



Add a permission의

AWS Organizations



AWS Organizations: Add a permission의

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

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon 계열사, 관련 업체 또는 Amazon의 지원 업체 여부에 상관없이 해당 소유자의 자산입니다.

Table of Contents

AWS Organizations란 무엇인가요?	1
특성	2
사용 사례	3
용어 및 개념	4
사용 가능한 기능 모음	5
조직 구조	6
초대 및 핸드셰이크	9
조직 정책	10
할당량 및 서비스 한도	11
이름 지정 지침	11
고려 사항	12
최대값 및 최소값	12
핸드셰이크 만료 시간	16
엔터티에 연결할 수 있는 정책 수	17
제한 한계	18
리전 지원	22
사용 가능한 리전 목록	23
결제 및 요금	27
결제 책임	27
결제 구조	27
지원 및 의견	27
기타 AWS 리소스	27
모범 사례	29
계정 및 자격 증명	29
루트 액세스 관리를 활성화하여 멤버 계정의 루트 사용자 자격 증명 관리 단순화	29
연락 전화번호를 최신 상태로 유지하기	30
루트 계정에 그룹 이메일 주소 사용하기	30
조직 구조 및 워크로드	30
단일 조직 내에서 계정 관리	30
보고 구조가 아닌 비즈니스 목적에 따라 워크로드 그룹화	30
여러 계정을 사용하여 워크로드 정리하기	31
서비스 및 비용 관리	31
AWS 서비스 콘솔 또는 API/CLI 작업을 사용하여 조직 수준에서 서비스 활성화	31
결제 도구를 사용하여 비용 추적 및 리소스 사용 최적화	31

조직 리소스 전반의 태그 지정 전략 및 태그 적용 계획	31
시작하기	32
에 가입 AWS	32
에 가입 AWS 계정	32
관리자 액세스 권한이 있는 사용자 생성	33
액세스 AWS Organizations	34
자습서: 조직 생성 및 구성	35
사전 조건	36
1단계: 조직 만들기	37
2단계: 조직 단위 만들기	40
3단계: 서비스 제어 정책 생성	42
4단계: 조직 정책 테스트	46
자습서: Amazon EventBridge를 사용하여 조직 모니터링	47
사전 조건	48
1단계: 추적 및 이벤트 선택기 구성	48
2단계: Lambda 함수 구성	50
3단계: 구독자에게 이메일을 전송하는 Amazon SNS 주제 생성	51
4단계: Amazon EventBridge 규칙 생성	51
5단계: Amazon EventBridge 규칙 테스트	52
정리: 더 이상 필요하지 않은 리소스 제거	54
AWS SDKs 작업	54
전체 조직 관리	56
조직 생성	56
조직 생성	56
이메일 주소 확인	61
이메일 주소 확인	61
확인 이메일 재전송	61
이메일 주소 변경	62
모든 기능 활성화	62
고려 사항	63
표준 마이그레이션 프로세스	64
지원 마이그레이션 프로세스	73
조직 세부 정보 보기	74
조직 삭제	75
고려 사항	75
조직 삭제	76

조직 내 계정 관리	80
관리 계정	80
관리 계정의 모범 사례	81
관리 계정 해지	82
멤버 계정	83
멤버 계정의 모범 사례	84
멤버 계정 생성	86
멤버 계정 액세스	91
멤버 계정 달기	97
해지하지 않도록 멤버 계정 보호	99
멤버 계정 제거	101
멤버 계정에서 조직 탈퇴	106
멤버 계정의 계정 이름 업데이트	110
멤버 계정의 루트 사용자 이메일 업데이트	110
계정 초대	111
고려 사항	112
초대 보내기	113
보류 중인 초대 관리	116
초대 수락 또는 거부	121
계정 마이그레이션	125
사전 마이그레이션	126
마이그레이션	128
마이그레이션 후	128
계정 세부 정보 보기	129
계정 세부 정보 내보내기	131
AWS 계정 조직 내 모든 목록 내보내기	131
계정 상태 모니터링	132
의 상태 보기 AWS 계정	134
계정의 대체 연락처 업데이트	136
계정의 기본 연락처 업데이트	136
AWS 리전 계정 업데이트	136
조직 단위(OU)	137
OU 모범 사례	138
이해 AWS Organizations	138
권장 기본 OU	139
권장 추가 OU	140

결론	142
루트 및 트리 탐색	142
OU 세부 정보 보기	143
OU 생성	145
OU 이름 변경	149
OU 태그 지정	150
OU 간 계정 이동	152
루트 세부 정보 보기	153
OU 삭제	155
조직 정책	158
정책 유형	158
권한 부여 정책	158
관리 정책	159
권한 부여 정책	161
SCP 및 RCP 간의 차이점	161
SCPs 및 RCPs 사용	162
서비스 제어 정책	163
리소스 제어 정책	194
관리 정책	207
사전 조건 및 권한	208
정책 상속 이해	209
유효 정책 보기	224
잘못된 정책 알림	227
선언적 정책	230
백업 정책	251
- 태그 정책	297
채팅 애플리케이션 정책	627
AI 서비스 옵트아웃 정책	641
Security Hub 정책	651
Amazon Bedrock 정책	661
Amazon Inspector 정책	665
롤아웃 정책 업그레이드	677
Amazon S3 정책	691
AWS Shield Network Security Director 정책	695
에 대한 위임된 관리자 AWS Organizations	698
리소스 기반 위임 정책 생성	698

리소스 기반 위임 정책 업데이트	703
리소스 기반 위임 정책 보기	707
리소스 기반 위임 정책 삭제	708
정책 유형 활성화	710
정책 유형 비활성화	711
고려 사항	711
정책 유형 비활성화	712
정책 생성	713
서비스 제어 정책(SCP) 생성	713
리소스 제어 정책(RCP) 생성	718
선언적 정책 생성	722
백업 정책 생성	725
태그 정책 생성	729
채팅 애플리케이션 정책 생성	733
AI 서비스 옵트아웃 정책 생성	737
업그레이드 롤아웃 정책 생성	739
Security Hub 정책 생성	742
정책 업데이트	745
서비스 제어 정책(SCP) 업데이트	745
리소스 제어 정책(RCP) 업데이트	748
선언적 정책 업데이트	751
백업 정책 업데이트	752
태그 정책 업데이트	756
채팅 애플리케이션 정책 업데이트	759
AI 서비스 옵트아웃 정책 업데이트	760
Security Hub 정책 업데이트	763
정책에 연결된 태그 편집	765
서비스 제어 정책(SCP)에 연결된 태그 편집	766
리소스 제어 정책(RCP)에 연결된 태그 편집	767
선언적 정책에 연결된 태그 편집	768
백업 정책에 연결된 태그 편집	769
태그 정책에 연결된 태그 편집	771
채팅 애플리케이션 정책에 연결된 태그 편집	772
AI 서비스 옵트아웃 정책에 연결된 태그 편집	773
Security Hub 정책에 연결된 태그 편집	774
정책 연결	775

정책 연결	776
정책 분리	788
정책 분리	788
정책 세부 정보 가져오기	800
모든 정책 나열	800
연결된 정책 나열	805
모든 연결 나열	807
정책 세부 정보 확인	808
정책 삭제	811
정책 삭제	812
리소스에 태그 지정	819
고려 사항	819
태그 사용	820
태그 추가, 업데이트 및 제거	820
리소스를 생성할 때 리소스에 태그 추가	820
기존 리소스에 대한 태그 추가 또는 업데이트	821
다자간 승인	824
기타 사용 AWS 서비스	825
신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한	826
신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한	827
신뢰할 수 있는 액세스를 활성화 또는 비활성화하는 방법	828
AWS Organizations 및 서비스 연결 역할	830
AWSServiceRoleForDeclarativePoliciesEC2Report 서비스 연결 역할 사용	831
Organizations와 연동되는 서비스	832
AWS Account Management	876
AWS Application Migration Service	879
AWS Artifact	884
AWS Audit Manager	887
AWS Backup	891
AWS 결제 및 비용 관리	893
AWS CloudFormation StackSets	895
AWS CloudTrail	899
Amazon CloudWatch	903
AWS Compute Optimizer	907
AWS Config	911
AWS Cost Optimization Hub	914

AWS Control Tower	918
Amazon Detective	920
Amazon DevOps Guru	923
AWS Directory Service	928
- Amazon Elastic Compute Cloud	930
EC2 용량 관리자	932
Amazon Elastic Kubernetes Service:	937
AWS Firewall Manager	939
Amazon GuardDuty	943
AWS Health	945
AWS Identity and Access Management	949
Amazon Inspector	952
AWS License Manager	956
AWS Managed Services (AMS) 셀프 서비스 보고(SSR)	958
Amazon Macie	961
AWS Marketplace	963
AWS Marketplace 프라이빗 마켓플레이스	966
AWS Marketplace 조달 인사이트 대시보드	970
AWS Network Manager	973
Amazon Q Developer	976
AWS Resource Access Manager	978
AWS Resource Explorer	981
AWS Security Hub CSPM	985
Amazon S3 Storage Lens	988
AWS 보안 인시던트 대응	991
Amazon Security Lake	996
AWS Service Catalog	1000
Service Quotas	1004
AWS IAM Identity Center	1005
AWS Systems Manager	1009
AWS User Notifications	1014
- 태그 정책	1016
AWS Trusted Advisor	1017
AWS Well-Architected Tool	1020
Amazon VPC IP Address Manager(IPAM)	1024
Amazon VPC Reachability Analyzer	1027

통합을 위한 위임된 관리자 AWS 서비스	1030
위임된 관리자 계정에 부여된 권한	1031
보안	1033
AWS PrivateLink	1033
에 AWS PrivateLink 대한의 제한 및 제약 AWS Organizations	1034
VPC 엔드포인트 생성	1034
VPC 엔드포인트 정책 생성	1035
자격 증명 및 액세스 관리	1035
대상	1036
ID를 통한 인증	1036
정책을 사용하여 액세스 관리	1038
AWS Organizations 에서 IAM을 사용하는 방법	1039
조직에 대한 액세스 권한 관리	1044
ID 기반 정책 예시	1053
리소스 기반 정책 예제	1059
AWS 관리형 정책	1069
태그를 사용한 속성 기반 액세스 제어	1073
문제 해결	1078
로깅 및 모니터링	1080
AWS CloudTrail	1080
Amazon EventBridge	1092
규정 준수 확인	1093
복원력	1093
인프라 보안	1093
문제 해결	1095
일반적인 문제 해결	1095
에 요청할 때 "액세스 거부" 메시지가 표시됨 AWS Organizations	1095
임시 보안 자격 증명으로 요청하면 "액세스 거부" 메시지가 표시됩니다	1096
멤버 계정으로 조직을 나가거나 관리 계정으로 멤버 계정을 제거하려고 하면 "액세스 거부" 메시지가 표시됩니다	1096
조직에 계정을 추가하려고 하면 "할당량 초과" 메시지가 표시됩니다.	1096
계정을 추가 또는 제거할 때 "이 작업에는 대기 시간이 필요합니다."라는 메시지가 표시됩니	
다.	1097
조직에 계정을 추가하려고 하면 "조직이 아직 초기화 중임"이라는 메시지가 표시됩니다.	1097
내 조직에 계정을 초대하려고 할 때 "초대장이 비활성화되었습니다."라는 메시지가 표시됩니	
다.	1097

변경 사항이 매번 즉시 표시되는 것은 아닙니다.	1097
이미 조직의 일부인 계정에 액세스하려고 하면 ‘등록 완료’ 메시지가 표시됩니다.	1098
HTTP 쿼리 요청 실행	1099
엔드포인트	1099
HTTPS 필요	1100
AWS Organizations API 요청 서명	1100
코드 예제	1101
기본 사항	1102
작업	1103
시나리오	1143
권한 정책은 AWS Compute Optimizer Automation이 권장 작업을 적용하도록 허용합니다.	1144
조직 전반의 자동화를 활성화하기 위한 권한 정책	1145
계정의 자동화를 활성화하기 위한 권한 정책	1146
조직의 관리 계정에 Compute Optimizer 자동화에 대한 전체 액세스 권한을 부여하기 위한 권 한 정책	1147
독립 실행형 AWS 계정에 대한 Compute Optimizer Automation에 대한 전체 액세스 권한을 부 여하는 권한 정책	1148
조직의 관리 계정에 Compute Optimizer 자동화에 대한 읽기 전용 액세스 권한을 부여하기 위 한 권한 정책	1148
독립 실행형 AWS 계정에 대해 Compute Optimizer Automation에 대한 읽기 전용 액세스 권한 을 부여하는 권한 정책	1149
컴퓨팅 최적화 자동화에 대한 서비스 연결 역할 권한을 부여하는 권한 정책	1150
문서 기록	1152
.....	mclxvi

AWS Organizations란 무엇인가요?

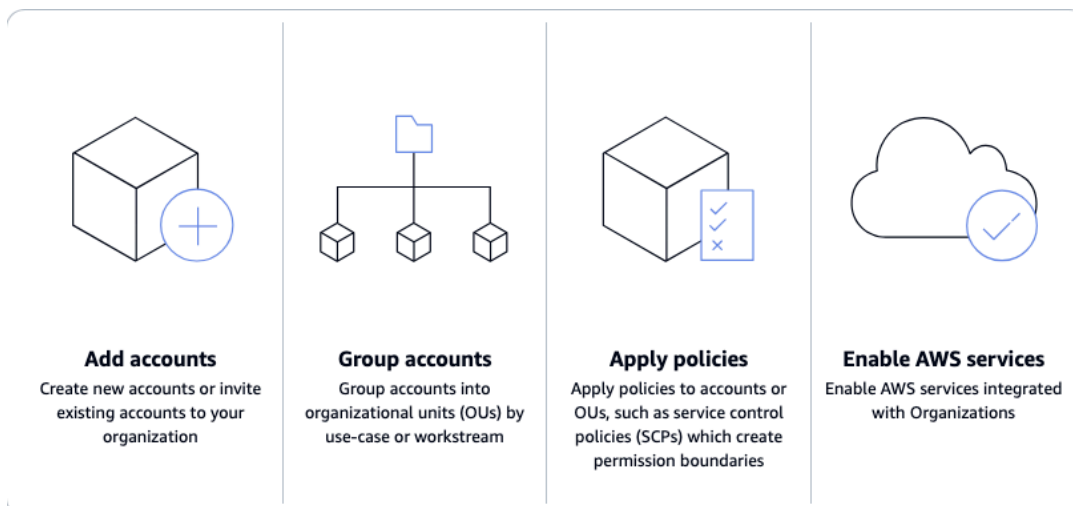
AWS 리소스를 확장할 때 환경을 중앙에서 관리

AWS Organizations 를 사용하면 AWS 리소스를 확장하고 확장할 때 환경을 중앙에서 관리하고 관리할 수 있습니다. Organizations를 사용하면 계정을 만들고 리소스를 할당하며, 계정을 그룹화하여 워크폴로를 구성하고, 거버넌스를 위해 정책을 적용하고, 모든 계정에 대해 단일 결제 방법을 사용하여 청구를 간소화할 수 있습니다.

Organizations는 다른 조직과 통합 AWS 서비스 되므로 조직의 계정 간에 중앙 구성, 보안 메커니즘, 감사 요구 사항 및 리소스 공유를 정의할 수 있습니다. 자세한 내용은 [다른 AWS Organizations 와 함께 사용 AWS 서비스](#) 단원을 참조하십시오.

다음 다이어그램은 AWS Organizations를 사용하는 방법에 대한 자세한 설명을 보여줍니다.

- 계정 추가
- 계정 그룹화
- 정책 적용
- 를 활성화합니다 AWS 서비스.



주제

- [의 기능 AWS Organizations](#)
- [에 대한 사용 사례 AWS Organizations](#)
- [의 용어 및 개념 AWS Organizations](#)

- [AWS Organizations에 대한 할당량 및 서비스 제한](#)
- [예 대한 리전 지원 AWS Organizations](#)
- [예 대한 결제 및 요금 AWS Organizations](#)
- [예 대한 지원 및 피드백 AWS Organizations](#)

의 기능 AWS Organizations

AWS Organizations 는 다음 기능을 제공합니다.

관리 AWS 계정

AWS 계정 는 권한, 보안, 비용 및 워크로드의 자연스러운 경계입니다. 다중 계정 환경을 사용하는 것이 클라우드 환경을 확장할 때 권장되는 모범 사례입니다. AWS Command Line Interface (AWS CLI), SDKs 또는 APIs를 사용하여 프로그래밍 방식으로 새 계정을 생성하여 계정 생성을 간소화하고 [AWS CloudFormation StackSets](#).

조직 정의 및 관리

새 계정을 생성할 때 조직 단위(OU) 또는 단일 애플리케이션 또는 서비스를 제공하는 계정 그룹으로 계정을 그룹화할 수 있습니다. 태그 정책을 적용하여 조직의 리소스를 분류하거나 추적하고 사용자 또는 애플리케이션에 대한 속성 기반 액세스 제어를 제공합니다. 또한 사용자가 조직을 대신하여 관리할 수 있도록 지원되는에 대한 책임을 AWS 서비스 계정에 위임할 수 있습니다.

계정 보안 및 모니터링

보안 팀이 조직을 대신하여 보안 요구 사항을 관리할 수 있도록 도구와 액세스를 중앙에서 제공할 수 있습니다. 예를 들어 계정 간에 읽기 전용 보안 액세스를 제공하고, [Amazon GuardDuty](#)를 사용하여 위협을 탐지 및 완화하고, [IAM Access Analyzer](#)를 사용하여 리소스에 대한 의도하지 않은 액세스를 검토하고, [Amazon Macie](#)를 사용하여 민감한 데이터를 보호할 수 있습니다.

액세스 및 권한 제어

활성 디렉터리를 사용하여 AWS 계정 및 리소스에 대한 액세스를 제공하고 별도의 작업 역할에 따라 권한을 사용자 지정하도록 [AWS IAM Identity Center](#)를 설정합니다. 사용자, 계정 또는 OU에 [조직 정책](#)을 적용할 수도 있습니다. 예를 들어 [서비스 제어 정책\(SCPs\)](#)을 사용하면 조직 내 AWS 리소스, 서비스 및 리전에 대한 액세스를 제어할 수 있습니다. [리소스 제어 정책\(RCPs\)](#)을 사용하면 AWS 리소스의 의도하지 않은 사용을 중앙에서 방지할 수 있습니다. [채팅 애플리케이션 정책](#)을 사용하면 Slack 및 Microsoft Teams와 같은 채팅 애플리케이션에서 조직의 계정에 대한 액세스를 제어할 수 있습니다.

계정 간 리소스 공유

[AWS Resource Access Manager \(AWS RAM\)](#)를 사용하여 조직 내에서 AWS 리소스를 공유할 수 있습니다. 예를 들어 [Amazon Virtual Private Cloud\(Amazon VPC\)](#) 서브넷을 한 번 생성하면 조직 전체에서 공유할 수 있습니다. 또한 [AWS License Manager](#)를 사용하여 소프트웨어 라이선스에 중앙에서 동의할 수 있으며 [AWS Service Catalog](#)를 사용하여 계정 간에 IT 서비스 및 사용자 지정 제품의 카탈로그를 공유할 수 있습니다.

규정 준수를 위해 환경 감사

계정 전체에서 [AWS CloudTrail](#)을 활성화할 수 있습니다. 이렇게 하면 멤버 계정에서 끄거나 수정할 수 없는 클라우드 환경의 모든 활동에 대한 로그가 생성됩니다. 또한 [AWS Config](#)를 사용하여 지정된 주기에 백업을 적용하도록 정책을 설정 [AWS Backup](#)하거나 계정 간 및 AWS 리전 사용하여 리소스에 대한 권장 구성 설정을 정의할 수 있습니다 [AWS Config](#).

중앙에서 결제 및 비용 관리

Organizations는 단일 통합 청구서를 제공합니다. 또한 [AWS Cost Explorer](#)를 사용하여 계정 전반의 리소스에서 사용량을 확인하고 비용을 추적하고 [AWS Compute Optimizer](#)를 사용하여 컴퓨팅 리소스 사용을 최적화할 수 있습니다.

에 대한 사용 사례 AWS Organizations

다음은 몇 가지 사용 사례입니다 AWS Organizations.

워크로드 생성 AWS 계정 및 분류 자동화

의 생성을 자동화 AWS 계정 하여 새 워크로드를 빠르게 시작할 수 있습니다. 즉각적인 보안 정책 애플리케이션, 비접촉 인프라 배포 및 감사를 위해 사용자 정의 그룹에 계정을 추가합니다. 별도의 그룹을 생성하여 개발 및 프로덕션 계정을 분류하고 [AWS CloudFormation StackSets](#)를 사용하여 각 그룹에 서비스와 권한을 프로비저닝합니다.

감사 및 규정 준수 정책 정의 및 시행

서비스 제어 정책(SCP)을 적용하여 사용자가 보안 및 규정 준수 요구 사항을 충족하는 작업만 수행하도록 할 수 있습니다. 을 사용하여 조직 전체에서 수행된 모든 작업에 대한 중앙 로그를 생성합니다. [AWS CloudTrail](#) 를 AWS 리전 사용하여 계정 및 간에 표준 리소스 구성을 보고 적용합니다 [AWS Config](#). 을 사용하여 일반 백업을 자동으로 적용합니다. [AWS Backup](#) [AWS Control Tower](#)를 사용하여 AWS 워크로드의 보안, 운영 및 규정 준수를 위한 사전 패키징된 거버넌스 규칙을 적용합니다.

개발을 장려하는 동시에 보안 팀에 도구 및 액세스 권한 제공

보안 그룹을 생성하고 모든 리소스에 대한 읽기 전용 액세스를 제공하여 보안 문제를 식별하고 완화합니다. 해당 그룹이 [Amazon GuardDuty](#)를 관리하도록 허용하여 워크로드에 대한 위협을 적극적으로 모니터링하고 완화할 수 있으며, [IAM Access Analyzer](#)는 리소스에 대한 의도하지 않은 액세스를 신속하게 식별할 수 있습니다.

계정 간에 공통 리소스 공유

조직은 계정 전체에서 중요한 중앙 리소스를 쉽게 공유할 수 있도록 합니다. 예를 들어 애플리케이션이 중앙 자격 증명 스토어에 액세스할 수 있도록 중앙 [AWS Directory Service for Microsoft Active Directory](#)를 공유할 수 있습니다.

계정 간에 중요한 중앙 리소스 공유

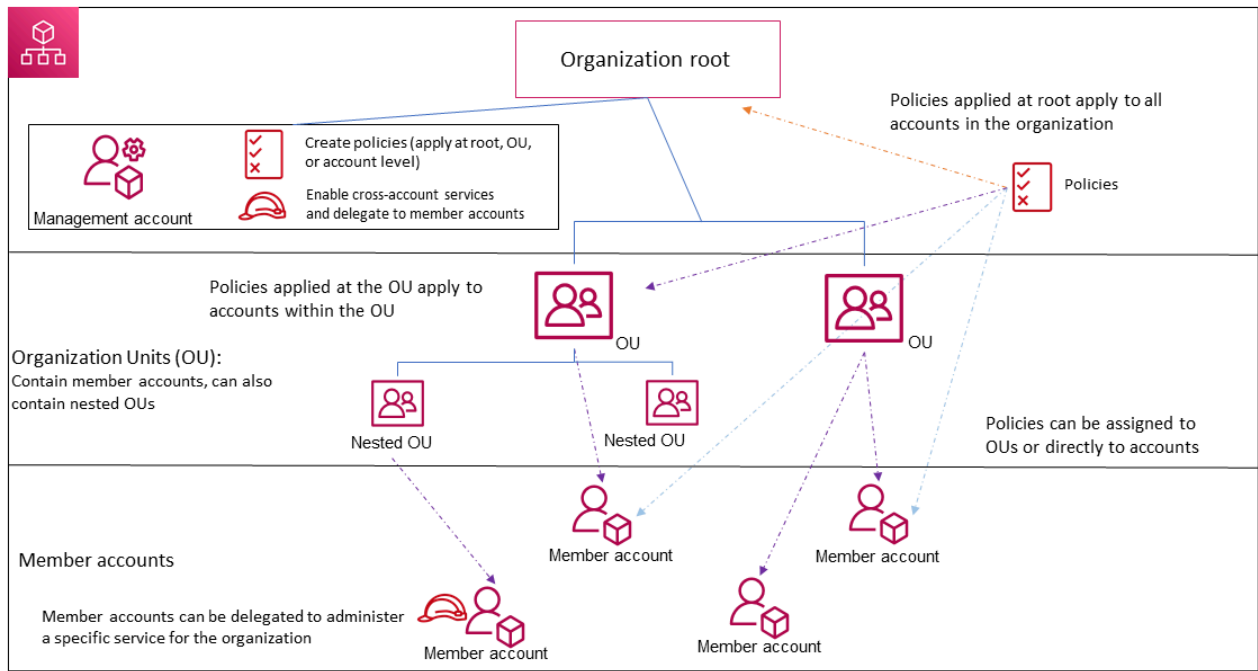
[AWS Directory Service for Microsoft Active Directory](#)를 애플리케이션의 중앙 자격 증명 스토어로 공유합니다. 사용자가 승인된 서비스를 빠르게 검색하고 배포할 수 있도록 [AWS Service Catalog](#)를 사용하여 지정된 계정에서 IT 서비스를 공유합니다. 애플리케이션 리소스는 중앙에서 한 번 정의하고 [AWS Resource Access Manager \(AWS RAM\)](#)를 사용하여 조직 전체에서 공유하여 [Amazon Virtual Private Cloud\(Amazon VPC\)](#) 서브넷에서 생성해야 합니다.

의 용어 및 개념 AWS Organizations

이 주제에서는 몇 가지 주요 개념을 설명합니다 AWS Organizations.

다음 다이어그램은 루트 아래에 4가지 조직 단위(OU)로 구분되는 계정 5개로 구성된 조직을 보여줍니다. 또 조직에는 일부 OU에 연결되거나 계정에 직접 적용되는 다양한 정책이 있습니다.

각 항목에 대한 설명은 이번 주제에 나오는 정의를 참조하세요.



주제

- [사용 가능한 기능 모음](#)
- [조직 구조](#)
- [초대 및 핸드셰이크](#)
- [조직 정책](#)

사용 가능한 기능 모음

모든 기능(권장)

모든 기능은 사용 가능한 기본 기능 세트입니다 AWS Organizations. 전체 조직에 대한 중앙 정책 및 구성 요구 사항을 설정하고, 조직 내에서 사용자 지정 권한 또는 기능을 생성하고, 단일 청구서로 계정을 관리 및 구성하고, 조직을 대신하여 다른 계정에 책임을 위임할 수 있습니다. 다른 AWS 서비스와의 통합을 사용하여 조직의 모든 멤버 계정에서 중앙 구성, 보안 메커니즘, 감사 요구 사항 및 리소스 공유를 정의할 수도 있습니다. 자세한 내용은 [다른 AWS Organizations 와 함께 사용 AWS 서비스](#) 단원을 참조하십시오.

모든 기능 모드는 관리 기능과 함께 통합 결제의 모든 기능을 제공합니다.

Consolidated billing

통합 결제는 공유 결제 기능을 제공하지만의 고급 기능은 포함하지 않는 기능 세트입니다 AWS Organizations. 예를 들어 다른 AWS 서비스를 조직과 통합하여 모든 계정에서 작업하거나 정책을 사용하여 다른 계정의 사용자와 역할이 수행할 수 있는 작업을 제한할 수 없습니다.

원래 통합 결제 기능만 제공하는 조직에 대해 모든 기능을 활성화할 수 있습니다. 모든 기능을 활성화하려면 초대받은 멤버 계정 모두가 관리 계정이 과정을 시작하면서 전송한 초대를 수락해 변경 사항을 승인해야 합니다. 자세한 내용은 [를 사용하여 조직의 모든 기능 활성화 AWS Organizations](#) 단원을 참조하십시오.

조직 구조

Organization

조직은 중앙에서 관리할 수 있으며, 최상단에 [루트](#)가 있고 그 아래에는 [조직 단위](#)가 중첩된 트리형 계층 구조로 구성할 수 있는 [AWS 계정](#)의 모음입니다. 각 계정은 루트에 바로 배치하거나, 계층 구조 내의 OU 중 하나에 배치할 수 있습니다.

각 조직은 다음으로 구성됩니다.

- [관리 계정](#)
- [멤버 계정](#)(없을 수도 있음)
- [조직 단위\(OU\)](#)(없을 수도 있음)
- [정책](#)(없을 수도 있음)

조직은 사용자가 설정하는 [기능 모음](#)으로 결정되는 다양한 기능을 보유합니다.

루트

관리 루트(루트)는 [관리 계정](#)에 포함되어 있으며 [AWS 계정](#)을 구성하기 위한 시작점입니다. 루트는 조직의 계층 구조에서 가장 위에 있는 컨테이너입니다. 이 루트 아래에 [조직 단위\(OU\)](#)를 생성하여 계정을 논리적으로 그룹화하고 이러한 OU를 필요에 가장 적합한 계층 구조로 구성할 수 있습니다.

[관리 정책](#)을 루트에 적용하면 해당 정책은 모든 [조직 단위\(OU\)](#)와 조직의 관리 계정을 포함한 모든 [계정](#)에 적용됩니다.

권한 부여 정책(예: 서비스 제어 정책(SCP))을 루트에 적용하는 경우 조직의 모든 조직 단위(OU)와 [멤버 계정](#)에 적용됩니다. 조직 내 관리 계정에는 적용되지 않습니다.

Note

조직을 생성할 때 root. AWS Organizations automatically가 루트를 하나만 생성할 수 있습니다.

조직 단위(OU)

조직 단위(OU)는 조직 내의 [AWS 계정](#) 그룹입니다. OU에는 계층을 생성할 수 있는 다른 OU도 포함될 수 있습니다. 예를 들어 동일한 부서에 속한 모든 계정을 부서별 OU로 그룹화할 수 있습니다. 마찬가지로 보안 서비스를 실행하는 모든 계정을 보안 OU로 그룹화할 수도 있습니다.

OU는 조직 내 계정 하위 집합에 동일한 제어를 적용해야 할 때 유용합니다. OU를 중첩하면 더 작은 단위로 관리할 수 있습니다. 예를 들어 각 워크로드에 대해 OU를 생성한 다음 각 워크로드 OU에 중첩된 OU를 두 개 생성하여 사전 프로덕션 워크로드와 프로덕션 워크로드를 나눌 수 있습니다. 이러한 OU는 팀 수준 OU에 직접 할당된 제어 외에도 상위 OU에서 정책을 상속합니다. 가장 낮은 OUs에서 AWS 계정 생성된 [루트](#)를 포함하여 계층 구조는 5단계 깊이일 수 있습니다.

AWS 계정

AWS 계정은 AWS 리소스의 컨테이너입니다. 에서 AWS 리소스를 생성하고 관리하며 AWS 계정, 는 액세스 및 결제를 위한 관리 기능을 AWS 계정 제공합니다.

여러를 사용하는 것은 비용 청구 경계를 제공하고, 보안을 위해 리소스를 격리하고, 새로운 프로세스에 맞게 조정할 수 있을 뿐만 아니라 유연성 또는 개인과 팀을 제공하기 때문에 환경을 확장하는 모범 사례 AWS 계정입니다.

Note

AWS 계정이 사용자와 다릅니다. [사용자](#)는 AWS Identity and Access Management (IAM)를 사용하여 생성하는 자격 증명으로서, [장기 자격 증명을 갖는 IAM 사용자](#) 또는 [단기 자격 증명을 갖는 IAM 역할](#)의 형태를 취합니다. 단일 AWS 계정에는 많은 사용자와 역할이 포함될 수 있으며 일반적으로 포함됩니다.

조직에는 두 가지 유형의 계정이 있습니다. 하나는 [관리 계정](#)으로 지정된 단일 계정이며 다른 하나는 하나 이상의 [멤버 계정](#)입니다.

관리 계정

관리 계정은 조직을 생성하는 데 AWS 계정 사용하는입니다. 관리 계정에서는 다음을 수행할 수 있습니다.

- 조직 내에서 다른 계정 생성
- 조직에 가입하도록 다른 계정 [초대 및 초대 관리](#)
- [위임된 관리자 계정](#) 지정
- 조직에서 계정 제거
- [루트](#), [조직 단위\(OU\)](#) 또는 조직 내 계정과 같은 엔터티에 정책 연결
- 지원되는 AWS 서비스와의 통합을 활성화하여 조직의 모든 계정에 서비스 기능을 제공합니다.

관리 계정은 조직의 최종 소유자로, 보안, 인프라 및 재무 정책을 최종적으로 제어할 수 있습니다. 이 계정은 지급인 계정의 역할을 하며 조직의 계정에서 발생한 모든 요금을 지불할 책임이 있습니다.

Notes

- 조직 내 어떤 계정이 관리 계정인지 변경할 수 없습니다.
- 관리 계정은 루트 바로 아래에 있을 필요는 없으며 조직 내 어디에나 배치할 수 있습니다.

멤버 계정

멤버 계정은 관리 계정이 AWS 계정아닌 조직의 일부인입니다. 조직의 [관리자](#)인 경우 조직에서 멤버 계정을 생성하고 기존 계정을 조직에 가입하도록 초대할 수 있습니다. 멤버 계정에 정책을 적용할 수도 있습니다.

Note

멤버 계정은 한 번에 하나의 조직에만 속할 수 있습니다. 멤버 계정을 위임된 관리자 계정으로 지정할 수 있습니다.

위임된 관리자

관리 계정과 그 사용자 및 역할은 해당 계정으로 수행해야 하는 작업에 대해서만 사용하는 것이 좋습니다. AWS 리소스를 조직의 다른 멤버 계정에 저장하고 관리 계정에는 저장하지 않는 것이 좋습니다.

니다. 이는 Organizations 서비스 제어 정책(SCP)과 같은 보안 기능이 관리 계정의 사용자나 역할을 제한하지 않기 때문입니다. 관리 계정에서 리소스를 분리하면 인보이스의 요금을 파악하는 데도 도움이 될 수 있습니다. 조직의 관리 계정에서 하나 이상의 멤버 계정을 위임된 관리자 계정으로 지정하면 이 권장 사항을 구현하는 데 도움이 됩니다. 위임된 관리자에는 다음 두 가지 유형이 있습니다.

- Organizations의 위임된 관리자: 이 계정에서는 조직 정책을 관리하고 조직 내 엔터티(루트, OU 또는 계정)에 정책을 연결할 수 있습니다. 관리 계정은 세분화된 수준에서 위임 권한을 제어할 수 있습니다. 자세한 내용은 [에 대한 위임된 관리자 AWS Organizations](#) 단원을 참조하십시오.
- AWS 서비스의 위임된 관리자: 이러한 계정에서 Organizations와 통합되는 AWS 서비스를 관리할 수 있습니다. 관리 계정은 필요에 따라 여러 멤버 계정을 여러 서비스에 위임된 관리자로 등록할 수 있습니다. 이러한 계정에는 특정 서비스에 대한 관리 권한과 함께 Organizations 읽기 전용 작업에 대한 권한이 있습니다. 자세한 내용은 [Organizations에서 작업 AWS 서비스 하는의 위임된 관리자](#) 섹션을 참조하세요.

초대 및 핸드셰이크

초대

초대는 조직의 관리 계정이 다른 [계정에](#) 보내는 요청입니다. 예를 들어, 초대는 독립형 계정이 [조직](#)에 가입할 것을 요청하는 과정입니다.

초대는 [핸드셰이크](#)로 구현됩니다. AWS Organizations 콘솔에서 작업할 때는 핸드셰이크가 표시되지 않을 수 있습니다. 그러나 AWS CLI 또는 AWS Organizations API를 사용하는 경우 핸드셰이크를 사용하여 직접 작업해야 합니다.

핸드셰이크

핸드셰이크는 발신자와 수신자라는 두 AWS 계정 간의 안전한 정보 교환입니다.

다음 핸드셰이크가 지원됩니다.

- INVITE: 독립형 계정이 발신자의 조직에 가입하도록 핸드셰이크가 전송되었습니다.
- ENABLE_ALL_FEATURES: 조직에 대한 모든 기능을 활성화하기 위해 초대된 멤버 계정으로 핸드셰이크가 전송되었습니다.
- APPROVE_ALL_FEATURES: 초대된 모든 멤버 계정이 모든 기능 활성화를 승인하면 핸드셰이크가 관리 계정으로 전송됩니다.

일반적으로 AWS Organizations API 또는와 같은 명령줄 도구로 작업하는 경우에만 핸드셰이크와 직접 상호 작용해야 합니다 AWS CLI.

조직 정책

정책은 그룹에 적용하려는 제어를 정의하는 하나 이상의 문이 있는 "문서"입니다. AWS 계정은 권한 부여 정책 및 관리 정책을 AWS Organizations 지원합니다.

권한 부여 정책

권한 부여 정책은 조직 AWS 계정 전체의 보안을 중앙에서 관리하는 데 도움이 됩니다.

서비스 제어 정책(SCP)

서비스 제어 정책은 조직 IAM 사용자 및 IAM 역할에 사용 가능한 최대 권한에 대한 중앙 제어를 제공하는 정책 유형입니다.

이는 SCP가 위탁자 중심 제어를 지정함을 뜻합니다. SCP는 권한 가드레일을 생성하거나 멤버 계정의 위탁자가 사용할 수 있는 최대 권한에 대한 제한을 설정합니다. 조직의 위탁자에 대해 일관된 액세스 제어를 중앙에서 적용하려는 경우 SCP를 사용합니다.

여기에는 IAM 사용자와 IAM 역할이 액세스할 수 있는 서비스, 액세스할 수 있는 리소스 또는 요청을 수행할 수 있는 조건(예: 특정 리전 또는 네트워크)을 지정하는 것이 포함될 수 있습니다. 자세한 내용을 알아보려면 [SCP](#)를 참조하십시오.

리소스 제어 정책(RCP)

리소스 제어 정책은 조직의 리소스에 대해 사용 가능한 최대 권한을 중앙에서 제어하는 정책 유형입니다.

즉, RCP는 리소스 중심 제어를 지정한다는 뜻입니다. RCP는 권한 가드레일을 생성하거나 멤버 계정의 리소스가 사용할 수 있는 최대 권한에 대한 제한을 설정합니다. 조직의 리소스 간에 일관된 액세스 제어를 중앙에서 적용하려는 경우 RCP를 사용합니다.

여기에는 조직에 속한 자격 증명만 액세스할 수 있도록 리소스에 대한 액세스를 제한하거나 조직 외부의 자격 증명이 리소스에 액세스할 수 있는 조건을 지정하는 것이 포함될 수 있습니다. 자세한 내용을 알아보려면 [RCP](#)를 참조하십시오.

관리 정책

관리 정책은 조직 전체에서 AWS 서비스 및 해당 기능을 중앙에서 구성하고 관리하는 데 도움이 됩니다.

- [선언적 정책을](#) 사용하면 조직 전체에서 지정된에 대해 원하는 구성을 중앙 AWS 서비스 에서 선언하고 적용할 수 있습니다. 연결되면 서비스가 새 기능 또는 API를 추가할 때 구성이 항상 유지됩니다.
- [백업 정책을](#) 사용하면 조직의 계정 전체에서 백업 계획을 중앙에서 관리하고 AWS 리소스에 적용할 수 있습니다.
- [태그 정책을](#) 사용하면 조직 계정의 AWS 리소스에 연결된 태그를 표준화할 수 있습니다.
- [채팅 애플리케이션 정책](#)을 사용하면 Slack 및 Microsoft Teams와 같은 채팅 애플리케이션에서 조직의 계정에 대한 액세스를 제어할 수 있습니다.
- [AI 서비스 옵트아웃 정책](#)을 사용하면 조직의 모든 계정에 대한 AWS AI 서비스의 데이터 수집을 제어할 수 있습니다.
- [Security Hub 정책](#)을 통해 조직의 보안 요구 사항에 부합하도록 조직 전반에 이를 중앙에서 적용함으로써 보안 적용 범위 격차를 해소할 수 있습니다.
- [Amazon Inspector 정책](#)을 사용하면 AWS 조직의 여러 계정에서 Amazon Inspector를 중앙에서 활성화하고 관리할 수 있습니다.
- [Amazon Bedrock 정책](#)을 사용하면 Amazon Bedrock에 대한 모든 모델 추론 호출에 대해 조직 구조의 모든 요소에 Amazon Bedrock Guardrails에 구성된 보호 기능을 자동으로 적용할 수 있습니다.
- [업그레이드 롤아웃 정책](#)을 사용하면 조직의 여러 AWS 리소스 및 계정에서 자동 업그레이드를 중앙에서 관리하고 시차를 지정할 수 있습니다.
- [Amazon S3 정책](#)을 사용하면 조직의 계정 전체에서 Amazon S3 리소스에 대한 구성을 대규모로 중앙에서 관리할 수 있습니다.
- [AWS Shield Network Security Director 정책](#)을 사용하면 조직의 계정 전체에서 AWS Shield Network Security Director를 중앙에서 활성화하고 관리할 수 있습니다.

AWS Organizations에 대한 할당량 및 서비스 제한

이 주제에서는 AWS Organizations에 대한 할당량 및 서비스 제한에 대해 설명합니다.

이름 지정 지침

다음은 계정 이름 AWS Organizations, 조직 단위(OU), 루트 및 정책을 포함하여 생성하는 이름에 대한 지침입니다.

- 이름은 반드시 유니코드 문자로 구성해야 합니다.
- 이름의 최대 문자열 길이는 객체에 따라 다릅니다. 각 객체의 실제 한도에 대한 자세한 내용은 [AWS Organizations API 참조](#)를 참조하여 객체를 생성하는 API 작업을 찾아 해당 작업의 Name 파라미터에 대한 세부 정보를 확인하세요. 예: [계정 이름](#) 또는 [OU 이름](#).

