적으로 보여줍니다.

AWS Supply Chain의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 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 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 정보는 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라 뿐만 아니라 AWS Supply Chain도 데이터 복원력과 백업 요구 사항을 지원하는 다양한 기능을 제공합니다.

로깅 및 모니터링 AWS Supply Chain

로깅 및 모니터링은 AWS 공급망 및 기타 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. AWS AWS 공급망을 감시하고, 문제 발생 시 보고하고, 적절한 경우 자동 조치를 취할 수 있는 AWS CloudTrail 모니터링 도구를 제공합니다.

> **Note**
>
> AWS Supply Chain 콘솔에서만 호출되는 API는 에서 AWS CloudTrail캡처됩니다.

AWS CloudTrail은 직접 수행하거나 AWS 계정 을 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.com에서 AWS 공급망 이벤트를 볼 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

> **Note**
>
> 다음 AWS Supply Chain내용을 참고하십시오.
>
> - 액세스 권한이 없는 사용자를 초대하면 해당 사용자는 웹 애플리케이션에서 받는 알림 정보를 받지 못합니다. AWS Supply Chain초대된 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 추가하면 해당 사용자에게 액세스 권한이 AWS KMS key부여됩니다. 사용자 권한을 관리하여 사용자를 추가하거나 제거할 수 있습니다. 사용자 권한에 대한 자세한 내용은 사용자 권한 역할 단원을 참조하세요.

AWS Supply Chain 의 데이터 이벤트 CloudTrail

데이터 이벤트는 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 데이터 이벤트를 기록하지 CloudTrail 않습니다. CloudTrail 이벤트 기록에는 데이터 이벤트가 기록되지 않습니다.

데이터 이벤트에는 추가 요금이 적용됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하십시오.

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

- CloudTrail 콘솔을 사용하여 데이터 이벤트를 기록하려면 트레일 또는 이벤트 데이터 저장소를 생성하여 데이터 이벤트를 기록하거나 기존 트레일 또는 이벤트 데이터 저장소를 업데이트하여 데이터 이벤트를 기록하십시오.

  1. 데이터 이벤트를 선택하여 데이터 이벤트를 기록합니다.
  2. 데이터 이벤트 유형 목록에서 데이터 이벤트를 기록하려는 리소스 유형을 선택합니다.
  3. 사용하려는 로그 선택기 템플릿을 선택합니다. 리소스 유형에 대한 모든 데이터 이벤트를 기록하거나, 모든 이벤트를 기록하거나, 모든 `readOnly` 이벤트를 기록하거나 `readOnlyeventName`, 및 `resources.ARN` 필드를 기준으로 필터링할 사용자 지정 로그 선택기 템플릿을 만들 수 있습니다. `writeOnly`

- 를 사용하여 데이터 이벤트를 기록하려면 필드를 리소스 유형 값과 같게 설정하고 `eventCategory` 필드를 리소스 유형 값과 같게 `Data` 설정하도록 `--advanced-event-selectors` 매개 변수를 구성하십시오. AWS CLI`resources.type` 조건을 추가하여 `readOnlyeventName`, 및 `resources.ARN` 필드의 값을 기준으로 필터링할 수 있습니다.
  - 데이터 이벤트를 기록하도록 트레일을 구성하려면 put-event-selectors명령을 실행합니다. 자세한 내용은 를 사용한 트레일의 데이터 이벤트 로깅을 AWS CLI 참조하십시오.

- 데이터 이벤트를 기록하도록 이벤트 데이터 저장소를 구성하려면 create-event-data-store명령을 실행하여 데이터 이벤트를 기록할 새 이벤트 데이터 저장소를 만들거나 update-event-data-store명령을 실행하여 기존 이벤트 데이터 저장소를 업데이트하십시오. 자세한 내용은 를 사용한 이벤트 데이터 저장소의 데이터 이벤트 로깅을 참조하십시오 AWS CLI.

*고급 이벤트 선택기를 구성하여`eventName`,`readOnly`, `resources.ARN` 필드를 기준으로 필터링하여 중요한 이벤트만 기록하도록 할 수 있습니다. 필드에 대한 자세한 내용은 AdvancedFieldSelector 섹션을 참조하세요.

AWS Supply Chain 의 관리 이벤트 CloudTrail

관리 이벤트는 AWS 계정의 리소스에서 수행되는 관리 작업에 대한 정보를 제공합니다. 이를 제어 영역 작업이라고도 합니다. 기본적으로 관리 이벤트를 CloudTrail 기록합니다.