고려 사항

서비스 할당량 코드는 업데이트로 인해 시간이 지남에 따라 변경될 수 있습니다. 할당량 값이나 이름에는 영향을 주지 않습니다. 특정 할당량에 대한 할당량 코드를 찾으려면 [ListServiceQuotas](#) 작업을 사용하고 원하는 할당량에 대한 출력에서 QuotaCode 응답을 찾습니다.

최대값 및 최소값

다음은 AWS Organizations에서 엔터티의 기본 최대값입니다.

Note

AWS Organizations 할당량에 관 다음 정보를 확인하세요.

- [Service Quotas 콘솔](#)을 사용하여 이러한 값 중 일부에 대해 상향을 요청할 수 있습니다.
- AWS Organizations 달리 지정하지 않는 한 조직 수준에서 제한이 적용됩니다. 많은 할당량은 AWS Organizations 관리 계정에서 수행된 작업에만 적용됩니다.
- AWS Organizations 는 미국 동부(버지니아 북부) 리전()에서 물리적으로 호스팅되는 글로벌 서비스입니다us-east-1. 따라서 Service Quotas 콘솔, AWS CLI또는 AWS SDKus-east-1를 사용할 때를 사용하여 이러한 할당량에 액세스해야 합니다.

설명	Limit
최대 계정 수	10 - 조직에 허용되는 최대 계정 수입니다. 이 할당량은 조정 가능하며, Service Quotas 콘솔을 사용하여 늘릴 수 있습니다. 참고: 조직의 관리 계정만 이 할당량 증가 요청을 제출할 수 있습니다. 한도 증가는 고객 자격 및 요구 사항에 따라 최대 50,000개의 계정에 부여할 수 있습니다. 새로 생성된 계정 및 조직의 경우 할당량이 기본값인 계정 10개 미만일 수 있습니다. 계정으로 전송되는 초대 개수는 이 할당량을 기준으로 계산됩니다. 초대된 계정에서 초대를 거부하면 해당 카운트가 반환되고 관리 계정이 초대를 취소하거나 초대가 만료됩니다. 계정이 해지되면 영구적으로 해지될 때까지 이 할당량 계산에서 제외되지 않습니다. 계정이 영구적으로 해지되는 시점에 대한 자세한 내용

설명	Limit
	은 AWS Account Management 참조 안내서의 해지 후 기간을 참조하세요. 일부 서비스에는 조직에서 허용되는 최대 계정 수와 별도의 계정 한도가 있습니다. 자세한 내용은 AWS 서비스별 제한을 참조하세요.
생성한 계정을 삭제할 수 있는 최소 기간	각 지원 리전: 7 — 생성된 계정을 조직에서 제거하기 전에 해당 계정이 존재해야 하는 최소 일수입니다.
조직의 루트 개수	1
조직의 OU 개수	2000
조직 내 각 유형별 정책 개수	서비스 제어 정책: 10,000 리소스 제어 정책: 1000 선언적 정책: 1000 백업 정책: 1000 태그 정책: 1000 채팅 애플리케이션 정책: 1000 AI 서비스 옵트아웃 정책: 1000 Security Hub 정책: 1000

설명	Limit
정책 문서의 최대 크기	서비스 제어 정책: 5,120자 리소스 제어 정책: 5,120자 선언적 정책: 10,000자 백업 정책: 10,000자 채팅 애플리케이션 정책: 10,000자 AI 서비스 옵트아웃 정책: 2,500자 태그 정책: 10,000자 Security Hub 정책: 10,000자 참고:를 사용하여 정책을 저장하면 JSON 요소와 인용 부호 외부 사이의 AWS Management Console추가 공백(예: 공백 및 줄 바꿈)이 제거되고 계산되지 않습니다. SDK 작업 또는를 사용하여 정책을 저장 AWS CLI하면 제공된 대로 정책이 정확히 저장되며 문자가 자동으로 제거되지 않습니다.
루트의 OU 최대 중첩 수	루트 아래 5개 레벨의 OU 깊이
24시간 동안 수행할 수 있는 최대 초대 횟수입니다.	20개, 또는 조직에 허용된 최대 계정 수 중 더 큰 수입니다. 수락된 초대 는 이 할당량에 포함되지 않습니다. 하나의 초대가 수락되는 즉시 다른 초대를 같은 날에 전송할 수 있습니다. 조직에 허용되는 최대 계정 수가 20개 미만인 경우 조직이 수용할 수 있는 것보다 더 많은 계정을 초대하려고 하면 "계정 제한 초과" 예외가 발생합니다. 그러나 초대를 취소하고 하루에 최대 20회까지 새 초대장을 보낼 수 있습니다.
동시에 만들 수 있는 멤버 계정의 수	5 — 한 계정의 생성이 끝나면 바로 다른 계정 생성을 시작할 수 있지만, 한 번에 5개의 계정 생성만 진행 가능.

설명	Limit
30일 동안 해지할 수 있는 계정의 수입니다.	조직 내 멤버 계정의 20% 또는 250 중 더 높은 쪽, 최대 1,000개. 이 할당량은 조정할 수 없습니다. • < 1,250개 계정 - 최대 250개의 멤버 계정을 해지할 수 있습니다. • 1,250~5,000개 계정 - 멤버 계정의 최대 20%를 해지할 수 있습니다. • > 5,000개 계정 - 최대 1,000개의 멤버 계정을 해지할 수 있습니다. 이 할당량에 도달한 후에는 계정을 추가로 해지하거나 해당 할당량이 초기화될 때까지 대기할 수 있습니다. 자세한 내용은 AWS 계정 관리 안내서의 계정 달기를 참조하세요. AWS
동시에 해지할 수 있는 멤버 계정의 수	3 - 동시에 3개까지만 해지할 수 있습니다. 한 계정의 해지를 완료한 후, 곧바로 다른 계정을 해지할 수 있습니다.
정책에 연결할 수 있는 엔터티 개수	무제한
루트, OU 또는 계정에 연결할 수 있는 태그 수	50
리소스 기반 위임 정책의 최대 크기	4만 자

AWS 서비스별 제한

대부분은 조직에서 보유할 수 있는 명시된 최대 계정 수를 AWS 서비스 지원합니다. 그러나 일부 서비스에는 조직에서 허용되는 최대 계정 수와 별도의 계정 한도가 있습니다.

다음 표는 별도의 계정 제한이 있는 서비스를 보여줍니다.

AWS 서비스	Limit	높일 수 있음	서비스 설명서
AWS Directory Service (디렉터리 공유 사용)	디렉터리 공유 계정 용량은 에디션	예	Directory Service 할당량

AWS 서비스	Limit	높일 수 있음	서비스 설명서
가능 AWS Managed Microsoft AD)	에 따라 다릅니다.		
AWS Audit Manager	250	예	AWS Audit Manager 할당량
Amazon Detective	1200	예	Amazon Detective 할당량
AWS IAM Identity Center	3000	예	AWS IAM Identity Center 할당량
AWS Application Migration Service	5000	아니요	AWS 할당량
AWS Security Hub	10000	아니요	AWS Security Hub 할당량
Amazon Macie	10000	아니요	Amazon Macie 할당량
AWS Control Tower	10000	아니요	AWS Control Tower 할당량
Amazon Inspector –	10000	아니요	Amazon Inspector 할당량
AWS Firewall Manager	10000	예	AWS Firewall Manager 할당량
Amazon DevOps Guru	10000	예	Amazon DevOps Guru 할당량

핸드셰이크 만료 시간

다음은 핸드셰이크의 제한 시간입니다 AWS Organizations.

설명	Limit
조직 참여 초대	15일
조직의 모든 기능 활성화 요청	90일

설명	Limit
핸드셰이크가 삭제되고 더 이상 목록에 표시되지 않습니다.	30일 이후에 핸드셰이크가 실행됩니다.

엔터티에 연결할 수 있는 정책 수

최소값 및 최대값은 정책 유형과 정책을 연결하는 엔터티에 따라 다릅니다. 다음 표는 각 정책 유형과 각 유형을 연결할 수 있는 개체 수를 보여줍니다.

Note

이러한 수는 OU 또는 계정에 직접 연결된 정책에만 적용됩니다. 상속이 OU 또는 계정에 영향을 미치는 정책은 이러한 제한에 포함되지 않습니다. 모든 정책 한도는 하드 한도입니다.

정책 유형	엔터티에 연결된 최소값	루트에 연결된 최대값	OU별로 연결된 최대값	계정별로 연결된 최대값
서비스 제어 정책	1 — SCP 활성화 시, 모든 엔터티에는 언제나 SCP가 하나 이상 연결되어 있어야 합니다. 개체의 마지막 SCP는 제거할 수 없습니다.	5	5	5
리소스 제어 정책	1 - RCP를 활성화 하면 RCPFullAWSSAccess 정책이 루트, 모든 OU 및 조직의 모든 계정에 자동으로 연결됩니다. 이 정책은 분리할 수 없으며 5개	5	5	5

정책 유형	엔터티에 연결된 최소 값	루트에 연결된 최대값	OU별로 연결된 최대값	계정별로 연결된 최대값
	의 정책 할당량에 포함됩니다.			
선언적 정책	0	10	10	10
백업 정책	0	10	10	10
태그 정책	0	10	10	10
채팅 애플리케이션 정책	0	5	5	5
AI 서비스 옵트아웃 정책	0	5	5	5
Security Hub 정책	0	10	10	10

Note

조직은 루트를 하나만 가질 수 있습니다.

제한 한계

다음 표에는 관리 범주별로 AWS Organizations APIs 나열되어 있으며 계정 및 조직 수준에서 해당 제한 속도가 나와 있습니다.

AWS Organizations 는 [토큰 버킷 알고리즘](#)을 사용하여 API 제한을 구현합니다. 이 알고리즘을 사용하면 계정에 특정 수의 토큰을 보관하는 버킷이 있습니다. 버킷의 토큰 수는 지정된 초당 제한 할당량을 나타냅니다.

속도는 토큰이 토큰 버킷에 추가되는 고정된 초당 속도입니다.

버스트는 추가할 수 있는 최대 토큰 수와 초당 사용할 수 있는 최대 토큰 수입니다.

예를 들어 DescribeAccount API는 기존 속도로 단일 AWS 계정 에 대하여 초당 20개의 요청과 버스트 속도로 초당 30개의 요청으로 제한됩니다. 초당 30개 요청의 버스트 속도를 사용하면 초당 20개 요청의 기존 속도를 일시적으로 초과할 수 있습니다.

처음 1초 동안 기존 속도인 20개의 요청을 할 수 있습니다. 다음 1초에는 30개의 요청을 하여 기준을 초과하지만 버스트 속도인 30개 이내로 유지할 수 있습니다. 그러나 그다음 1초에 20개 이상의 요청을 하려고 하면 기존 속도를 초과하고 버스트 용량이 사용되었으므로 속도가 제한될 것입니다.

버스트 속도를 사용하면 시간 경과에 따른 초당 평균 요청이 기준 한도 내에 있는 한 제한 없이 일시적인 트래픽 급증을 처리할 수 있습니다.

계정 관리 한도

다음 표에는 계정 관리를 위한 AWS Organizations APIs 나열되어 있습니다.

AWS Organizations API	계정당 한도(속도, 버스트)	조직당 한도(속도, 버스트)
CloseAccount	.05, 1	
CreateAccount, CreateGovCloudAccount	0.1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	2, 2	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5, 8	6, 10

핸드셰이크 관리 한도

다음 표에는 계정 핸드셰이크를 위한 AWS Organizations APIs 나열되어 있습니다.

AWS Organizations API	계정당 한도(속도, 버스트)	조직당 한도(속도, 버스트)
AcceptHandshake	1, 2	5, 5
DescribeHandshake	1, 2	6, 10

AWS Organizations API	계정당 한도(속도, 버스트)	조직당 한도(속도, 버스트)
CancelHandshake	2, 3	
DeclineHandshake	1, 1	5, 5
InviteAccountToOrganization	3, 5	
ListHandshakesForAccount, ListHandshakesForOrganization	5, 8	6, 10

조직 관리 한도

다음 표에는 조직 관리를 위한 AWS Organizations APIs가 나열되어 있습니다.

AWS Organizations API	계정당 한도(속도, 버스트)	조직당 한도(속도, 버스트)
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1, 2	
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2, 3	
DescribeOrganizationalUnit	2, 2	2, 3
ListAccounts	8, 12	9, 15
ListChildren	6, 10	7, 12
ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent	5, 8	6, 10

AWS Organizations API	계정당 한도(속도, 버스트)	조직당 한도(속도, 버스트)
ListRoots	1, 2	1, 3
ListTagsForResource	10, 15	12, 18
RemoveAccountFromOrganization	2, 2	
TagResource, UntagResource	4, 6	

정책 관리 한도

다음 표에는 정책 관리를 위한 AWS Organizations APIs가 나열되어 있습니다.

AWS Organizations API	계정당 한도(속도, 버스트)	조직당 한도(속도, 버스트)
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2, 3	
DescribePolicy	2, 2	2, 3
DisablePolicyType, EnablePolicyType	1, 1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5, 8	6, 10
UpdatePolicy	2, 3	

서비스 관리 한도

다음 표에는 서비스 관리를 위한 AWS Organizations APIs가 나열되어 있습니다.

AWS Organizations API	계정당 한도(속도, 버스트)	조직당 한도(속도, 버스트)
EnableAWSServiceAccess, DisableAWSServiceAccess	1, 2	

AWS Organizations API	계정당 한도(속도, 버스트)	조직당 한도(속도, 버스트)
ListAWSServiceAccessForOrganization, ListDelegatedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5, 8	6, 10
RegisterDelegatedAdministrator, DeregisterDelegatedAdministrator	1, 2	

에 대한 리전 지원 AWS Organizations

AWS Organizations 는 모든 AWS 상용 리전 AWS GovCloud (US) Regions 및 중국 리전에서 사용할 수 있습니다.

의 기능 차이점 목록은의 섹션을 AWS GovCloud (US) Regions참조 [AWS Organizations 하세요 AWS GovCloud \(US\)](#).

중국 리전의 기능 차이 목록은 [중국의AWS Organizations 섹션](#)을 참조하세요.

Organizations의 서비스 엔드포인트 위치

- 상용 조직: 미국 동부(버지니아 북부)
- AWS GovCloud (US) 조직용 In AWS GovCloud(미국 서부)
- 중국 조직: 중국(닝샤). Ningxia Western Cloud Data Technology Co. Ltd (NWCD)에서 운영합니다.

현재 AWS Identity and Access Management (IAM) 작동 방식과 마찬가지로 중국에서 관리되는 조직을 제외한 모든 조직 엔터티에 전역적으로 액세스할 수 있습니다. 조직을 생성하고 관리할 AWS 리전 때를 지정할 필요는 없지만 중국에서 사용되는 계정에 대해 별도의 조직을 생성해야 합니다. 의 사용자는 해당 서비스를 사용할 AWS 계정 수 있는 모든 지리적 리전 AWS 서비스 에서 사용할 수 있습니다.

Note

태그 정책은 리전의 하위 집합에서만 지원됨

태그 정책은 조직의 계정에 있는 리소스 전체에서 태그를 표준화하는 데 도움이 될 수 있는 정책의 한 유형입니다. 태그 정책은 Organizations가 지원되는 리전의 하위 집합에서만 지원됩니다. 태그 정책이 지원되는 리전 목록은 [태그 정책 | 지원 리전](#)을 참조하세요.

사용 가능한 목록 AWS 리전

다음 표에는 사용 가능한 모든 AWS 리전이 나열되어 있습니다.

리전 이름	리전	엔드포인트	프로토콜
미국 동부 (오하이오)	us-east-2	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
미국 동부 (버지니아 북부)	us-east-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
미국 서부 (캘리포니아 북부)	us-west-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
미국 서부 (오레곤)	us-west-2	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
아프리카 (케이프타운)	af-south-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
아시아 태평양 (홍콩)	ap-east-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
아시아 태평양 (하이데라바드)	ap-south-2	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS

리전 이름	리전	엔드포인트	프로토콜	
아시아 태평양(자카르타)	ap-southeast-3	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
아시아 태평양(말레이시아)	ap-southeast-5	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
아시아 태평양(멜버른)	ap-southeast-4	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
아시아 태평양(뭄바이)	ap-south-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
아시아 태평양(뉴질랜드)	ap-southeast-6	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
아시아 태평양(오사카)	ap-northeast-3	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
아시아 태평양(서울)	ap-northeast-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
아시아 태평양(싱가포르)	ap-southeast-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
아시아 태평양(시드니)	ap-southeast-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	

리전 이름	리전	엔드포인트	프로토콜	
아시아 태평양(타이베이)	ap-east-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
아시아 태평양(태국)	ap-southeast-7	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
아시아 태평양(도쿄)	ap-northeast-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
캐나다(중부)	ca-central-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
캐나다 서부(캘거리)	ca-west-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
유럽(프랑크푸르트)	eu-central-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
유럽(아일랜드)	eu-west-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
유럽(런던)	eu-west-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
유럽(밀라노)	eu-south-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
유럽(파리)	eu-west-3	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	

리전 이름	리전	엔드포인트	프로토콜	
유럽(스페인)	eu-south-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
유럽(스톡홀름)	eu-north-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
유럽(칠리히)	eu-central-2	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
이스라엘(텔아비브)	il-central-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
멕시코(중부)	mx-central-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
중동(바레인)	me-south-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
중동(UAE)	me-central-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
남아메리카(상파울루)	sa-east-1	organizations.us-east-1.amazonaws.com	HTTPS	
		organizations-fips.us-east-1.amazonaws.com	HTTPS	
AWS GovCloud(미국 동부)	us-gov-east-1	organizations.us-gov-west-1.amazonaws.com	HTTPS	

리전 이름	리전	엔드포인트	프로토콜	
AWS GovCloud(미국 서부)	us-gov-west-1	organizations.us-gov-west-1.amazonaws.com	HTTPS	

에 대한 결제 및 요금 AWS Organizations

AWS Organizations 는 추가 비용 없이 제공됩니다. 멤버 계정의 사용자 및 역할이 사용하는 AWS 리소스에 대해서만 요금이 부과됩니다. 예를 들어 멤버 계정의 사용자나 역할이 사용한 Amazon EC2 인스턴스에 대한 표준 요금이 청구됩니다. 다른 AWS 서비스의 요금에 대한 자세한 내용은 [AWS 요금을](#) 참조하세요.

내 조직의 AWS 멤버 계정에서 사용자가 사용한 요금은 누가 지불하나요?

[관리 계정](#)의 소유자는 조직의 계정에서 사용하는 모든 사용량, 데이터 및 리소스에 대한 비용을 지불할 책임이 있습니다.

청구서에 조직에서 생성한 조직 단위 구조가 반영되나요?

청구서에는 조직에서 정의한 구조가 반영되지 않습니다. [비용 할당 태그](#)를 개별적으로 사용하여 AWS 비용을 AWS 계정 분류하고 추적할 수 있으며, 이 할당은 조직의 통합 청구서에 표시됩니다.

에 대한 지원 및 피드백 AWS Organizations

우리는 여러분의 의견을 환영합니다. 또한 [AWS Organizations 지원 포럼](#)에 의견과 질문을 올리셔도 됩니다. AWS 지원 포럼에 대한 자세한 내용은 [포럼 도움말을 참조하세요](#).

기타 AWS 리소스

- [AWS 훈련 및 과정](#) - AWS 기술을 연마하고 실용적인 경험을 얻는 데 도움이 되는 역할 기반 및 특수 과정과 자기 주도형 실습에 대한 링크입니다.
- [AWS 개발자 도구](#) - 혁신적인 애플리케이션을 구축하는 데 도움이 되는 설명서, 코드 예제, 릴리스 정보 및 기타 정보를 제공하는 개발자 도구 및 리소스에 대한 링크입니다 AWS.

- [AWS Support 센터](#) - AWS 지원 사례를 생성하고 관리하기 위한 허브입니다. 또한 포럼, 기술 FAQ, 서비스 상태 및 AWS Trusted Advisor 등의 기타 유용한 자료에 대한 링크가 있습니다.
- [AWS 지원](#) - 클라우드에서 애플리케이션을 구축하고 실행하는 데 도움이 되는 one-on-one 빠른 응답 지원 채널인 AWS 지원에 대한 정보를 제공하는 기본 웹 페이지입니다.
- [문의처](#) - AWS 결제, 계정, 이벤트, 침해 및 기타 문제에 대한 문의를 위한 중앙 연락 창구입니다.
- [AWS 사이트 약관](#) - 저작권 및 상표, 계정, 라이선스, 사이트 액세스 및 기타 주제에 대한 자세한 정보입니다.

다중 계정 환경 모범 사례

다음 권장 사항을 따르면에서 다중 계정 환경을 설정하고 관리하는 과정을 안내할 수 있습니다 AWS Organizations.

주제

- [계정 및 자격 증명](#)
- [조직 구조 및 워크로드](#)
- [서비스 및 비용 관리](#)

계정 및 자격 증명

루트 액세스 관리를 활성화하여 멤버 계정의 루트 사용자 자격 증명 관리 단순화

멤버 계정의 루트 사용자 자격 증명을 모니터링하고 제거하는 데 도움이 되도록 루트 액세스 관리를 활성화하는 것이 좋습니다. 루트 액세스 관리는 루트 사용자 자격 증명 복구를 방지하여 조직의 계정 보안을 개선합니다.

- 멤버 계정 루트 사용자 자격 증명을 제거하여 루트 사용자의 계정 복구를 방지합니다. 이는 또한 멤버 계정이 루트 사용자를 복구하지 못하게 합니다.
- 권한 있는 세션을 맡아 멤버 계정에서 다음 작업을 수행합니다.
 - 모든 위탁자의 Amazon S3 버킷 액세스를 거부하는 잘못 구성된 버킷 정책을 제거합니다.
 - 모든 위탁자가 Amazon SQS 대기열에 액세스하는 것을 거부하는 Amazon Simple Queue Service 리소스 기반 정책을 삭제합니다.
 - 멤버 계정이 루트 사용자 자격 증명을 복구하도록 허용합니다. 그러면 멤버 계정의 루트 사용자 이메일 받은 편지함에 액세스할 수 있는 사람이 루트 사용자 암호를 재설정하고 멤버 계정 루트 사용자로 로그인할 수 있습니다.

루트 액세스 관리가 활성화된 후 새로 생성된 멤버 계정은 보안 내재화되며 루트 사용자 자격 증명 없으므로 프로비저닝 후 MFA와 같은 추가 보안이 필요하지 않습니다.

자세한 내용은 AWS Identity and Access Management 사용 설명서의 [멤버 계정의 루트 사용자 자격 증명 중앙 집중화](#)를 참조하세요.

연락 전화번호를 최신 상태로 유지하기

에 대한 액세스를 복구하려면 문자 메시지 또는 전화를 받을 수 있는 유효하고 활성 상태인 연락처 전화번호가 AWS 계정 있어야 합니다. 계정 지원 및 복구를 위해에서 연락할 AWS 수 있도록 전용 전화번호를 사용하는 것이 좋습니다. AWS Management Console 또는 계정 관리 APIs.

가 연락을 취할 수 있도록 전용 전화번호를 얻는 방법에는 여러 가지가 AWS 있습니다. 전용 SIM 카드와 실제 휴대폰을 구입하는 것이 가장 좋습니다. 휴대폰과 SIM을 장기간 안전하게 보관하여 계정 복구 시 전화번호를 사용할 수 있도록 하세요. 또한 모바일 청구서를 담당하는 팀은 이 번호가 장기간 비활성 상태로 남아 있더라도 그 유지의 중요성을 이해해야 합니다. 보호를 강화하기 위해 조직 내에서 이 전화번호를 기밀로 유지해야 합니다.

AWS 연락처 정보 콘솔 페이지에 전화번호를 문서화하고 조직에서 해당 전화번호에 대해 알아야 하는 특정 팀과 세부 정보를 공유합니다. 이러한 방식으로 전화번호를 다른 SIM으로 이전할 때 발생하는 위험을 최소화하는 데 도움이 됩니다. 기존 정보 보안 정책에 따라 전화를 보관합니다. 그러나 전화를 다른 관련 자격 증명 정보와 같은 위치에 저장하면 안 됩니다. 전화 또는 전화의 보관 위치에 대한 모든 액세스는 기록하고 모니터링해야 합니다. 계정과 연결된 전화번호가 변경될 경우 기존 문서에서 전화번호를 업데이트하는 프로세스를 구현합니다.

루트 계정에 그룹 이메일 주소 사용하기

회사에서 관리하는 이메일 주소를 사용합니다. 받은 메시지를 사용자 그룹에 직접 전달하는 이메일 주소를 사용합니다. 예를 들어 액세스를 확인하기 위해가 계정 소유자에게 문의 AWS 해야 하는 경우 이메일 메시지는 여러 당사자에게 배포됩니다. 이러한 방식은 개인이 휴가 중이거나 아프거나 회사를 떠난 경우에도 응답이 지연될 위험을 줄이는 데 도움이 됩니다.

조직 구조 및 워크로드

단일 조직 내에서 계정 관리

단일 조직을 만들고 이 조직 내에서 모든 계정을 관리하는 것이 좋습니다. 조직은 사용자 환경 내 계정 간에 일관성을 유지할 수 있게 해주는 보안 경계입니다. 중앙에서 조직 내 계정 전체에 정책 또는 서비스 수준 구성을 적용할 수 있습니다. 다중 계정 환경 전반에서 일관된 정책, 중앙집중식 가시성, 프로그래밍적 제어를 구현하려면 단일 조직 내에서 이 작업을 수행하는 것이 가장 좋습니다.

보고 구조가 아닌 비즈니스 목적에 따라 워크로드 그룹화

프로덕션 워크로드 환경과 데이터를 최상위 워크로드 중심 OU에 분리하는 것이 좋습니다. OU는 회사의 보고 구조를 반영하기보다는 공통된 제어 집합을 기반으로 해야 합니다. 프로덕션 OU와는 별도로,

워크로드를 개발하고 테스트하는 데 사용되는 계정 및 워크로드 환경이 포함된 비-프로덕션 OU를 하나 이상 정의하는 것이 좋습니다. 추가적인 안내는 [워크로드 지향 OU 구성](#)을 참조하십시오.

여러 계정을 사용하여 워크로드 정리하기

는 AWS 리소스에 대한 자연스러운 보안, 액세스 및 결제 경계를 AWS 계정 제공합니다. 여러 계정을 사용하면 계정 수준의 할당량과 API 요청 속도 한도를, 여기에 나열된 [추가 혜택](#)을 분산할 수 있어 이점이 있습니다. 보안, 로그, 인프라용 계정과 같은 [전사적 차원의 기본 계정](#)을 여러 개 사용하는 것이 좋습니다. 워크로드 계정의 경우 [테스트/개발 워크로드에서 프로덕션 워크로드를 별도의 계정에 분리해야](#) 합니다.

서비스 및 비용 관리

AWS 서비스 콘솔 또는 API/CLI 작업을 사용하여 조직 수준에서 서비스 활성화

가장 좋은 방법은 해당 서비스의 콘솔 또는 API 작업/CLI 명령 등가를 AWS Organizations 사용하여 통합하려는 서비스를 활성화하거나 비활성화하는 것입니다. 이 방법을 사용하면 AWS 서비스는 필요한 리소스를 생성하고 서비스를 비활성화할 때 리소스를 정리하는 등 조직에 필요한 모든 초기화 단계를 수행할 수 있습니다. AWS Account Management 는 AWS Organizations 콘솔 또는 APIs를 사용하여를 활성화해야 하는 유일한 서비스입니다. 와 통합된 서비스 목록을 검토하려면 섹션을 AWS Organizations참조하세요[AWS 서비스와 함께 사용할 수 있는 AWS Organizations](#).

결제 도구를 사용하여 비용 추적 및 리소스 사용 최적화

조직을 관리하면 조직 내 계정에서 발생하는 모든 요금이 포함된 통합 청구서를 받게 됩니다. 비용 가시성에 대한 액세스가 필요한 비즈니스 사용자의 경우, 관리 계정의 역할에 결제 및 비용 도구를 검토할 수 있는 제한적 읽기 전용 권한을 부여할 수 있습니다. 예를 들어, 결제 보고서에 액세스할 수 있는 [권한 집합을 만들거나](#) AWS Cost Explorer Service (시간 경과에 따른 비용 추세를 보는 도구) 및 [Amazon S3 Storage Lens](#) 및 [AWS Compute Optimizer](#)와 같은 비용 효율성 서비스를 사용할 수 있습니다.

조직 리소스 전반의 태그 지정 전략 및 태그 적용 계획

계정과 워크로드가 확장되면 비용 추적, 액세스 제어 및 리소스 구성에 태그 기능이 유용할 수 있습니다. 태그 지정 이름 지정 전략의 경우 [AWS 리소스 태그 지정의 지침을 따르세요](#). 리소스 외에도 조직 루트, 계정, OU, 정책의 태그를 만들 수 있습니다. 자세한 내용은 [태깅 전략 구축](#)을 참조하십시오.

시작하기 AWS Organizations

다음 주제는 AWS Organizations 사용을 시작하는 데 도움이 되는 정보를 제공합니다. 다음 자습서를 사용하여 AWS Organizations를 사용한 작업 수행을 시작할 수도 있습니다.

[자습서: 조직 생성 및 구성](#)

단계별 지침에 따라 설정하고 실행해 나만의 조직을 만들고, 첫 번째 멤버 계정을 초대하고, 사용자의 계정을 포함하는 OU 계층을 만들고, 일부 서비스 제어 정책(SCP)을 적용해보십시오.

[자습서: Amazon EventBridge를 사용하여 조직에 대한 중요 변경 사항 모니터링](#)

지정한 작업이 조직에서 발생하면 이메일, SMS 문자 메시지 또는 로그 항목의 형식으로 경보를 트리거하도록 Amazon EventBridge를 구성하여 조직의 주요 변경 사항을 모니터링합니다. 예를 들어, 많은 조직에서 새 계정이 생성되는 경우, 계정이 조직에서 탈퇴하려고 하는 경우 등을 알고 싶어 합니다.

주제

- [에 가입 AWS](#)
- [액세스 AWS Organizations](#)
- [자습서: 조직 생성 및 구성](#)
- [자습서: Amazon EventBridge를 사용하여 조직에 대한 중요 변경 사항 모니터링](#)
- [AWS SDK AWS Organizations 에서 사용](#)

에 가입 AWS

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 따르세요.

등록 절차 중 전화 또는 텍스트 메시지를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

에 가입하면 AWS 계정AWS 계정 루트 사용자의 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 확인하고 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 필요하면 AWS Sign-In 사용 설명서의 [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 활성화를 참조하세요.](#)

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

지침은 AWS IAM Identity Center 사용 설명서의 [AWS IAM Identity Center설정](#)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 의 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 필요하면 AWS Sign-In 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 [그룹 추가](#)를 참조하세요.

액세스 AWS Organizations

다음 AWS Organizations 방법 중 하나를 사용할 수 있습니다.

AWS Management Console

[AWS Organizations 콘솔](#)은 조직과 AWS 리소스를 관리하는 데 사용할 수 있는 브라우저 기반 인터페이스입니다. 콘솔을 사용하여 조직에서 모든 작업을 수행할 수 있습니다.

AWS 명령줄 도구

AWS 명령줄 도구를 사용하면 시스템의 명령줄에서 명령을 실행하여 AWS Organizations 및 AWS 작업을 수행할 수 있습니다. 명령줄로 작업하는 것이 콘솔을 사용하는 것보다 더 빠르고 편리할 수 있습니다. AWS 작업을 수행하는 스크립트를 작성할 때도 명령줄 도구가 유용합니다.

AWS 는 두 가지 명령줄 도구 세트를 제공합니다.

- [AWS Command Line Interface](#)

AWS Command Line Interface (AWS CLI)를 관리하기 위한 통합 도구입니다 AWS 서비스. 다운로드 및 구성할 도구를 하나만 사용하면 명령줄 AWS 서비스 에서 여러를 제어하고 스크립트를 통해 자동화할 수 있습니다.

설치 및 사용에 대한 자세한 내용은 [AWS Command Line Interface 사용 설명서](#)를 AWS CLI참조하세요.

- [AWS Tools for Windows PowerShell](#)

Tools for Windows PowerShell을 사용하면 개발자와 관리자가 PowerShell 스크립팅 환경에서 AWS 서비스 및 리소스를 관리할 수 있습니다. Windows, Linux 및 MacOS 환경을 관리하는 데 사용하는 것과 동일한 PowerShell 도구를 사용하여 AWS 리소스를 관리할 수 있습니다.

Tools for Windows PowerShell 도구를 설치하고 사용하는 방법에 대한 자세한 내용은 [AWS Tools for PowerShell 사용 설명서](#)를 참조하세요.

AWS SDK

AWS SDKs는 다양한 프로그래밍 언어 및 플랫폼(예: Java, Python, Ruby, .NET, iOS, Android)을 위한 라이브러리와 샘플 코드로 구성됩니다. SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 처리합니다. 다운로드 및 설치 방법을 포함하여 AWS SDKs에 대한 자세한 내용은 [Amazon Web Services용 도구](#)를 참조하세요.

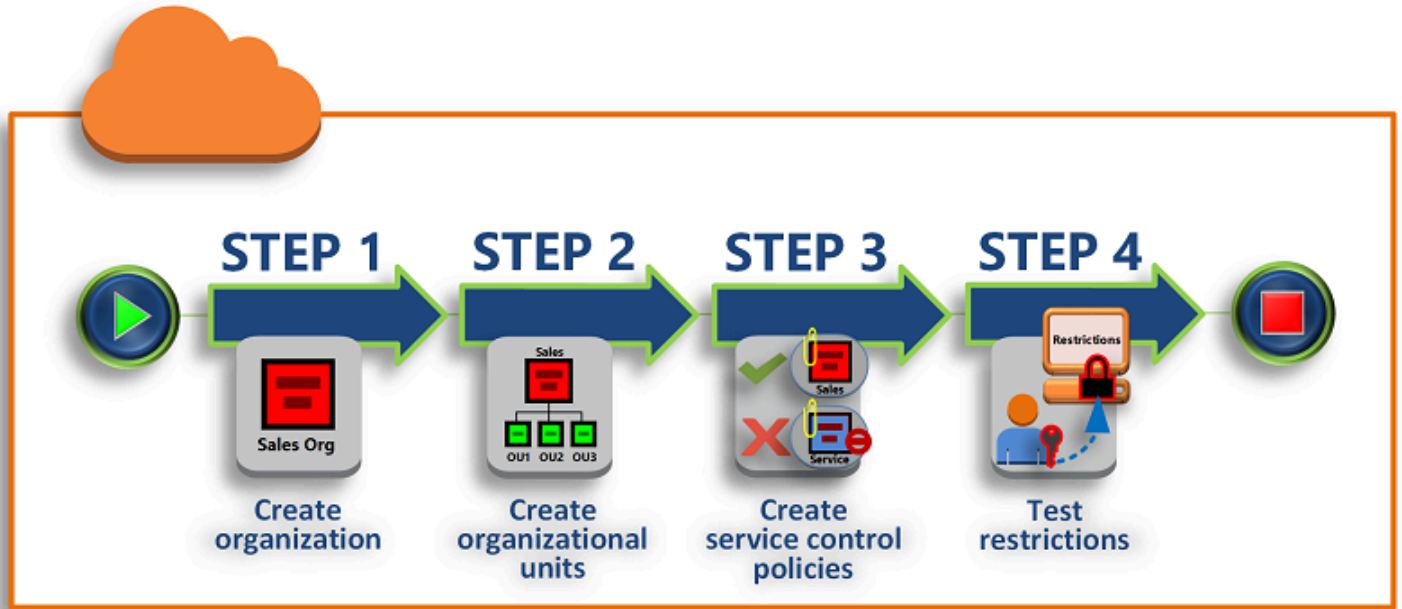
AWS Organizations HTTPS 쿼리 API

AWS Organizations HTTPS 쿼리 API를 사용하면 AWS Organizations 및에 프로그래밍 방식으로 액세스할 수 있습니다 AWS. HTTPS 쿼리 API를 이용하면 HTTPS 요청을 서비스에 바로 보낼 수 있습니다. HTTPS API를 사용할 때는 자격 증명을 사용하여 요청에 디지털 방식으로 서명하는 코드를 포함해야 합니다. 자세한 정보는 [HTTP 쿼리 요청을 통한 API 호출](#) 및 [AWS Organizations API 참조](#)를 참조하세요.

자습서: 조직 생성 및 구성

이 자습서에서는 조직을 생성하고 두 개의 AWS 멤버 계정으로 구성합니다. 조직 내 멤버 계정 하나를 만들고, 다른 계정을 조직에 초대합니다. 그런 다음에는 [허용 목록](#) 기법을 사용하여 명시적으로 나열된 서비스와 작업만 계정 관리자가 위임할 수 있도록 지정합니다. 이를 통해 관리자는에서 AWS 제공하는 새로운 서비스를 회사 내 다른 사람이 사용하도록 허용하기 전에 검증할 수 있습니다. 이렇게 하면에서 새 서비스를 AWS 도입하는 경우 관리자가 적절한 정책의 허용 목록에 서비스를 추가할 때까지 해당 서비스는 계속 금지됩니다. 또한이 자습서에서는 [거부 목록](#)을 사용하여 멤버 계정의 어떤 사용자도 AWS CloudTrail 생성하는 감사 로그의 구성을 변경할 수 없도록 하는 방법을 보여줍니다.

다음 그림은 자습서의 기본 단계를 보여줍니다.



1단계: 조직 만들기

이 단계에서는 현재를 AWS 계정 관리 계정으로 사용하여 조직을 생성합니다. 또한 조직에 가입 AWS 계정 하도록 초대하고 두 번째 계정을 멤버 계정으로 생성합니다.

2단계: 조직 단위 만들기

그런 다음에는 새로운 조직 내에 조직 단위(OU) 2개를 만들고 OU에 멤버 계정을 배치합니다.

3단계: 서비스 제어 정책 생성

서비스 제어 정책(SCP)을 사용하여 멤버 계정 사용자와 역할에 위임할 수 있는 작업을 제한할 수도 있습니다. 이 단계에서는 SCP 2개를 생성하고 조직의 OU에 연결해봅니다.

4단계: 조직 정책 테스트

각 테스트 계정에서 사용자로 로그인해 SCP가 해당 계정에 어떤 효과를 주는지 살펴보세요.

이 자습서의 어떤 단계도 AWS 청구서에 비용을 발생시키지 않습니다. AWS Organizations 는 무료 서비스입니다.

사전 조건

이 자습서에서는 두 개의 기존에 액세스할 수 있고 AWS 계정 (이 자습서의 일부로 세 번째를 생성) 각 에 관리자로 로그인할 수 있다고 가정합니다.

이 자습서에서 계정은 다음과 같은 의미가 있습니다.

- 111111111111 - 조직을 만들 때 사용하는 계정입니다. 이 계정은 관리 계정이 됩니다. 이 계정의 소유자는 OrgAccount111@example.com이라는 이메일 주소를 가집니다.
- 222222222222 - 멤버 계정으로 조직에 초대된 계정입니다. 이 계정의 소유자는 member222@example.com이라는 이메일 주소를 가집니다.
- 333333333333 - 조직의 멤버로 생성한 계정입니다. 이 계정의 소유자는 member333@example.com이라는 이메일 주소를 가집니다.

위의 값을 테스트 계정과 관련된 값으로 대체하세요. 이 자습서에서는 되도록 프로덕션 계정은 사용하지 마세요.

1단계: 조직 만들기

이번 단계에서는 111111111111 계정에 관리자로 로그인해 해당 계정을 관리 계정으로 이용해 조직을 생성하고, 기존 계정 222222222222를 멤버 계정으로 조직에 초대합니다.

AWS Management Console

1. 계정 111111111111의 관리자 AWS 로에 로그인하고 [AWS Organizations 콘솔](#)을 엽니다.
2. 소개 페이지에서 조직 생성(Create organization)을 선택합니다.
3. 확인 대화 상자에서 조직 생성(Create organization)을 선택합니다.

Note

기본적으로 조직은 모든 기능이 활성화된 상태로 생성됩니다. [통합 결제 기능](#)만 활성화하여 조직을 생성할 수도 있습니다.

AWS 는 조직을 생성하고 [AWS 계정](#) 페이지를 표시합니다. 다른 페이지에 있는 경우 왼쪽의 탐색 창에서 AWS 계정을 선택합니다.

AWS에서 이메일 주소를 확인한 적이 없는 계정을 사용하는 경우 확인 이메일이 관리 계정과 연결된 주소로 자동 전송됩니다. 확인 이메일을 받기까지 어느 정도 시간이 걸릴 수 있습니다.

4. 24시간 내에 이메일 주소를 확인하세요. 자세한 정보는 [를 사용한 이메일 주소 확인 AWS Organizations](#) 섹션을 참조하세요.

이제 여러분의 계정이 유일한 멤버 계정인 조직을 만들었습니다. 이것은 조직의 관리 계정입니다.

기존 계정을 조직에 가입하도록 초대

이제 조직을 확보했으니, 조직 내 계정 만들기를 시작할 수 있습니다. 이번 섹션의 단계에서는 기존 계정을 초대해 조직의 멤버가 되게 합니다.

AWS Management Console

기존 계정을 가입 초대하려면

1. [AWS 계정](#) 페이지로 이동하고 AWS 계정추가를 선택합니다.
2. [추가 AWS 계정](#) 페이지에서 기존 초대를 AWS 계정 선택합니다.
3. 초대할 AWS 계정 의 이메일 주소 또는 계정 ID 상자에서, 초대할 계정 소유자의 이메일 주소 (예: **member222@example.com**)를 입력합니다. 또는 AWS 계정 ID 번호를 알고 있는 경우 대신 입력할 수 있습니다.
4. 초대 이메일 메시지에 포함할 메시지(Message to include in the invitation email message) 상자에서, 원하는 텍스트를 입력합니다. 이 텍스트는 이메일에 포함되어 계정 소유자에게 전송됩니다.
5. 초대 전송을 선택합니다. 계정 소유자에게 초대를 AWS Organizations 보냅니다.

Important

메시지가 길 경우 오류 메시지를 펼칩니다. 조직에 대한 계정 한도를 초과했거나 조직이 아직 초기화되고 있기 때문에 계정을 추가할 수 없음을 나타내는 오류인 경우 조직을 생성한 후 한 시간 동안 기다렸다가 다시 시도합니다. 오류가 지속될 경우 [AWS 지원](#)에 문의하세요.

6. 자습서 목적 상 지금은 여러분 자신이 보낸 초대를 수락해야 합니다. 다음 중 하나를 수행하여 콘솔의 [Invitations] 페이지로 이동합니다.
 - 관리 계정에서 AWS 보낸 이메일을 열고 링크를 선택하여 초대를 수락합니다. 로그인 메시지가 나타나면, 초대받은 멤버 계정의 관리자로 로그인합니다.
 - [AWS Organizations 콘솔](#)을 열고 [초대](#) 페이지로 이동합니다.
7. [AWS 계정](#) 페이지에서 수락(Accept)과 확인(Confirm)을 차례로 선택합니다.

 Tip

초대 메시지의 수신이 지연될 수 있으며, 이 경우 초대를 수락하려면 기다려야 할 수 있습니다.

8. 멤버 계정에서 로그아웃한 다음 관리 계정 관리자로 다시 로그인합니다.

멤버 계정 생성

이 섹션의 단계에서 AWS 계정 는 자동으로 조직의 멤버인을 생성합니다. 자습서에서 이 계정을 333333333333이라고 하겠습니다.

AWS Management Console

멤버 계정을 만들려면

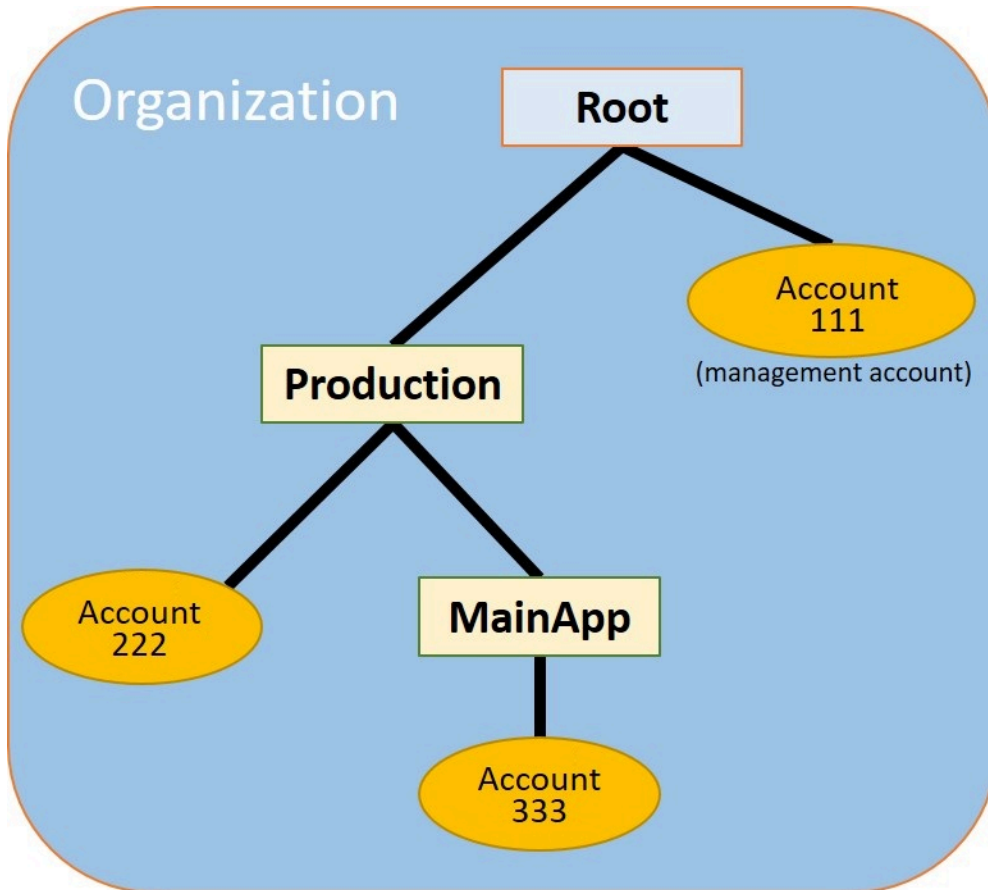
1. AWS Organizations 콘솔의 [AWS 계정](#) 페이지에서 추가 AWS 계정을 선택합니다.
2. [AWS 계정추가](#) 페이지에서 AWS 계정생성을 선택합니다.
3. AWS 계정 이름에 계정 이름을 입력합니다(예: **MainApp Account**).
4. 계정 루트 사용자의 이메일 주소(Email address of the account's root user)에서, 계정을 대표하여 소식을 받을 사람의 이메일 주소를 입력합니다. 이 값은 하나만 존재해야 합니다. 두 계정이 같은 이메일 주소를 가지면 안 됩니다. 예를 들면 **mainapp@example.com** 등을 사용할 수 있습니다.
5. [IAM role name]을 공란으로 두어 기존 역할 이름인 OrganizationAccountAccessRole을 자동으로 사용하게 하거나, 이름을 직접 입력합니다. 이 역할은 사용자가 관리 계정의 IAM 사용자로 로그인하면 새로운 멤버 계정에 액세스할 수 있게 합니다. 본 자습서에서는 이 역할 이름을 공란으로 두어 AWS Organizations 가 기본 이름으로 역할을 생성하도록 할 것입니다.
6. 생성(Create) AWS 계정을 선택합니다. [AWS 계정](#) 페이지에 새 계정이 표시되려면 페이지를 새로 고치고 잠시 기다려야 합니다.

 Important

조직에 대한 계정 한도를 초과했거나 조직이 아직 초기화되고 있기 때문에 계정을 추가할 수 없음을 나타내는 오류가 발생하면 조직을 생성한 후 한 시간 동안 기다렸다가 다시 시도하세요. 오류가 지속될 경우 [AWS 지원](#)에 문의하세요.

2단계: 조직 단위 만들기

이 섹션의 단계에서는 조직 단위(OU)를 만들고 조직 단위 내에 멤버 계정을 배치합니다. 작업이 완료되면 계층 구조가 다음 그림처럼 보일 것입니다. 관리 계정은 계속 루트에 남습니다. 멤버 계정 하나는 생산 OU로 이동하고 다른 멤버 계정은 생산 OU의 하위 OU인 MainApp OU로 이동합니다.



AWS Management Console

OU를 만들거나 채우려면

Note

다음 단계에서는 객체 자체의 이름이나 객체 옆의 라디오 버튼을 선택할 수 있는 객체와 상호 작용합니다.

- 객체 이름을 선택하면 객체 세부 정보를 표시하는 새 페이지가 열립니다.
- 객체 옆에 있는 라디오 버튼을 선택하면 메뉴 옵션 선택 등의 다른 작업 시 해당 객체가 작업을 수행하게 됩니다.

다음 단계에서는 메뉴 선택 시 연결된 객체에 대해 작업을 수행할 수 있도록 라디오 버튼을 선택할 것입니다.

1. [AWS Organizations 콘솔](#)에서 [AWS 계정](#) 페이지로 이동합니다.
 2. 루트(Root) 컨테이너 옆의 확인란 ☒ 을 선택합니다.
 3. 작업 드롭다운을 선택한 다음 조직 단위에서 새로 생성을 선택합니다.
 4. 루트에 조직 단위 생성(Create organizational unit in Root) 페이지에서 조직 단위 이름(Organizational unit name)에 **Production**을 입력한 다음 조직 단위 생성(Create organizational unit)을 선택합니다.
 5. 새 Production OU 옆에 있는 확인란 ☒ 을 선택합니다.
 6. 작업(Actions)을 선택한 다음 조직 단위(Organizational unit)에서 새로 만들기(Create new)를 선택합니다.
 7. Production에 조직 단위 생성(Create organizational unit in Production) 페이지에서 두 번째 OU 이름에 **MainApp**을 입력한 다음 조직 단위 생성(Create organizational unit)을 선택합니다.
- 이제 멤버 계정을 이상의 OU로 이동할 수 있습니다.
8. [AWS 계정](#) 페이지로 돌아가서 프로덕션 OU 옆에 있는 삼각형  을 선택해 그 아래의 트리를 확장합니다. 이렇게 하면 Production의 하위 항목인 MainApp OU가 표시됩니다.
 9. 333333333333 옆에 있는 확인란 ☒ (이름 아님)을(를) 선택하고 작업 선택 후 AWS 계정에서 이동을 선택합니다.
 10. 이동 AWS 계정 '333333333333' 페이지에서 프로덕션 옆의 삼각형  (이름 아님)을(를) 선택한 다음 AWS 계정이동을 선택합니다.

11. 222222222222 옆에 있는 확인란



(이

름 아님)을(를) 선택하고 작업 선택 후 AWS 계정에서 이동을 선택합니다.

12. 이동 AWS 계정 '222222222222' 페이지의 프로덕션 옆에 있는 라디오 버튼(이름 아님)을 선택한 다음 이동을 AWS 계정선택합니다.

3단계: 서비스 제어 정책 생성

이 섹션의 단계에서는 3가지 [서비스 제어 정책\(SCP\)](#)을 만들고 루트와 OU에 연결해 사용자가 조직 계정으로 할 수 있는 일을 제한합니다. 첫 번째 SCP는 멤버 계정의 모든 사용자가 구성한 AWS CloudTrail 로그를 생성하거나 수정하지 못하도록 합니다. 관리 계정은 어떤 SCP의 영향도 받지 않으므로 CloudTrail SCP를 적용하고 나면 관리 계정에서 로그를 생성해야 합니다.

조직에 대해 서비스 제어 정책 유형 활성화

루트 내의 OU에 특정 유형의 정책을 연결하려면, 먼저 해당 조직에 정책 유형을 활성화해야 합니다. 정책 유형은 기본적으로 비활성화되어 있습니다. 이 섹션의 단계에서는 조직에 대해 서비스 제어 정책(SCP) 유형을 활성화하는 방법을 확인할 수 있습니다.

AWS Management Console

조직에 대해 SCP를 활성화하려면

1. [정책](#) 페이지로 이동한 다음 서비스 제어 정책을 선택합니다.
2. [서비스 제어 정책](#) 페이지에서 서비스 제어 정책 활성화(Enable service control policies)를 선택합니다.

이제 조직에서 SCP를 만들 수 있음을 알리는 녹색 배너가 나타납니다.

SCP 생성

이제 조직에서 서비스 제어 정책을 활성화했으므로 이 자습서에 필요한 세 가지 정책을 만들 수 있습니다.

AWS Management Console

CloudTrail 구성 작업을 차단하는 첫 번째 SCP를 만들려면

1. [정책](#) 페이지로 이동한 다음 서비스 제어 정책을 선택합니다.

2. [서비스 제어 정책 페이지\(Service control policies\)](#)에서 정책 생성(Create policy)을 선택합니다.
3. 정책 이름(Policy name)에 **Block CloudTrail Configuration Actions**를 입력합니다.
4. 정책 섹션의 오른쪽에 있는 서비스 목록에서 CloudTrail을 서비스로 선택합니다. 그런 다음 AddTags, CreateTrail, DeleteTrail, RemoveTags, StartLogging, StopLogging 및 UpdateTrail 작업을 선택합니다.
5. 오른쪽 창에서 리소스 추가를 선택하고 CloudTrail 및 모든 리소스를 지정합니다. 그런 다음 리소스 추가를 선택합니다.

왼쪽의 정책 문은 다음과 유사해야 합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567890123",
      "Effect": "Deny",
      "Action": [
        "cloudtrail:AddTags",
        "cloudtrail:CreateTrail",
        "cloudtrail:DeleteTrail",
        "cloudtrail:RemoveTags",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

6. 정책 생성을 선택합니다.

두 번째 정책은 Production OU의 사용자와 역할에 대해 활성화하려는 서비스와 작업의 [허용 목록](#)을 정의합니다. 작업이 완료되면 Production OU의 사용자는 나열된 서비스 및 작업에만 액세스할 수 있습니다.

AWS Management Console

Production OU에 대해 승인된 서비스를 허용하는 두 번째 정책을 생성하려면

1. [서비스 제어 정책\(Service control policies\)](#) 페이지에서 정책 생성(Create policy)을 선택합니다.
2. 정책 이름(Policy name)에 **Allow List for All Approved Services**를 입력합니다.
3. 커서를 정책 섹션의 오른쪽 창에 놓고 다음과 같은 정책을 붙여 넣습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt11111111111111",
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "elasticloadbalancing:*",
        "codecommit:*",
        "cloudtrail:*",
        "codedeploy:*"
      ],
      "Resource": [ "*" ]
    }
  ]
}
```

4. 정책 생성을 선택합니다.

최종 정책은 MainApp OU에서 사용이 차단된 서비스의 [거부 목록](#)을 제공합니다. 이 자습서의 경우 MainApp OU에 있는 계정의 Amazon DynamoDB에 대한 액세스를 차단합니다.

AWS Management Console

MainApp OU에서 사용할 수 없는 서비스에 대한 액세스를 거부하는 세 번째 정책을 생성하려면

1. [서비스 제어 정책\(Service control policies\)](#) 페이지에서 정책 생성(Create policy)을 선택합니다.
2. 정책 이름(Policy name)에 **Deny List for MainApp Prohibited Services**를 입력합니다.

3. 정책(Policy) 섹션의 왼쪽에서 Amazon DynamoDB를 서비스로 선택합니다. 작업으로 모든 작업을 선택합니다.
4. 왼쪽 창에서 리소스 추가(Add resource)를 선택하고 DynamoDB 및 모든 리소스(All Resources)를 지정합니다. 그런 다음 리소스 추가를 선택합니다.

오른쪽의 정책 문이 다음과 유사하게 업데이트됩니다.

JSON

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

5. [Create policy]를 선택하여 SCP를 저장합니다.

OU에 SCP 연결

이제 SCP가 루트에서 활성화되었고, SCP를 루트와 OU에 연결할 수도 있습니다.

AWS Management Console

루트와 OU에 정책을 연결하려면

1. [AWS 계정](#) 페이지로 이동합니다.
2. [AWS 계정](#) 페이지에서 루트(라디오 버튼이 아닌 이름)를 선택하여 세부 정보 페이지로 이동합니다.
3. 루트 세부 정보 페이지에서 정책(Policies) 탭을 선택한 다음 서비스 제어 정책(Service Control Policies)에서 연결(Attach)을 선택합니다.
4. 서비스 제어 정책 연결(Attach a service control policy) 페이지에서 Block CloudTrail Configuration Actions라는 SCP 옆의 라디오 버튼을 선택한 다음 연결(Attach)을 선택합니다. 이 자습서에서는 모든 멤버 계정에 영향을 미치도록 루트에 연결하므로 다른 사람이 CloudTrail 구성을 변경하지 못합니다.

루트(Root) 세부 정보 페이지의 정책(Policies) 탭에서 이제 2개의 SCP가 루트에 연결된 것이 보입니다. 방금 연결한 것과 기본 FullAWSAccess SCP입니다.

5. 다시 [AWS 계정](#) 페이지로 이동해 프로덕션 OU(라디오 버튼이 아닌 이름)를 선택하여 세부 정보 페이지로 이동합니다.
6. Production OU의 세부 정보 페이지에서 정책(Policies) 탭을 선택합니다.
7. 서비스 제어 정책(Service Control Policies)에서 연결(Attach)을 선택합니다.
8. 서비스 제어 정책 연결(Attach a service control policy) 페이지에서 Allow List for All Approved Services 옆의 라디오 버튼을 선택한 다음 연결(Attach)을 선택합니다. 이렇게 하면 Production의 멤버 계정에 속한 사용자와 역할이 승인된 서비스에 액세스할 수 있습니다.
9. 정책(Policies) 탭을 다시 선택하면 2개의 SCP가 OU에 연결된 것이 보입니다. 방금 연결한 것과 기본 FullAWSAccess SCP입니다. 하지만 FullAWSAccess SCP는 모든 서비스와 작업을 허용하는 허용 목록이기 때문에, 승인된 서비스만 허용되도록 하려면 이제 이 SCP를 분리해야 합니다.
10. Production OU에서 기본 정책을 제거하려면 FullAWSAccess의 라디오 버튼을 선택하고, 분리(Detach)를 선택한 다음 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

이 기본 정책을 제거하면, Production OU 아래에 있는 모든 멤버 계정은 이전 단계에서 연결한 허용 목록 SCP에 없는 모든 작업 및 서비스에 대한 액세스 권한을 즉시 잃어버리게 됩니다. 모든 승인된 서비스에 대한 허용 목록 SCP에 포함되지 않은 작업을 사용하기 위한 요청은 거부됩니다. 이러한 결과는 계정의 관리자가 멤버 계정 중 하나의 사용자에게 IAM 권한 정책을 연결하여 다른 서비스에 대한 액세스 권한을 부여하는 경우에도 마찬가지입니다.

11. 이제 Deny List for MainApp Prohibited services라는 SCP를 연결해 MainApp OU에 있는 계정 사용자 전원이 제한된 서비스를 이용하지 못하도록 할 수 있습니다.

이렇게 하려면 [AWS 계정](#) 페이지로 이동하여 삼각형 아이콘을 선택하여 프로덕션 OU의 가지를 확장한 다음 MainApp OU(라디오 버튼이 아닌 이름)를 선택해 해당 콘텐츠로 이동합니다.

12. MainApp 세부 정보 페이지에서 정책(Policies) 탭을 선택합니다.
13. 서비스 제어 정책(Service Control Policies)에서 연결(Attach)을 선택한 다음, 사용 가능한 정책 목록에서 MainApp 금지 서비스에 대한 거부 목록(Deny List for MainApp Prohibited Services) 옆에 있는 라디오 버튼을 선택한 다음 정책 연결(Attach policy)을 선택합니다.

4단계: 조직 정책 테스트

이제 멤버 계정의 사용자로 [로그인](#)해 다양한 AWS 작업을 수행해볼 수 있습니다.

- 관리 계정 사용자로 로그인하면, IAM 권한 정책이 허용하는 모든 작업을 수행할 수 있습니다. SCP는 관리 계정이 어떤 루트나 OU에 있더라도 계정의 사용자나 역할에는 영향을 주지 않습니다.
- 계정 222222222222의 사용자로 로그인하는 경우 허용 목록에서 허용되는 모든 작업을 수행할 수 있습니다.는 허용 목록에 없는 모든 서비스에서 작업을 수행하려는 시도를 AWS Organizations 거부합니다. 또한 CloudTrail 구성 작업 중 하나를 수행하려는 시도를 AWS Organizations 거부합니다.
- 333333333333 계정의 사용자로 로그인하면, 허용 목록에서 허용되고 거부 목록에서 차단되지 않는 모든 작업을 수행할 수 있습니다. AWS Organizations 는 허용 목록 정책에 없는 작업과 거부 목록 정책에 있는 작업을 수행하려는 시도를 거부합니다. 또한 CloudTrail 구성 작업 중 하나를 수행하려는 시도를 AWS Organizations 거부합니다.

자습서: Amazon EventBridge를 사용하여 조직에 대한 중요 변경 사항 모니터링

이 자습서에서는 조직에 대한 변경 사항을 모니터링하도록 Amazon EventBridge(이전 Amazon CloudWatch Events)를 구성합니다. 먼저, 사용자가 특정 AWS Organizations 작업을 호출하면 트리거되는 규칙을 구성합니다. 그런 다음 규칙이 트리거될 때 AWS Lambda 함수를 실행하도록 Amazon EventBridge를 구성하고 이벤트에 대한 세부 정보가 포함된 이메일을 보내도록 Amazon SNS를 구성합니다.

다음 그림은 자습서의 기본 단계를 보여줍니다.

1단계: 추적 및 이벤트 선택기 구성

에서 추적이라는 로그를 생성합니다 AWS CloudTrail. 모든 API 호출을 캡처하도록 이를 구성합니다.

2단계: Lambda 함수 구성

이벤트에 대한 세부 정보를 S3 버킷에 로깅하는 AWS Lambda 함수를 생성합니다.

3단계: 구독자에게 이메일을 전송하는 Amazon SNS 주제 생성

이메일을 구독자에게 보내는 Amazon SNS 주제를 생성한 후, 주제를 직접 구독합니다.

4단계: Amazon EventBridge 규칙 생성

Amazon EventBridge가 지정된 API 호출 세부 사항을 Lambda 함수 및 SNS 주제 구독자에게 전달하도록 하는 규칙을 생성합니다.

5단계: Amazon EventBridge 규칙 테스트

모니터링되는 작업 중 하나를 실행하여 새 규칙을 테스트합니다. 이 자습서에서는 모니터링되는 작업이 조직 단위(OU)를 만드는 작업입니다. Lambda 함수가 생성하는 로그 항목을 확인하고, Amazon SNS가 구독자에게 보내는 이메일을 확인합니다.

도움말

이 자습서를 비슷한 작업(계정 생성 완료 시 이메일 알림 전송 등)을 구성하기 위한 가이드로 사용할 수도 있습니다. 계정 생성은 비동기 작업이기 때문에 기본적으로 완료 시 알림이 발송되지 않습니다. AWS CloudTrail 및와 함께 Amazon EventBridge를 사용하는 방법에 대한 자세한 내용은 섹션을 AWS Organizations참조하세요 [에서 로깅 및 모니터링 AWS Organizations](#).

사전 조건

이 튜토리얼은 다음과 같이 가정합니다.

- 조직의 관리 계정에서 IAM 사용자 AWS Management Console 로에 로그인할 수 있습니다. IAM 사용자에게는 CloudTrail에 로그를, Lambda에 함수를, Amazon SNS에 주제를, 그리고 Amazon EventBridge에 규칙을 생성하고 구성할 수 있는 권한이 있어야 합니다. 권한 부여에 대한 자세한 내용은 IAM 사용 설명서의 [액세스 관리](#), 또는 액세스를 구성하려는 서비스의 설명서를 참조하세요.
- 1단계에서 구성한 CloudTrail 로그를 수신하려면 기존 Amazon Simple Storage Service(Amazon S3) 버킷에 대한 액세스 권한이 있거나 버킷을 생성할 수 있는 권한이 있어야 합니다.

⚠ Important

현재 AWS Organizations 는 미국 동부(버지니아 북부) 리전에서만 호스팅됩니다(전 세계적으로 사용 가능하더라도). 이 자습서의 단계를 수행하려면 해당 리전을 사용하도록 AWS Management Console 를 구성해야 합니다.

1단계: 추적 및 이벤트 선택기 구성

이 단계에서는 관리 계정에 로그인하고 AWS CloudTrail에 로그(추적이라고 함)를 구성합니다. 또한 모든 읽기/쓰기 API 호출을 캡처하여 Amazon EventBridge에서 트리거를 일으킬 호출이 발생되도록 추적에 이벤트 선택기도 구성합니다.

추적을 생성하려면

1. 조직 관리 계정의 관리자 AWS 로에 로그인한 다음에서 CloudTrail 콘솔을 엽니다 <https://console.aws.amazon.com/cloudtrail/>.
 2. 콘솔의 오른쪽 상단에 있는 탐색 모음에서 미국 동부(버지니아 북부) 리전을 선택합니다. 다른 리전을 선택하면 Amazon EventBridge 구성 설정에 옵션으로 AWS Organizations 표시되지 않으며 CloudTrail은 관련 정보를 캡처하지 않습니다 AWS Organizations.
 3. 탐색 창에서 [Trails]를 선택합니다.
 4. 추적 생성을 선택합니다.
 5. 추적 이름에 **My-Test-Trail**을 입력합니다.
 6. 다음 옵션 중 하나를 수행하여 CloudTrail이 해당 로그를 제공하는 위치를 지정합니다.
 - 버킷을 생성해야 하는 경우 Create new S3 bucket(새 S3 버킷 생성)을 선택한 다음 Trail log bucket and folder(추적 로그 버킷 및 폴더)에 새 버킷의 이름을 입력합니다.
-  **Note**
S3 버킷 이름은 전역적으로 고유해야 합니다.
- 버킷이 이미 있는 경우 Use existing S3 bucket(기존 S3 버킷 사용)을 선택한 다음 S3 bucket(S3 버킷) 목록에서 버킷 이름을 선택합니다.
 7. 다음을 선택합니다.
 8. Choose log events(로그 이벤트 선택) 페이지의 Management events(관리 이벤트) 섹션에서 Read(읽기)와 Write(쓰기)를 선택합니다.
 9. 다음을 선택합니다.
 10. 선택 사항을 검토하고 Create trail(추적 생성)을 선택합니다.

Amazon EventBridge를 사용하면 경보 규칙이 들어오는 API 호출과 일치하는 경우 경보를 보내는 여러 가지 방법을 선택할 수 있습니다. 이 자습서에서는 API 호출을 기록할 수 있는 Lambda 함수를 호출하는 방법과, 주제의 구독자에게 이메일이나 문자 메시지를 보내는 Amazon SNS 주제에 정보를 전송하는 방법 등 두 가지 방법을 설명합니다. 다음 두 단계에서는 필요한 구성 요소인 Lambda 함수 및 Amazon SNS 주제를 생성합니다.

2단계: Lambda 함수 구성

이 단계에서는 사용자가 나중에 구성하는 Amazon EventBridge 규칙에 따라 이 함수에 전송되는 API 활동을 기록하는 Lambda 함수를 만듭니다.

Amazon EventBridge 이벤트를 기록하는 Lambda 함수를 만들려면

1. 에서 AWS Lambda 콘솔을 엽니다 <https://console.aws.amazon.com/lambda/>.
2. Lambda를 처음 사용하는 경우 시작 페이지에서 Get Started Now(지금 시작)를 선택합니다. 처음 사용하는 경우가 아니라면 Create function(함수 만들기)을 선택합니다.
3. 함수 생성 페이지에서 청사진 사용을 선택합니다.
4. 블루프린트 검색 상자에 필터로 **hello**를 입력하고 hello-world 블루프린트를 선택합니다.
5. 구성을 선택합니다.
6. 기본 정보 페이지에서 다음을 수행합니다.
 - a. Lambda 함수 이름에서 이름(Name)에 **LogOrganizationEvents**를 입력합니다.
 - b. 역할(Role)에서 기본 Lambda 권한을 가진 새 역할 생성(Create a new role with basic Lambda permissions)을 선택합니다. 이 역할은 필요한 데이터에 액세스할 수 있고 출력 로그를 쓸 수 있는 권한을 Lambda 함수에 부여합니다.
7. 다음 예와 같이 Lambda 함수 코드를 편집합니다.

```
console.log('Loading function');

exports.handler = async (event, context) => {
  console.log('LogOrganizationsEvents');
  console.log('Received event:', JSON.stringify(event, null, 2));
  return event.key1; // Echo back the first key value
  // throw new Error('Something went wrong');
};
```

이 샘플 코드는 **LogOrganizationEvents** 마커 문자열이 있는 이벤트를, 이벤트를 구성하는 JSON 문자열 앞에 기록합니다.

8. 함수 생성을 선택합니다.

3단계: 구독자에게 이메일을 전송하는 Amazon SNS 주제 생성

이 단계에서는 정보를 구독자에게 이메일로 보내는 Amazon SNS 주제를 생성합니다. 이 주제를 나중에 만드는 Amazon EventBridge 규칙의 대상으로 지정합니다.

Amazon SNS 주제를 만들어 구독자에게 이메일을 전송하려면

1. <https://console.aws.amazon.com/sns/v3/>에서 Amazon SNS 콘솔을 엽니다.
2. 탐색 창에서 주제를 선택합니다.
3. [Create new topic]을 선택합니다.
 - a. 주제 이름에 **OrganizationsCloudWatchTopic**을 입력합니다.
 - b. 표시 이름에 **OrgsCWEvnt**를 입력합니다.
 - c. 주제 생성을 선택합니다.
4. 이제 주제에 대한 구독을 생성할 수 있습니다. 방금 생성한 주제에 대한 ARN을 선택합니다.
5. 구독 생성을 선택합니다.
 - a. [Create subscription] 페이지에서 [Protocol]에 대해 [Email]을 선택합니다.
 - b. 엔드포인트에 이메일 주소를 입력합니다.
 - c. 구독 생성을 선택합니다. 이전 단계에서 지정한 이메일 주소로 이메일을 AWS 보냅니다. 해당 이메일에 도착할 때까지 기다렸다가 이메일의 구독 확인 링크를 선택하여 이메일을 잘 수신했음을 확인합니다.
 - d. 콘솔로 돌아가 페이지를 새로 고칩니다. [Pending confirmation] 메시지가 사라지고 대신 유효한 구독 ID가 표시됩니다.

4단계: Amazon EventBridge 규칙 생성

이제 필요한 Lambda 함수가 계정에 존재하므로 규칙의 기준이 충족되면 이 함수를 호출하는 Amazon EventBridge 규칙을 만듭니다.

EventBridge 규칙을 생성하려면

1. <https://console.aws.amazon.com/events/>에서 Amazon EventBridge 콘솔을 엽니다.
2. 콘솔을 미국 동부(버지니아 북부) 리전으로 설정해야 합니다. 그렇지 않으면 Organizations에 대한 정보를 사용할 수 없습니다. 콘솔의 오른쪽 상단에 있는 탐색 모음에서 미국 동부(버지니아 북부) 리전을 선택합니다.

3. 규칙을 만드는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서에서 [Amazon EventBridge의 규칙](#)을 참조하세요.

5단계: Amazon EventBridge 규칙 테스트

이 단계에서는 조직 단위(OU)를 생성한 다음 Amazon EventBridge 규칙을 살펴보고, 로그 항목을 생성하고, 이벤트에 대한 세부 정보가 들어 있는 이메일을 본인에게 전송합니다.

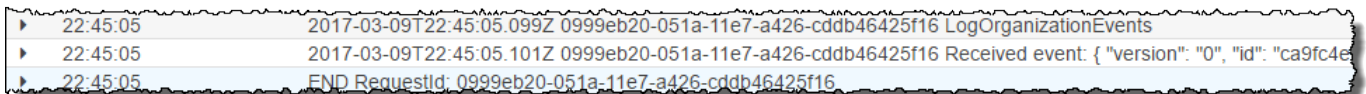
AWS Management Console

OU를 생성하려면

1. AWS Organizations 콘솔을 열어 [AWS 계정 페이지](#)로 이동합니다.
2. Root OU 확인란 ☒ 을 선택하고, 작업(Actions)을 선택한 다음 조직 단위(Organizational unit)에서 새로 만들기(Create new)를 선택합니다.
3. OU의 이름에는 **TestCWEOU**을 입력한 후 조직 단위 생성을 선택합니다.

EventBridge 로그 항목을 보려면

1. <https://console.aws.amazon.com/cloudwatch/>에서 CloudWatch 콘솔을 엽니다.
2. 탐색 페이지에서 로그를 선택합니다.
3. 로그 그룹(Log Groups) 아래에서 Lambda 함수 /aws/lambda/LogOrganizationEvents와 연결된 그룹을 선택합니다.
4. 각 그룹에는 하나 이상의 스트림이 있어야 하고, 현 시점에 그룹이 한 개 있어야 합니다. 이 값을 선택합니다.
5. 로그를 확인합니다. 다음과 같은 행이 표시될 것입니다.



```

22:45:05 2017-03-09T22:45:05.099Z 0999eb20-051a-11e7-a426-cddb46425f16 LogOrganizationEvents
22:45:05 2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event: { "version": "0", "id": "ca9fc4e
22:45:05 END RequestId: 0999eb20-051a-11e7-a426-cddb46425f16
  
```

6. 항목의 가운데 행을 선택하여 수신한 이벤트의 전체 JSON 텍스트를 확인합니다. 출력의 requestParameters 및 responseElements 섹션에서 API 요청의 세부 정보를 모두 볼 수 있습니다.

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
```

```
{
  "version": "0",
  "id": "123456-EXAMPLE-GUID-123456",
  "detail-type": "AWS API Call via CloudTrail",
  "source": "aws.organizations",
  "account": "123456789012",
  "time": "2017-03-09T22:44:26Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "eventVersion": "1.04",
    "userIdentity": {
      ...
    },
    "eventTime": "2017-03-09T22:44:26Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent": "AWS Organizations Console, aws-internal/3",
    "requestParameters": {
      "parentId": "r-exampleRootId",
      "name": "TestCWEOU"
    },
    "responseElements": {
      "organizationalUnit": {
        "name": "TestCWEOU",
        "id": "ou-exampleRootId-exampleOUIId",
        "arn": "arn:aws:organizations::123456789012:ou/o-exampleOrgId/ou-exampleRootId-exampeOUIId",
        "path": "o-exampleOrgId/r-exampleRootId/ou-exampleRootId-exampleOUIId/"
      }
    },
    "requestID": "123456-EXAMPLE-GUID-123456",
    "eventID": "123456-EXAMPLE-GUID-123456",
    "eventType": "AwsApiCall"
  }
}
```

7. 이메일 계정에서 OrgsCWEvnt(Amazon SNS 주제의 표시 이름)에서 보낸 메시지를 확인합니다. 이메일 본문에는 이전 단계에서 표시된 로그 항목과 동일한 JSON 텍스트 출력이 들어 있습니다.

정리: 더 이상 필요하지 않은 리소스 제거

요금이 발생하지 않도록 하려면 유지하지 않으려는 이 자습서의 일부로 생성한 모든 AWS 리소스를 삭제해야 합니다.

AWS 환경을 정리하려면

1. [CloudTrail 콘솔](#)을 사용하여 1단계에서 생성한 **My-Test-Trail**이라는 추적을 삭제합니다.
2. 1단계에서 Amazon S3 버킷을 만는 경우 [Amazon S3 콘솔](#)을 사용하여 버킷을 삭제합니다.
3. [Lambda 콘솔](#)을 사용하여 2단계에서 생성한 **LogOrganizationEvents**라는 함수를 삭제합니다.
4. [Amazon SNS 콘솔](#)을 사용해 3단계에서 생성한 **OrganizationsCloudWatchTopic**이라는 Amazon SNS 주제를 삭제합니다.
5. [CloudWatch 콘솔](#)을 사용하여 4단계에서 생성한 **OrgsMonitorRule**이라는 EventBridge 규칙을 삭제합니다.
6. 마지막으로 [Organizations 콘솔](#)을 사용하여 5단계에서 생성한 **TestCWE0U**라는 OU를 삭제합니다.

그러면 다 된 것입니다. 이 자습서에서는 조직에 대한 변경 사항을 모니터링하도록 EventBridge를 구성했습니다. 또한 사용자가 특정 AWS Organizations 작업을 호출하면 트리거되는 규칙을 구성했습니다. 이 규칙은 이벤트를 기록하고 해당 이벤트에 대한 세부 정보가 들어 있는 이메일을 전송하는 Lambda 함수를 실행했습니다.

AWS SDK AWS Organizations 에서 사용

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

SDK 설명서	코드 예제
AWS SDK for C++	AWS SDK for C++ 코드 예제
AWS CLI	AWS CLI 코드 예제
AWS SDK for Go	AWS SDK for Go 코드 예제
AWS SDK for Java	AWS SDK for Java 코드 예제

SDK 설명서	코드 예제
AWS SDK for JavaScript	AWS SDK for JavaScript 코드 예제
AWS SDK for Kotlin	AWS SDK for Kotlin 코드 예제
AWS SDK for .NET	AWS SDK for .NET 코드 예제
AWS SDK for PHP	AWS SDK for PHP 코드 예제
AWS Tools for PowerShell	AWS Tools for PowerShell 코드 예제
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 코드 예제
AWS SDK for Ruby	AWS SDK for Ruby 코드 예제
AWS SDK for Rust	AWS SDK for Rust 코드 예제
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP 코드 예제
AWS SDK for Swift	AWS SDK for Swift 코드 예제

예제 가용성

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

를 사용하여 조직 관리 AWS Organizations

조직은 중앙에서 관리하고 최상위에 루트가 있고 루트 아래에 조직 단위가 있는 계층적 트리형 구조로 구성할 수 있는 AWS 계정 있는 모음입니다. 각 계정은 루트에 바로 배치하거나, 계층 구조 내의 OU 중 하나에 배치할 수 있습니다.

각 조직은 다음으로 구성됩니다.

- 관리 계정
- 멤버 계정(없을 수도 있음)
- 조직 단위(OU)(없을 수도 있음)
- 정책(없을 수도 있음)

조직은 사용자가 설정하는 [기능 모음](#)으로 결정되는 다양한 기능을 보유합니다.

주제

- [를 사용하여 조직 생성 AWS Organizations](#)
- [를 사용한 이메일 주소 확인 AWS Organizations](#)
- [를 사용하여 확인 이메일 재전송 AWS Organizations](#)
- [를 사용하여 조직의 이메일 주소 변경 AWS Organizations](#)
- [를 사용하여 조직의 모든 기능 활성화 AWS Organizations](#)
- [관리 계정에서 조직 세부 정보 보기](#)
- [를 사용하여 조직 삭제 AWS Organizations](#)

를 사용하여 조직 생성 AWS Organizations

를 관리 계정으로 사용하여 조직을 생성할 수 있는 AWS 계정 있습니다. 조직을 생성할 때 조직이 [통합 결제](#) 기능만 지원할지, 아니면 [모든 기능\(권장\)](#)을 지원할지를 선택할 수 있습니다. 기본적으로 생성하는 조직은 모든 기능을 지원합니다.

조직 생성

를 사용하거나 AWS Management Console 또는 SDK API 중 AWS CLI 하나의 명령을 사용하여 조직을 생성할 수 있습니다. APIs

i 최소 권한

현재 로 조직을 생성하려면 다음 권한이 AWS 계정 있어야 합니다.

- organizations:CreateOrganization
- iam:CreateServiceLinkedRole

이 권한은 서비스 보안 주체 organizations.amazonaws.com에 대해서만 제한할 수 있습니다.

AWS Management Console

조직을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 기본적으로 조직은 모든 기능이 활성화된 상태로 생성됩니다. 그러나 다음 단계 중 하나를 선택할 수 있습니다.
 - 모든 기능을 활성화한 상태로 조직을 생성하려면 소개 페이지에서 조직 생성(Create an organization)을 선택합니다.
 - 통합 결제 기능만 있는 조직을 생성하려면 소개 페이지의 조직 생성(Create an organization)에서 통합 결제 기능(consolidated billing features)을 선택하고 확인 대화 상자에서 조직 생성(Create an organization)을 선택합니다.

실수로 잘못된 옵션을 선택했다면 즉시 [설정\(Settings\)](#) 페이지로 이동한 다음 조직 삭제>Delete organization)를 선택하여 다시 시작할 수 있습니다.

3. 조직이 생성되고 [AWS 계정](#) 페이지가 표시됩니다. 표시되는 유일한 계정은 관리 계정입니다. 이 계정은 현재 [루트 조직 단위\(OU\)](#)에 저장되어 있습니다.

필요한 경우 Organizations가 관리 계정과 연결된 주소로 확인 이메일을 자동으로 전송합니다. 확인 이메일을 받기까지 어느 정도 시간이 걸릴 수 있습니다. 24시간 내에 이메일 주소를 확인하세요. 자세한 정보는 [를 사용한 이메일 주소 확인 AWS Organizations](#) 섹션을 참조하세요. 관리 계정의 이메일 주소를 확인하지 않고 새 계정을 만들어 조직에 추가할 수 있습니다. 그러나 기존 계정을 초대하는 경우 먼저 이메일 확인을 완료해야 합니다.

Note

해당 계정에서 이전에 이메일 주소를 확인한 경우 계정을 사용하여 조직을 만들 때 다시 요청되지 않습니다.

AWS CLI & AWS SDKs

다음 코드 예시는 CreateOrganization의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
public class CreateOrganization
{
    /// <summary>
    /// Creates an Organizations client object and then uses it to create
    /// a new organization with the default user as the administrator, and
    /// then displays information about the new organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var response = await client.CreateOrganizationAsync(new
        CreateOrganizationRequest
```

```

        {
            FeatureSet = "ALL",
        });

        Organization newOrg = response.Organization;

        Console.WriteLine($"Organization: {newOrg.Id} Main Account:
{newOrg.MasterAccountId}");
    }
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [CreateOrganization](#)을 참조하세요.

CLI

AWS CLI

예 1: 새 조직을 생성하는 방법

Bill은 111111111111 계정의 자격 증명을 사용하여 조직을 만들려고 합니다. 다음 예시에서는 해당 계정이 새 조직의 마스터 계정이 되는 것을 보여줍니다. Bill이 기능 세트를 지정하지 않기 때문에 새 조직에서는 기본적으로 모든 기능이 활성화되고 서비스 제어 정책은 루트에서 활성화됩니다.

```
aws organizations create-organization
```

출력에는 새 조직의 세부 정보가 있는 조직 객체가 포함됩니다.

```

{
    "Organization": {
        "AvailablePolicyTypes": [
            {
                "Status": "ENABLED",
                "Type": "SERVICE_CONTROL_POLICY"
            }
        ],
        "MasterAccountId": "111111111111",
        "MasterAccountArn": "arn:aws:organizations::111111111111:account/o-exampleorgid/111111111111",
    }
}

```

```

        "MasterAccountEmail": "bill@example.com",
        "FeatureSet": "ALL",
        "Id": "o-exampleorgid",
        "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
    }
}

```

예 2: 통합 결제 기능만 활성화된 새 조직 생성

다음 예시에서는 통합 결제 기능만 지원하는 조직을 만듭니다.