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

AWS Supply Chain 웹 애플리케이션 API

이 섹션에 나열된 API는 연동 사용자를 대신하여 AWS Supply Chain 애플리케이션에서 호출합니다. 이러한 API는 CloudTrail 로그에 표시되지 않으며 서비스 권한 부여 참조 문서에 캡처되지 않습니다 (참조). AWS Supply Chain 이러한 API에 대한 액세스는 연동 사용자 역할 권한을 기반으로 AWS Supply Chain 애플리케이션에 의해 제어됩니다. 애플리케이션 방해를 방지하기 위해 이러한 API에 대한 액세스를 제어하려고 해서는 안 됩니다. AWS Supply Chain

사용자 역할

에서 사용자, 사용자 역할, 사용자 알림 및 채팅 메시지를 관리하는 데 사용되는 API는 다음과 같습니다. 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:CreateSapODataConnection
scn:CreateUpdateDatasetSchemaJob
scn:DeleteConnection
scn:DeleteDataflow
scn:DeleteExtractFlows
scn:DeleteSapODataConnection
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 확인하는 데 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:ListCustomAttributeValues
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

예측, 수요 계획 또는 AWS Supply Chain 워크북을 생성하고 관리하는 데 사용되는 API는 다음과 같습니다.

```
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

공급 계획을 생성하고 관리하는 데 사용되는 API는 다음과 같습니다. AWS Supply Chain

```
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
```

에 대한 할당량 AWS Supply Chain

AWS 계정 Your에는 각각에 대해 기본 할당량 (이전에는 한도라고 함) 이 있습니다. AWS 서비스 다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다. 계정 수준에 맞게 설정된 리소스의 할당량을 늘리도록 요청할 수 있습니다. 계정 수준 할당량에 대한 자세한 내용은 아래 표를 참조하십시오.

에 대한 AWS Supply Chain 할당량을 보려면 Service Quotas 콘솔을 엽니다. 탐색 창에서 AWS 서비스를 선택하고 AWS Supply Chain을 선택합니다.

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하십시오. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 한도 증가 양식을 사용합니다.

다음과 관련된 AWS 계정 할당량이 있습니다. AWS Supply Chain

Resource	기본값	조정 가능
인스턴스 개수 **Note** 계정 내에서 최대 10개의 인스턴스를 만들 수 있습니다. AWS	10	아니요
Amazon S3 버킷 수	100	아니요
계정 내 활성 초대와 보류 중인 초대 AWS	30	예
계정 내 데이터 요청 AWS	4,000	예
관심 목록별 인사이트 라인 항목	1,000	아니요
계정 내 인스턴스별 인사이트 감시 목록 AWS	1,000	예
계정 내 사용자별 인사이트 관심 목록 AWS	100	예

AWS Supply Chain에 대한 관리 지원 받기

관리자인 경우 AWS Supply Chain에 대한 지원이 필요하면 다음 방법 중 하나를 선택합니다.

- AWS Support 계정이 있는 경우 지원 센터로 이동하여 티켓을 제출합니다.
- AWS Management Console을 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 안내서를 위한 문서 기록

다음 표에는 의 설명서 릴리스가 설명되어 AWS Supply Chain있습니다.

변경 사항	설명	날짜
KMS 정책 업데이트	키에 액세스할 수 AWS Supply Chain 있도록 KMS 정책을 업데이트했습니다. AWS KMS	2024년 3월 18일
PrivateLink 지원	인터페이스 엔드포인트 (AWS PrivateLink) AWS Supply Chain 를 사용하여 액세스할 수 있습니다.	2024년 2월 26일
그룹 추가	사용자가 AWS Supply Chain 에 액세스하려면 IAM Identity Center 그룹에 속해야 합니다.	2023년 11월 14일
업데이트된 AWS 관리형 정책	AWS Supply Chain 연동 사용자가 IAM Identity Center의 ListProfileAssociations 작업에 액세스할 수 있도록 관리형 정책을 업데이트했습니다.	2023년 11월 1일
관리형 정책이 업데이트되었습니다 AWS .	AWS Supply Chain 연동 사용자가 arn:aws:s3: ::aws-supply- chain-data-* 리소스를 사용하여 전용 Amazon S3 버킷의 PutObject 및 GetObject 작업에 액세스할 수 있도록 관리형 정책을 업데이트했습니다.	2023년 9월 21일
리전 지원에 대한 정보 업데이트	AWS Supply Chain 수요 계획은 이제 아시아 태평양 (시드니) 지역에서도 지원됩니다.	2023년 9월 12일

AWS 콘솔을 사용하여 옵트인 및 옵트아웃을 할 수 있습니다. AWS Supply Chain	AWS Supply Chain 이제 사용자는 AWS 콘솔을 사용하여 AWS Organizations에 사용자 콘텐츠를 사용하거나 AWS Supply Chain 저장하기 위해 옵트인 및 옵트아웃할 수 있습니다.	2023년 9월 7일
리전 지원에 대한 정보 업데이트	AWS Supply Chain 이제 아시아 태평양 (시드니) 지역 및 유럽 (아일랜드) 지역에서도 지원됩니다.	2023년 7월 19일
AWS Support에 문의하고 인스턴스를 생성하는 방법에 대한 정보 업데이트	AWS Supply Chain 이제 사용자는 AWS Support에 문의하여 도움을 요청하고 인스턴스 생성 방법에 대한 콘텐츠를 업데이트할 수 있습니다.	2023년 4월 3일
AWS 관리형 정책이 추가되었습니다.	AWS Supply Chain은 Supply Chain 애플리케이션 내에서 작업을 수행하는 데 필요한 권한을 포함하여 연동 사용자가 AWS Supply Chain 애플리케이션에 액세스할 수 있도록 하는 새 정책을 추가했습니다. AWS	2023년 3월 1일
최초 릴리스	AWS Supply Chain 관리자 안내서의 최초 릴리스.	2022년 11월 29일

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