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

출력에는 새 조직의 세부 정보가 있는 조직 객체가 포함됩니다.

```

{
    "Organization": {
        "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
        "AvailablePolicyTypes": [],
        "Id": "o-exampleorgid",
        "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
        "MasterAccountEmail": "bill@example.com",
        "MasterAccountId": "111111111111",
        "FeatureSet": "CONSOLIDATED_BILLING"
    }
}

```

자세한 내용은 AWS Organizations 사용자 안내서의 조직 생성을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 [CreateOrganization](#)을 참조하세요.

조직을 생성한 후 관리 계정에서 다음과 같은 방법으로 조직에 계정을 추가할 수 있습니다.

- [조직에 멤버 계정으로 자동 추가되는 다른 AWS 계정을 만듭니다.](#)
- [이메일 주소를 확인한 후 기존 AWS 계정을 초대](#)하여 조직에 멤버 계정으로 가입시킬 수 있습니다.

를 사용한 이메일 주소 확인 AWS Organizations

조직을 생성한 후 조직에 가입하도록 계정을 초대하려면 조직의 관리 계정에 대해 제공한 이메일 주소의 소유자임을 입증해야 합니다.

조직을 생성할 때 관리 계정이 이전에 확인되지 않은 경우는 지정된 이메일 주소로 확인 이메일을 AWS 자동으로 보냅니다. 확인 이메일을 받기까지 어느 정도 시간이 걸릴 수 있습니다.

이메일 주소 확인

24시간 내에 이메일의 지침을 따라 이메일 주소를 확인합니다. 24시간 이상 경과한 경우 [확인 이메일 재전송](#)을 참조하세요.

를 사용하여 확인 이메일 재전송 AWS Organizations

24시간 내에 이메일 주소를 확인하지 않은 경우 확인 요청을 다시 보낼 수 있습니다. 이메일 주소를 확인한 후 다른 조직에 초대 AWS 계정 할 수 있습니다. 확인 이메일을 받지 못한 경우 이메일 주소가 올바른지 확인하고, 필요한 경우 수정하세요.

- 관리 계정과 연결된 이메일 주소를 확인하려면 [관리 계정에서 조직 세부 정보 보기](#) 단원을 참조하세요.
- 관리 계정과 연결된 이메일 주소를 변경하려면 AWS Billing 사용 설명서의 [AWS 계정관리](#)를 참조하세요.

AWS Management Console

확인 요청을 재전송하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [설정\(Settings\)](#) 페이지로 이동한 다음 확인 요청 보내기(Send verification request)를 선택합니다. 이 옵션은 관리 계정이 확인되지 않은 경우에만 표시됩니다.
3. 24시간 내에 이메일 주소를 확인하세요.

이메일 주소를 확인한 후 다른 AWS 계정 을 초대하여 조직에 가입시킬 수 있습니다. 자세한 내용은 [를 사용하여 계정 초대 관리 AWS Organizations](#) 단원을 참조하십시오.

를 사용하여 조직의 이메일 주소 변경 AWS Organizations

관리 계정과 연결된 이메일 주소를 변경하려면 AWS Account Management 참조 안내서의 [루트 사용자의 AWS 계정 이름, 이메일 주소 또는 암호 업데이트](#)를 참조하세요.

관리 계정의 이메일 주소를 변경할 경우 계정의 상태가 "확인되지 않은 이메일"로 돌아가고 새로운 이메일 주소에 대해 확인 프로세스를 완료해야 합니다.

Note

관리 계정의 이메일 주소를 변경하기 전에 조직에 가입하도록 계정을 초대했는데 해당 초대가 아직 수락되지 않은 경우 관리 계정의 새 이메일 주소를 확인할 때까지 초대를 수락할 수 없습니다. 먼저 [확인 요청을 다시 보내야](#) 합니다. 이메일에 응답하여 프로세스를 완료한 후에 초대된 계정에서 초대를 수락할 수 있습니다.

를 사용하여 조직의 모든 기능 활성화 AWS Organizations

AWS Organizations에는 두 가지 기능 세트가 있습니다.

- [모든 기능](#) -이 기능 세트는 선호하는 기본 작업 방법 AWS Organizations이며 결제 통합의 모든 기능을 포함합니다. 조직을 생성할 때 모든 기능 활성화가 기본값입니다. 모든 기능을 활성화하면 [지원되는 AWS 서비스 및 조직 정책과의 통합과 같이 조직에서 사용할 수 있는 고급 계정 관리 기능을 사용할 수 있습니다](#).
- [통합 결제 기능](#) -이 기능 세트는 조직 전체에서 단일 청구서를 생성하는 것으로 제한됩니다. 통합 결제에서는 다른 관리 기능을 사용할 수 없습니다.

조직을 생성할 때 통합 결제 기능만 활성화하더라도 나중에 모든 기능을 활성화할 수 있습니다. 그러나 모든 기능이 활성화된 후에는 모든 기능에서 통합 결제로 마이그레이션할 수 없습니다.

표준 마이그레이션 및 지원 마이그레이션

모든 기능으로 마이그레이션하기 위한 두 가지 접근 방식은 표준 마이그레이션과 지원 마이그레이션입니다.

표준 마이그레이션은 모든 AWS Organizations 고객이 모든 기능 모드를 활성화할 수 있는 셀프 서비스 프로세스입니다.

지원 마이그레이션은 Enterprise Support 플랜 고객이 조직을 사용자를 대신하여 모든 기능 모드로 AWS 마이그레이션하도록 요청하는 프로세스입니다.

Note

단방향 프로세스 및 롤백 프로세스

- 통합 결제 기능에서 모든 기능으로 마이그레이션하는 것은 단방향 작업입니다. 조직을 모든 기능 활성화에서 통합 결제 기능 전용으로 다시 바꿀 수는 없습니다.
- 지원 마이그레이션 프로세스를 시작한 후에는 롤백할 수 없습니다. 대신 표준 프로세스를 진행하려면 프로세스가 완료될 때까지 90일을 대기해야 합니다.

주제

- [고려 사항](#)
- [Organizations를 사용하여 모든 기능을 활성화하는 표준 마이그레이션 프로세스](#)
- [Organizations를 사용하여 모든 기능을 활성화하는 지원 마이그레이션 프로세스](#)

고려 사항

통합 결제 기능만 지원하는 조직에서 모든 기능을 지원하는 조직으로 전환하기 전에 다음 사항을 고려하세요.

초대된 계정은 마이그레이션을 반드시 승인

모든 기능을 활성화하는 프로세스를 시작하면는 조직에 가입하도록 초대된 모든 멤버 계정에 요청을 AWS Organizations 보냅니다. 초대받은 모든 계정은 요청을 수락해 모든 기능 활성화를 승인해야 합니다. 승인을 받아야 조직 내 모든 기능을 활성화하는 과정을 완료할 수 있습니다. 계정이 요청을 거부하는 경우 조직에서 계정을 제거하거나 요청을 다시 보내야 합니다. 모든 기능을 활성화하는 프로세스를 완료하려면 먼저 요청을 수락해야 합니다. 으로 생성한 AWS Organizations 계정은 추가 제어 승인이 필요 없기 때문에 요청을 받지 않습니다.

초대된 계정에 현재 활성화된 기능 집합에 대한 알림 전송됨

초대된 계정의 소유자는 초대를 통해 통합 결제만 있는 조직에 가입하는지, 아니면 모든 기능이 활성화된 조직에 가입하는지를 알 수 있습니다. 모든 기능을 활성화하는 동안 계속해서 조직에 계정을 초대할 수 있습니다.

모든 기능을 활성화하는 프로세스 중에 계정을 초대하는 경우 가입하려는 조직에 모든 기능이 활성화되어 있다는 내용이 초대에 표시됩니다. 해당 계정이 초대를 수락하기 전에 모든 기능을 활성화하는 프로세스를 취소하면 해당 초대가 취소됩니다. 통합 결제 기능만 있는 조직의 멤버가 되게 하려면 계정을 다시 초대해야 합니다.

계정을 초대했는데 모든 기능을 활성화하기 위한 프로세스를 시작하기 전에 초대가 아직 수락되지 않은 경우 초대가 취소됩니다. 조직에 통합 결제 기능만 있다고 초대에 명시되어 있기 때문입니다. 모든 기능을 활성화한 조직의 멤버가 되게 하려면 계정을 다시 초대해야 합니다.

조직에서 계정을 생성하는 프로세스는 마이그레이션의 영향을 받지 않음

조직에 계정을 계속 만들 수도 있습니다. 이 프로세스는 해당 변경의 영향을 받지 않습니다.

AWSServiceRoleForOrganizations 서비스 연결 역할 필요

AWS Organizations 는 모든 멤버 계정에 라는 서비스 연결 역할이 있는지 확인합니다 **AWSServiceRoleForOrganizations**. 이 역할은 모든 계정에서 모든 기능을 활성화하는 데 필수적입니다. 초대된 계정의 역할을 삭제했다면 모든 기능을 활성화하는 초대를 수락하여 역할을 다시 생성합니다. 를 사용하여 생성된 계정에서 역할을 삭제한 경우 AWS Organizations 해당 계정은 해당 역할을 다시 생성하라는 초대를 받습니다. 조직이 모든 기능을 활성화하는 절차를 완료하려면 이러한 모든 초대가 수락되어야 합니다.

Organizations를 사용하여 모든 기능을 활성화하는 표준 마이그레이션 프로세스

이 주제에서는 표준 마이그레이션 프로세스를 통해 모든 기능을 활성화하는 방법을 설명합니다.

1단계: 초대된 계정에 마이그레이션을 승인하도록 요청(관리 계정)

조직의 관리 계정에 로그인하면, 모든 기능을 활성화하는 프로세스를 시작할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

최소 권한

조직 내 모든 기능을 활성화하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:EnableAllFeatures`
- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

초대한 멤버 계정에 조직 내 모든 기능 활성화에 동의하도록 요청

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [설정](#) 탭에서 모든 기능을 활성화하는 프로세스 시작을 선택합니다.
3. [모든 기능 활성화](#) 페이지에서 모든 기능을 활성화하는 프로세스 시작을 선택하여 전환한 후에는 통합 결제 기능만으로는 돌아갈 수 없다는 점을 양해해 주시기 바랍니다.

AWS Organizations 는 조직의 모든 기능을 활성화하기 위한 승인을 요청하는 요청을 조직의 모든 초대된(생성되지 않은) 계정으로 보냅니다. 를 사용하여 생성된 계정이 AWS Organizations 있고 멤버 계정 관리자가 라는 서비스 연결 역할을 삭제한 경우는 해당 계정에 역할을 다시 생성하라는 요청을 AWSServiceRoleForOrganizations AWS Organizations 보냅니다.

콘솔에 초대된 계정의 요청 승인 상태(Request approval status) 목록이 표시됩니다.

Tip

나중에 이 페이지로 돌아가려면 [설정\(Settings\)](#) 페이지를 열고 요청 전송 날짜(Request sent date) 섹션에서 상태 보기(View status)를 선택합니다.

4. [모든 기능 활성화\(Enable all features\)](#) 페이지에 조직의 각 계정에 대한 현재 요청 상태가 표시됩니다. 요청에 동의한 계정에는 수락함(ACCEPTED) 상태가 표시됩니다. 아직 동의하지 않은 계정에는 미결(OPEN) 상태가 표시됩니다.

AWS CLI & AWS SDKs

초대한 멤버 계정에 조직 내 모든 기능 활성화에 동의하도록 요청

다음 명령 중 하나를 사용하여 조직의 모든 기능을 활성화할 수 있습니다.

- AWS CLI: [enable-all-features](#)

다음 명령은 조직의 모든 기능을 활성화하는 프로세스를 시작합니다.

```
$ aws organizations enable-all-features
{
  "Handshake": {
```



```

    "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
    "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
    "Parties": [
      {
        "Id": "a1b2c3d4e5",
        "Type": "ORGANIZATION"
      }
    ],
    "State": "REQUESTED",
    "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
    "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
    "Action": "ENABLE_ALL_FEATURES",
    "Resources": [
      {
        "Value": "o-a1b2c3d4e5",
        "Type": "ORGANIZATION"
      }
    ]
  }
}

```

출력 결과에는 초대된 멤버 계정이 동의해야 하는 핸드셰이크의 세부 정보가 나타납니다.

- AWS SDKs: [EnableAllFeatures](#)

참고

- 요청이 멤버 계정에 전송되면 90일 카운트다운이 시작됩니다. 모든 계정은 해당 기간 내에 요청을 승인해야 하며, 승인하지 않으면 요청은 만료됩니다. 요청이 만료되면 요청 시도와 관련된 모든 요청은 취소되며, 2단계부터 다시 시작해야 합니다.
- 모든 기능을 활성화하도록 요청하면 기존의 수락되지 않은 계정 초대는 모두 취소됩니다.
- 모든 기능 마이그레이션 프로세스 중에도 새 계정 초대를 시작하고 새 계정을 생성할 수 있습니다.

조직의 초대된 모든 계정이 요청을 승인하면, 프로세스를 완료하고 모든 기능을 활성화할 수 있습니다. 또한 조직에 초대 받은 멤버 계정이 없다면 과정을 즉시 완료할 수 있습니다. 프로세스를 완료하려면 [3단계: 마이그레이션 프로세스를 완료하여 모든 기능 활성화\(관리 계정\)](#) 단원으로 진행합니다.

2단계 모든 기능을 활성화하거나 서비스 연결 역할을 다시 생성하는 요청 승인(초대된 계정)

조직의 초대 받은 멤버 계정 중 하나에 로그인하면, 관리 계정이 보낸 요청을 승인할 수 있습니다. 계정이 조직에 가입하도록 원래 초대된 경우 해당 초대는 모든 기능을 활성화하는 것이고, 필요한 경우 `AWSServiceRoleForOrganizations` 역할의 재생성 승인을 묵시적으로 포함합니다. 대신을 사용하여 계정을 생성하고 `AWSServiceRoleForOrganizations` 서비스 연결 역할을 삭제 AWS Organizations 한 경우 역할을 다시 생성하라는 초대만 받게 됩니다. 이렇게 하려면 다음 단계를 완료하세요.

Important

모든 기능을 활성화하면 조직의 관리 계정은 멤버 계정에 정책 기반 제어를 적용할 수 있습니다. 이러한 제어를 통해 사용자와 관리자가 계정에서 수행할 수 있는 작업을 제한할 수 있습니다. 이러한 제한은 계정을 조직에서 나가지 못하게 할 수 있습니다.

최소 권한

멤버 계정에 대한 모든 기능을 활성화하는 요청을 승인하려면 멤버 계정에 다음과 같은 권한이 있어야 합니다.

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:ListHandshakesForAccount` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `iam:CreateServiceLinkedRole` - 멤버 계정에 `AWSServiceRoleForOrganizations` 역할을 다시 생성해야 하는 경우에만 필요합니다.

AWS Management Console

조직 내 모든 기능 활성화 요청을 수락하는 방법

1. AWS Organizations 콘솔에서 [AWS Organizations 콘솔](#)에 로그인합니다. 멤버 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 수임하거나, 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

- 조직 내 모든 기능 활성화에 대한 동의가 계정에 어떤 의미가 있는지 읽은 다음 [Accept]를 선택합니다. 조직 내 모든 계정이 요청을 수락하고 관리 계정 관리자가 과정을 완료하기 전까지는 페이지에 진행 과정이 미완수로 표시됩니다.

AWS CLI & AWS SDKs

조직 내 모든 기능 활성화 요청을 수락하는 방법

요청을 수락하려면 "Action": "APPROVE_ALL_FEATURES"로 핸드셰이크를 수락해야 합니다.

- AWS CLI:
 - [accept-handshake](#)
 - [list-handshakes-for-account](#)

다음 예제에서는 계정에 사용할 수 있는 핸드셰이크를 표시하는 방법을 보여 줍니다. 출력의 네 번째 줄에 있는 "Id" 값은 다음 명령을 위해 필요한 값입니다.

```
$ aws organizations list-handshakes-for-account
{
  "Handshakes": [
    {
      "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
      "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
      "Parties": [
        {
          "Id": "a1b2c3d4e5",
          "Type": "ORGANIZATION"
        },
        {
          "Id": "111122223333",
          "Type": "ACCOUNT"
        }
      ],
      "State": "OPEN",
      "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
      "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
      "Action": "APPROVE_ALL_FEATURES",
      "Resources": [
        {
          "Value": "c440da758cab44068cdafc812EXAMPLE",
```

```

        "Type": "PARENT_HANDSHAKE"
      },
      {
        "Value": "o-aa111bb222",
        "Type": "ORGANIZATION"
      },
      {
        "Value": "111122223333",
        "Type": "ACCOUNT"
      }
    ]
  }
}

```

다음 예제에서는 이전 명령의 핸드셰이크 ID를 사용하여 해당 핸드셰이크를 수락합니다.

```

$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
  "Handshake": {
    "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
    "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
    "Parties": [
      {
        "Id": "a1b2c3d4e5",
        "Type": "ORGANIZATION"
      },
      {
        "Id": "111122223333",
        "Type": "ACCOUNT"
      }
    ],
    "State": "ACCEPTED",
    "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
    "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
    "Action": "APPROVE_ALL_FEATURES",
    "Resources": [
      {
        "Value": "c440da758cab44068cdafc812EXAMPLE",
        "Type": "PARENT_HANDSHAKE"
      }
    ]
  }
}

```

```
{
  {
    "Value": "o-aa111bb222",
    "Type": "ORGANIZATION"
  },
  {
    "Value": "111122223333",
    "Type": "ACCOUNT"
  }
]
}
```

- AWS SDKs
 - [list-handshakes-for-account](#)
 - [AcceptHandshake](#)

3단계: 마이그레이션 프로세스를 완료하여 모든 기능 활성화(관리 계정)

모든 초대받은 멤버 계정이 모든 기능을 활성화하는 요청을 승인해야 합니다. 조직에 초대받은 멤버 계정이 존재하지 않는 경우, [Enable all features progress] 페이지에 프로세스를 완료할 수 있음을 알리는 녹색 배너가 표시됩니다.

최소 권한

조직에 모든 기능을 활성화하는 과정을 완료하려면 다음과 같은 권한이 있어야 합니다.

- organizations:AcceptHandshake
- organizations:ListHandshakesForOrganization
- organizations:DescribeOrganization – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

모든 기능 활성화 과정 완료

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

2. [설정\(Settings\)](#) 페이지에서, 초대된 모든 계정이 모든 기능을 활성화하는 요청을 수락한 경우 페이지 상단에 녹색 상자가 나타나 이를 알려줍니다. 녹색 상자에서 계속해서 완료(Go to finalize)를 선택합니다.
3. [모든 기능 활성화](#) 페이지에서 완료를 선택한 다음 완료를 다시 선택합니다.
4. 이제 조직에 모든 기능이 활성화되었습니다.

AWS CLI & AWS SDKs

모든 기능 활성화 과정 완료

과정을 완료하려면 "Action": "ENABLE_ALL_FEATURES"로 핸드셰이크를 수락해야 합니다.

- AWS CLI:
 - [list-handshakes-for-organization](#)
 - [accept-handshake](#)

```
$ aws organizations list-handshakes-for-organization
{
  "Handshakes": [
    {
      "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
      "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
      "Parties": [
        {
          "Id": "a1b2c3d4e5",
          "Type": "ORGANIZATION"
        }
      ],
      "State": "OPEN",
      "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
      "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
      "Action": "ENABLE_ALL_FEATURES",
      "Resources": [
        {
          "Value": "o-aa111bb222",
          "Type": "ORGANIZATION"
        }
      ]
    }
  ]
}
```

```
}
```

다음 예제에서는 조직에 사용할 수 있는 핸드셰이크를 표시하는 방법을 보여 줍니다. 출력의 네 번째 줄에 있는 "Id" 값은 다음 명령을 위해 필요한 값입니다.

```
$ aws organizations accept-handshake \
  --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
  "Handshake": {
    "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
    "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
    "Parties": [
      {
        "Id": "a1b2c3d4e5",
        "Type": "ORGANIZATION"
      }
    ],
    "State": "ACCEPTED",
    "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
    "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
    "Action": "ENABLE_ALL_FEATURES",
    "Resources": [
      {
        "Value": "o-aa111bb222",
        "Type": "ORGANIZATION"
      }
    ]
  }
}
```

- AWS SDKs
 - [ListHandshakesForOrganization](#)
 - [AcceptHandshake](#)

Organizations를 사용하여 모든 기능을 활성화하는 지원 마이그레이션 프로세스

엔터프라이즈 고객인 경우 관리해야 하는 계정 수가 많아 표준 마이그레이션 프로세스를 완료하기 어려울 수 있습니다. 예를 들어 대규모 조직에서 초대된 모든 계정을 마이그레이션하기 위한 승인을 얻는데 어려움이 있을 수 있습니다.

지원 마이그레이션은 Enterprise Support 플랜을 보유한 고객이 조직을 모든 기능으로 AWS 마이그레이션하도록 요청할 수 있도록 하여이 프로세스에 도움이 됩니다. 이 프로세스를 수행하려면 모든 계정을 소유하고 있음을 확인하는 계약에 서명해야 합니다. 그런 다음 조직의 모든 멤버 계정에 마이그레이션 알림이 이메일로 전송되고 이메일 알림은 14일의 대기 기간을 트리거합니다. 이 대기 기간은 모든 기능으로의 마이그레이션이 적용되기 전에 계정을 떠나는 시간을 제공합니다.

AWS Management Console

지원 마이그레이션을 사용하여 모든 기능으로 마이그레이션하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [설정](#) 페이지에서 모든 기능 활성화를 선택한 다음 지원 마이그레이션을 선택합니다.
3. 계약 약관을 읽고 수락을 선택한 다음 모든 기능 활성화 프로세스 시작을 선택하여 마이그레이션을 시작합니다.

Note

지원 마이그레이션 프로세스를 시작하면 표준 마이그레이션 프로세스가 재정의됩니다. 현재 표준 마이그레이션 프로세스를 사용하여 모든 기능이 활성화되어 있다면 해당 프로세스가 취소되고 지원 마이그레이션 프로세스가 시작됩니다.

지원 마이그레이션 프로세스는 단방향이며 롤백 불가능

지원 마이그레이션 프로세스를 시작한 후에는 롤백할 수 없습니다. 대신 표준 프로세스를 진행하려면 프로세스가 만료될 때까지 90일을 대기해야 합니다.

지원 마이그레이션을 사용하는 경우 모든 기능에 대한 마이그레이션을 수락하기 위해 루트 사용자로 초대된 계정에 액세스하는 것을 걱정할 필요가 없습니다.

Technical Account Manager(TAM)에게 문의하여 지원 마이그레이션에 대한 정확한 세부 정보, 진행 상황 및 일정을 확인할 수 있습니다.

관리 계정에서 조직 세부 정보 보기

[AWS Organizations 콘솔](#)에서 조직의 관리 계정에 로그인하면 조직의 세부 정보를 확인할 수 있습니다.

최소 권한

조직에 대한 세부 정보를 보려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization`

AWS Management Console

조직에 대한 세부 정보를 보려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [설정\(Settings\)](#) 페이지로 이동합니다. 이 페이지에는 조직 ID, 조직의 관리 계정에 할당된 계정 이름 및 이메일 주소를 비롯해 조직에 대한 세부 정보가 표시됩니다.

AWS CLI & AWS SDKs

조직에 대한 세부 정보를 보려면

다음 명령 중 하나를 사용하여 조직의 세부 정보를 볼 수 있습니다.

- AWS CLI: [describe-organization](#)

다음 예제에서는 이 명령의 출력에 포함되는 정보를 보여줍니다.

```
$ aws organizations describe-organization
{
  "Organization": {
    "Id": "o-aa111bb222",
    "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
    "FeatureSet": "ALL",
    "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-aa111bb222/123456789012",
    "MasterAccountId": "123456789012",
```

```

    "MasterAccountEmail": "admin@example.com",
    "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
  }
}

```

⚠ Important

AvailablePolicyTypes 필드는 더 이상 사용되지 않으며 조직에서 활성화된 정책에 대한 정확한 정보를 담고 있지 않습니다. 조직에 대해 실제로 활성화된 정책 유형의 정확하고 완전한 목록을 보려면 다음 섹션의 AWS CLI 부분에 설명된 대로 ListRoots 명령을 사용합니다.

- AWS SDKs: [DescribeOrganization](#)

를 사용하여 조직 삭제 AWS Organizations

조직이 더 이상 필요 없다면, 삭제할 수 있습니다. 조직을 삭제해도 관리 계정이 해지되는 것은 아니며 조직에서 관리 계정이 제거되고 조직 자체가 삭제됩니다.

이전 관리 계정은 더 이상에서 관리하지 AWS 계정 않는 독립 실행형 계정이 됩니다 AWS Organizations. 다음과 같은 세 가지 옵션이 있습니다.

- 독립 실행형 계정으로 계속 사용할 수 있습니다.
- 이를 사용하여 다른 조직을 생성할 수 있습니다.
- 다른 조직의 초대를 수락하여 해당 조직에 멤버 계정으로 계정을 추가할 수 있습니다.

주제

- [고려 사항](#)
- [조직 삭제](#)

고려 사항

삭제된 조직은 복구할 수 없습니다.

삭제한 조직은 복구할 수 없습니다. 조직 내에 어떤 정책을 생성했든 간에 모든 계정이 삭제되며 복구할 수 없습니다.

모든 멤버 계정이 제거된 후에만 조직을 삭제할 수 있습니다.

조직의 모든 멤버 계정을 제거한 후에만 조직을 삭제할 수 있습니다. 를 사용하여 일부 멤버 계정을 생성한 경우 해당 계정 제거가 차단될 AWS Organizations 수 있습니다. 독립형 AWS 계정으로 작동하는데 필요한 모든 정보가 있는 경우에만 멤버 계정을 제거할 수 있습니다. 이러한 필수 정보를 제공한 후 계정을 삭제하는 자세한 방법은 [를 사용하여 멤버 계정에서 조직 탈퇴 AWS Organizations](#) 단원을 참조하세요.

'일시 중지됨' 상태의 멤버 계정은 조직에서 제거할 수 없습니다.

조직에서 제거하기 전에 멤버 계정을 해지한 경우 일정 기간 동안 Closed 상태가 되며 최종적으로 해지될 때까지 조직에서 계정을 제거할 수 없습니다. 이 과정에는 최대 90일이 소요될 수 있으며 모든 멤버 계정이 완전히 해지될 때까지 조직을 삭제하지 못할 수 있습니다.

조직을 삭제하여 조직에서 관리 계정을 제거하면 해당 계정에 다음과 같은 방식으로 영향을 미칠 수 있습니다.

- 계정은 자체 요금만 지불할 책임이 있으며 더 이상 다른 계정에서 발생하는 요금에 대해서는 책임이 없습니다.
- 다른 서비스와의 통합이 비활성화될 수 있습니다. 예를 들어 AWS IAM Identity Center 는 조직을 운영해야 하므로 IAM Identity Center를 지원하는 조직에서 계정을 제거하면 해당 계정의 사용자가 더 이상 해당 서비스를 사용할 수 없습니다.

조직의 관리 계정은 서비스 제어 정책(SCP)의 영향을 받지 않으므로, SCP를 더 이상 사용할 수 없게 되더라도 권한 변경은 없습니다.

모든 보고서 백업

관리 계정에서 보고서(특히 결제 보고서)를 내보내거나 백업해야 합니다. 조직을 삭제할 때는 조직 수준 보고서와 기록이 저장되지 않습니다. 모든 비용 데이터(예: Cost Explorer 데이터 세트)가 삭제됩니다. 모든 결제 기록을 완전히 내보내는 것이 좋습니다.

자세한 내용은 [비용 및 사용량 보고서](#), [Cost Explorer 보고서](#), [절감형 플랜 보고서](#), [예약 인스턴스\(RI\) 사용률 및 담당률](#)을 참조하세요.

조직 삭제

다음 절차에 따라 이전 관리 계정을 더 이상 관리되지 않는 독립 실행형으로 되돌 AWS 계정 리는 조직을 삭제합니다 AWS Organizations.

i 최소 권한

조직을 삭제하려면 관리 계정의 사용자 또는 역할로 로그인하고 다음과 같은 권한이 있어야 합니다.

- `organizations:DeleteOrganization`
- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

조직 삭제

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 조직을 삭제하기 전에 먼저 조직의 모든 계정을 제거해야 합니다. 자세한 정보는 [를 사용하여 조직에서 멤버 계정 제거 AWS Organizations](#) 섹션을 참조하세요.
3. [설정\(Settings\)](#) 페이지로 이동한 다음 조직 삭제>Delete organization)를 선택합니다.
4. 조직 삭제>Delete organization) 확인 대화 상자에서 텍스트 상자 윗줄에 표시된 조직 ID를 입력합니다. 그런 다음 조직 삭제>Delete organization)를 선택합니다.

⚠ Important

이 작업을 수행하여도 관리 계정이 해지되지는 않으며 대신 독립형 AWS 계정(으)로 돌아갑니다. 계정을 해지하려면 [를 사용하여 조직의 멤버 계정 해지 AWS Organizations](#)의 단계를 따르십시오.

AWS CLI & AWS SDKs

다음 코드 예시는 DeleteOrganization의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
{
    /// <summary>
    /// Initializes the Organizations client and then calls
    /// DeleteOrganizationAsync to delete the organization.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine("Successfully deleted organization.");
        }
        else
        {
            Console.WriteLine("Could not delete organization.");
        }
    }
}
```

```
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 [DeleteOrganization](#)을 참조하세요.

CLI

AWS CLI

조직을 삭제하는 방법

다음 예시에서는 조직을 삭제하는 방법을 보여줍니다. 이 작업을 수행하려면 조직의 마스터 계정 관리자여야 합니다. 이 예시에서는 이전에 조직에서 모든 멤버 계정, OU 및 정책을 제거했다고 가정합니다.

```
aws organizations delete-organization
```

- API 세부 정보는 AWS CLI 명령 참조의 [DeleteOrganization](#)을 참조하세요.

를 사용하여 조직의 계정 관리 AWS Organizations

AWS 계정은 AWS 리소스의 컨테이너입니다. 에서 AWS 리소스를 생성하고 관리합니다 AWS 계정.

이 주제에서는의 계정을 관리하는 방법을 설명합니다 AWS Organizations.

주제

- [를 사용하여 관리 계정 관리 AWS Organizations](#)
- [를 사용하여 멤버 계정 관리 AWS Organizations](#)
- [를 사용하여 계정 초대 관리 AWS Organizations](#)
- [를 사용하여 계정을 다른 조직으로 마이그레이션 AWS Organizations](#)
- [에서 계정 세부 정보 보기 AWS Organizations](#)
- [의 모든 계정에 대한 세부 정보 내보내기 AWS Organizations](#)
- [의 상태 모니터링 AWS 계정](#)
- [에서 계정의 대체 연락처 업데이트 AWS Organizations](#)
- [에서 계정의 기본 연락처 정보 업데이트 AWS Organizations](#)
- [에서 AWS 리전 계정 업데이트 AWS Organizations](#)

를 사용하여 관리 계정 관리 AWS Organizations

관리 계정은 조직을 생성하는 데 AWS 계정 사용하는 입니다.

관리 계정은 조직의 최종 소유자로, 보안, 인프라 및 재무 정책을 최종적으로 제어할 수 있습니다. 이 계정은 지급인 계정의 역할을 하며 조직의 계정에서 발생한 모든 요금을 지불할 책임이 있습니다.

이 주제에서는를 사용하여 관리 계정을 관리하는 방법을 설명합니다 AWS Organizations.

주제

- [관리 계정의 모범 사례](#)
- [조직 내 관리 계정 해지](#)

관리 계정의 모범 사례

AWS Organizations의 관리 계정을 안전하게 보호하려면 다음 권장 사항을 따르는 것이 좋습니다. 이러한 권장 사항에서는 [루트 사용자가 실제로 필요한 작업에만 루트 사용자를 사용하는 모범 사례 또한 준수한다고](#) 가정합니다.

주제

- [관리 계정에 액세스할 수 있는 사용자 제한](#)
- [액세스 권한이 있는 사람에 대한 검토 및 추적](#)
- [관리 계정이 필요한 작업에 대해서만 관리 계정 사용](#)
- [조직의 관리 계정에 워크로드를 배포하지 않기](#)
- [탈중앙화를 위해 관리 계정 외부에 책임 위임하기](#)

관리 계정에 액세스할 수 있는 사용자 제한

관리 계정은 계정 관리, 정책, 다른 AWS 서비스와의 통합, 통합 결제 등과 같은 언급된 모든 관리 작업의 핵심입니다. 따라서 조직을 변경할 권한이 필요한 관리자만 관리 계정에 액세스할 수 있도록 제한하십시오.

액세스 권한이 있는 사람에 대한 검토 및 추적

관리 계정에 대한 액세스 권한이 관리되고 있는지 확인하기 위해 해당 계정에 연결된 이메일 주소, 암호, MFA 및 전화번호에 액세스할 수 있는 회사 직원을 정기적으로 검토합니다. 기존의 회사 절차에 맞게 검토를 수행합니다. 적절한 사람만 액세스할 수 있도록 이 정보에 대한 월별 또는 분기별 검토를 추가합니다. 루트 사용자 자격 증명에 대한 액세스를 복구하거나 재설정하는 프로세스가 특정 개인에 의존하여 완료되지 않도록 합니다. 모든 프로세스는 당사자가 없을 가능성을 고려해야 합니다.

관리 계정이 필요한 작업에 대해서만 관리 계정 사용

관리 계정과 그 사용자 및 역할은 해당 계정으로 수행해야 하는 작업에 대해서만 사용하는 것이 좋습니다. 모든 AWS 리소스를 AWS 계정 조직의 다른 계정에 저장하고 관리 계정에서 제외합니다. 리소스를 다른 계정에 보관하는 것이 중요한 한 가지 이유는 Organizations 서비스 제어 정책(SCP)의 작동상 관리 계정의 사용자 또는 역할을 제한하지 않기 때문입니다. 관리 계정에서 리소스를 분리하면 인보이스의 요금을 파악하는 데도 도움이 됩니다.

관리 계정에서 호출해야 하는 작업 목록은 [조직의 관리 계정에서만 호출할 수 있는 작업](#)을 참조하세요.

조직의 관리 계정에 워크로드를 배포하지 않기

권한 있는 작업은 조직의 관리 계정 내에서 수행할 수 있으며 SCP는 관리 계정에는 적용되지 않습니다. 그러므로 관리 계정에 포함된 클라우드 리소스와 데이터는 관리 계정에서 관리해야 하는 항목으로만 제한해야 합니다.

탈중앙화를 위해 관리 계정 외부에 책임 위임하기

가능하면 관리 계정 외부에 책임과 서비스를 위임하는 것이 좋습니다. 관리 계정에 액세스하지 않고도 조직의 요구 사항을 관리할 수 있도록 팀에 자체 계정 권한을 부여합니다. 또한 조직 전체의 소프트웨어 AWS Service Catalog 공유 또는 스택 작성 및 배포를 위한 CloudFormation StackSets와 같이 이 기능을 지원하는 서비스에 여러 위임된 관리자를 등록할 수 있습니다.

자세한 내용은 [보안 참조 아키텍처](#), [여러 계정을 사용하여 AWS 환경 구성](#) 및 멤버 계정을 다양한 AWS 서비스의 위임된 관리자로 등록하는 방법에 대한 [AWS 서비스와 함께 사용할 수 있는 AWS Organizations](#) 제안을 참조하세요.

위임된 관리자 설정에 대한 자세한 내용은 [AWS Account Management에 대해 위임된 관리자 계정 활성화](#) 및 [에 대한 위임된 관리자 AWS Organizations](#)을(를) 참조하십시오.

조직 내 관리 계정 해지

조직 내 관리 계정을 해지하려면 먼저 조직의 모든 멤버 계정을 [해지](#)하거나 [제거](#)해야 합니다. 관리 계정을 해지하는 작업은 [해지 후 기간](#)이 만료된 후 해당 조직 내에서 생성한 모든 정책 및 AWS Organizations 인스턴스도 삭제합니다.

관리 계정 해지

다음 절차에 따라 관리 계정을 해지합니다.

Important

관리 계정을 해지하기 전에 고려 사항을 검토하고 계정 해지의 영향을 이해하는 것이 좋습니다. 자세한 내용은 AWS 계정 관리 안내서의 [계정을 해지하기 전에 알아야 할 사항](#)과 [계정을 해지한 후 예상되는 사항](#)을 참조하세요.

AWS Management Console

계정 페이지에서 관리 계정을 해지하려면

Note

AWS Organizations 콘솔에서 직접 관리 계정을 해지할 수 없습니다.

1. 종료하려는 관리 계정 [의 루트 사용자 AWS Management Console 로 로그인](#)합니다. IAM 사용자 또는 역할로 로그인한 상태에서는 계정을 해지할 수 없습니다.
2. 조직에 활성 멤버 계정이 남아 있는지 확인합니다. 이렇게 하려면 [AWS Organizations 콘솔](#)을 사용합니다. 아직 활성 상태인 멤버 계정이 있는 경우 다음 단계로 넘어가기 전에 [를 사용하여 조직의 멤버 계정 해지 AWS Organizations](#) 또는 [조직에서 멤버 계정 제거](#)에 제공된 지침을 따라야 합니다.
3. 상단 오른쪽 모서리의 탐색 모음에서 계정 이름이나 번호를 선택한 다음 계정을 선택합니다.
4. [계정 페이지에서](#) 계정 해지 버튼을 선택합니다. 계정 해지 지침을 읽고 이해해야 합니다.
5. 계정 해지 버튼을 선택하여 계정 해지 프로세스를 시작합니다.
6. 몇 분 내에 계정이 해지되었다는 확인 이메일을 받게 됩니다.

AWS CLI & AWS SDKs

이 작업은 AWS CLI 에서 또는 AWS SDKs. 이 작업을 사용해야만 수행할 수 있습니다 AWS Management Console.

를 사용하여 멤버 계정 관리 AWS Organizations

멤버 계정은 관리 계정이 AWS 계정 아닌 조직의 일부인입니다.

이 주제에서는를 사용하여 멤버 계정을 관리하는 방법을 설명합니다 AWS Organizations.

주제

- [멤버 계정의 모범 사례](#)
- [를 사용하여 조직에 멤버 계정 생성 AWS Organizations](#)
- [를 사용하여 조직의 멤버 계정에 액세스 AWS Organizations](#)

- [를 사용하여 조직의 멤버 계정 해지 AWS Organizations](#)
- [를 사용하여 멤버 계정이 해지되지 않도록 보호 AWS Organizations](#)
- [를 사용하여 조직에서 멤버 계정 제거 AWS Organizations](#)
- [를 사용하여 멤버 계정에서 조직 탈퇴 AWS Organizations](#)
- [를 사용하여 멤버 계정의 계정 이름 업데이트 AWS Organizations](#)
- [를 사용하여 멤버 계정의 루트 사용자 이메일 주소 업데이트 AWS Organizations](#)

멤버 계정의 모범 사례

조직의 멤버 계정 보안을 유지하려면 다음 권장 사항을 따르십시오. 이러한 권장 사항에서는 [루트 사용자가 실제로 필요한 작업에만 루트 사용자를 사용하는 모범 사례 또한 준수한다고](#) 가정합니다.

주제

- [계정 이름 및 속성 정의](#)
- [환경 및 계정 사용의 효율적 확장](#)
- [루트 액세스 관리를 활성화하여 멤버 계정의 루트 사용자 자격 증명 관리 단순화](#)

계정 이름 및 속성 정의

멤버 계정의 경우 계정 용도를 반영하는 명명 구조와 이메일 주소를 사용하십시오. 예를 들어, WorkloadsFooADev에는 Workloads+fooA+dev@domain.com, WorkloadsFooBDev에는 Workloads+fooB+dev@domain.com 등입니다. 조직에 대해 정의된 사용자 지정 태그가 있는 경우, 해당 태그는 계정 사용량, 비용 센터, 환경 및 프로젝트를 반영하는 계정에 할당하는 것이 좋습니다. 이렇게 하면 계정을 쉽게 식별, 구성, 검색할 수 있습니다.

환경 및 계정 사용의 효율적 확장

확장할 때 새 계정을 생성하기 전에 불필요한 중복을 방지하기 위해 유사한 요구 사항에 대한 계정이 아직 존재하지 않는지 확인합니다.는 공통 액세스 요구 사항을 기반으로 해야 AWS 계정 합니다. 샌드박스 계정 등의 계정을 재사용하려는 경우 계정에서 불필요한 리소스나 워크로드를 정리하되 나중에 사용할 수 있도록 계정을 저장해 두는 것이 좋습니다.

계정을 해지하기 전에 해지 계정 할당량 한도가 적용된다는 점을 참고하세요. 자세한 내용은 [AWS Organizations에 대한 할당량 및 서비스 제한](#) 단원을 참조하십시오. 가능하면 계정을 해지하고 새 계정을 만드는 대신 계정을 재사용하는 정리 프로세스를 구현하는 것이 좋습니다. 이렇게 하면 리소스 실행으로 인한 비용 발생과 [CloseAccount API](#) 한도에 도달하는 것을 방지할 수 있습니다.

루트 액세스 관리를 활성화하여 멤버 계정의 루트 사용자 자격 증명 관리 단순화

멤버 계정의 루트 사용자 자격 증명을 모니터링하고 제거하는 데 도움이 되도록 루트 액세스 관리를 활성화하는 것이 좋습니다. 루트 액세스 관리는 루트 사용자 자격 증명 복구를 방지하여 조직의 계정 보안을 개선합니다.

- 멤버 계정 루트 사용자 자격 증명을 제거하여 루트 사용자의 계정 복구를 방지합니다. 이는 또한 멤버 계정이 루트 사용자를 복구하지 못하게 합니다.
- 권한 있는 세션을 맡아 멤버 계정에서 다음 작업을 수행합니다.
 - 모든 위탁자의 Amazon S3 버킷 액세스를 거부하는 잘못 구성된 버킷 정책을 제거합니다.
 - 모든 위탁자가 Amazon SQS 대기열에 액세스하는 것을 거부하는 Amazon Simple Queue Service 리소스 기반 정책을 삭제합니다.
 - 멤버 계정이 루트 사용자 자격 증명을 복구하도록 허용합니다. 그러면 멤버 계정의 루트 사용자 이메일 받은 편지함에 액세스할 수 있는 사람이 루트 사용자 암호를 재설정하고 멤버 계정 루트 사용자로 로그인할 수 있습니다.

루트 액세스 관리가 활성화된 후 새로 생성된 멤버 계정은 보안 내재화되며 루트 사용자 자격 증명 없으므로 프로비저닝 후 MFA와 같은 추가 보안이 필요하지 않습니다.

자세한 내용은 AWS Identity and Access Management 사용 설명서의 [멤버 계정의 루트 사용자 자격 증명 중앙 집중화](#)를 참조하세요.

SCP를 사용하여 멤버 계정의 루트 사용자가 수행할 수 있는 작업을 제한합니다.

조직에서 서비스 제어 정책(SCP)을 만들고 조직의 루트에 연결하여 모든 멤버 계정에 적용하는 것이 좋습니다. 자세한 내용은 [조직 계정 루트 사용자 보안 인증 보안](#)을 참조하십시오.

멤버 계정에서 수행해야 하는 특정 루트 전용 작업을 제외한 모든 루트 작업을 거부할 수 있습니다. 예를 들어 다음 SCP는 멤버 계정의 루트 사용자가 “잘못 구성된 S3 버킷 정책 업데이트 및 모든 보안 주체에 대한 액세스 거부”(루트 자격 증명에 필요한 작업 중 하나)를 제외하고 AWS 서비스 API를 호출하지 못하도록 합니다. 자세한 내용은 IAM 사용 설명서의 [루트 사용자 자격 증명에 필요한 작업](#)을 참조하세요.

JSON

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

```

    {
      "Effect": "Deny",
      "NotAction": [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:DeleteBucketPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }
      }
    }
  ]
}

```

대부분의 상황에서 모든 관리 작업은 관련 관리자 권한을 보유한 멤버 계정의 AWS Identity and Access Management (IAM) 역할로 수행할 수 있습니다. 이러한 역할에는 활동을 제한하고, 기록하고, 모니터링하는 적절한 제어 기능이 적용되어야 합니다.

를 사용하여 조직에 멤버 계정 생성 AWS Organizations

이 주제에서는 조직 AWS 계정 내에서 생성하는 방법을 설명합니다 AWS Organizations. 단일 생성에 대한 자세한 내용은 [시작하기 리소스 센터](#)를 AWS 계정 참조하세요.

멤버 계정 생성 전 고려 사항

조직은 멤버 계정에 대한 **OrganizationAccountAccessRole** IAM 역할을 자동으로 생성

조직 내 멤버 계정을 생성할 때 Organizations는 멤버 계정 내에 **OrganizationAccountAccessRole** IAM 역할을 자동적으로 생성하여 관리 계정 내 사용자 및 역할이 멤버 계정에 대한 전체 관리 제어를 사용할 수 있도록 합니다. 정책이 업데이트될 때마다 동일한 관리형 정책에 연결된 추가 계정이 자동으로 업데이트됩니다. 이 역할에는 멤버 계정에 적용되는 모든 [서비스 제어 정책\(SCP\)](#)이 적용됩니다.

조직은 멤버 계정에 대한 **AWSServiceRoleForOrganizations** 서비스 연결 역할을 자동으로 생성

조직에서 멤버 계정을 생성하면 Organizations는 일부 서비스와 통합할 수 있는 AWS 서비스 연결 역할을 **AWSServiceRoleForOrganizations** 멤버 계정에 자동으로 생성합니다. 다른 서비스가 통합을 허용하도록 구성해야 합니다. 자세한 내용은 [AWS Organizations 및 서비스 연결 역할](#) 단원을 참조하십시오.

멤버 계정은 조직의 루트에서만 생성 가능

조직의 멤버 계정은 조직의 루트에서만 생성 가능합니다. 조직의 멤버 계정 루트를 생성한 후에는 OU 간에 루트를 이동할 수 있습니다. 자세한 내용은 [를 사용하여 계정을 조직 단위\(OU\)로 또는 루트와 OUs 간에 이동 AWS Organizations](#) 단원을 참조하십시오.

루트에 연결된 정책은 즉시 적용

루트에 연결된 정책이 있는 경우 생성된 계정의 모든 사용자 및 역할에 해당 정책이 즉시 적용됩니다.

조직의 [다른 AWS 서비스에 대한 서비스 신뢰를 활성화](#)한 경우 해당 신뢰할 수 있는 서비스는 서비스 연결 역할을 생성하거나 생성된 계정을 포함하여 조직의 모든 멤버 계정에서 작업을 수행할 수 있습니다.

마케팅 이메일을 수신하려면 멤버 계정 반드시 옵트인

조직의 일부로 생성한 멤버 계정은 AWS 마케팅 이메일을 자동으로 구독하지 않습니다. 마케팅 이메일을 수신하도록 계정을 옵트인하려면 <https://pages.awscloud.com/communication-preferences>을(를) 참조하세요.

에서 관리하는 조직의 멤버 계정에서 생성 AWS Control Tower 해야 합니다. AWS Control Tower

에서 조직을 관리하는 경우 AWS Control Tower 콘솔의 계정 팩토리를 사용하거나 AWS Control Tower APIs를 사용하여 멤버 AWS Control Tower 계정을 생성하는 AWS Control Tower 것이 좋습니다.

조직을 관리할 때 Organizations에서 멤버 계정을 생성하면 AWS Control Tower 계정이 등록되지 않습니다 AWS Control Tower. 자세한 내용은 AWS Control Tower 사용 설명서의 [AWS Control Tower 외부 리소스 참조](#)를 참조하세요.

멤버 계정 생성

조직의 관리 계정에 로그인하면 조직의 일부가 되는 멤버 계정을 생성할 수 있습니다.

다음 절차를 사용하여 계정을 생성하면 관리 계정에서 새 멤버 계정으로 다음 기본 연락처 정보를 AWS Organizations 자동으로 복사합니다.

- 전화번호
- 회사 이름
- 웹사이트 URL
- Address

또한 Organizations는 관리 계정에서 통신 언어 및 Marketplace 정보(일부 계정의 공급업체 AWS 리전)를 복사합니다.

최소 권한

조직의 멤버 계정을 만들려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:CreateAccount`

AWS Management Console

조직의 일부 AWS 계정 인를 자동으로 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 AWS 계정추가를 선택합니다.
3. [추가 AWS 계정](#) 페이지에서 생성 AWS 계정을 선택합니다(기본으로 선택되어 있음).
4. [생성 AWS 계정](#) 페이지의 AWS 계정 이름에서 계정에 할당할 이름을 입력합니다. 이 이름은 계정을 조직 내 다른 모든 계정과 구분하는 데 도움이 되며, 소유자의 IAM 별칭이나 이메일 이름과는 다릅니다.
5. 계정 소유자의 이메일 주소(Email address of the account's owner)에 계정 소유자의 이메일 주소를 입력합니다. 이 이메일 주소는 계정의 루트 사용자의 사용자 이름 자격 증명이 AWS 계정 되므로 이미 다른와 연결할 수 없습니다.
6. (선택 사항) 새 계정에서 자동으로 생성되는 IAM 역할에 할당할 이름을 지정합니다. 이 역할은 새로 만든 멤버 계정에 액세스할 수 있는 권한을 조직의 관리 계정에 부여합니다. 이름을 지정하지 않으면는 역할에의 기본 이름을 `AWS Organizations 부여합니다OrganizationAccountAccessRole`. 일관성을 위해 모든 계정에 기본 이름을 사용하는 것이 좋습니다.

Important

이 역할 이름을 기억해 두세요. 나중에 관리 계정을 이용하는 사용자 및 역할에게 새 계정에 대한 액세스 권한을 부여할 때 필요합니다.

7. (선택 사항) 태그 섹션에서 태그 추가를 선택하고 키 및 값(선택 사항)을 입력하여 새 계정에 하나 이상의 태그를 추가합니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 계정에는 최대 50개의 태그를 연결할 수 있습니다.
8. 생성(Create) AWS 계정을 선택합니다.
 - 조직의 계정 할당량을 초과했음을 나타내는 오류가 발생하면 [조직에 계정을 추가하려고 하면 "할당량 초과" 메시지가 표시됩니다.](#) 단원을 참조하세요.
 - 조직이 아직 초기화되고 있기 때문에 계정을 추가할 수 없음을 나타내는 오류가 발생하면 한 시간 동안 기다렸다가 다시 시도하세요.
 - AWS CloudTrail 로그에서 계정 생성 성공 여부에 대한 정보를 확인할 수도 있습니다. 자세한 내용은 [에서 로깅 및 모니터링 AWS Organizations](#) 단원을 참조하십시오.
 - 오류가 지속될 경우 [AWS Support](#)에 문의하세요.

[AWS 계정](#) 페이지가 나타나고 새 계정이 목록에 추가됩니다.

9. 이제 계정이 존재하고 관리 계정에서 사용자에게 관리자 액세스 권한을 부여하는 IAM 역할을 갖게 되었으므로 [를 사용하여 조직의 멤버 계정에 액세스 AWS Organizations](#)의 단계에 따라 계정에 액세스할 수 있습니다.

AWS CLI & AWS SDKs

다음 코드 예시는 CreateAccount의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;
```



```

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var accountName = "ExampleAccount";
        var email = "someone@example.com";

        var request = new CreateAccountRequest
        {
            AccountName = accountName,
            Email = email,
        };

        var response = await client.CreateAccountAsync(request);
        var status = response.CreateAccountStatus;

        Console.WriteLine($"The status of {status.AccountName} is
{status.State}.");
    }
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [CreateAccount](#)를 참조하세요.

CLI

AWS CLI

자동으로 조직의 일부가 되는 멤버 계정을 생성하는 방법

다음 예시에서는 조직 내에 멤버 계정을 생성하는 방법을 보여줍니다. 멤버 계정은 Production Account라는 이름과 susan@example.com이라는 이메일 주소로 구성됩니다. roleName 파라미터가 지정되지 않았으므로 Organizations는 OrganizationAccountAccessRole의 기본 이름을 사

용하여 IAM 역할을 자동으로 생성합니다. 또한 `IamUserAccessToBilling` 파라미터가 지정되지 않았으므로 IAM 사용자 또는 역할에 계정 결제 데이터에 액세스할 수 있는 충분한 권한을 허용하는 설정은 기본값인 `ALLOW`로 설정됩니다. Organizations는 Susan에게 "Welcome to AWS" 이메일을 자동으로 보냅니다.

```
aws organizations create-account --email susan@example.com --account-name "Production Account"
```

출력에는 현재 `IN_PROGRESS` 상태임을 보여주는 요청 객체가 포함됩니다.

```
{
  "CreateAccountStatus": {
    "State": "IN_PROGRESS",
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

나중에 `describe-create-account-status` 명령에 대한 `Id` 응답 값을 `create-account-request-id` 파라미터의 값으로 제공하여 요청의 현재 상태를 쿼리할 수 있습니다.

자세한 내용은 AWS Organizations 사용 설명서의 조직에서 AWS 계정 생성을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 [CreateAccount](#)를 참조하세요.

를 사용하여 조직의 멤버 계정에 액세스 AWS Organizations

조직에서 계정을 생성하면 AWS Organizations에서는 루트 사용자 외에 기본적으로 `OrganizationAccountAccessRole`이라는 IAM 역할을 자동으로 생성합니다. 이름을 생성할 때 다른 이름을 지정할 수 있지만 모든 계정에서 일관되게 이름을 지정하는 것이 좋습니다. AWS Organizations는 다른 사용자 또는 역할을 생성하지 않습니다.

조직 내 계정에 액세스하려면 다음 방법 중 하나를 사용해야 합니다.

최소 권한

조직의 다른 계정 AWS 계정 에서에 액세스하려면 다음 권한이 있어야 합니다.

- `sts:AssumeRole` – Resource 요소는 별표(*), 또는 새로운 멤버 계정에 액세스해야 하는 사용자의 계정 ID 번호로 설정해야 합니다.

Using the root user (Not recommended for everyday tasks)

조직에서 새 멤버 계정을 생성할 때 계정에는 기본적으로 루트 사용자 자격 증명이 없습니다. 계정 복구가 활성화되지 않으면 멤버 계정은 루트 사용자로 로그인하거나 루트 사용자의 암호 복구를 수행할 수 없습니다.

[멤버 계정에 대한 루트 액세스를 중앙 집중화](#)한 후 조직의 기존 멤버 계정에서 루트 사용자 자격 증명을 제거할 수 있습니다. 루트 사용자 자격 증명을 삭제하면 루트 사용자 암호, 액세스 키, 서명 인증서가 제거되고 멤버 계정의 다중 인증(MFA)이 비활성화됩니다. 이러한 멤버 계정은 루트 사용자 자격 증명 없이, 루트 사용자로 로그인할 수 없으며, 루트 사용자 암호를 복구할 수 없습니다. Organizations에서 생성하는 새 계정에는 기본적으로 루트 사용자 자격 증명 없이 생성됩니다.

루트 사용자 자격 증명 없이 멤버 계정에서 루트 사용자 자격 증명에 필요한 작업을 수행해야 하는 경우 관리자에게 문의하십시오.

루트 사용자로 멤버 계정에 액세스하려면 암호 복구 프로세스를 거쳐야 합니다. 자세한 정보는 AWS 로그인 사용 설명서의 [내 AWS 계정의 루트 사용자 암호를 잊음](#)을 참조하십시오.

루트 사용자로 멤버 계정에 액세스해야 하는 경우 다음 모범 사례를 따르십시오.

- 권한이 더욱 제한된 다른 사용자 역할을 만드는 경우를 제외하고는 루트 사용자로 계정에 액세스하지 않습니다. 그런 다음 해당 사용자나 역할로 로그인하십시오.
- [루트 사용자에서 다중 인증\(MFA\) 활성화](#) 암호를 재설정 후 [루트 사용자에게 MFA 디바이스를 할당](#)합니다.

루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 [루트 사용자 보안 인증이 필요한 작업](#)을 참조하십시오. 추가 루트 사용자 보안 권장 사항은 IAM 사용 설명서의 [AWS 계정의 루트 사용자 모범 사례](#)를 참조하십시오.

Using trusted access for IAM Identity Center

[AWS IAM Identity Center](#)에서 IAM Identity Center에 대한 신뢰할 수 있는 액세스를 사용하고 활성화합니다 AWS Organizations. 이를 통해 사용자는 회사 자격 증명으로 AWS 액세스 포털에 로그인하고 할당된 관리 계정 또는 멤버 계정의 리소스에 액세스할 수 있습니다.

자세한 내용은 AWS IAM Identity Center 사용 설명서의 [다중 계정 권한](#)을 참조하십시오. IAM Identity Center의 신뢰할 수 있는 액세스 설정에 대한 자세한 내용은 [AWS IAM Identity Center 및 AWS Organizations](#) 단원을 참조하십시오.

Using the IAM role OrganizationAccountAccessRole

의 일부로 제공된 도구를 사용하여 계정을 생성하는 경우 이러한 방식으로 생성하는 모든 새 계정에 OrganizationAccountAccessRole 있는 라는 미리 구성된 역할을 사용하여 계정에 액세스할 AWS Organizations 수 있습니다. 자세한 내용은 [를 사용하여 OrganizationAccountAccessRole이 있는 멤버 계정에 액세스 AWS Organizations](#) 단원을 참조하십시오.

기존 계정을 조직에 가입하도록 초대하고 해당 계정에서 초대를 수락한 경우, 초대받은 멤버 계정에 관리 계정이 액세스할 수 있게 허용하는 IAM 역할을 생성할 수 있습니다. 이 역할은 AWS Organizations를 사용하여 만든 계정에 자동으로 추가된 역할과 동일합니다.

이 역할을 생성하려면 [를 사용하여 초대된 계정에 대한 OrganizationAccountAccessRole 생성 AWS Organizations](#) 단원을 참조하세요.

역할을 생성한 후에는 [를 사용하여 OrganizationAccountAccessRole이 있는 멤버 계정에 액세스 AWS Organizations](#)에 있는 단계를 이용해 역할에 액세스할 수 있습니다.

주제

- [를 사용하여 초대된 계정에 대한 OrganizationAccountAccessRole 생성 AWS Organizations](#)
- [를 사용하여 OrganizationAccountAccessRole이 있는 멤버 계정에 액세스 AWS Organizations](#)

를 사용하여 초대된 계정에 대한 OrganizationAccountAccessRole 생성 AWS Organizations

조직의 일부인 멤버 계정을 생성했다면 AWS 는 기본적으로 역할을 맡을 수 있는 관리 계정의 IAM 사용자에게 관리자 권한을 부여하는 계정에 역할을 자동으로 생성합니다. 기본적으로 역할 이름은 OrganizationAccountAccessRole입니다. 자세한 정보는 [를 사용하여 OrganizationAccountAccessRole이 있는 멤버 계정에 액세스 AWS Organizations](#)을 참조하세요.

그러나 조직에 초대된 멤버 계정은 생성한 관리자 역할을 자동으로 받지 않습니다. 다음 절차에 따라 직접 획득해야 합니다. 이 작업은 생성된 계정을 위해 자동으로 설정된 역할을 복제합니다. 일관성을 유지하고 기억하기 쉽도록 되도록 직접 만든 역할과 같은 이름인 OrganizationAccountAccessRole을 사용하세요.

AWS Management Console

멤버 계정에서 AWS Organizations 관리자 역할을 생성하려면

1. <https://console.aws.amazon.com/iam/>에서 IAM 콘솔에 로그인합니다. 멤버 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 수임하거나, 루트 사용자로 로그인(권장되지 않음)해야 합니다. 사용자 또는 역할에게 IAM 역할 및 정책을 생성할 권한이 있어야 합니다.
2. IAM 콘솔에서 역할로 이동한 후 역할 생성을 선택합니다.
3. AWS 계정을 선택한 다음 다른 AWS 계정을 선택합니다.
4. 관리자 액세스를 부여하려는 관리 계정의 12자리 계정 ID 번호를 입력합니다. 옵션에서 다음 사항에 유의하세요.
 - 계정은 회사 내부의 계정이기 때문에 이 역할에 대해 외부 ID 필요(Require external ID)를 선택해서는 안 됩니다. 외부 ID 옵션에 대한 자세한 내용은 IAM 사용 설명서의 [언제 외부 ID를 사용해야 하나요?](#)를 참조하세요.
 - MFA를 활성화하고 구성했다면 멀티 팩터 인증 장치를 이용한 인증을 요구하게 할 수도 있습니다. MFA에 관한 자세한 내용은 IAM 사용 설명서의 [AWS에서 다중 인증\(MFA\) 사용](#)을 참조하세요.
5. 다음을 선택합니다.
6. 권한 추가 페이지에서 AdministratorAccess라는 AWS 관리형 정책을 선택한 후 다음을 선택합니다.
7. 이름 지정, 검토 및 생성 페이지에서 역할 이름과 설명(선택 사항)을 입력합니다. 되도록 새 계정의 역할에 할당된 기본 이름과 동일한 OrganizationAccountAccessRole을 사용하세요. [Create role]을 선택하여 변경 사항을 커밋합니다.
8. 새로운 역할이 이용 가능한 역할 목록에 표시됩니다. 새 역할의 이름을 선택하여 세부 정보를 봅니다. 제공된 링크 URL에 특히 유의해야 합니다. 이 URL을 역할에 액세스해야 하는 멤버 계정 사용자에게 제공합니다. 또한 15단계에서 필요하므로 역할 ARN을 기록해 두세요.
9. <https://console.aws.amazon.com/iam/>에서 IAM 콘솔에 로그인합니다. 이번에는 정책을 만들어서 사용자나 그룹에 할당할 권한이 있는 관리 계정의 사용자로 로그인합니다.
10. 정책으로 이동한 후 정책 생성을 선택합니다.
11. [Service]에서 [STS]를 선택합니다.
12. 작업(Actions)에서 필터 상자에 **AssumeRole**을 입력하기 시작하고 해당 항목이 나타나면 그 옆에 있는 확인란을 선택합니다.
13. 리소스에서 특정을 선택했는지 확인한 후 ARN 추가를 선택합니다.

14. AWS 멤버 계정 ID 번호를 입력한 다음 1~8단계에서 이전에 생성한 역할의 이름을 입력합니다. ARN 추가를 선택합니다.
15. 여러 멤버 계정의 역할을 맡는 권한을 부여하는 경우 각 계정에 대해 14단계 및 15단계를 반복합니다.
16. 다음을 선택합니다.
17. 검토 및 생성 페이지에서 새 정책의 이름을 입력하고 정책 생성을 선택하여 변경 사항을 저장합니다.
18. 탐색 창에서 사용자 그룹을 선택한 다음 멤버 계정의 관리를 위임하는 데 사용하려는 그룹의 이름(확인란이 아니라)을 선택합니다.
19. 권한 탭을 선택합니다.
20. 권한 추가를 선택하고 정책 연결을 선택한 다음 11~18단계에서 생성한 정책을 선택합니다.

선택한 그룹의 멤버인 사용자는 이제 9단계에서 캡처한 URL을 이용해 멤버 계정의 역할에 액세스할 수 있습니다. 이들은 조직에서 사용자가 생성한 계정에 액세스할 때와 같은 방식으로 멤버 계정에 액세스할 수 있습니다. 역할을 이용해 멤버 계정을 관리하는 방법에 대한 자세한 내용은 [를 사용하여 OrganizationAccountAccessRole이 있는 멤버 계정에 액세스 AWS Organizations](#)을(를) 참조하세요.

를 사용하여 OrganizationAccountAccessRole이 있는 멤버 계정에 액세스 AWS Organizations

AWS Organizations 콘솔을 사용하여 멤버 계정을 생성하면 OrganizationAccountAccessRole 계정에 라는 IAM 역할을 AWS Organizations 자동으로 생성합니다. 이 역할은 멤버 계정에 대한 완전한 관리 권한을 갖습니다. 이 역할에 대한 액세스 범위에는 관리 계정의 모든 보안 주체가 포함되며, 조직의 관리 계정에 해당 액세스 권한을 부여하도록 역할이 구성됩니다.

[를 사용하여 초대된 계정에 대한 OrganizationAccountAccessRole 생성 AWS Organizations](#)에 있는 단계를 이용하면 초대된 멤버 계정과 같은 역할을 만들 수 있습니다.

이 역할을 이용해 멤버 계정에 액세스하려면, 역할을 맡을 수 있는 권한이 있는 관리 계정에서 사용자로 로그인해야 합니다. 이러한 권한을 구성하려면 다음 절차를 수행해야 합니다. 관리 용이성을 위해 되도록 사용자 대신 그룹에 권한을 부여하세요.

AWS Management Console

역할 액세스를 위해 관리 계정에 있는 IAM 그룹의 멤버에게 권한을 부여하려면

1. 관리 계정에서 관리자 권한이 있는 사용자로 <https://console.aws.amazon.com/iam/>의 IAM 콘솔에 로그인합니다. 해당 사용자가 멤버 계정의 역할에 액세스하도록 IAM 그룹에 권한을 위임하기 위해 필요한 작업입니다.
2. [???](#)에서 나중에 필요한 관리형 정책 생성부터 시작합니다.

탐색 창에서 정책을 선택한 후 정책 생성을 선택합니다.

3. Visual 편집기 탭에서 서비스 선택을 선택하고 검색 상자에 **STS**를 입력하여 목록을 필터링한 다음 STS 옵션을 선택합니다.
4. 작업 섹션에서 검색 상자를 **assume**을 입력하여 목록을 필터링한 다음 AssumeRole 옵션을 선택합니다.
5. 리소스 섹션에서 특징을 선택하고 ARN 추가를 선택합니다.
6. ARN 지정 섹션에서 리소스에 대한 기타 계정을 선택합니다.
7. 방금 생성한 멤버 계정의 ID를 입력합니다.
8. 경로가 포함된 리소스 역할 이름에 이전 섹션에서 생성한 역할의 이름을 입력합니다 (OrganizationAccountAccessRole로 이름 지정 권장).
9. 대화 상자에 올바른 ARN이 표시되면 ARN 추가를 선택합니다.
10. (선택 사항) 멀티 팩터 인증(MFA)을 요구하거나 지정된 IP 주소 범위에서 역할에 대한 액세스를 제한하려면 요청 조건 섹션을 확장하고 적용할 옵션을 선택합니다.
11. 다음을 선택합니다.
12. 검토 및 생성 페이지에 새 정책 이름을 입력합니다. 예:
GrantAccessToOrganizationAccountAccessRole. 또한 설명(선택 사항)을 추가할 수도 있습니다.
13. 정책 생성을 선택하여 새로운 관리형 정책을 저장합니다.
14. 정책을 사용할 수 있으므로 그룹에 연결할 수 있습니다.

탐색 창에서 사용자 그룹을 선택하고, 멤버 계정에서 역할을 수임하도록 하고 싶은 멤버의 그룹 이름(확인란이 아니라)을 선택합니다. 필요한 경우 그룹을 새로 만들어도 됩니다.

15. 권한 탭을 선택하고 권한 추가, 정책 연결을 차례로 선택합니다.
16. (선택 사항) 검색 상자에 [Step 2](#)에서 [Step 13](#)까지 방금 생성한 정책의 이름이 표시될 때까지 정책 이름을 입력하여 목록을 필터링할 수 있습니다. 모든 정책을 선택한 다음 고객 관리형을 선택하여 모든 AWS 관리형 정책을 필터링할 수도 있습니다.

17. 정책 옆의 확인란을 선택한 다음 정책 연결을 선택합니다.

그룹의 멤버인 IAM 사용자는 이제 다음 절차에 따라 AWS Organizations 콘솔에서 새 역할로 전환할 수 있는 권한이 있습니다.

AWS Management Console

멤버 계정의 역할로 전환하려면

역할을 이용할 때, 사용자는 새 멤버 계정의 관리자 권한을 얻습니다. 새 역할로의 전환을 위해 그룹 멤버인 IAM 사용자에게 다음을 수행하도록 지시합니다.

1. AWS Organizations 콘솔의 오른쪽 상단에서 현재 로그인 이름이 포함된 링크를 선택한 다음 역할 전환을 선택합니다.
2. 관리자가 제공한 계정 ID 번호와 역할 이름을 입력합니다.
3. 표시 이름에 역할을 사용하는 동안 탐색 모음 오른쪽 위에 사용자 이름 대신 표시할 텍스트를 입력합니다. 색상을 선택할 수도 있습니다.
4. 역할 전환을 선택합니다. 이제 수행하는 모든 작업은 전환한 역할에 부여된 권한으로 수행하게 됩니다. 다시 전환할 때까지는 원래 IAM 사용자와 관련된 권한을 더 이상 이용할 수 없습니다.
5. 역할의 권한이 필요한 작업을 수행 완료했으면, 다시 일반 IAM 사용자로 전환해도 됩니다. 상단 오른쪽 모서리 부분에 표시된 역할 이름(표시 이름에 지정한 이름)을 선택한 후 **UserName**으로 돌아가기를 선택합니다.

를 사용하여 조직의 멤버 계정 해지 AWS Organizations

조직의 멤버 계정이 더 이상 필요하지 않으면 이 주제의 지침을 따라 [AWS Organizations 콘솔](#)에서 계정을 해지할 수 있습니다. 조직이 [모든 기능](#) 모드에 있는 경우에만 AWS Organizations 콘솔을 사용하여 멤버 계정을 해지할 수 있습니다.

루트 사용자로 로그인한 AWS Management Console 후의 [계정 페이지에서](#) AWS 계정 직접를 닫을 수 있습니다. 단계별 지침은 AWS 계정 관리 안내서의 [AWS 계정해지](#)를 참조하세요.

관리 계정을 해지하려면 [조직 내 관리 계정 해지](#) 섹션을 참조하세요.

멤버 계정 해지

조직의 관리 계정에 로그인하면 조직에 속한 멤버 계정을 해지할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

⚠ Important

멤버 계정을 해지하기 전에 고려 사항을 검토하고 계정 해지의 영향을 이해하는 것이 좋습니다. 자세한 내용은 AWS 계정 관리 안내서의 [계정을 해지하기 전에 알아야 할 사항](#)과 [계정을 해지한 후 예상되는 사항](#)을 참조하세요.

AWS Management Console

AWS Organizations 콘솔에서 멤버 계정을 닫으려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 해지하려는 멤버 계정의 이름을 찾아서 선택합니다. OU 계층 구조를 탐색하거나, OU 구조 없이 단순 계정 목록만 볼 수 있습니다.
3. 페이지 상단에 계정 이름 옆에 있는 해지(Close)를 선택합니다. 이 옵션은 AWS 조직이 [모든 기능](#) 모드에 있는 경우에만 사용할 수 있습니다.

i Note

[통합 결제](#) 모드를 사용하는 조직은 콘솔에서 닫기 버튼이 보이지 않습니다. 통합 결제 모드에서 계정을 해지하려면 루트 사용자로 해지하려는 계정에 로그인합니다. 계정 페이지에서 계정 해지 버튼을 선택하고 계정 ID를 입력한 다음 계정 해지 버튼을 선택합니다.

4. 계정 해지 지침을 읽고 이해해야 합니다.
5. 멤버 계정 ID를 입력한 다음 계정 해지를 선택합니다.

i Note

해지하는 모든 멤버 계정은 원래 해지 날짜 후 최대 90일 동안 AWS Organizations 콘솔의 계정 이름 옆에 CLOSED 레이블을 표시합니다. 90일이 지나면 멤버 계정이 영구적으로 닫히고 AWS Organizations 콘솔에 더 이상 표시되지 않습니다. 영구 해지 후 조직에서 계정을 제거하는 데 며칠이 걸릴 수 있습니다.

계정 페이지에서 멤버 계정을 해지하려면

선택적으로의 계정 페이지에서 직접 AWS 멤버 계정을 해지할 수 있습니다 AWS Management Console. 단계별 지침은 AWS 계정 관리 안내서의 [AWS 계정해지](#) 지침을 따르세요.

AWS CLI & AWS SDKs

를 닫으려면 AWS 계정

다음 명령 중 하나를 사용하여 AWS 계정을 해지할 수 있습니다.

- AWS CLI: [close-account](#)

```
$ aws organizations close-account \
  --account-id 123456789012
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDKs: [CloseAccount](#)

를 사용하여 멤버 계정이 해지되지 않도록 보호 AWS Organizations

멤버 계정이 우발적으로 해지되지 않도록 보호하고 싶다면 IAM 정책을 생성하여 해지가 면제되는 계정을 지정할 수 있습니다. 이 정책은 보호된 멤버 계정의 해지를 방지합니다.

다음 방법 중 하나를 사용하여 계정 해지를 거부하는 IAM 정책을 생성합니다.

- ARN을 사용하여 정책의 Resource 요소에 보호된 계정을 명시적으로 나열합니다.
- 개별 계정에 태그를 지정하고 `aws:ResourceTag` 전역 조건 키를 사용하여 태그가 지정된 계정이 해지되지 않도록 합니다.

Note

서비스 제어 정책(SCP)은 관리 계정의 IAM 주체에 영향을 주지 않습니다.

멤버 계정 해지를 방지하는 IAM 정책 예제

다음 코드 예제는 멤버 계정이 계정을 해지하지 못하도록 제한하는 데 사용할 수 있는 두 가지 방법을 보여줍니다.

Prevent member accounts with tags from getting closed

관리 계정의 자격 증명에 다음 정책을 연결할 수 있습니다. 이 정책은 `aws:ResourceTag` 태그 전역 조건 `AccountType` 키, `Critical` 태그 값을 포함하여 태그 지정된 모든 멤버가 관리 계정의 보안 주체에 의해 해지되지 않도록 방지합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PreventCloseAccountForTaggedAccts",
      "Effect": "Deny",
      "Action": "organizations:CloseAccount",
      "Resource": "*",
      "Condition": {
        "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
      }
    }
  ]
}
```

Prevent member accounts listed in this policy from getting closed

관리 계정의 자격 증명에 다음 정책을 연결할 수 있습니다. 이 정책은 관리 계정의 보안 주체가 `Resource` 요소에 명시적으로 지정된 멤버 계정을 해지하지 않도록 방지합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PreventCloseAccount",
      "Effect": "Deny",
      "Action": "organizations:CloseAccount",
      "Resource": [
        "arn:aws:organizations::555555555555:account/o-12345abcdef/123456789012",
        "arn:aws:organizations::555555555555:account/o-12345abcdef/123456789014"
      ]
    }
  ]
}
```

를 사용하여 조직에서 멤버 계정 제거 AWS Organizations

구성원 계정을 제거하면 해당 계정이 해지되는 것이 아니라 조직에서 해당 구성원 계정이 제거됩니다. 이전 멤버 계정은 더 이상에서 관리하지 AWS 계정 않는 독립 실행형 계정이 됩니다 AWS Organizations.

이후, 해당 계정에는 더 이상 정책이 적용되지 않으며 자체 청구서 결제에 대한 책임이 있습니다. 계정이 조직에서 제거된 후, 조직의 관리 계정은 해당 계정에서 발생한 비용에 대해 더 이상 청구되지 않습니다.

고려 사항

관리 계정에서 생성한 IAM 액세스 역할은 자동으로 삭제되지 않음

조직에서 멤버 계정을 제거해도 조직의 관리 계정으로 액세스할 수 있도록 생성된 IAM 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하려면 IAM 역할을 수동으로 삭제해야 합니다. 역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 [역할 또는 인스턴스 프로파일 삭제](#)를 참조하세요.

계정에 독립 실행형 계정으로 작동하는 데 필요한 정보가 있는 경우에만 조직에서 계정 제거 가능

계정에 독립형 계정으로 작동하는 데 필요한 정보가 있는 경우에만 조직에서 계정을 제거할 수 있습니다. AWS Organizations 콘솔, API 또는 AWS CLI 명령을 사용하여 조직에서 계정을 생성하면 독립 실행형 계정에 필요한 모든 정보가 자동으로 수집되지 않습니다.

독립 실행형으로 만들려는 각 계정에 대해 지원 플랜을 선택하고, 필요한 연락처 정보를 제공 및 확인하고, 현재 결제 방법을 제공해야 합니다.는 계정이 조직에 연결되어 있지 않은 동안 발생하는 청구 가능한(AWS 프리 티어가 아닌) AWS 활동에 대해 결제 방법을 AWS 사용하여 요금을 청구합니다. 아직 이 정보가 없는 계정을 제거하려면 [를 사용하여 멤버 계정에서 조직 탈퇴 AWS Organizations](#)의 단계를 따르세요.

계정이 생성된 후 최소 4일이 지날 때까지 반드시 대기

조직에서 생성된 계정을 제거하려면 계정을 만든 후 4일 이상 기다려야 합니다. 초대된 계정에는 이 대기 기간이 적용되지 않습니다.

탈퇴하는 계정의 소유자에는 새로 발생하는 모든 비용에 대해 책임 있음

계정이 조직을 성공적으로 떠나는 즉시의 소유자 AWS 계정 는 발생한 모든 새 AWS 비용에 대해 책임을 지며 계정의 결제 방법이 사용됩니다. 조직의 관리 계정은 더 이상 책임이 없습니다.

계정은 조직에 대해 활성화된 AWS 서비스의 위임된 관리자 계정이 될 수 없습니다.

제거하려는 계정은 조직에 대해 활성화된 AWS 서비스의 위임된 관리자 계정이 아니어야 합니다. 계정이 위임된 관리자인 경우 먼저 위임된 관리자 계정을 조직에 남아 있는 다른 계정으로 변경해야 합니다. AWS 서비스의 위임된 관리자 계정을 비활성화하거나 변경하는 방법에 대한 자세한 내용은 해당 서비스의 설명서를 참조하세요.

계정은 더 이상 비용 및 사용량 데이터에 액세스할 수 없습니다.

멤버 계정이 조직을 탈퇴할 때 해당 계정은 조직의 멤버였을 때의 시간 범위로부터 비용 및 사용량 데이터에 대한 액세스를 할 수 없습니다. 하지만 조직의 관리 계정은 여전히 데이터에 액세스할 수 있습니다. 멤버 계정이 조직에 다시 가입하면 계정은 다시 데이터에 액세스할 수 있습니다.

계정에 연결된 태그 삭제됨

멤버 계정이 조직을 나가면 계정에 연결된 모든 태그가 삭제됩니다.

계정의 위탁자는 더 이상 조직에 적용된 정책의 영향을 받지 않음

계정의 보안 주체는 더 이상 조직에 적용된 [정책](#)의 영향을 받지 않습니다. 즉, SCP에 의해 가해지는 제한이 사라지므로 해당 계정의 사용자와 역할은 이전보다 더 많은 권한을 갖게 될 수 있습니다. 다른 조직 정책 유형은 더 이상 적용하거나 처리할 수 없습니다.

계정은 더 이상 조직 계약의 적용을 받지 않음

조직에서 삭제된 멤버 계정에는 해당 조직 계약이 더 이상 적용되지 않습니다. 필요한 경우 멤버 계정이 새 계약을 체결할 수 있도록 관리 계정 관리자는 조직에서 멤버 계정을 삭제하기 전에 이 사실을 해당 멤버 계정에게 알려줘야 합니다. 활성 조직 계약 목록은 AWS Artifact 콘솔의 [AWS Artifact 조직 계약 페이지에서 볼 수 있습니다](#).

다른 서비스와의 통합이 비활성화될 수 있음

다른 서비스와의 통합이 비활성화될 수 있습니다. AWS 서비스와의 통합이 활성화된 조직에서 계정을 제거하면 해당 계정의 사용자는 더 이상 해당 서비스를 사용할 수 없습니다.

조직에서 멤버 계정 제거

조직의 관리 계정에 로그인하면 조직에서 더 이상 필요 없는 멤버 계정을 제거할 수 있습니다. 이렇게 하려면 다음 절차를 완료하세요. 이 절차는 멤버 계정에만 적용됩니다. 관리 계정을 제거하려면 [조직을 삭제](#)해야 합니다.

❗ 최소 권한

조직에서 하나 이상의 멤버 계정을 제거하려면 다음 권한이 있는 관리 계정의 사용자 또는 역할로 로그인해야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:RemoveAccountFromOrganization`

5단계에서 멤버 계정의 사용자 또는 역할로 로그인하도록 선택할 경우 해당 사용자 또는 역할은 다음 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:LeaveOrganization` – 조직 관리자는 이 권한을 제거한 계정에 정책을 적용하여 조직에서 계정을 제거하지 못하도록 할 수 있습니다.
- IAM 사용자로 로그인했는데 계정에 결제 정보가 없는 경우 사용자에게 `aws-portal:ModifyBilling` 및 `aws-portal:ModifyPaymentMethods` 권한(계정이 아직 세분화된 권한으로 마이그레이션되지 않은 경우) 또는 `payments:CreatePaymentInstrument` 및 `payments:UpdatePaymentPreferences` 권한(계정이 세분화된 권한으로 마이그레이션된 경우)이 있어야 합니다. 또한 멤버 계정에는 결제에 대한 IAM 사용자 액세스가 활성화되어야 합니다. 아직 활성화되지 않은 경우 AWS Billing 사용 설명서의 [Billing and Cost Management 콘솔에 대한 액세스 활성화](#)를 참조하세요.

AWS Management Console

조직에서 멤버 계정을 제거하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서, 조직에서 제거할 각 멤버 계정을 찾아서 그 옆에 있는 확인란 ☒ 선택합니다. OU 계층 구조를 탐색하거나 보기 AWS 계정 전용을 활성화하여 OU 구조가 없는 계정의 플랫폼 목록을 볼 수 있습니다. 계정이 많은 경우 이동할 모든 항목을 찾기 위해 목록 하단

을

에 있는 'ou-name'에서 추가 계정 로드(Load more accounts in 'ou-name')를 선택해야 할 수도 있습니다.

[AWS 계정](#) 페이지에서, 조직에서 제거할 멤버 계정의 이름을 찾아서 선택합니다. 원하는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다



선택).

3. 작업(Actions)을 선택한 다음 AWS 계정에서 조직에서 제거(Remove from organization)를 선택합니다.
4. 'account-name'(#account-id-num) 계정을 조직에서 제거하시겠습니까?라는 대화 상자에서 계정 제거(Remove account)를 선택합니다.
5. 가 하나 이상의 계정을 제거 AWS Organizations 하지 못하는 경우 이는 일반적으로 계정이 독립 실행형 계정으로 작동하는 데 필요한 모든 정보를 제공하지 않았기 때문입니다. 다음 단계를 수행합니다.
 - a. 실패한 계정에 로그인합니다. [Copy link]를 선택하고 이를 새로운 익명 브라우저 창의 주소 표시줄에 붙여넣음으로써 로그인하는 것이 좋습니다. 링크 복사가 보이지 않는 경우 [이 링크](#)를 사용하여 AWS가입 페이지로 이동하여 누락된 등록 단계를 완료합니다. 익명 창을 사용하지 않는 경우, 관리 계정에서 로그아웃되고 이 대화 상자로 다시 돌아갈 수 없습니다.
 - b. 브라우저에서 이 계정에서 누락된 모든 단계를 완료할 로그인 절차로 직접 이동합니다. 제시되는 모든 단계를 수행합니다. 이러한 단계에는 다음 작업이 포함되어 있을 수 있습니다.
 - 연락처 정보 제공
 - 올바른 결제 방법 제공
 - 전화 번호 확인
 - 지원 플랜 옵션 선택
 - c. 마지막 가입 단계를 완료하면 AWS 가 자동으로 브라우저를 멤버 계정의 AWS Organizations 콘솔로 리디렉션합니다. [Leave organization]을 선택한 다음 확인 대화 상자에서 확인을 선택합니다. 다른 조직에 대해 보류 중인 계정 가입 초대장을 확인할 수 있는 AWS Organizations 콘솔의 시작하기 페이지로 이동했습니다.
 - d. 계정에 대한 액세스 권한을 부여하는 IAM 역할을 조직에서 제거합니다.

⚠ Important

조직에서 계정이 생성된 경우 Organizations는 조직의 관리 계정에 의한 액세스를 활성화한 IAM 역할을 계정에 자동으로 생성했습니다. 계정이 가입하도록 초대된 경우 Organizations에서 해당 역할을 자동으로 생성하지는 않았지만 사용자 또는 다른 관리자가 동일한 혜택을 받기 위해 계정을 생성했을 수 있습니다. 두 경우 모두 조직에서 계정을 제거할 때 이러한 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하려면 이 IAM 역할을 수동으로 삭제해야 합니다. 역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 [역할 또는 인스턴스 프로필 삭제](#)를 참조하세요.

AWS CLI & AWS SDKs

조직에서 멤버 계정을 제거하려면

다음 명령 중 하나를 사용하여 멤버 계정을 삭제할 수 있습니다.

- AWS CLI: [remove-account-from-organization](#)

```
$ aws organizations remove-account-from-organization \
  --account-id 123456789012
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDKs: [RemoveAccountFromOrganization](#)

조직에서 멤버 계정이 제거된 후에는 조직에서 계정에 대한 액세스 권한을 부여하는 IAM 역할을 제거해야 합니다.

⚠ Important

조직에서 계정이 생성된 경우 Organizations는 조직의 관리 계정에 의한 액세스를 활성화한 IAM 역할을 계정에 자동으로 생성했습니다. 계정이 가입하도록 초대된 경우 Organizations에서 해당 역할을 자동으로 생성하지는 않았지만 사용자 또는 다른 관리자가 동일한 혜택을 받기 위해 계정을 생성했을 수 있습니다. 두 경우 모두 조직에서 계정을 제거할 때 이러한 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하러

면 이 IAM 역할을 수동으로 삭제해야 합니다. 역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 [역할 또는 인스턴스 프로파일 삭제](#)를 참조하세요.

멤버 계정은 대신 [조직 탈퇴](#)를 통해 스스로 제거할 수 있습니다. 자세한 내용은 [를 사용하여 멤버 계정에서 조직 탈퇴 AWS Organizations](#) 단원을 참조하십시오.

를 사용하여 멤버 계정에서 조직 탈퇴 AWS Organizations

멤버 계정에 로그인하면 조직을 탈퇴할 수 있습니다. 관리 계정은 이 방법을 사용하여 조직에서 나갈 수 없습니다. 관리 계정을 제거하려면 [조직을 삭제](#)해야 합니다.

고려 사항

조직에서 계정의 상태는 어떤 비용 및 사용량 데이터가 표시되는지에 영향 받음

계정은 조직 멤버십 변경에 관계없이 자신에게 전달된 모든 과거 인보이스와 해당 인보이스가 생성한 모든 청구서 데이터에 대한 액세스를 유지합니다. 그러나 Cost Explorer 데이터 가시성은 현재 조직 멤버십과 관련이 있습니다. 아래 표는 세 가지 공통 계정 전환이 데이터 가시성에 미치는 영향을 보여줍니다.

	인보이스 가용성	청구서 가용성(예: 청구서 페이지)	Cost Explorer 가용성
시나리오 1 멤버 계정은 organizationA를 탈퇴하고 독립 실행형 계정이 됩니다.	계정은 자신에게 전달된 모든 기록 인보이스에 대한 액세스를 유지합니다.	계정은 organizationA의 멤버로 생성한 모든 과거 청구서 데이터에 대한 액세스를 유지합니다.	계정은 organizationA의 멤버로서 생성한 과거 비용 및 사용 데이터에 대한 액세스 권한을 잃습니다.
시나리오 2 멤버 계정은 organizationA를 탈퇴하고	계정은 자신에게 전달된 모든 기록 인보이스에 대한 액세스를 유지합니다.	계정은 organizationA의 멤버로 생성한 모든 과거 청구서 데이터에 대한 액세스를 유지합니다.	계정은 organizationA의 멤버로서 생성한 과거 비용 및 사용 데이터에 대한 액세스 권한을 잃습니다.

	인보이스 가용성	청구서 가용성(예: 청구서 페이지)	Cost Explorer 가용성
organizationB에 가입합니다.			
시나리오 3 계정은 이전에 속한 조직에 다시 가입합니다.	계정은 자신에게 전달된 모든 기록 인보이스에 대한 액세스를 유지합니다.	계정은 생성한 모든 과거 청구서 데이터에 대한 액세스를 유지합니다(독립 실행형 계정 또는 다른 조직의 구성원으로 생성된 경우 무관).	계정은 조직의 멤버였던 전체 기간 동안 비용 및 사용량 데이터에 대한 액세스 권한을 다시 획득하지만 현재 조직 외부에서 생성된 모든 과거 비용 및 사용량에 대한 액세스 권한은 상실합니다.

계정이 더 이상 해당 계정을 대신하여 수락된 조직 계약의 적용을 받지 않음

조직에서 나가면 조직의 관리 계정에서 사용자를 대신하여 수락한 조직 계약이 더 이상 적용되지 않습니다. AWS Artifact 콘솔의 조직 계약 페이지에서 이러한 [AWS Artifact 조직 계약 목록을 볼 수 있습니다](#). 조직을 떠나기 전에 해당되는 경우 법무, 개인정보 보호 또는 규정 준수 팀의 도움을 받아 새 계약이 필요한지에 대한 여부를 결정해야 합니다.

계정의 할당량 한도가 변경되어 영향을 미칠 수 있습니다.

조직을 멤버 계정으로 남겨 두면 해당 계정에서 사용할 수 있는 서비스 할당량 제한에 영향을 미칠 수 있습니다. 더 높은 제한이 필요한 자동화된 워크로드가 있는 경우 조직을 떠난 후 서비스 할당량 콘솔에서 할당량을 다시 확인하여 중단 없는 경험을 보장하세요. 조직을 떠난 후 [AWS Support 센터](#)에 문의하여 도움을 받으세요.

멤버 계정에서 조직 탈퇴

조직을 탈퇴하려면 다음 절차를 완료합니다.

최소 권한

조직을 탈퇴하려면 다음 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

- `organizations:LeaveOrganization` – 조직 관리자는 이 권한을 제거한 계정에 정책을 적용하여 조직에서 계정을 제거하지 못하도록 할 수 있습니다.
- IAM 사용자로 로그인했는데 계정에 결제 정보가 없는 경우 사용자에게 `aws-portal:ModifyBilling` 및 `aws-portal:ModifyPaymentMethods` 권한(계정이 아직 세분화된 권한으로 마이그레이션되지 않은 경우) 또는 `payments:CreatePaymentInstrument` 및 `payments:UpdatePaymentPreferences` 권한(계정이 세분화된 권한으로 마이그레이션된 경우)이 있어야 합니다. 또한 멤버 계정에는 결제에 대한 IAM 사용자 액세스가 활성화되어야 합니다. 아직 활성화되지 않은 경우 AWS Billing 사용 설명서의 [Billing and Cost Management 콘솔에 대한 액세스 활성화](#)를 참조하세요.

AWS Management Console

멤버 계정에서 조직을 탈퇴하려면

1. AWS Organizations 콘솔에서 [AWS Organizations 콘솔](#)에 로그인합니다. 멤버 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 수임하거나, 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

기본적으로를 사용하여 생성된 멤버 계정의 루트 사용자 암호에 액세스할 수 없습니다 AWS Organizations. 필요한 경우, [를 사용하여 조직의 멤버 계정에 액세스 AWS Organizations](#)의 루트 사용자 사용(일상 작업에는 권장되지 않음)의 단계에 따라 루트 사용자 암호를 복구합니다.

2. [조직 대시보드](#) 페이지에서 이 조직 탈퇴를 선택합니다.
3. 조직 탈퇴 확인 대화 상자에서 조직 탈퇴를 선택합니다. 확인 메시지가 나타나면 계정 제거 선택을 확인합니다. 확인하면 AWS Organizations 콘솔의 시작하기 페이지로 리디렉션됩니다.이 페이지에서 다른 조직에 가입하기 위해 보류 중인 계정 초대를 볼 수 있습니다.

아직 조직을 탈퇴할 수 없음이라는 메시지가 나타나면 해당 계정에 독립 실행형 계정으로 작동하는 데 필요한 정보 중 일부가 없는 것입니다. 이 경우, 다음 단계로 가세요.

4. 조직 탈퇴 확인 대화 상자에 아직 조직을 탈퇴할 수 없음이 표시되면 계정 가입 단계 완료 링크를 선택합니다.

계정 가입 단계 완료 링크가 표시되지 않으면 [이 링크](#)를 사용하여 AWS가입 페이지로 이동하여 누락된 등록 단계를 완료합니다.

5. AWS에 가입 페이지에서 이 계정이 독립 실행형 계정이 되는 데 필요한 모든 필수 정보를 입력합니다. 여기에는 다음과 같은 유형의 정보가 포함됩니다.

- 담당자 이름 및 주소
- 올바른 결제 방법
- 전화번호 확인
- Support 플랜 옵션

6. 로그인 절차가 완료되었다는 대화 상자가 표시되면 [Leave organization]을 선택합니다.

확인 대화 상자가 표시됩니다. 계정 제거 선택을 확인합니다. AWS Organizations 콘솔의 시작하기 페이지로 리디렉션됩니다. 이 페이지에서 다른 조직에 가입하기 위해 보류 중인 계정 초대를 볼 수 있습니다.

7. 계정에 대한 액세스 권한을 부여하는 IAM 역할을 조직에서 제거합니다.

Important

조직에서 계정이 생성된 경우 Organizations는 조직의 관리 계정에 의한 액세스를 활성화한 IAM 역할을 계정에 자동으로 생성했습니다. 계정이 가입하도록 초대된 경우 Organizations에서 해당 역할을 자동으로 생성하지는 않았지만 사용자 또는 다른 관리자가 동일한 혜택을 받기 위해 계정을 생성했을 수 있습니다. 두 경우 모두 조직에서 계정을 제거할 때 이러한 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하려면 이 IAM 역할을 수동으로 삭제해야 합니다. 역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 [역할 또는 인스턴스 프로파일 삭제](#)를 참조하세요.

AWS CLI & AWS SDKs

멤버 계정으로 조직에서 나가려면

다음 명령 중 하나를 사용하여 조직을 나갈 수 있습니다.

- AWS CLI: [leave-organization](#)

다음 예제는 명령 실행에 사용되는 자격 증명을 가진 계정이 조직을 나가도록 합니다.

```
$ aws organizations leave-organization
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDKs: [LeaveOrganization](#)

멤버 계정이 조직을 떠난 후에는 조직에서 계정에 대한 액세스 권한을 부여하는 IAM 역할을 제거해야 합니다.

Important

조직에서 계정이 생성된 경우 Organizations는 조직의 관리 계정에 의한 액세스를 활성화한 IAM 역할을 계정에 자동으로 생성했습니다. 계정이 가입하도록 초대된 경우 Organizations에서 해당 역할을 자동으로 생성하지는 않았지만 사용자 또는 다른 관리자가 동일한 혜택을 받기 위해 계정을 생성했을 수 있습니다. 두 경우 모두 조직에서 계정을 제거할 때 이러한 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하려면 이 IAM 역할을 수동으로 삭제해야 합니다. 역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 [역할 또는 인스턴스 프로필 삭제](#)를 참조하세요.

관리 계정의 사용자가 대신 [조직에서 계정 제거](#)를 사용하여 멤버 계정을 제거할 수도 있습니다. 자세한 내용은 [조직에서 멤버 계정 제거](#) 단원을 참조하십시오.

를 사용하여 멤버 계정의 계정 이름 업데이트 AWS Organizations

조직의 관리 계정에 로그인하면 멤버 계정의 계정 이름을 업데이트할 수 있습니다. 멤버 계정 이름을 업데이트하는 방법을 알아보려면 AWS Account Management 참조 안내서의 [조직 AWS 계정 내 모든의 계정 이름 업데이트](#)의 단계를 따르세요.

를 사용하여 멤버 계정의 루트 사용자 이메일 주소 업데이트 AWS Organizations

보안 및 관리 복원력을 높이기 위해 관리 계정의 IAM 위탁자(필요한 IAM 권한이 있음)는 각 계정에 개별적으로 로그인할 필요 없이 모든 멤버 계정의 루트 사용자 이메일 주소(기본 이메일 주소라고도 함)를 중앙에서 업데이트할 수 있습니다. 이렇게 하면 관리 계정(또는 위임된 관리자 계정)의 관리자가 멤버 계정에 대한 더 많은 제어를 할 수 있습니다. 또한 원래 루트 사용자 이메일 주소 또는 관리 자격 증명에 대한 액세스 권한을 잃어버렸더라도 속한 모든 멤버 계정의 루트 사용자 이메일 주소 최신 상태로 유지할 AWS Organizations 수 있습니다.

관리 계정 관리자가 루트 사용자 이메일 주소를 중앙에서 변경하면 암호와 MFA 구성 모두 변경 전과 동일하게 유지됩니다. 계정의 루트 사용자 이메일 주소와 기본 연락 전화번호를 제어하는 사용자는 MFA를 우회할 수 있습니다.

조직 내 멤버 계정의 루트 사용자 이메일 주소 업데이트하려면 조직에서 이전에 [모든 기능](#) 모드를 활성화해야 합니다. 통합 결제 모드 또는 조직에 속하지 않은 계정 AWS Organizations 에서는 루트 사용자 이메일 주소 중앙에서 업데이트할 수 없습니다. API에서 지원하지 않는 계정의 루트 사용자 이메일 주소를 변경하려는 사용자는 계속해서 결제 콘솔을 사용하여 루트 사용자 이메일 주소를 관리해야 합니다.

멤버 계정의 루트 사용자 이메일 주소 업데이트하는 방법에 대한 step-by-step 지침은 AWS Account Management 참조 안내서 [의 조직의 모든 AWS 계정 에 대한 루트 사용자 이메일A](#) 업데이트를 참조하세요.

를 사용하여 계정 초대 관리 AWS Organizations

[조직을 생성하고](#) 관리 계정과 연결된 [이메일 주소를 소유하고 있는지 확인한](#) 후 기존를 조직에 초대 AWS 계정 할 수 있습니다. AWS Organizations 콘솔을 사용하여 다른 계정으로 보내는 초대를 시작하고 관리합니다. 조직의 관리 계정에서만 다른 계정에 초대를 보낼 수 있습니다.

계정을 초대하면가 초대를 수락하거나 거부할 수 있는 계정 소유자에게 초대를 AWS Organizations 보냅니다.

의 관리자인 경우 조직의 초대를 수락하거나 거부할 AWS 계정수도 있습니다. 수락한 경우 사용자의 계정은 조직의 멤버가 됩니다.

자동으로 조직의 일부가 되는 계정을 생성하는 방법은 [를 사용하여 조직에 멤버 계정 생성 AWS Organizations](#) 섹션을 참조하세요.

Important

조직의 모든 계정은 관리 계정과 동일한 AWS 파티션에서 가져와야 합니다. 상용 AWS 리전 파티션의 계정은 중국 리전 파티션의 계정 또는 리전 파티션의 계정이 있는 조직에 있을 수 없습니다 AWS GovCloud (US) .

주제

- [고려 사항](#)
- [를 사용하여 계정 초대 전송 AWS Organizations](#)
- [를 사용하여 보류 중인 계정 초대 관리 AWS Organizations](#)
- [를 사용하여 계정 초대 수락 또는 거부 AWS Organizations](#)

고려 사항

하루에 보낼 수 있는 초대 수 제한

하루에 보낼 수 있는 초대 수 제한에 대해서는 [최대값 및 최소값](#) 섹션을 참조하세요. 수락된 초대는 이 할당량에 포함되지 않습니다. 하나의 초대가 수락되는 즉시 다른 초대를 같은 날에 전송할 수 있습니다. 각 초대는 15일 이내에 응답받아야 하며 응답이 없으면 만료됩니다.

계정으로 전송된 초대는 조직의 계정 할당량을 기준으로 계산됩니다. 초대된 계정이 초대를 거부하거나, 관리 계정이 초대를 취소하거나, 초대가 만료되면 횟수가 초기화됩니다.

계정은 하나의 조직에만 가입 가능

계정은 하나의 조직에만 가입할 수 있습니다. 초대를 여러 번 받은 경우 하나만 수락할 수 있습니다.

결제 기록 및 보고서는 관리 계정에 유지

모든 계정에 대한 청구 내역 및 보고서는 조직의 관리 계정에 유지됩니다. 계정을 새 조직으로 이동하기 전에 유지하려는 멤버 계정에 대한 청구 및 보고서 내역을 내보내거나 백업하세요. 여기에는 [비용 및 사용량 보고서](#), [Cost Explorer 보고서](#), [절감형 플랜 보고서](#), [예약 인스턴스\(RI\) 사용률 및 담당률](#)이 포함될 수 있습니다.

관리 계정에는 멤버 계정에서 발생하는 모든 요금에 대한 책임 있음

계정이 초대를 수락하여 조직에 가입하면 새 멤버 계정에 의해 발생한 모든 비용은 조직의 관리 계정이 책임지게 됩니다. 멤버 계정에 연결된 결제 방법이 더 이상 사용되지 않습니다. 대신 조직의 관리 계정에 연결된 결제 방법이 멤버 계정에서 발생한 모든 요금을 지불합니다.

Organizations는 **AWSServiceRoleForOrganizations** 서비스 연결 역할을 자동으로 생성

AWS Organizations 는 라는 서비스 연결 역할을 생성[AWSServiceRoleForOrganizations](#)하여 AWS Organizations 와 다른 AWS 서비스 간의 통합을 지원합니다. 자세한 내용은 [AWS Organizations 및 서비스 연결 역할](#) 단원을 참조하십시오. 조직이 [모든 기능](#)을 지원하려면 초대된 계정에 이 역할이 있어야 합니다. 조직이 [통합 결제](#) 기능 세트만 지원하는 경우 이 역할을 삭제할 수 있습니다. 이 역할을 삭제한 후 나중에 조직의 모든 기능을 활성화하면가 계정에 대해이 역할을 AWS Organizations 다시 생성합니다.

조직은 **OrganizationAccountAccessRole** IAM 역할을 자동으로 생성하지 않음

초대된 멤버 계정의 경우 AWS Organizations 는 IAM 역할을 자동으로 생성하지 않습니다 [OrganizationAccountAccessRole](#). 이 역할은 관리 계정의 사용자에게 멤버 계정에 대한 관리

액세스 권한을 부여합니다. 초대된 계정에 대해 관리 제어 수준을 활성화하려면 직접 역할을 추가할 수 있습니다. 자세한 내용은 [를 사용하여 초대된 계정에 대한 OrganizationAccountAccessRole 생성 AWS Organizations](#) 단원을 참조하십시오.

Note

기존 계정을 초대하는 대신 조직에 계정을 생성하면 OrganizationAccountAccessRole 기본적으로 IAM 역할을 AWS Organizations 자동으로 생성합니다.

계정이 포함된 루트 또는 OU에 연결된 정책은 즉시 적용됨

초대된 계정이 포함된 루트 또는 조직 단위(OU)에 연결된 정책이 있는 경우 초대된 계정의 모든 사용자 및 역할에 해당 정책이 즉시 적용됩니다.

조직의 [다른 서비스에 대한 AWS 서비스 신뢰를 활성화](#)할 수 있습니다. 이렇게 하면 신뢰할 수 있는 해당 서비스는 초대된 계정이 포함된 조직의 멤버 계정에서 서비스 연결 역할을 생성하거나 작업을 수행할 수 있습니다.

통합 결제 기능 세트만 있는 조직도 계속 계정 초대 가능

통합 결제 기능만 활성화된 조직에 가입하도록 계정을 초대할 수 있습니다. 나중에 조직의 모든 기능을 활성화하려면 초대된 계정이 변경 사항을 승인해야 합니다.

를 사용하여 계정 초대 전송 AWS Organizations

계정을 조직에 초대하려면 먼저 관리 계정과 연결된 이메일 주소의 소유자임을 입증해야 합니다. 자세한 정보는 [를 사용한 이메일 주소 확인 AWS Organizations](#) 섹션을 참조하세요. 이메일 주소를 확인한 후 다음 단계에 따라 계정을 조직에 초대합니다.

최소 권한

조직에 가입 AWS 계정 하도록 초대하려면 다음 권한이 있어야 합니다.

- organizations:DescribeOrganization(콘솔 전용)
- organizations:InviteAccountToOrganization

AWS Management Console

다른 계정을 조직에 초대하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 에서 이미 이메일 주소를 확인한 경우 이 단계를 AWS 건너뛰니다.

이메일 주소를 아직 확인하지 않은 경우 조직 생성 후 24시간 내에 [확인 이메일](#)의 지침을 따릅니다. 확인 이메일 메시지를 받기까지 어느 정도 시간이 걸릴 수 있습니다. 이메일 주소를 확인할 때까지 다른 계정을 초대하여 조직에 가입시킬 수 없습니다.

3. [AWS 계정](#) 페이지로 이동하고 AWS 계정 추가를 선택합니다.
4. [AWS 계정계정 추가](#) 페이지에서 기존 AWS 계정 초대를 선택합니다.
5. [기존 초대 AWS](#) 페이지의 초대 AWS 계정 할의 이메일 주소 또는 계정 ID에 초대할 계정과 연결된 이메일 주소 또는 계정 ID 번호를 입력합니다.
6. (선택 사항) 초대 이메일 메시지에 포함할 메시지(Message to include in the invitation email message)에서, 초대된 계정 소유자에게 보내는 이메일 초대장에 넣을 텍스트를 입력합니다.
7. (선택 사항) 태그 추가(Add tags) 섹션에서, 관리자가 초대를 수락한 후 계정에 자동으로 적용되는 태그를 하나 이상 지정합니다. 이렇게 하려면 태그 추가(Add tag)를 선택한 다음 키 및 값(선택 사항)을 입력합니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. AWS 계정에는 최대 50개의 태그를 연결할 수 있습니다.
8. [Send invitation]을 선택합니다.

 Important

조직의 계정 할당량을 초과했거나 조직이 초기화 중이므로 계정을 추가할 수 없다는 메시지를 받은 경우 [AWS Support](#)에 문의하세요.

9. [초대\(Invitations\)](#) 페이지로 리디렉션되면, 이 페이지에서 미결 및 수락 상태의 모든 초대를 확인할 수 있습니다. 방금 생성한 초대가 목록 상단에 표시되며 상태는 OPEN으로 설정됩니다.

AWS Organizations 는 조직에 초대된 계정 소유자의 이메일 주소로 초대를 보냅니다. 이 이메일 메시지는 계정 소유자가 세부 정보를 보고 초대를 수락하거나 거부할 수 있는 AWS Organizations 콘솔 링크가 포함되어 있습니다. 또는 초대된 계정의 소유자는 이메일 메시지를 우회하고 콘솔로 직접 이동하여 초대를 AWS Organizations 보고 수락하거나 거부할 수 있습니다.

이 계정에 대한 초대는 조직에 있을 수 있는 최대 계정 수를 기준으로 즉시 계산됩니다. AWS Organizations에서는 계정이 초대를 수락할 때까지 기다리지 않습니다. 초대된 계정이 거부한 경우 관리 계정은 초대를 취소합니다. 초대된 계정이 지정된 시간 내에 응답하지 않은 경우 초대는 만료됩니다. 어느 경우든 초대는 더 이상 할당량에 포함되지 않습니다.

AWS CLI & AWS SDKs

다른 계정을 조직에 초대하려면

다음 명령 중 하나를 사용하여 다른 계정이 조직에 가입하도록 초대할 수 있습니다.

- AWS CLI: [invite-account-to-organization](#)

```
$ aws organizations invite-account-to-organization \
  --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
  --notes "This is a request for Juan's account to join Bill's organization."
{
  "Handshake": {
    "Action": "INVITE",
    "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/invite/h-examplehandshakeid111",
    "ExpirationTimestamp": 1482952459.257,
    "Id": "h-examplehandshakeid111",
    "Parties": [
      {
        "Id": "o-exampleorgid",
        "Type": "ORGANIZATION"
      },
      {
        "Id": "juan@example.com",
        "Type": "EMAIL"
      }
    ],
    "RequestedTimestamp": 1481656459.257,
    "Resources": [
      {
        "Resources": [
          {
            "Type": "MASTER_EMAIL",
            "Value": "bill@amazon.com"
          }
        ]
      }
    ]
  }
}
```

```

        "Type": "MASTER_NAME",
        "Value": "Management Account"
    },
    {
        "Type": "ORGANIZATION_FEATURE_SET",
        "Value": "FULL"
    }
],
"Type": "ORGANIZATION",
"Value": "o-exampleorgid"
},
{
    "Type": "EMAIL",
    "Value": "juan@example.com"
}
],
"State": "OPEN"
}
}

```

- AWS SDKs: [InviteAccountToOrganization](#)

를 사용하여 보류 중인 계정 초대 관리 AWS Organizations

관리 계정에 로그인하면 조직의 연결된 AWS 계정 을 모두 확인하고 보류 중인(미결) 초대를 취소할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

최소 권한

조직에 대해 보류 중인 초대를 관리하려면, 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:ListHandshakesForOrganization`
- `organizations:CancelHandshake`

AWS Management Console

조직이 다른 계정에 보낸 초대를 확인하거나 취소하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [초대\(Invitations\)](#) 페이지로 이동합니다.

이 페이지에 조직이 전송한 모든 초대와 초대의 현재 상태가 표시됩니다.

초대가 보이지 않는 경우 초대된 계정이 다른 조직의 관리 계정인지 확인합니다. 멤버 계정과 독립형 계정만 초대를 받을 수 있습니다. 관리 계정은 초대를 받을 수 없습니다.

다른 조직의 관리 계정인 계정을 초대하려면 해당 계정을 독립형 계정으로 만드는 것이 좋습니다.

Note

수락, 취소 및 거부된 초대는 30일 동안 계속해서 목록에 나타납니다. 그 후에는 삭제되어 목록에 더 이상 표시되지 않습니다.

3. 취소하려는 초대 옆에 있는 라디오 버튼



선택한 다음 초대 취소(Cancel invitation)를 선택합니다. 라디오 버튼이 회색으로 표시되어 있으면 초대를 취소할 수 없습니다.

초대 상태가 미결(OPEN)에서 취소됨(CANCELED)으로 변경됩니다.

AWS 는 초대를 취소했음을 알리는 이메일 메시지를 계정 소유자에게 보냅니다. 새 초대를 보내지 않는 한 해당 계정은 조직에 가입할 수 없게 됩니다.

AWS CLI & AWS SDKs

조직이 다른 계정에 보낸 초대를 확인하거나 취소하려면

다음 명령을 사용하여 초대를 보거나 취소할 수 있습니다.

- AWS CLI: [list-handshakes-for-organization](#), [cancel-handshake](#)
- 다음 예는 해당 조직이 다른 계정으로 보낸 초대를 보여 줍니다.

```
$ aws organizations list-handshakes-for-organization
{
  "Handshakes": [
    {
      "Action": "INVITE",
      "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/invite/h-examplehandshakeid111",
      "ExpirationTimestamp": 1482952459.257,
      "Id": "h-examplehandshakeid111",
      "Parties": [
        {
          "Id": "o-exampleorgid",
          "Type": "ORGANIZATION"
        },
        {
          "Id": "juan@example.com",
          "Type": "EMAIL"
        }
      ],
      "RequestedTimestamp": 1481656459.257,
      "Resources": [
        {
          "Resources": [
            {
              "Type": "MASTER_EMAIL",
              "Value": "bill@amazon.com"
            },
            {
              "Type": "MASTER_NAME",
              "Value": "Management Account"
            },
            {
              "Type": "ORGANIZATION_FEATURE_SET",
              "Value": "FULL"
            }
          ],
          "Type": "ORGANIZATION",
          "Value": "o-exampleorgid"
        },
        {
          "Type": "EMAIL",
          "Value": "juan@example.com"
        }
      ],
    }
  ]
}
```

```

        {
            "Type": "NOTES",
            "Value": "This is an invitation to Juan's account to join
Bill's organization."
        }
    ],
    "State": "OPEN"
},
{
    "Action": "INVITE",
    "State": "ACCEPTED",
    "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
    "ExpirationTimestamp": 1.471797437427E9,
    "Id": "h-examplehandshakeid222",
    "Parties": [
        {
            "Id": "o-exampleorgid",
            "Type": "ORGANIZATION"
        },
        {
            "Id": "anika@example.com",
            "Type": "EMAIL"
        }
    ],
    "RequestedTimestamp": 1.469205437427E9,
    "Resources": [
        {
            "Resources": [
                {
                    "Type": "MASTER_EMAIL",
                    "Value": "bill@example.com"
                },
                {
                    "Type": "MASTER_NAME",
                    "Value": "Management Account"
                }
            ],
            "Type": "ORGANIZATION",
            "Value": "o-exampleorgid"
        },
        {
            "Type": "EMAIL",
            "Value": "anika@example.com"
        }
    ]
}

```

```

    },
    {
      "Type": "NOTES",
      "Value": "This is an invitation to Anika's account to join
Bill's organization."
    }
  ]
}
]
}

```

다음 예는 계정에 대한 초대를 취소하는 방법을 보여 줍니다.

```

$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
  "Handshake": {
    "Id": "h-examplehandshakeid111",
    "State": "CANCELED",
    "Action": "INVITE",
    "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
    "Parties": [
      {
        "Id": "o-exampleorgid",
        "Type": "ORGANIZATION"
      },
      {
        "Id": "susan@example.com",
        "Type": "EMAIL"
      }
    ],
    "Resources": [
      {
        "Type": "ORGANIZATION",
        "Value": "o-exampleorgid",
        "Resources": [
          {
            "Type": "MASTER_EMAIL",
            "Value": "bill@example.com"
          },
          {
            "Type": "MASTER_NAME",
            "Value": "Management Account"
          }
        ]
      }
    ]
  }
}

```

```

        },
        {
            "Type": "ORGANIZATION_FEATURE_SET",
            "Value": "CONSOLIDATED_BILLING"
        }
    ],
    },
    {
        "Type": "EMAIL",
        "Value": "anika@example.com"
    },
    {
        "Type": "NOTES",
        "Value": "This is a request for Susan's account to join Bob's
organization."
    }
],
    "RequestedTimestamp": 1.47008383521E9,
    "ExpirationTimestamp": 1.47137983521E9
}
}

```

- AWS SDKs: [ListHandshakesForOrganization](#), [CancelHandshake](#)

를 사용하여 계정 초대 수락 또는 거부 AWS Organizations

조직에 가입하도록 초대를 받은 경우 초대를 수락하거나 거부할 수 있습니다.

고려 사항

조직에서 계정의 상태는 어떤 비용 및 사용량 데이터가 표시되는지에 영향 받음

멤버 계정이 조직을 탈퇴하여 독립형 계정이 되는 경우 해당 계정은 조직의 멤버였을 때의 시간 범위부터 비용 및 사용량 데이터에 대한 액세스를 할 수 없습니다. 해당 계정은 독립형 계정으로 생성된 데이터에만 액세스할 수 있습니다.

멤버 계정이 조직 A를 탈퇴하여 조직 B에 가입하는 경우 계정은 조직 A의 계정이었을 때의 시간 범위로부터 비용 및 사용량에 대한 데이터에 액세스할 수 없습니다. 해당 계정은 조직 B의 멤버로 생성된 데이터에만 액세스할 수 있습니다.

계정이 이전에 속했던 조직에 다시 가입하는 경우 계정은 과거 비용 및 사용량 데이터에 대한 액세스를 다시 얻습니다.

멤버 계정과 독립 실행형 계정에서만 초대 수락하거나 거부 가능

멤버 계정과 독립형 계정에서만 조직 가입 초대를 수락하거나 거절할 수 있습니다. 이미 조직에 속한 관리 계정으로 초대를 받은 경우 조직에서 [조직에서 모든 멤버 계정을 제거](#)하고 [조직을 삭제](#)하기 전까지는 해당 계정에서 초대를 수락할 수 없습니다.

CloudTrail 로깅은 작업을 수행하는 계정에서 수행됩니다.

멤버 계정 또는 독립 실행형 계정이 계정 초대를 수락하거나 거부하는 경우 해당 작업은 작업 계정의 CloudTrail 로그에 기록됩니다. 작업 계정이 멤버 계정인 경우 해당 작업은 관리 계정의 CloudTrail 로그에 기록되지 않습니다. 이는 관련 시나리오의 CloudTrail 로깅과 일치합니다(예: 조직을 떠나는 멤버 계정은 멤버 계정 추적에 로깅되고, 멤버 계정을 제거하는 관리 계정은 관리 계정 추적에 로깅됩니다).

초대를 수락하거나 거부하려면

초대를 수락하거나 거부하려면 다음 단계를 완료합니다.

최소 권한

조직 가입 초대를 수락하거나 거부하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:ListHandshakesForAccount` - AWS Organizations 콘솔에서 초대 목록을 보는 데 필요합니다.
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `organizations:LeaveOrganization` - 계정이 이미 조직의 멤버인 경우 초대를 수락하는 경우에만 필요합니다.
- `iam:CreateServiceLinkedRole` - 초대를 수락하기 위해 멤버 계정에서 다른 AWS 서비스와의 통합을 지원할 서비스 연결 역할을 생성해야 하는 경우에만 필요합니다. 자세한 내용은 [AWS Organizations 및 서비스 연결 역할](#) 단원을 참조하십시오.

AWS Management Console

초대를 수락하거나 거부하려면

1. 조직 가입 초대는 계정 소유자의 이메일 주소로 전송됩니다. 초대 이메일 메시지를 받은 계정 소유자는 이메일 초대장의 지침을 따르거나, 브라우저에서 [AWS Organizations 콘솔](#)로 이동한 후 초대를 선택하거나, [멤버 계정의 초대](#)로 곧바로 이동할 수 있습니다.

2. 메시지가 표시되면 초대된 계정에 IAM 사용자로 로그인하거나, IAM 역할을 맡거나, 계정의 루트 사용자로 로그인([권장되지 않음](#))합니다.
3. [멤버 계정의 초대\(member account's Invitation\)](#) 페이지에 계정의 미결 조직 가입 초대가 표시됩니다.

초대 수락(Accept invitation) 또는 초대 거부(Decline invitation)를 적절히 선택합니다.

- 앞선 단계에서 초대 수락(Accept invitation)을 선택한 경우 내 계정이 멤버가 된 조직의 세부 정보를 보여주는 [조직 보기\(Organization overview\)](#) 페이지가 콘솔에 나타납니다. 조직의 ID와 소유자의 이메일 주소를 확인할 수 있습니다.

Note

수락된 초대는 30일 동안 계속해서 목록에 나타납니다. 그 후에는 삭제되어 목록에 더 이상 표시되지 않습니다.

AWS Organizations 는 AWS Organizations 와 다른 간의 통합을 지원하기 위해 새 멤버 계정에 서비스 연결 역할을 자동으로 생성합니다 AWS 서비스. 자세한 내용은 [AWS Organizations 및 서비스 연결 역할](#) 단원을 참조하십시오.

AWS 는 초대를 수락했음을 알리는 이메일 메시지를 조직의 관리 계정 소유자에게 보냅니다. 또한 멤버 계정 소유자에게는 계정이 조직의 멤버가 되었음을 알리는 이메일 메시지가 전송됩니다.

- 이전 단계에서 거부(Decline)를 선택했다면, 계정은 다른 보류 중인 초대를 표시하는 [멤버 계정의 초대](#) 페이지에 계속 표시됩니다.

AWS 는 초대를 거부했음을 알리는 이메일 메시지를 조직의 관리 계정 소유자에게 보냅니다.

Note

거부된 초대는 30일 동안 목록에 계속 나타납니다. 그 후에는 삭제되어 목록에 더 이상 표시되지 않습니다.

AWS CLI & AWS SDKs

초대를 수락하거나 거부하려면

다음 명령을 사용하여 초대를 수락하거나 거부할 수 있습니다.

- AWS CLI: [accept-handshake](#), [decline-handshake](#)

다음 예는 조직 가입 초대를 수락하는 방법을 보여 줍니다.

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
  "Handshake": {
    "Action": "INVITE",
    "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/invite/h-examplehandshakeid111",
    "RequestedTimestamp": 1481656459.257,
    "ExpirationTimestamp": 1482952459.257,
    "Id": "h-examplehandshakeid111",
    "Parties": [
      {
        "Id": "o-exampleorgid",
        "Type": "ORGANIZATION"
      },
      {
        "Id": "juan@example.com",
        "Type": "EMAIL"
      }
    ],
    "Resources": [
      {
        "Resources": [
          {
            "Type": "MASTER_EMAIL",
            "Value": "bill@amazon.com"
          },
          {
            "Type": "MASTER_NAME",
            "Value": "Management Account"
          },
          {
            "Type": "ORGANIZATION_FEATURE_SET",
            "Value": "ALL"
          }
        ],
        "Type": "ORGANIZATION",
        "Value": "o-exampleorgid"
      }
    ]
  }
}
```

```

    },
    {
      "Type": "EMAIL",
      "Value": "juan@example.com"
    }
  ],
  "State": "ACCEPTED"
}
}

```

다음 예는 조직 가입 초대를 거부하는 방법을 보여 줍니다.

- AWS SDKs: [AcceptHandshake](#), [DeclineHandshake](#)

를 사용하여 계정을 다른 조직으로 마이그레이션 AWS Organizations

언제든지 AWS 계정 한 조직에서 다른 조직으로 마이그레이션할 수 있습니다. 예를 들어, AWS 계정 여러 조직의 하나 이상을 하나의 조직으로 통합해야 하는 인수 합병의 경우 계정을 마이그레이션하는 것이 유용할 수 있습니다.

사용 사례에 관계없이 조직 간에 계정을 마이그레이션하려면 새 조직의 관리 계정에서 초대를 보내고 초대된 계정을 사용하여 새 조직에 가입하라는 초대를 수락해야 합니다.

Note

해지되거나 일시 중지된 계정은 마이그레이션할 수 없습니다.

해지된 계정이나 일시 중지된 계정은 마이그레이션할 수 없습니다. 계정을 다시 활성화하려면 [지원](#)에 문의하세요.

4일 기간 요건

조직에서 생성한 계정을 마이그레이션하려면 계정을 생성한 후 최소 4일이 지날 때까지 대기해야 합니다. 초대된 계정에는 이 대기 기간이 적용되지 않습니다.

계정 간 데이터 복제

다음 AWS 권장 가이드에서는 AWS 계정 [리소스 복제 또는 마이그레이션 AWS 계정](#) 간의 데이터 복제 전략에 대한 정보를 제공합니다.

계정을 마이그레이션하기 전에 수행해야 할 작업

한 조직에서 다른 조직 AWS 계정 으로를 마이그레이션하기 전에 다음 단계를 완료했는지 확인합니다.

1단계: 계정을 마이그레이션하는 데 필요한 IAM 권한이 있는지 확인

1단계

계정을 마이그레이션하는 데 필요한 권한을 각 조직에 적용했는지 확인합니다.

조직을 탈퇴하려면 다음 권한이 있어야 합니다.

- `organizations:DescribeOrganization`(콘솔 전용)
- `organizations:LeaveOrganization`

자세한 내용은 [멤버 계정에서 조직 탈퇴](#)를 참조하세요.

조직에 가입 AWS 계정 하도록을 초대하려면 다음 권한이 있어야 합니다.

- `organizations:DescribeOrganization`(콘솔 전용)
- `organizations:InviteAccountToOrganization`

자세한 내용은 [조직에 가입 AWS 계정 하도록 초대](#)를 참조하세요.

계정을 마이그레이션하려면 마이그레이션을 방지하는 IAM 정책 또는 서비스 제어 정책을 가질 수 없습니다.

관리 계정 또는 위임된 관리자인 경우 조직 내 IAM 자격 증명(사용자, 그룹 및 역할)에 권한 정책을 연결하여 AWS 리소스에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 [AWS Organizations에 대한 IAM 정책](#)을 참조하세요.

계정을 마이그레이션하기 전에.

- 계정의 마이그레이션을 방지하는 IAM 정책 또는 서비스 제어 정책(SCP)이 없는지 확인합니다.
- 계정을 마이그레이션하려는 조직에서 복제해야 하는 기존 IAM 정책 및 서비스 제어 정책(SCP)을 식별합니다.
- 조직 ID를 지정하는 기존 IAM 정책을 식별합니다. 예: [aws:PrincipalOrgID](#)

자세한 내용은 IAM 사용 설명서의 [IAM 정책 관리](#) 및 [서비스 제어 정책\(SCP\)](#)을 참조하세요.

2단계: 이전 관리 계정에 대한 액세스를 활성화하는 IAM 권한을 제거했는지 확인

단계 2

이전 관리 계정에 대한 액세스를 활성화하는 IAM 권한(예: `OrganizationAccountAccessRole`)을 제거했는지 확인합니다.

조직에서 멤버 계정을 제거해도 조직의 관리 계정으로 액세스할 수 있도록 생성된 IAM 역할은 자동으로 삭제되지 않습니다. 이전 조직의 관리 계정에서 이 액세스를 종료하려면 IAM 역할을 수동으로 삭제해야 합니다.

역할 삭제 방법에 대한 내용은 IAM 사용 설명서의 [역할 또는 인스턴스 프로파일 삭제](#)를 참조하세요.

3단계: 모든 보고서 백업

3단계

관리 계정에서 보고서(특히 결제 보고서)를 내보내거나 백업해야 합니다. 계정을 마이그레이션할 때는 조직 수준 보고서와 기록이 저장되지 않습니다. 모든 결제 기록을 완전히 내보내는 것이 좋습니다. AWS CloudTrail 이벤트 기록 및 계정 결제 기록과 같은 멤버 계정에 대한 보고서에 계속 액세스할 수 있습니다.

Important

관리 계정의 조직 결제 정보와 같은 모든 조직 수준 보고 및 기록은 조직에서 계정이 제거된 후에 삭제됩니다.

자세한 내용은 [비용 및 사용량 보고서](#), [Cost Explorer 보고서](#), [절감형 플랜 보고서](#), [예약 인스턴스\(RI\) 사용률 및 담당률](#)을 참조하세요.

4단계: 조직 종속성 확인

단계 4

마이그레이션하는 계정에 조직 관련 종속성이 없는지 확인합니다.

확인할 종속성:

- 계정이 위임된 관리자인 경우 계정을 마이그레이션하기 전에 위임된 관리자 권한의 등록을 취소해야 합니다. 자세한 내용은 함께 [사용할 수 있는 서비스를 참조하세요 AWS Organizations](#).

- 계정이 관리 계정인 경우 마이그레이션하기 전에 조직에서 모든 멤버 계정을 제거하고 조직을 삭제해야 합니다. 조직을 삭제한 후에는 관리 계정이 독립 실행형 계정으로 작동합니다. 마이그레이션 후 관리 계정은 새 조직의 멤버 계정이 됩니다. 자세한 내용은 [조직 삭제](#)를 참조하세요.
- IAM 권한이 계정에 종속된 경우 이전 조직이 이전과 같이 작동하려면 새 조직으로 계정을 마이그레이션한 후 이전 조직에 대한 권한을 조정해야 합니다. 자세한 내용은 [조직에 대한 액세스 권한 관리](#)를 참조하세요.
- 계정 또는 조직 단위(OU) 태그를 사용하는 경우 새 조직에서 태그를 다시 생성해야 합니다.

(선택 사항) 5단계:를 사용하는 경우 지침 검토 AWS Control Tower

(선택 사항) 5단계

에서 관리하는 조직으로 또는 조직에서 계정을 마이그레이션하는 경우 AWS 권장 가이드: 멤버 계정을에서 로 마이그레이션을 AWS Control Tower검토하세요. [AWSAWS OrganizationsAWS Control Tower](#)

계정을 마이그레이션하기 위해 수행해야 할 작업

마이그레이션 프로세스를 수행하려면 새 조직이 마이그레이션 계정에 초대장을 보내고, 마이그레이션 계정이 새 조직의 초대장을 수락하여 새 조직에 가입해야 합니다.

계정을 마이그레이션하려면

1. 새 조직의 관리 계정에서 마이그레이션하는 계정으로 초대장을 보냅니다. 계정 초대장에 대한 자세한 내용은 [조직에 가입 AWS 계정 하도록 초대장을 참조하세요](#).
2. 새 조직에 가입하라는 초대장을 수락합니다. 자세한 내용은 [조직의 초대 수락](#)을 참조하세요. 한 조직에서 다른 조직으로 마이그레이션되는 계정은 새 조직의 루트에 자동으로 추가됩니다. 계정을 새 조직의 조직 단위(OU)로 이동하기 전에 마이그레이션 계정에 적절한 조직 정책 및 OU 권한이 있는지 확인하는 것이 좋습니다.
3. 관리 계정을 마이그레이션하려면 새 조직으로 관리 계정을 마이그레이션하기 전에 조직에서 [모든 멤버 계정을 제거](#)하고 [조직을 삭제](#)해야 합니다. 이전 조직을 삭제한 후에는 관리 계정이 독립 실행형 계정으로 작동하며 새 조직의 초대장을 수락하여 새 조직에 가입할 수 있습니다. 초대장을 수락하면 관리 계정은 새 조직의 멤버 계정이 됩니다.

계정을 마이그레이션한 후에 수행해야 할 작업

한 조직에서 다른 조직으로 계정을 마이그레이션한 후에는 다음 단계를 완료했는지 확인하세요.

마이그레이션 후 검토

1. 마이그레이션된 계정의 모든 [결제 도구 구성](#)(예: 비용 범주, 예산 및 결제 경보)을 평가합니다.
2. 한 조직에서 다른 조직으로 마이그레이션한 계정에 대해 다음 금전적 정보를 검토하고 업데이트합니다.
 - a. 필요한 경우 계정의 [세금 설정을 업데이트](#)합니다.
 - b. 마이그레이션하는 계정의 [지원 플랜](#)이 새 조직의 지급인 계정과 일치하는지 확인합니다.
 - c. 마이그레이션한 계정에 적용할 수 있는 [세금 공제](#)를 검토합니다.
3. 마이그레이션한 계정에 대한 기존 IAM 정책 및 서비스 제어 정책(SCP)을 검증하고 확인합니다. 예를 들어 새 조직을 반영하기 위해 일부 IAM 정책의 조직 ID를 업데이트해야 할 수 있습니다.
4. 계정을 마이그레이션한 새 조직의 [비용 할당 태그](#)를 업데이트합니다. 마이그레이션한 계정에서 수집한 이전 비용 할당 태그를 모두 업데이트해야 합니다.
5. [예약 인스턴스](#) 및 [절감형 플랜](#)은 계정과 함께 마이그레이션됩니다. 이는 이전 조직에 유지되지 않습니다. 이전 조직으로 이전해야 하는 지원 경우에 문의하세요.

에서 계정 세부 정보 보기 AWS Organizations

[AWS Organizations 콘솔](#)에서 조직의 관리 계정에 로그인하면 멤버 계정의 세부 정보를 확인할 수 있습니다.

최소 권한

의 세부 정보를 보려면 다음 권한이 AWS 계정 있어야 합니다.

- organizations:DescribeAccount
- organizations:DescribeOrganization – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- organizations:ListAccounts – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

의 세부 정보를 보려면 AWS 계정

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

2. [AWS 계정](#) 페이지로 이동해 검토하려는 계정의 이름(라디오 버튼 아님)을 선택합니다. 원하는 계정이 OU의 하위 계정인 경우 하위 계정을 확인하기 위해 OU 옆에 있는 삼각형 아이콘을 선택해 확장해야 할 수 있습니다. 계정을 찾을 때까지 반복합니다. 계정 세부 정보(Account details) 상자에 계정에 대한 정보가 표시됩니다.

AWS CLI & AWS SDKs

의 세부 정보를 보려면 AWS 계정

다음 명령을 사용하여 계정의 세부 정보를 볼 수 있습니다.

- AWS CLI:
 - [list-accounts](#) – 조직 내 모든 계정의 세부 정보를 나열합니다.
 - [describe-account](#) – 지정한 계정의 세부 정보만 나열합니다.

두 명령 모두 각 계정에 대해 동일한 세부 정보를 응답에 포함하여 반환합니다.

다음 예제에서는 지정한 계정의 세부 정보를 검색하는 방법을 보여줍니다.

```
$ aws organizations describe-account --account-id 123456789012

{
  "Account": {
    "Id": "123456789012",
    "Arn": "arn:aws:organizations::123456789012:account/o-aa111bb222/123456789012",
    "Email": "admin@example.com",
    "Name": "Example.com Organization's Management Account",
    "Status": "ACTIVE",
    "JoinedMethod": "INVITED",
    "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00",
    "Paths": [
      "o-aa111bb222/r-a1b2/123456789012/"
    ]
  }
}
```

- AWS SDKs
 - [ListAccounts](#)

- [DescribeAccount](#)

의 모든 계정에 대한 세부 정보 내보내기 AWS Organizations

를 사용하면 조직의 AWS Organizations관리 계정 사용자와 위임된 관리자가 조직 내 모든 계정 세부 정보가 포함된 .csv 파일을 내보낼 수 있습니다. 그 결과 조직 관리자는 계정을 쉽게 보고 상태별로 (PENDING_ACTIVATION, ACTIVE, SUSPENDED, PENDING_CLOSURE 또는 CLOSED) 필터링할 수 있습니다. 조직에 많은 계정이 있는 경우.csv 파일 다운로드 옵션을 사용하면 스프레드시트에서 계정 세부 정보를 쉽게 보고 정렬할 수 있습니다. 현재 계정 정보를 유지하려면 이전에 저장된 버전을 사용하지 않고 새 CSV 내보내기를 생성하는 것이 좋습니다.

Important

2025년 9월 9일에 AWS Organizations 콘솔에서 Accounts 객체의 계정 Status 파라미터를 사용 중지했습니다. 이제 계정 내보내기 파일에 Status 파라미터가 아닌 State 파라미터가 표시됩니다. 내보낸 파일 Organization_accounts_information.csv를 사용하는 모든 다운스트림 프로세스는 Status 대신 State 파라미터를 사용하도록 업데이트해야 합니다.

Note

관리 계정의 보안 주체만 계정 목록을 다운로드할 수 있습니다.

AWS 계정 조직 내 모든 목록 내보내기

조직의 관리 계정에 로그인하면 조직에 속한 모든 계정 목록을 .csv 파일로 가져올 수 있습니다. 목록에는 개별 계정 세부 정보가 포함되어 있지만 계정이 속한 조직 단위(OU)는 지정하지 않습니다.

.csv 파일에는 각 계정에 대한 다음 정보가 포함되어 있습니다.

- 계정 ID - 숫자 계정 식별자입니다. 예: 123456789012
- ARN - 계정에 Amazon 리소스 이름입니다. 예:
arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012.
- 이메일 - 계정과 연결된 이메일 주소입니다. 예: marymajor@example.com
- 이름 - 계정 생성자가 제공한 계정 이름입니다. 예: 단계 테스트 계정

- 상태 - 조직 내 계정 상태입니다. 값은 PENDING, ACTIVE 또는 SUSPENDED일 수 있습니다.
- 상태 - 조직 내 운영 계정 상태입니다. 값은 PENDING_ACTIVATION, ACTIVE, SUSPENDED, PENDING_CLOSURE, 또는 CLOSED일 수 있습니다.
- 가입 방법 - 계정 생성 방법을 지정합니다. 값은 INVITED 또는 CREATED일 수 있습니다.
- 가입 타임스탬프 - 계정이 조직에 가입한 날짜 및 시간입니다.

최소 권한

조직의 모든 멤버 계정으로 .csv 파일을 내보내려면 다음 권한이 있어야 합니다.

- `organizations:DescribeOrganization`
- `organizations:ListAccounts`

AWS Management Console

조직의 모든 AWS 계정 에 대해 .csv 파일을 내보내려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 작업(Actions)을 선택한 다음 AWS 계정에서 계정 목록 내보내기(Export account list)를 선택합니다. 페이지 상단의 파란색 배너는 “내보내기가 진행 중입니다!”를 나타냅니다.
3. 파일이 준비되면 배너가 녹색으로 바뀌고 “다운로드가 준비되었습니다!”를 나타냅니다. Download CSV를 선택합니다. 파일 `Organization_accounts_information.csv`가 디바이스에 다운로드됩니다.

AWS CLI & AWS SDKs

계정 세부 정보가 포함된 .csv 파일을 내보내는 유일한 방법은 AWS Management Console을 사용하는 것입니다. AWS CLI를 사용하여 계정 목록 .csv 파일을 내보낼 수 없습니다.

의 상태 모니터링 AWS 계정

AWS Organizations 는 조직 내 모든 계정의 상태와 운영 상태를 빠르게 평가할 수 있는 방법을 제공합니다. AWS Organizations 콘솔 내의 상태 열을 사용하거나 AWS Organizations APIs. 이를 통해 생성부터 종료까지 수명 주기에서 각 AWS 계정 의 위치를 추적할 수 있습니다.

계정 상태를 지속적으로 추적하면 다음 이점이 있습니다.

- 주의 또는 조치가 필요한 계정을 빠르게 식별
- 계정 관리 프로세스 간소화
- 정보에 입각한 리소스 할당 및 액세스 제어 의사 결정
- 조직 전체에서 전반적인 보안 및 규정 준수 개선

아래 표에서는 AWS 계정에서 가능한 5가지 계정 상태와 의미를 설명합니다.

계정 상태

State	설명
활성화 보류 중	이 상태에서는 계정 가입 프로세스가 시작되었지만 완료되지 않아 계정을 사용할 수 없습니다. 계정 소유자는 전화 확인 또는 결제 정보 제공과 같은 나머지 가입 단계를 완료해야 합니다. 이 단계를 완료하면 계정이 활성 상태로 전환됩니다.
ACTIVE	이 상태는 계정이 완전히 작동하고 사용 가능함을 나타냅니다. 사용자는 계정의 권한 및 조직 정책에 따라 AWS 서비스 및 리소스에 정상적으로 액세스할 수 있습니다. 이 상태에서는 리소스 시작, 서비스 관리, 요금 발생과 같은 정기적인 AWS 활동이 발생할 수 있습니다.
SUSPENDED	이 상태에서는가 액세스를 AWS 제한했기 때문에 계정을 사용할 수 없습니다. 계정 소유자는 여전히 결제 정보와 연락처를 볼 수 있으며 지원,이 연락처는 계정이 일시 중지된 이유를 설명할 수 있습니다.
해지 보류 중	이 임시 상태는 계정을 해지하라는 활성 요청을 나타내지만 해지 프로세스가 아직 완료되지 않았습니다. 계정은 계속 작동하며 종료 요청이 처리되는 동안 AWS 서비스에 액세스하는 데 계속 사용할 수 있습니다. 가 종료 요청을 AWS 처리한 후 계정은 CLOSED 상태로 전환됩니다.
CLOSED	이 상태는 계정 소유자의 요청 또는에 의해 계정이 해지되었음을 나타내며 해지 AWS 가 시작된 후 90일 동안 AWS Organizations 콘솔의 계정 이름 옆에 표시됩니다. 이 기간 동안에는 AWS 서비스에 액세스할 수 없지만 지원 에 문의하여 계정을 복원하거나 중요한 데이터를 복구할 수 있습니다. 해지 후 90일이 경과하면 계정이 영구적으로 해지되고 AWS Organizations 콘솔에 더 이상 표시되지 않습니다.

의 상태 보기 AWS 계정

AWS Organizations 콘솔을 사용하거나 DescribeAccount, ListAccounts 및 ListAccountsForParent APIs.

Important

의 계정 Status 파라미터는 2026년 9월 9일에 사용 중지 AWS Organizations 됩니다. 현재 AWS Organizations APIs(DescribeAccount, ListAccounts, ListAccountsForParent)에서 계정 파라미터 State와 계정 Status 파라미터를 모두 사용할 수 있지만 2026년 9월 9일 Status 이전에 대신 State 파라미터를 사용하도록 스크립트 또는 기타 코드를 업데이트하는 것이 좋습니다.

AWS Management Console

의 상태를 보려면 AWS 계정

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지로 이동하여 살펴보려는 멤버 계정 옆의 상태 열의 값을 확인합니다. 원하는 계정이 OU의 하위 계정인 경우 하위 계정을 확인하기 위해 OU 옆에 있는 삼각형 아이콘을 선택해 확장해야 할 수 있습니다. 계정을 찾을 때까지 반복합니다.

Note

AWS Organizations 콘솔의 계정 세부 정보 페이지에서 상태 필드의 값을 볼 수도 있습니다.

AWS CLI & AWS SDKs

의 상태를 보려면 AWS 계정

다음 명령을 사용하여 계정 상태를 볼 수 있습니다.

Note

API 응답에서 계정 상태 값을 보려면 AWS CLI 버전 2.29.0 이상 또는 2025년 9월 9일 이후에 릴리스된 SDK 버전을 사용합니다. 최신 AWS CLI 또는 SDK 버전을 모범 사례로 사용하는 것이 좋습니다. 자세한 내용은 AWS SDK 및 도구 참조 설명서에서 [AWS SDK 및 도구 버전 수명 주기](#)를 참조하세요.

- AWS CLI:
 - [list-accounts](#) – 조직 내 모든 계정의 세부 정보를 나열합니다.
 - [list-accounts-for-parent](#) – 지정된 대상 루트 또는 조직 단위(OU)에 포함된 조직 내 모든 계정의 세부 정보를 나열합니다.
 - [describe-account](#) – 지정한 계정의 세부 정보만 나열합니다.

두 명령 모두 각 계정에 대해 동일한 세부 정보를 응답에 포함하여 반환합니다.

다음 예제에서는 State 값을 포함한 지정된 계정의 세부 정보를 검색하는 방법을 보여줍니다.

```
$ aws organizations describe-account --account-id 123456789012

{
  "Account": {
    "Id": "123456789012",
    "Arn": "arn:aws:organizations::123456789012:account/o-aa111bb222/123456789012",
    "Email": "admin@example.com",
    "Name": "Example.com Organization's Management Account",
    "State": "CLOSED",
    "Status": "SUSPENDED",
    "JoinedMethod": "INVITED",
    "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00",
    "Paths": [
      "o-aa111bb222/r-a1b2/123456789012/"
    ]
  }
}
```

- AWS SDKs
 - [ListAccounts](#)
 - [ListAccountsForParent](#)

- [DescribeAccount](#)

에서 계정의 대체 연락처 업데이트 AWS Organizations

조직 콘솔을 사용하거나 AWS CLI 또는 SDK를 AWS 사용하여 조직 내 계정의 대체 연락처를 프로그래밍 방식으로 업데이트할 수 있습니다. AWS SDKs 대체 연락처를 업데이트하는 방법을 알아보려면 계정 관리 참조의 [조직 AWS 계정 내 모든에 대한 대체 연락처 업데이트를 참조하세요](#). AWS

에서 계정의 기본 연락처 정보 업데이트 AWS Organizations

조직 콘솔을 사용하거나 AWS CLI 또는 SDK를 AWS 사용하여 조직 내 계정의 기본 연락처 정보를 프로그래밍 방식으로 업데이트할 수 있습니다. AWS SDKs 기본 연락처 정보를 업데이트하는 방법을 알아보려면 계정 관리 참조의 [조직 AWS 계정 내 모든의 기본 연락처 업데이트를 참조하세요](#). AWS

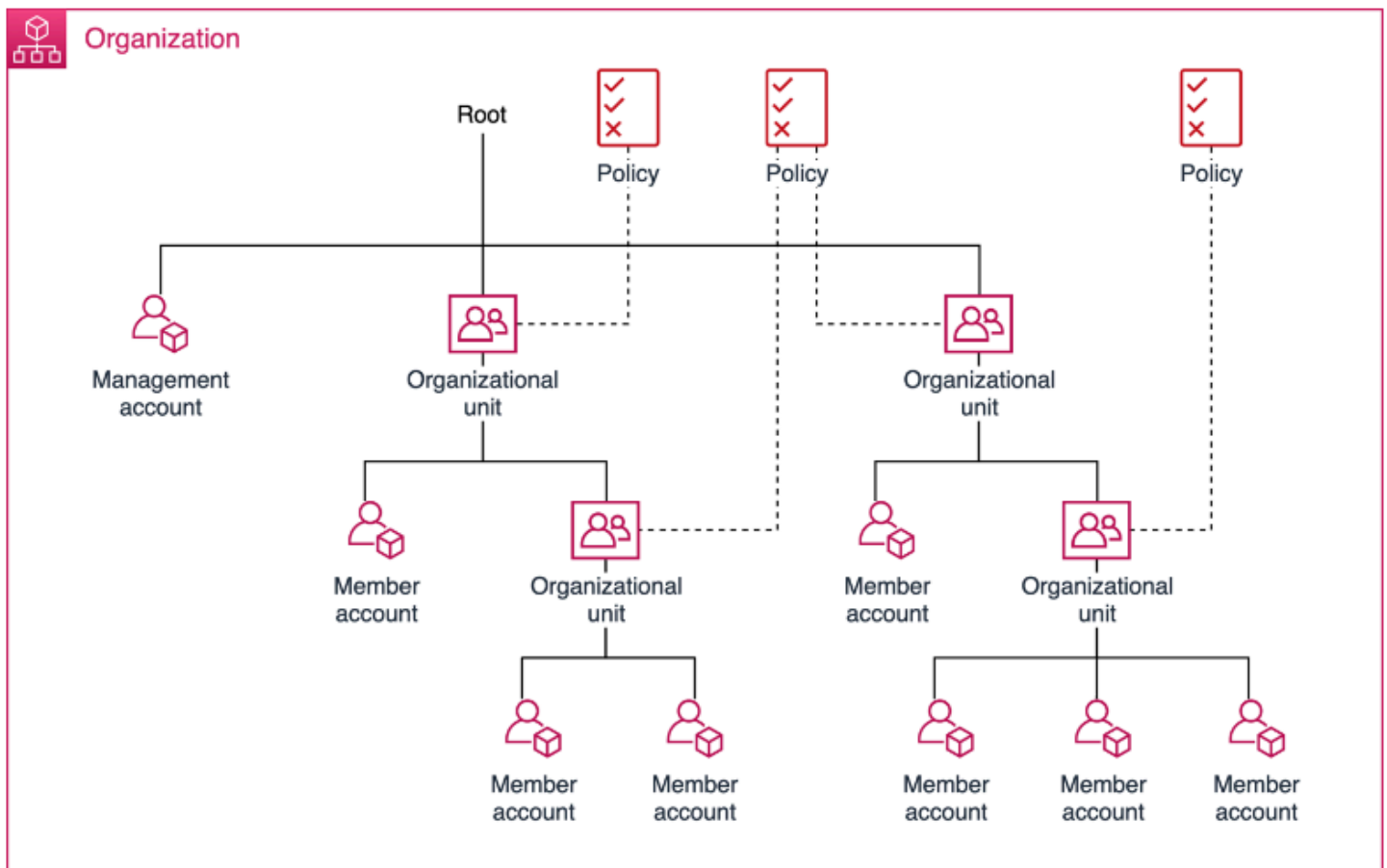
에서 AWS 리전 계정 업데이트 AWS Organizations

AWS Organizations 콘솔을 사용하여 조직 내 계정에 AWS 리전 대해 활성화된를 업데이트할 수 있습니다. 활성화를 업데이트하는 방법을 알아보려면 계정 AWS 관리 AWS 리전참조 [의 계정 AWS 리전 에서 활성화 또는 비활성화를 참조하세요](#).

OUs) 관리 AWS Organizations

조직 단위(OU)를 사용하면 계정을 그룹으로 만들어 단일 유닛으로 관리할 수 있습니다. 이 기능을 이용하면 계정 관리가 대단히 간편해집니다. 예를 들어 정책 기반 제어를 OU에 연결하면, OU 안의 모든 계정이 정책을 자동으로 상속합니다. 단일 조직에서 여러 OU를 생성하고, 다른 OU 안에 OU를 만들 수도 있습니다. OU 하나에 여러 개의 계정을 적용할 수 있고, 계정을 다른 OU로 옮길 수도 있습니다. 하지만 상위 OU나 루트에는 고유한 OU 이름만 존재해야 합니다.

다음 다이어그램은 루트 아래에 4가지 OU로 구분되는 계정 7개로 구성된 조직을 보여줍니다. 조직에는 OU에 적용되는 몇 가지 정책도 있습니다.



Note

조직에는 루트가 하나 있으며, 이 루트는 조직을 처음 설정할 때가 AWS Organizations 자동으로 생성합니다.

주제

- [를 사용하여 조직 단위\(OUs\)를 관리하는 모범 사례 AWS Organizations](#)
- [를 사용하여 루트 및 조직 단위\(OU\) 계층 구조 탐색 AWS Organizations](#)
- [를 사용하여 조직 단위\(OU\)의 세부 정보 보기 AWS Organizations](#)
- [를 사용하여 조직 단위\(OU\) 생성 AWS Organizations](#)
- [를 사용하여 조직 단위\(OU\) 이름 바꾸기 AWS Organizations](#)
- [를 사용하여 조직 단위\(OU\)에 태그 지정 AWS Organizations](#)
- [를 사용하여 계정을 조직 단위\(OU\)로 또는 루트와 OUs 간에 이동 AWS Organizations](#)
- [를 사용하여 루트의 세부 정보 보기 AWS Organizations](#)
- [를 사용하여 조직 단위\(OU\) 삭제 AWS Organizations](#)

를 사용하여 조직 단위(OUs)를 관리하는 모범 사례 AWS Organizations

다음 권장 사항을 따르면 조직 단위(OU)를 AWS Organizations 사용하여에서 다중 계정 환경을 관리하는 과정을 안내할 수 있습니다.OUs

주제

- [이해 AWS Organizations](#)
- [권장 기본 조직 단위\(OU\)](#)
- [권장 추가 조직 단위\(OU\)](#)
- [결론](#)

이해 AWS Organizations

잘 설계된 다중 계정 AWS 환경의 기반은 이며 AWS Organizations, 이를 통해 여러 계정을 중앙에서 관리하고 관리할 수 있습니다. 조직 단위(OU)는 조직 내 계정의 논리적 그룹화입니다. OU를 사용하면 계정을 계층 구조로 구성하고 관리 제어를 적용하는 데 도움이 됩니다. Organizations [정책은](#) 그룹에 적용할 수 있는 제어를 정의합니다 AWS 계정. 예를 들어 [서비스 제어 정책\(SCP\)](#)은 조직의 계정이 수행할 수 있는 Amazon EC2 실행 인스턴스와 같은 AWS 서비스 작업을 정의하는 정책입니다.

단일 계정으로 AWS 여정을 시작할 수 있지만 워크로드의 크기와 복잡성이 증가함에 따라 여러 계정을 설정하는 것이 AWS 좋습니다. 다중 계정 환경을 사용하는 것은 다음과 같은 몇 가지 이점을 제공할 수 있는 AWS 모범 사례입니다.

- 다양한 요구 사항을 통한 신속한 혁신: 회사 내 AWS 계정 다양한 팀, 프로젝트 또는 제품에 할당하여 각 팀, 프로젝트 또는 제품이 신속하게 혁신하면서 자체 보안 요구 사항을 충족할 수 있도록 할 수 있습니다.
- 간소화된 결제: 여러를 사용하면 AWS 요금을 담당하는 제품 또는 서비스 라인을 식별하는 데 도움이 되므로 AWS 비용을 할당하는 방법을 간소화할 AWS 계정 수 있습니다.
- 유연한 보안 제어: 여러 AWS 계정 를 사용하여 특정 보안 요구 사항이 있거나 HIPAA 또는 PCI와 같은 엄격한 규정 준수 지침을 충족해야 하는 워크로드 또는 애플리케이션을 격리할 수 있습니다.
- 비즈니스 프로세스에 적응: 운영, 규제 및 예산 요구 사항이 서로 다른 회사 비즈니스 프로세스의 다양한 요구 사항을 가장 잘 반영하는 AWS 계정 방식으로 여러를 구성할 수 있습니다.

권장 기본 조직 단위(OU)

조직 단위(OU)는 회사의 보고 구조를 미러링하는 대신 기능이나 일반적인 제어 세트를 기반으로 해야 합니다. AWS 는 보안 및 인프라를 염두에 두고 시작할 것을 권장합니다. 대부분의 비즈니스에는 이러한 요구 사항에 맞게 조직 전체에 서비스를 제공하는 중앙 집중식 팀이 있습니다. 이러한 특정 함수에 대한 기본 OU 세트를 생성하는 것이 좋습니다.

- 보안: 보안 서비스에 사용됩니다. 로그 아카이브, 보안 읽기 전용 액세스, 보안 도구 및 break-glass에 대한 계정을 생성합니다.
- 인프라: 네트워킹 및 IT 서비스와 같은 공유 인프라 서비스에 사용됩니다. 필요한 각 유형의 인프라 서비스에 대한 계정을 생성합니다.

대부분의 회사가 프로덕션 워크로드에 대한 정책 요구 사항이 다르기 때문에 인프라와 보안은 비프로덕션(SDLC) 및 프로덕션(Prod)에 대해 중첩된 OU를 가질 수 있습니다. SDLC OU의 계정은 비프로덕션 워크로드를 호스팅하며 다른 계정의 프로덕션 종속성이 없어야 합니다. 수명 주기 단계 간에 OU 정책에 차이가 있는 경우 SDLC를 여러 OU로 분할할 수 있습니다(예: 개발 및 사전 프로덕션). Prod OU의 계정은 프로덕션 워크로드를 호스팅합니다.

요구 사항에 따라 OU 수준에서 정책을 적용하여 Prod 및 SDLC 환경을 관리합니다. 일반적으로 OU 수준에서 정책을 적용하는 것은 정책 관리 및 잠재적 문제 해결을 단순화하기 때문에 개별 계정 수준보다 더 좋은 방법입니다.

다음 다이어그램은 보안 및 인프라에 대한 기본 OU(Prod 및 SDLC)를 보여줍니다.



권장 추가 조직 단위(OU)

중앙 서비스가 설치된 후에는 제품 또는 서비스 구축 또는 실행과 직접 관련된 OU를 생성하는 것이 좋습니다. 많은 AWS 고객이 기반을 구축한 후 다음 OUs.

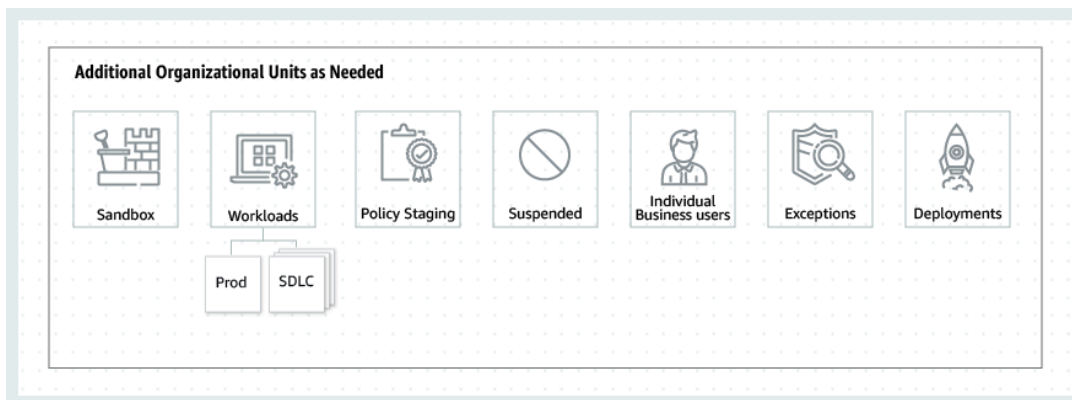
- 샌드박스: 개별 개발자 AWS 계정 가 실험에 사용할 수 있는롤 보유합니다 AWS 서비스. 이러한 계정을 내부 네트워크에서 분리할 수 있는지 확인합니다.
- 워크로드: 외부 애플리케이션 서비스를 호스팅 AWS 계정 하는이 포함되어 있습니다. 프로덕션 워크로드를 격리하고 엄격하게 제어하려면 SDLC 및 Prod 환경(기본 OU와 유사)에서 OU를 구성해야 합니다.

또한 특정 요구 사항에 따라 유지 관리 및 지속적인 확장을 위해 OU를 추가하는 것이 좋습니다. 다음은 기존 AWS 고객의 사례를 기반으로 하는 몇 가지 일반적인 테마입니다.

- 정책 스테이징: 제안된 정책 변경 사항을 조직에 광범위하게 적용하기 전에 테스트할 수 있는 AWS 계정을 보유합니다. 의도한 OU의 계정 수준에서 변경 사항을 구현하는 것부터 시작하여 다른 계정, OU 및 조직의 나머지 부분에서 천천히 작업합니다.

- 일시 중지됨: 닫혀 있고 조직에서 삭제되기를 기다리고 AWS 계정 있는가 포함되어 있습니다. 모든 작업을 거부하는 SCP를 이 OU에 연결합니다. 계정을 복원해야 하는 경우 추적성을 위해 계정에 세부 정보가 태그되어 있는지 확인합니다.
- 개별 비즈니스 사용자: 비즈니스 생산성 관련 애플리케이션을 생성해야 할 수 있는 비즈니스 사용자 (개발자가 아님)를 AWS 계정 위해가 포함된 제한된 액세스 OU입니다. 예를 들어, 보고서 또는 파일을 파트너와 공유하도록 S3 버킷을 설정합니다.
- 예외: 워크로드 OU에 정의된 것과 다른 사용자 지정 보안 또는 감사 요구 사항이 있는 비즈니스 사용자 사례에 AWS 계정 사용되는 보류입니다. 예를 들어 기밀 새 애플리케이션 또는 기능을 위해 AWS 계정 특별히를 설정합니다. 계정 수준에서 SCP를 사용하여 사용자 지정 요구 사항을 충족합니다. [Amazon EventBridge](#) 및 [AWS Config 규칙](#)을 사용하여 Detect 및 React 시스템을 설정하는 것이 좋습니다.
- 배포: 지속적 통합 및 지속적 전달/배포(CI/CD 배포)를 AWS 계정 위한를 포함합니다. 워크로드 OU(Prod 및 SDLC)의 계정과 비교하여 CI/CD 배포에 대한 거버넌스 및 운영 모델이 다른 경우 이 OU를 생성할 수 있습니다. CI/CD를 배포하면 중앙 팀이 운영하는 공유 CI/CD 환경에 대한 조직의 종속성을 줄일 수 있습니다. 워크로드 OU의 애플리케이션에 AWS 계정 대한 각 SDLC/Prod 세트에 대해 배포 OU에서 CI/CD 계정을 생성합니다.
- 전환: 조직의 표준 영역으로 이동하기 전에 기존 계정 및 워크로드의 임시 보관 영역으로 사용 됩니다. 이는 계정이 이전에 타사에서 관리한 인수의 일부이거나 이전 조직 구조의 레거시 계정이기 때문 일 수 있습니다.

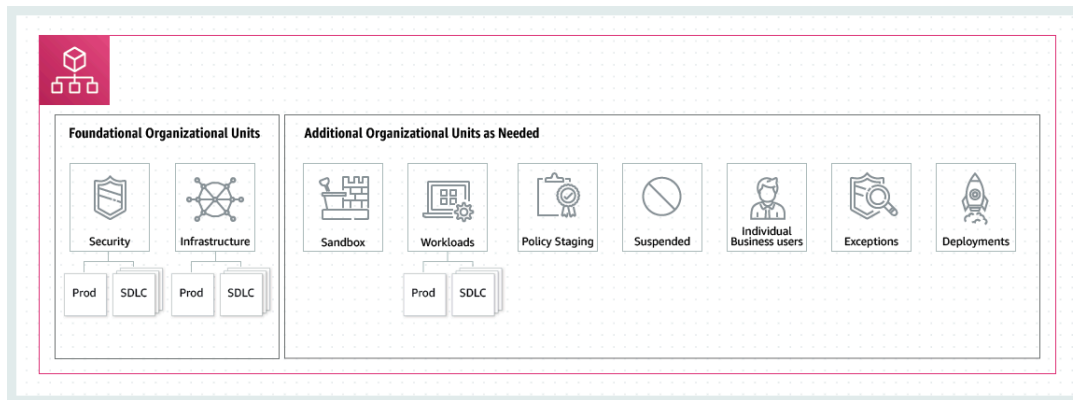
다음 다이어그램은 샌드박스, 워크로드, 정책 스테이징, 일시 중지, 개별 비즈니스 사용자, 예외, 배포 및 전환 계정에 대한 추가 OU를 보여줍니다.



결론

잘 설계된 다중 계정 전략은 혁신하는 데 도움이 되는 AWS동시에 보안 및 확장성 요구 사항을 충족하는 데 도움이 될 수 있습니다. 이 주제에 설명된 프레임워크는 AWS 여정의 출발점으로 사용해야 하는 AWS 모범 사례를 나타냅니다.

다음 다이어그램은 권장 기본 OU 및 추가 OU를 보여줍니다.



를 사용하여 루트 및 조직 단위(OU) 계층 구조 탐색 AWS Organizations

계정을 이동하거나 정책을 연결할 때 다른 OU 또는 루트로 이동하기 위해 기본 “트리” 보기를 사용할 수 있습니다.

AWS Management Console

조직을 '트리'로 탐색하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지의 조직(Organization) 섹션 상단에서 계층 구조(Hierarchy) 토글(목록(List) 대신)을 선택합니다.
3. 처음에 트리에는 하위 OU 및 계정의 첫 번째 레벨만 표시된 루트가 나타납니다. 하위 레벨을 더 표시하도록 트리를 확장하려면 상위 엔터티 옆에 있는 확장 아이콘 (▶) 을 선택합니다. 트리 가지를 축소하여 간단하게 표시하려면 확장된 상위 개체 옆에 있는 축소 아이콘 (▼) 을 선택합니다.

4. 세부 정보를 보고 특정 작업을 수행하려면 OU 또는 루트의 이름을 선택합니다. 또는 이름 옆의 라디오 버튼을 선택하고 작업(Actions) 메뉴에서 해당 엔터티에 대한 작업을 선택합니다.

또한 OU를 찾기 위해 먼저 탐색할 필요 없이 조직의 계정 목록만 표 형식으로 볼 수도 있습니다. 이 보기에서는 OU를 보거나 그에 연결된 정책을 조작할 수 없습니다.

AWS Management Console

계층 구조가 없는 단순 계정 목록으로 조직을 표시하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지의 조직 섹션 상단에서 보기 AWS 계정 전용 전환 아이콘을 선택하여 켭니다 
3. 계정 목록이 계층 구조 없이 표시됩니다.

를 사용하여 조직 단위(OU)의 세부 정보 보기 AWS Organizations

[AWS Organizations 콘솔](#)에서 조직의 관리 계정에 로그인하면 조직의 OU 세부 정보를 확인할 수 있습니다.

최소 권한

조직 단위(OU)에 대한 세부 정보를 보려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganizationalUnit`
- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:ListOrganizationsUnitsForParent` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:ListRoots` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

OU 세부 정보를 보려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 검토하려는 OU의 이름(라디오 버튼 아님)을 선택합니다. 원하는 OU가 다른 OU의 하위 항목이라면 상위 OU 옆에 있는 삼각형 아이콘을 선택해 확장한 후 계층 구조의 다음 레벨에 있는 OU를 확인합니다. 원하는 OU를 찾을 때까지 반복합니다.

조직 단위 세부 정보(Organizational unit details) 상자에 OU에 대한 정보가 나타납니다.

AWS CLI & AWS SDKs

OU 세부 정보를 보려면

다음 명령을 사용하여 OU의 세부 정보를 볼 수 있습니다.

- AWS CLI, AWS SDKs
 - [list-roots](#)
 - [list-children](#)
 - [describe-organizational-unit](#)

다음 예제에서는 AWS CLI를 사용해 OU에서 ID를 찾는 방법을 보여줍니다. 먼저 `list-roots` 명령으로 계층 구조를 트래버스한 다음 루트에서 `list-children`을 수행하고 원하는 대상을 찾을 때까지 각 하위 항목에 대해 반복적으로 수행하여 OU ID를 찾습니다.

```
$ aws organizations list-roots
{
  "Roots": [
    {
      "Id": "r-a1b2",
      "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
      "Name": "Root",
      "PolicyTypes": []
    }
  ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
ORGANIZATIONAL_UNIT
```

```
{
  "Children": [
    {
      "Id": "ou-a1b2-f6g7h111",
      "Type": "ORGANIZATIONAL_UNIT"
    }
  ]
}
```

OU의 ID를 찾았다면, 다음 예제에서 OU에 대한 세부 정보를 검색하는 방법을 보여 줍니다.

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-f6g7h111
{
  "OrganizationalUnit": {
    "Id": "ou-a1b2-f6g7h111",
    "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-f6g7h111",
    "Name": "Production-Apps",
    "Path": "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/"
  }
}
```

- AWS SDKs
 - [ListRoots](#)
 - [ListChildren](#)
 - [DescribeOrganizationalUnit](#)

를 사용하여 조직 단위(OU) 생성 AWS Organizations

조직의 관리 계정에 로그인하면 조직의 루트에서 OU를 생성할 수 있습니다. OU는 최대 5개까지 중첩할 수 있습니다. OU를 만들려면 다음 단계를 완료하세요.

Important

이 조직을 로 관리하는 경우 AWS Control Tower 콘솔 또는 APIs를 사용하여 OUs를 AWS Control Tower 생성합니다. Organizations에서 OU를 생성하면 해당 OU에 등록되지 않습니다. 자세한 내용은 AWS Control Tower 사용 설명서의 [AWS Control Tower 외부 리소스 참조](#)를 참조하세요.

i 최소 권한

조직의 루트 내에 OU를 만들려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:CreateOrganizationalUnit`

AWS Management Console

OU를 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지로 이동합니다.

콘솔에 루트 OU와 그 내용이 표시됩니다. 루트를 처음으로 방문하면 콘솔의 최상위 보기에 모든 AWS 계정 이 표시됩니다. 이전에 OU를 생성해 계정을 OU로 이동했다면, 콘솔은 최상위 OU와 아직 OU로 이동하지 않은 계정만 표시합니다.

3. (선택 사항) 기존 OU 내에 OU를 생성하려면, 하위 OU의 이름(확인란 아님)을 선택하거나 원하는 항목이 보일 때까지 트리 보기에서 OU 옆의



선택하여 [하위 OU로 이동](#)한 다음 이름을 선택합니다.

4. 계층 구조에서 올바른 상위 OU를 선택했으면 작업(Actions) 메뉴의 조직 단위(Organizational Unit)에서 새로 만들기(Create new)를 선택합니다.
5. 조직 단위 생성(Create organizational unit) 대화 상자에서 생성하려는 OU의 이름을 입력합니다.
6. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 하나 이상의 태그를 추가합니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. OU에는 최대 50개의 태그를 연결할 수 있습니다.
7. 마지막으로 조직 단위 생성(Create organizational unit)을 선택합니다.

새 OU가 상위 OU 내에 표시될 것입니다. 이제 [계정을 이 OU로 이동](#)하거나 OU에 정책을 연결할 수 있습니다.

AWS CLI & AWS SDKs

OU를 생성하려면

다음 코드 예시는 CreateOrganizationalUnit의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitName = "ProductDevelopmentUnit";

        var request = new CreateOrganizationalUnitRequest
        {
            Name = orgUnitName,
            ParentId = "r-0000",
```

```

    };

    var response = await client.CreateOrganizationalUnitAsync(request);

    if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
    {
        Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
        Console.WriteLine($"Organizational unit {orgUnitName} Details");
        Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
    }
    else
    {
        Console.WriteLine("Could not create new organizational unit.");
    }
}
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [CreateOrganizationalUnit](#)을 참조하세요.

CLI

AWS CLI

루트 또는 상위 OU에 OU를 생성하는 방법

다음 예시에서는 AccountingOU라는 OU를 생성하는 방법을 보여줍니다.

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

출력에는 새 OU의 세부 정보가 있는 organizationalUnit 객체가 포함됩니다.

```

{
    "OrganizationalUnit": {
        "Id": "ou-examplerootid111-exampleouid111",
        "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
        "Name": "AccountingOU"
    }
}

```

```
}
}
```

- API 세부 정보는 AWS CLI 명령 참조의 [CreateOrganizationalUnit](#)을 참조하세요.

를 사용하여 조직 단위(OU) 이름 바꾸기 AWS Organizations

조직의 관리 계정에 로그인하면 OU 이름을 바꿀 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

최소 권한

조직 루트에 있는 OU의 이름을 바꾸려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:UpdateOrganizationalUnit`

AWS Management Console

OU의 이름을 바꾸려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 이름을 바꿀 [OU로 이동](#)한 다음, 아래의 단계 중 하나를 수행합니다.
 - 이름을 변경할 OU 옆에 있는 라디오 버튼  을 선택합니다. 그런 다음 작업(Actions) 메뉴의 조직 단위(Organizational unit)에서 이름 바꾸기(Rename)를 선택합니다.
 - OU의 이름을 선택하여 OU의 세부 정보 페이지에 액세스합니다. 페이지 상단에서 이름 바꾸기(Rename)를 선택합니다.
3. 조직 단위 이름 바꾸기(Rename organizational unit) 대화 상자에서 새 이름을 입력하고 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

OU의 이름을 바꾸려면

다음 명령 중 하나를 사용하여 OU 이름 바꿀 수 있습니다.

- AWS CLI: [update-organizational-unit](#)

다음 예제에서는 OU의 이름을 바꾸는 방법을 보여 줍니다.

```
$ aws organizations update-organizational-unit \
  --organizational-unit-id ou-a1b2-f6g7h222 \
  --name "Renamed-OU"
{
  "OrganizationalUnit": {
    "Id": "ou-a1b2-f6g7h222",
    "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-f6g7h222",
    "Name": "Renamed-OU",
    "Path": "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/"
  }
}
```

- AWS SDKs: [UpdateOrganizationalUnit](#)

를 사용하여 조직 단위(OU)에 태그 지정 AWS Organizations

조직의 관리 계정으로 로그인하면 OU에 연결된 태그를 추가하거나 제거할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

최소 권한

조직 루트에 있는 OU에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:DescribeOrganizationalUnit` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

OU에 연결된 태그를 편집하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 태그를 편집하려는 [OU로 이동하여 이름을 선택합니다](#).
3. OU의 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 이 탭에서 다음과 같은 작업을 수행할 수 있습니다.
 - 이전 값 대신 새 값을 입력하여 태그의 값을 편집합니다. 태그 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
 - 제거하려는 태그 옆의 제거(Remove)를 선택하여 기존 태그를 제거합니다.
 - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 null이 아닌 빈 문자열이 됩니다.
5. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

OU에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 OU에 연결된 태그를 변경할 수 있습니다.

- AWS CLI: [tag-resource](#) 및 [untag-resource](#)

다음 예제에서는 "Department"="12345" 태그를 OU에 연결합니다. Key와 Value는 대소문자를 구분합니다.

```
$ aws organizations tag-resource \
  --resource-id ou-a1b2-f6g7h222 \
  --tags Key=Department,Value=12345
```

이 명령은 성공 시 출력을 생성하지 않습니다.

다음 예제에서는 OU에서 Department를 제거합니다.

```
$ aws organizations untag-resource \
  --resource-id ou-a1b2-f6g7h222 \
  --tag-keys Department
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDKs: [TagResource](#) 및 [UntagResource](#)

를 사용하여 계정을 조직 단위(OU)로 또는 루트와 OUs 간에 이동 AWS Organizations

조직의 관리 계정에 로그인하면, 조직의 계정을 루트에서 OU로 이동하거나, 한 OU에서 다른 OU로 이동하거나, OU에서 다시 루트로 이동할 수 있습니다. OU 내에 계정을 배치하면 계정은 상위 OU 및 루트까지의 상위 체인에 속한 모든 OU에 연결된 정책을 적용받게 됩니다. 계정이 OU 안에 있지 않다면, 계정은 루트에 바로 연결된 정책과 계정에 바로 연결된 정책을 적용받게 됩니다. 계정을 이동하려면 다음 단계를 수행합니다.

최소 권한

OU 계층 구조 내 새 위치로 계정을 이동하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:MoveAccount`

AWS Management Console

계정을 OU로 이동하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 이동할 계정을 찾습니다. OU 계층 구조를 탐색하거나, 만 AWS 계정 보기(View only)를 활성화하여 OU 구조 없이 단순 계정 목록을 표시할 수 있습니다. 계정이 많은 경우 이동할 모든 항목을 찾기 위해 목록 하단에 있는 'ou-name'에서 추가 계정 로드(Load more accounts in 'ou-name')를 선택해야 할 수도 있습니다.

3. 이동할 각 계정의 이름 옆에 있는 확인란



선택합니다.

4. 작업(Actions) 메뉴의 AWS 계정에서 이동(Move)을 선택합니다.

5. AWS 계정이동 대화 상자에서 계정을 옮길 OU나 루트를 선택한 다음 이동 AWS 계정을 선택합니다.

음

AWS CLI & AWS SDKs

계정을 OU로 이동하려면

다음 명령 중 하나를 사용하여 계정을 이동할 수 있습니다.

- AWS CLI: [move-account](#)

다음 예시에서는 루트 AWS 계정 에서 OU로 이동합니다. 원본 컨테이너의 ID와 대상 컨테이너의 ID를 모두 지정해야 합니다.

```
$ aws organizations move-account \
  --account-id 111122223333 \
  --source-parent-id r-a1b2 \
  --destination-parent-id ou-a1b2-f6g7h111
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS SDKs: [MoveAccount](#)

를 사용하여 루트의 세부 정보 보기 AWS Organizations

[AWS Organizations 콘솔](#)에서 조직의 관리 계정에 로그인하면 관리 루트의 세부 정보를 확인할 수 있습니다.

i 최소 권한

루트 세부 정보를 보려면 다음과 같은 권한이 있어야 합니다.

- organizations:DescribeOrganization(콘솔 전용)
- organizations:ListRoots

루트는 OU(조직 단위) 계층 구조에서 최상위 컨테이너이며 일반적으로 OU로서 동작합니다. 그러나 계층 구조의 맨 위에 있는 컨테이너는 루트를 변경하면 다른 모든 OU와 조직의 모든 OU AWS 계정에 영향을 미칩니다.

AWS Management Console

루트 세부 정보를 보려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지로 이동해 루트 OU(라디오 버튼이 아닌 이름)를 선택합니다.
3. 루트(Root) 세부 정보 페이지가 나타나고 루트의 세부 정보가 표시됩니다.

AWS CLI & AWS SDKs

루트 세부 정보를 보려면

다음 명령 중 하나를 사용하여 루트의 세부 정보를 볼 수 있습니다.

- AWS CLI: [list-roots](#)

다음 예제에서는 조직에서 현재 활성화된 정책 유형을 비롯해 루트의 세부 정보를 검색하는 방법을 보여줍니다.

```
$ aws organizations list-roots
{
  "Roots": [
    {
      "Id": "r-a1b2",
      "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
      "Name": "Root",
      "PolicyTypes": [
        {
          "Type": "BACKUP_POLICY",
          "Status": "ENABLED"
        }
      ]
    }
  ]
}
```

- AWS SDKs: [ListRoots](#)

를 사용하여 조직 단위(OU) 삭제 AWS Organizations

조직의 관리 계정에 로그인하면 더 이상 필요 없는 모든 OU를 삭제할 수 있습니다.

먼저 모든 계정을 해당 OU 및 모든 하위 OU 밖으로 옮긴 다음 하위 OU를 삭제해야 합니다.

최소 권한

OU를 삭제하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations>DeleteOrganizationalUnit`

AWS Management Console

OU를 삭제하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 삭제할 OU를 찾고 각 OU 이름 옆에 있는 확인란  을 선택합니다.
3. 작업(Actions)을 선택한 다음 조직 단위(Organizational unit)에서 삭제>Delete)를 선택합니다.
4. OU 삭제를 확인하려면 OU의 이름(하나만 삭제하기로 선택한 경우) 또는 'delete'라는 단어(둘 이상을 선택한 경우)를 입력한 다음 삭제>Delete)를 선택합니다.

AWS Organizations 는 OUs를 삭제하고 목록에서 제거합니다.

AWS CLI & AWS SDKs

OU를 삭제하는 방법

다음 코드 예시는 `DeleteOrganizationalUnit`의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
    /// with the selected ID.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitId = "ou-0000-000000000";

        var request = new DeleteOrganizationalUnitRequest
        {
            OrganizationalUnitId = orgUnitId,
        };

        var response = await client.DeleteOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {

```

```
        Console.WriteLine($"Successfully deleted the organizational unit  
with ID: {orgUnitId}.");  
    }  
    else  
    {  
        Console.WriteLine($"Could not delete the organizational unit with  
ID: {orgUnitId}.");  
    }  
}  
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 [DeleteOrganizationalUnit](#)을 참조하세요.

CLI

AWS CLI

OU를 삭제하는 방법

다음 예시에서는 OU를 삭제하는 방법을 보여줍니다. 이 예시에서는 이전에 OU에서 모든 계정과 다른 OU를 제거했다고 가정합니다.

```
aws organizations delete-organizational-unit --organizational-unit-id ou-  
examplerootid111-exampleouid111
```

- API 세부 정보는 AWS CLI 명령 참조의 [DeleteOrganizationalUnit](#)을 참조하세요.

를 사용하여 조직 정책 관리 AWS Organizations

의 정책을 AWS Organizations 사용하면 조직의 AWS 계정 에 추가 유형의 관리를 적용할 수 있습니다. 조직에서 [모든 기능이 활성화](#)되어 있을 때 정책을 사용할 수 있습니다.

AWS Organizations 콘솔에는 각 정책 유형에 대한 활성화 또는 비활성화 상태가 표시됩니다.

Organize accounts(계정 구성) 탭의 왼쪽 탐색 창에서 Root를 선택합니다. 화면 오른쪽의 세부 정보 창에는 사용 가능한 모든 정책 유형이 표시됩니다. 목록에는 해당 조직 루트에서 활성화된 항목과 비활성화된 항목이 표시됩니다. 활성화 옵션이 있으면 해당 유형이 현재 비활성화된 상태입니다. 비활성화 옵션이 있으면 해당 유형이 현재 활성화된 상태입니다.

주제

- [정책 유형](#)
- [의 권한 부여 정책 AWS Organizations](#)
- [의 관리 정책 AWS Organizations](#)
- [에 대한 위임된 관리자 AWS Organizations](#)
- [정책 유형 활성화](#)
- [정책 유형 비활성화](#)
- [를 사용하여 조직 정책 생성 AWS Organizations](#)
- [를 사용하여 조직 정책 업데이트 AWS Organizations](#)
- [를 사용하여 조직 정책에 연결된 태그 편집 AWS Organizations](#)
- [를 사용하여 조직 정책 연결 AWS Organizations](#)
- [를 사용하여 조직 정책 분리 AWS Organizations](#)
- [조직의 정책에 대한 정보 가져오기](#)
- [를 사용하여 조직 정책 삭제 AWS Organizations](#)

정책 유형

Organizations는 다음과 같은 두 가지 범주의 정책 유형을 제공합니다.

권한 부여 정책

권한 부여 정책은 조직 전체에서 AWS 계정 보안을 중앙에서 관리하는 데 도움을 줍니다.

- [서비스 제어 정책\(SCP\)](#)은 조직의 IAM 사용자 및 IAM 역할에 사용 가능한 최대 권한을 중앙에서 제어합니다.
- [리소스 제어 정책\(RCP\)](#)은 조직의 리소스에 사용할 수 있는 최대 권한을 중앙에서 제어할 수 있도록 합니다.

관리 정책

관리 정책은 조직 전체에서 AWS 서비스 및 해당 기능을 중앙에서 구성하고 관리하는 데 도움이 됩니다.

- [선언적 정책](#)을 사용하면 조직 전체에서 지정된에 대해 원하는 구성을 중앙 AWS 서비스에서 선언하고 적용할 수 있습니다. 연결되면 서비스가 새 기능 또는 API를 추가할 때 구성이 항상 유지됩니다.
- [백업 정책](#)을 사용하면 조직의 계정 전체에서 백업 계획을 중앙에서 관리하고 AWS 리소스에 적용할 수 있습니다.
- [태그 정책](#)을 사용하면 조직 계정의 AWS 리소스에 연결된 태그를 표준화할 수 있습니다.
- [채팅 애플리케이션 정책](#)을 사용하면 Slack 및 Microsoft Teams와 같은 채팅 애플리케이션에서 조직의 계정에 대한 액세스를 제어할 수 있습니다.
- [AI 서비스 옵트아웃 정책](#)을 사용하면 조직의 모든 계정에 대한 AWS AI 서비스의 데이터 수집을 제어할 수 있습니다.
- [Security Hub 정책](#)을 통해 조직의 보안 요구 사항에 부합하도록 조직 전반에 이를 중앙에서 적용함으로써 보안 적용 범위 격차를 해소할 수 있습니다.
- [Amazon Inspector 정책](#)을 사용하면 AWS 조직의 여러 계정에서 Amazon Inspector를 중앙에서 활성화하고 관리할 수 있습니다.
- [Amazon Bedrock 정책](#)을 사용하면 Amazon Bedrock에 대한 모든 모델 추론 호출에 대해 조직 구조의 모든 요소에 Amazon Bedrock Guardrails에 구성된 보호 기능을 자동으로 적용할 수 있습니다.
- [업그레이드 롤아웃 정책](#)을 사용하면 조직의 여러 AWS 리소스 및 계정에서 자동 업그레이드를 중앙에서 관리하고 시차를 지정할 수 있습니다.
- [Amazon S3 정책](#)을 사용하면 조직의 계정 전체에서 Amazon S3 리소스에 대한 구성을 대규모로 중앙에서 관리할 수 있습니다.

다음 표에는 각 정책 유형의 특성 중 일부가 요약되어 있습니다. 이러한 정책 유형에 대한 추가 특성은 [AWS Organizations에 대한 할당량 및 서비스 제한](#) 섹션을 참조하세요.

정책 유형	정책 범주	관리 계정 영 향	루트, OU 또 는 계정에 연 결할 수 있는 최대 수	최대 크기	OU 또는 계정 에 대한 효과 적인 정책 보 기 지원
SCP	권한 부여	⊗ 아니요	5	5,120자	⊗ 아니요
RCP	권한 부여	⊗ 아니요	5	5,120자	⊗ 아니요
선언적 정책	관리	☑ 예	10	10,000자	☑ 예
백업 정책	관리	☑ 예	10	10,000자	☑ 예
태그 정책	관리	☑ 예	10	10,000자	☑ 예
채팅 애플리 케이션 정책	관리	☑ 예	5	10,000자	☑ 예
AI 서비스 옹 트아웃 정책	관리	☑ 예	5	2,500자	☑ 예
Security Hub 정책	관리	☑ 예	10	10,000자	☑ 예
Amazon Inspector 정 책	관리	☑ 예	10	10,000자	☑ 예
Amazon Bedrock 정책	관리	☑ 예	10	10,000자	☑ 예
롤아웃 정책 업그레이드	관리	☑ 예	10	10,000자	☑ 예
S3 정책	관리	☑ 예	10	10,000자	☑ 예

의 권한 부여 정책 AWS Organizations

의 권한 부여 정책을 AWS Organizations 사용하면 멤버 계정의 보안 주체 및 리소스에 대한 액세스를 중앙에서 구성하고 관리할 수 있습니다. 이러한 정책이 적용되는 조직 단위(OU) 및 계정에 미치는 영향은 적용되는 권한 부여 정책의 유형에 따라 다릅니다.

에는 서비스 제어 정책(SCPs)과 리소스 제어 정책(RCP) AWS Organizations이라는 두 가지 유형의 권한 부여 정책이 있습니다.RCPs

주제

- [SCP 및 RCP 간의 차이점](#)
- [SCPs 및 RCPs 사용](#)
- [서비스 제어 정책\(SCP\)](#)
- [리소스 제어 정책\(RCP\)](#)

SCP 및 RCP 간의 차이점

SCP는 보안 주체 중심의 제어입니다. SCP는 권한 가드레일을 생성하거나 멤버 계정의 위탁자가 사용할 수 있는 최대 권한에 대한 제한을 설정합니다. 조직의 위탁자에 대해 일관된 액세스 제어를 중앙에서 적용하려는 경우 SCP를 사용할 수 있습니다. 여기에는 IAM 사용자와 IAM 역할이 액세스할 수 있는 서비스, 액세스할 수 있는 리소스 또는 요청을 수행할 수 있는 조건(예: 특정 리전 또는 네트워크)을 지정하는 것이 포함될 수 있습니다.

RCP는 리소스 중심 제어입니다. RCP는 권한 가드레일을 생성하거나 멤버 계정의 리소스가 사용할 수 있는 최대 권한에 대한 제한을 설정합니다. 조직의 리소스 간에 일관된 액세스 제어를 중앙에서 적용하려는 경우 RCP를 사용할 수 있습니다. 조직에 속한 자격 증명만 액세스할 수 있도록 리소스에 대한 액세스를 제한하거나 조직 외부의 자격 증명이 리소스에 액세스할 수 있는 조건을 지정할 수 있습니다.

일부 제어는 SCP와 RCP를 통해 비슷한 방식으로 적용될 수 있습니다. 예를 들어 [사용자가 암호화되지 않은 객체를 S3에 업로드하지 못하도록 할 수 있습니다](#). 이는 보안 주체가 S3 버킷에서 수행할 수 있는 작업에 대한 제어를 적용하기 위해 SCP로 작성할 수 있습니다. 이 제어는 보안 주체가 S3 버킷에 객체를 업로드할 때마다 암호화를 요구하도록 RCP로 작성할 수도 있습니다. 버킷이 타사 공급업체와 같은 조직 외부의 보안 주체가 S3 버킷에 객체를 업로드하도록 허용하는 경우 두 번째 옵션이 선호될 수 있습니다. 그러나 일부 제어는 RCP에서만 구현할 수 있으며 일부 제어는 SCP에서만 구현할 수 있습니다. 자세한 내용은 [SCP 및 RCP의 일반 사용 사례](#) 단원을 참조하십시오.

SCPs 및 RCPs 사용

SCP와 RCP는 독립적인 제어입니다. SCP 또는 RCP만 활성화하거나 두 정책 유형을 함께 사용하도록 선택할 수 있습니다. SCP와 RCP를 모두 사용하면 자격 증명과 리소스에 [데이터 경계](#)를 생성할 수 있습니다.

SCP는 사용자 자격증이 액세스할 수 있는 리소스를 제어하는 기능을 제공합니다. 예를 들어 자격증이 AWS 조직의 리소스에 액세스하도록 허용할 수 있습니다. 그러나 사용자 자격증이 조직 외부의 리소스에 액세스하지 못하도록 할 수 있습니다. SCP를 사용하여 이 제어를 시행할 수 있습니다.

RCP는 리소스에 액세스하는 자격 증명을 제어하는 기능을 제공합니다. 예를 들어 조직의 자격증이 조직의 리소스에 액세스하도록 허용할 수 있습니다. 그러나 조직 외부의 자격증이 리소스에 액세스하지 못하도록 할 수 있습니다. RCP를 사용하여 이 제어를 시행할 수 있습니다. RCP는 리소스에 액세스하는 조직 외부의 보안 주체에 대한 유효한 권한에 영향을 미치는 기능을 제공합니다. SCPs AWS 조직 내 보안 주체에 대한 유효 권한에만 영향을 미칠 수 있습니다.

SCP 및 RCP의 일반 사용 사례

다음 표는 일반적인 SCP 및 RCP 사용 사례를 자세히 설명합니다.

사용 사례:	정책 유형	영향			
		사용자 자격 증명	외부 자격 증명	리소스	외부 리소스 (요청 대상)
Restrict which services or actions your identities can use	SCP	X		X	X
Restrict which resources your identities can access	SCP	X		X	X
Enforce requirements on how	SCP	X		X	X

영향

your identities
can access
resources

Restrict which identities can access your resources	RCP	X	X	X

Protect sensitive resources in your organization	RCP	X	X	X

Enforce requirements on how your resources can be accessed	RCP	X	X	X

서비스 제어 정책(SCP)

서비스 제어 정책(SCP)은 조직의 권한을 관리하는 데 사용할 수 있는 조직 정책 유형입니다. SCP는 조직 내 모든 IAM 사용자 및 IAM 역할에 대해 사용 가능한 최대 권한을 중앙에서 제어합니다. SCP를 사용하면 조직의 액세스 제어 지침에 따라 계정을 유지할 수 있습니다. SCP는 [활성화된 모든 기능을 가진](#) 조직에서만 사용할 수 있습니다. 조직이 통합 결제 기능만 지원한다면 SCP를 이용할 수 없습니다. SCP 활성화에 대한 지침은 [정책 유형 활성화](#) 단원을 참조하세요.

SCP는 조직 내 IAM 사용자 및 IAM 역할에 권한을 부여하지 않습니다. SCP는 어떠한 권한도 부여하지 않습니다. SCP는 조직 내 IAM 사용자 및 IAM 역할이 수행할 수 있는 작업에 대한 권한 가드레일을 정의하거나 제한을 설정합니다. 권한을 부여하려면 관리자가 IAM 사용자 및 IAM 역할에 연결된 자격 증명 기반 정책, 계정의 리소스에 연결된 리소스 기반 정책 등 액세스를 제어하는 정책을 연결해야 합니다. 자세한 내용은 IAM 사용 설명서에서 [자격 증명 기반 정책 및 리소스 기반 정책](#)을 참조하세요.

유효 권한은 SCP와 리소스 제어 정책(RCP)이 허용하는 권한과 ID 및 리소스 기반 정책이 허용하는 권한 간의 논리적 교집합입니다.

⚠ SCP는 관리 계정의 사용자 또는 역할에 영향을 미치지 않습니다.

SCP는 관리 계정의 사용자 또는 역할에 영향을 미치지 않습니다. 조직의 멤버 계정에만 영향을 줍니다. 이는 또한 SCP가 위임된 관리자로 지정된 멤버 계정도 적용됨을 의미합니다.

이 페이지의 주제

- [SCP의 효과 테스트](#)
- [SCP의 최대 크기](#)
- [조직 내 여러 수준에 SCP 연결하기](#)
- [권한에 대한 SCP 효과](#)
- [액세스 데이터를 사용하여 SCP 개선](#)
- [작업 및 엔터티는 SCP로 제한할 수 없습니다.](#)
- [SCP 평가](#)
- [SCP 구문](#)
- [서비스 제어 정책 예](#)
- [를 사용하여 서비스 제어 정책\(SCPs\) 문제 해결 AWS Organizations](#)

SCP의 효과 테스트

AWS에서는 정책이 계정에 미치는 영향을 철저히 테스트하지 않고 SCPs를 조직의 루트에 연결하지 않을 것을 강력히 권장합니다. 대신 한 번에 하나씩, 또는 소량 단위로 계정을 옮길 수 있는 OU를 만들어 사용자가 주요 서비스를 이용하지 못하는 일이 없게 하세요. 서비스가 계정에 사용되는지 확인하는 한 가지 방법은 [IAM에서 마지막으로 데이터를 액세스한 서비스](#)를 살펴보는 것입니다. 또 다른 방법은 [를 사용하여 API 수준에서 서비스 사용량을 로깅 AWS CloudTrail 하는](#) 것입니다.

Note

FullAWSAccess 정책을 수정하거나 허용된 작업이 포함된 별도의 정책으로 대체하지 않는 한 이 정책을 제거해서는 안 됩니다. 그렇지 않으면 멤버 계정의 모든 AWS 작업이 실패합니다.

SCP의 최대 크기

SCP 내 모든 문자는 [최대 크기](#)를 기준으로 계수됩니다. 이 설명서의 예제는 가독성을 높이기 위한 추가 공백으로 포맷된 SCP를 보여 줍니다. 하지만 정책 크기가 최대 크기에 근접한 경우 공백을 저장하려면 인용 부호 바깥에 있는 공백 문자(예: 공백 및 줄 바꿈)를 모두 삭제할 수 있습니다.

Tip

시각적 편집기를 사용하여 SCP를 작성합니다. 편집기가 자동으로 불필요한 공백을 제거합니다.

조직 내 여러 수준에 SCP 연결하기

SCP가 작동하는 방식에 대한 자세한 설명은 [SCP 평가](#)을(를) 참조하세요.

권한에 대한 SCP 효과

SCPs는 AWS Identity and Access Management 권한 정책과 유사하며 거의 동일한 구문을 사용합니다. 그러나 SCP는 권한을 부여하지는 않습니다. 대신 SCP는 조직 내 IAM 사용자 및 IAM 역할에 대한 사용 가능한 최대 권한을 지정하는 액세스 제어입니다. 자세한 내용은 IAM 사용자 안내서의 [정책 평가 로직](#)을 참조하세요.

- SCP는 조직에 속한 계정이 관리하는 IAM 사용자 및 역할에만 영향을 줍니다. SCP는 리소스 기반 정책에 직접 영향을 주지 않습니다. 조직 외부 계정의 사용자 또는 역할에도 영향을 주지 않습니다. 예를 들어 조직의 A 계정이 소유하는 Amazon S3 버킷을 가정해 보겠습니다. 버킷 정책(리소스 기반 정책)은 조직 외부의 B 계정에 속한 사용자에게 액세스 권한을 부여합니다. A 계정에는 SCP가 연결되어 있습니다. 해당 SCP는 B 계정의 외부 사용자에게 적용되지 않습니다. 이 SCP는 조직의 A 계정이 관리하는 사용자에게만 적용됩니다.
- SCP는 멤버 계정의 IAM 사용자 및 역할(멤버 계정의 루트 사용자 포함)에 대해 권한을 제한합니다. 각 계정은 모든 상위 계정이 허용하는 권한만 갖게 됩니다. 권한이 계정 이상의 수준에서 묵시적으로나(Allow 정책문에 포함되지 않음) 명시적으로(Deny 정책문에 포함됨) 막혀 있다면, 영향받는 계정에 있는 사용자나 역할은 계정 관리자가 */* 권한이 있는 AdministratorAccess IAM 정책을 사용자에게 연결하더라도 해당 권한을 사용할 수 없습니다.
- SCP는 조직의 멤버 계정에만 영향을 미칩니다. 관리 계정의 사용자 또는 역할에는 영향을 미치지 않습니다. 이는 또한 SCP가 위임된 관리자로 지정된 멤버 계정도 적용됨을 의미합니다. 자세한 내용은 [관리 계정의 모범 사례](#) 단원을 참조하십시오.

- 사용자와 역할이 적절한 IAM 권한 정책으로 권한을 부여받아야 한다는 사실은 변하지 않습니다. IAM 권한 정책이 없는 사용자는 관련 SCP가 모든 서비스와 작업을 허용해도 액세스 권한이 없습니다.
- 사용자나 역할에게 관련 SCP가 허용하는 작업에 대한 액세스를 부여하는 IAM 권한 정책이 있으면 사용자나 역할이 해당 작업을 수행할 수 있습니다.
- 사용자나 역할에 관련 SCP가 허용하지 않거나 명시적으로 거부한 작업의 액세스 권한을 부여하는 IAM 권한 정책이 있으면 사용자나 역할이 해당 작업을 수행할 수 없습니다.
- SCP는 루트 사용자를 포함하여 추가된 계정의 모든 사용자와 역할에 영향을 줍니다. 유일한 예외는 [작업 및 엔터티는 SCP로 제한할 수 없습니다](#)에 설명되어 있습니다.
- SCP는 어떠한 서비스 연결 역할에도 영향을 미치지 않습니다. 서비스 연결 역할을 사용하면 다른 AWS 서비스 들과 통합할 수 AWS Organizations 있으며 SCPs에 의해 제한될 수 없습니다.
- 루트에서 SCP 정책 유형을 비활성화하면 해당 루트의 모든 AWS Organizations 엔터티에서 모든 SCPs가 자동으로 분리됩니다. AWS Organizations 엔터티에는 조직 단위, 조직 및 계정이 포함됩니다. 루트에서 SCP를 다시 활성화하면, 해당 루트는 루트의 모든 개체에 자동적으로 연결된 기본 FullAWSAccess 정책으로 돌아갑니다. SCP를 비활성화하기 전에 이루어진 SCP와 AWS Organizations 개체 연결은 모두 사라지며, 수동으로 다시 연결할 수는 있지만 자동으로 복원되지는 않습니다.
- 권한 경계(고급 IAM 기능)와 SCP가 둘 다 있는 경우 권한 경계, SCP 및 자격 증명 기반 정책 모두에서 해당 작업을 허용해야 합니다.

액세스 데이터를 사용하여 SCP 개선

관리 계정 자격 증명으로 로그인하면 IAM 콘솔의 AWS Organizations 섹션에서 AWS Organizations 엔터티 또는 정책에 대해 [마지막으로 액세스한 서비스 데이터를](#) 볼 수 있습니다. IAM의 AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 서비스에서 마지막으로 액세스한 데이터를 검색할 수도 있습니다. 이 데이터에는 AWS Organizations 계정의 IAM 사용자 및 역할이 마지막으로 액세스를 시도한 허용된 서비스 및 시기에 대한 정보가 포함됩니다. 이 정보를 사용하여 사용되지 않는 권한을 확인할 수 있으므로 SCP를 구체화함으로써 [최소 권한](#)의 원칙을 보다 잘 준수할 수 있습니다.

예를 들어 세 가지 AWS 서비스에 대한 액세스를 금지하는 [거부 목록 SCP](#)가 있다고 합시다. SCP의 Deny 문에 없는 모든 서비스는 허용됩니다. IAM에서 서비스가 마지막으로 액세스한 데이터는 SCP에서 AWS 서비스 허용하지만 사용되지 않는 데이터를 알려줍니다. 이 정보로 SCP를 업데이트하여 필요 없는 서비스에 대한 액세스를 거부할 수 있습니다.

자세한 내용은 IAM 사용 설명서에서 다음 주제를 참조하세요.

- [Organizations에서 서비스가 마지막으로 액세스한 데이터 보기](#)
- [데이터를 사용하여 조직 단위의 권한 구체화](#)

작업 및 엔터티는 SCP로 제한할 수 없습니다.

다음 작업은 SCP를 사용해 제한할 수 없습니다.

- 관리 계정이 수행하는 모든 작업
- 서비스 연결 역할에 연결된 권한을 사용한 모든 작업.
- 루트 사용자로 Enterprise Support 플랜 등록하기
- CloudFront 프라이빗 콘텐츠에 대한 신뢰할 수 있는 서명자 기능 제공
- 루트 사용자로 Amazon Lightsail 이메일 서버 및 Amazon EC2 인스턴스에 대한 역방향 DNS 구성
- 일부 AWS관련 서비스에 대한 작업:
 - Alexa Top Sites
 - Alexa Web Information Service
 - Amazon Mechanical Turk
 - Amazon 제품 마케팅 API

SCP 평가

Note

이 섹션의 정보는 백업 정책, 태그 정책, 채팅 애플리케이션 정책 또는 AI 서비스 옵트아웃 정책을 비롯한 관리 정책 유형에 적용되지 않습니다. 자세한 내용은 [관리 정책 상속에 대한 이해](#) 단원을 참조하십시오.

AWS Organizations에서 여러 수준의 다양한 서비스 제어 정책 (SCP) 을 연결할 수 있으므로 SCP가 평가되는 방식을 이해하면 올바른 결과를 산출하는 SCP를 작성하는 데 도움이 될 수 있습니다.

주제

- [SCP가 Allow와 협력하는 방식](#)
- [SCP가 거부를 처리하는 방식](#)
- [SCP 사용 전략](#)

SCP가 Allow와 협력하는 방식

특정 계정에 대한 권한을 허용하려면 계정(대상 계정 자체 포함)의 직접 경로에 대한 루트부터 각 OU 까지 모든 수준에서 명시적인 **Allow** 설명이 있어야 합니다. 따라서 SCPs 활성화하면가 모든 서비스 및 작업을 허용하는 [FullAWSAccess](#)라는 AWS 관리형 SCP 정책을 AWS Organizations 연결합니다. 조직의 어느 수준에서도 이 정책을 제거하고 교체하지 않으면 해당 수준 이하의 모든 OU와 계정은 어떤 조치도 취하지 못하게 됩니다.

예를 들어 그림 1과 2에 표시된 시나리오를 살펴보겠습니다. 계정 B에서 권한 또는 서비스를 허용하려면 권한 또는 서비스를 허용하는 SCP를 루트, 프로덕션 OU 및 계정 B 자체에 연결해야 합니다.

SCP 평가는 기본 거부 모델을 따릅니다. 즉, SCP에서 명시적으로 허용되지 않은 권한은 거부됩니다. 루트, 프로덕션 OU 또는 계정 B와 같은 수준의 SCP에 허용되는 설명이 없으면 액세스가 거부됩니다.

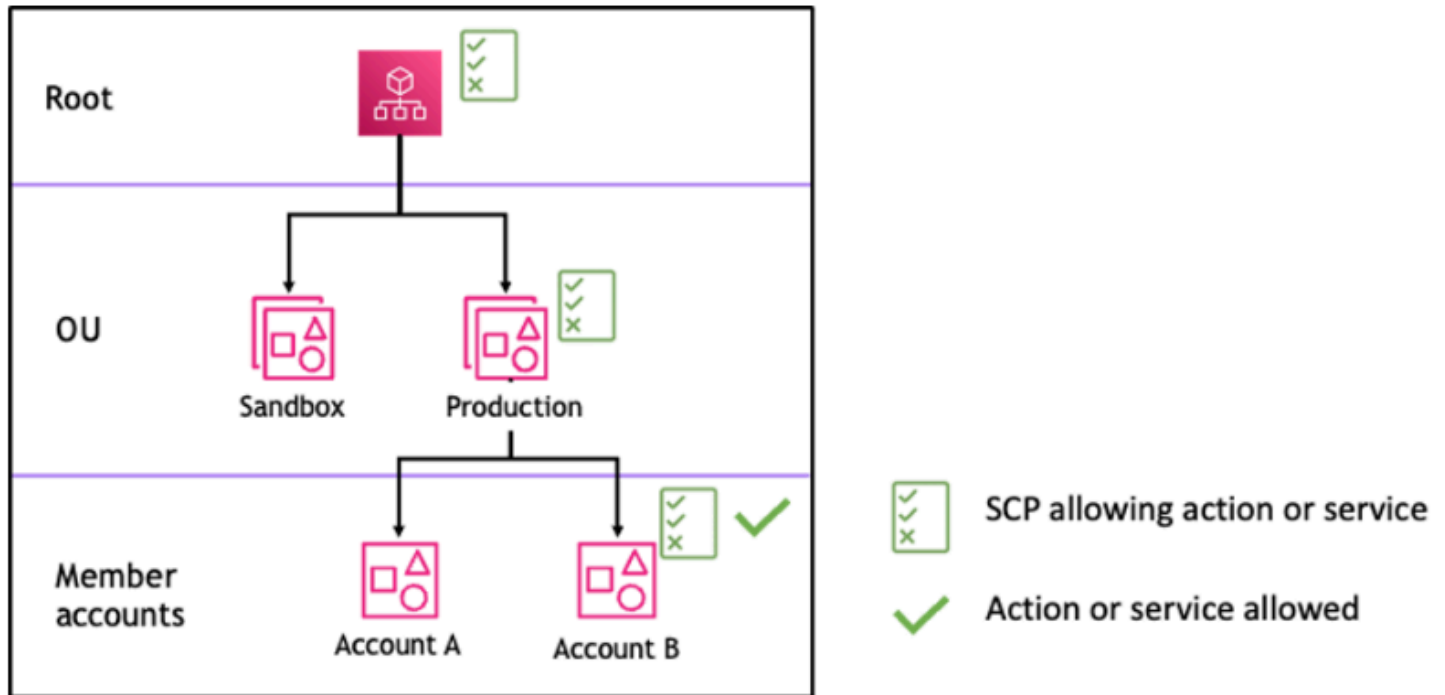


그림 1: 루트, 프로덕션 OU 및 계정 B에 Allow 문이 연결된 조직 구조의 예

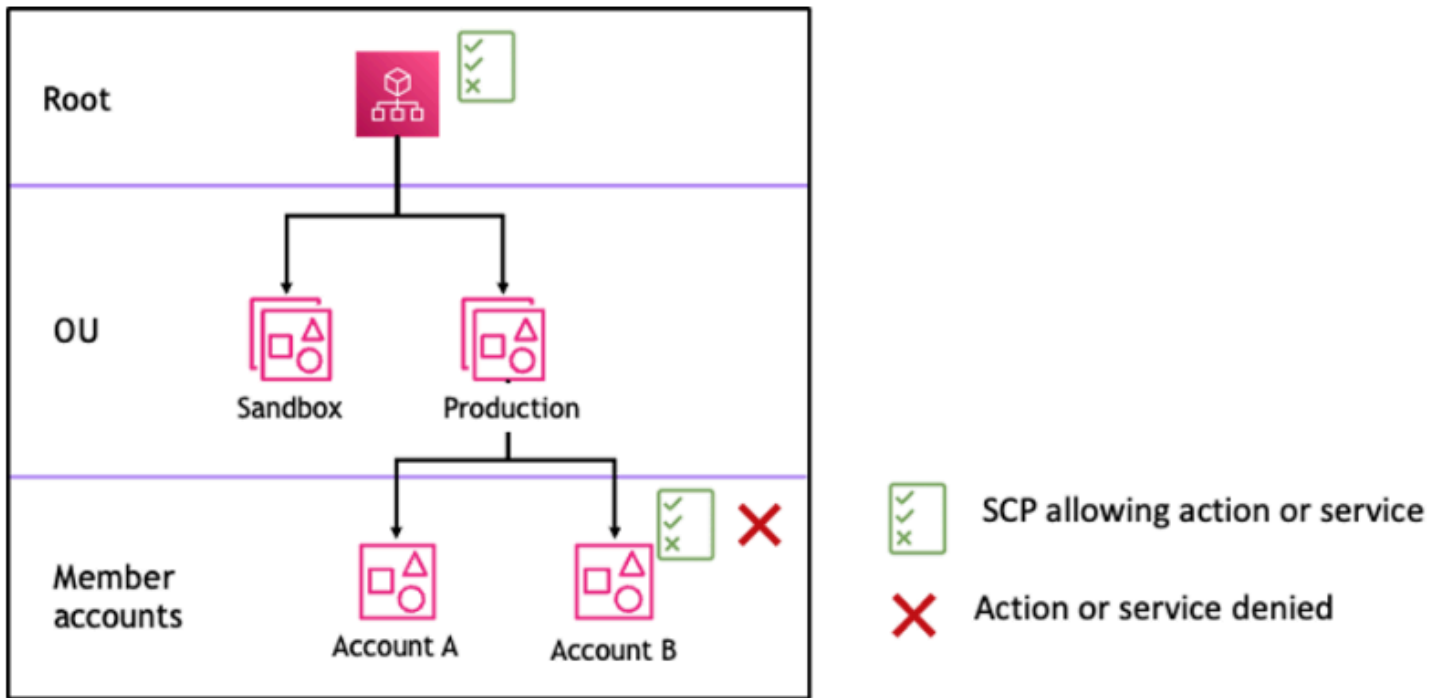


그림 2: 프로덕션 OU에서 누락된 Allow 문이 있는 조직 구조의 예와 이것이 계정 B에 미치는 영향

SCP가 거부를 처리하는 방식

특정 계정에 대한 권한이 거부되는 경우, 루트에서 각 OU를 거쳐 계정의 직접 경로(대상 계정 자체 포함)에 있는 모든 SCP가 해당 권한을 거부할 수 있습니다.

예를 들어 프로덕션 OU에 특정 서비스에 대한 명시적 Deny 설명이 있는 SCP가 연결되어 있다고 가정해 보겠습니다. 그림 3과 같이 루트와 계정 B에 연결된 또 다른 SCP가 있는데, 이는 동일한 서비스에 대한 액세스를 명시적으로 허용합니다. 따라서 조직의 모든 수준에 연결된 거부 정책을 모든 OU 및 해당 계정 아래에 있는 멤버 계정에서 평가하므로 계정 A와 계정 B 모두 서비스에 대한 액세스가 거부됩니다.

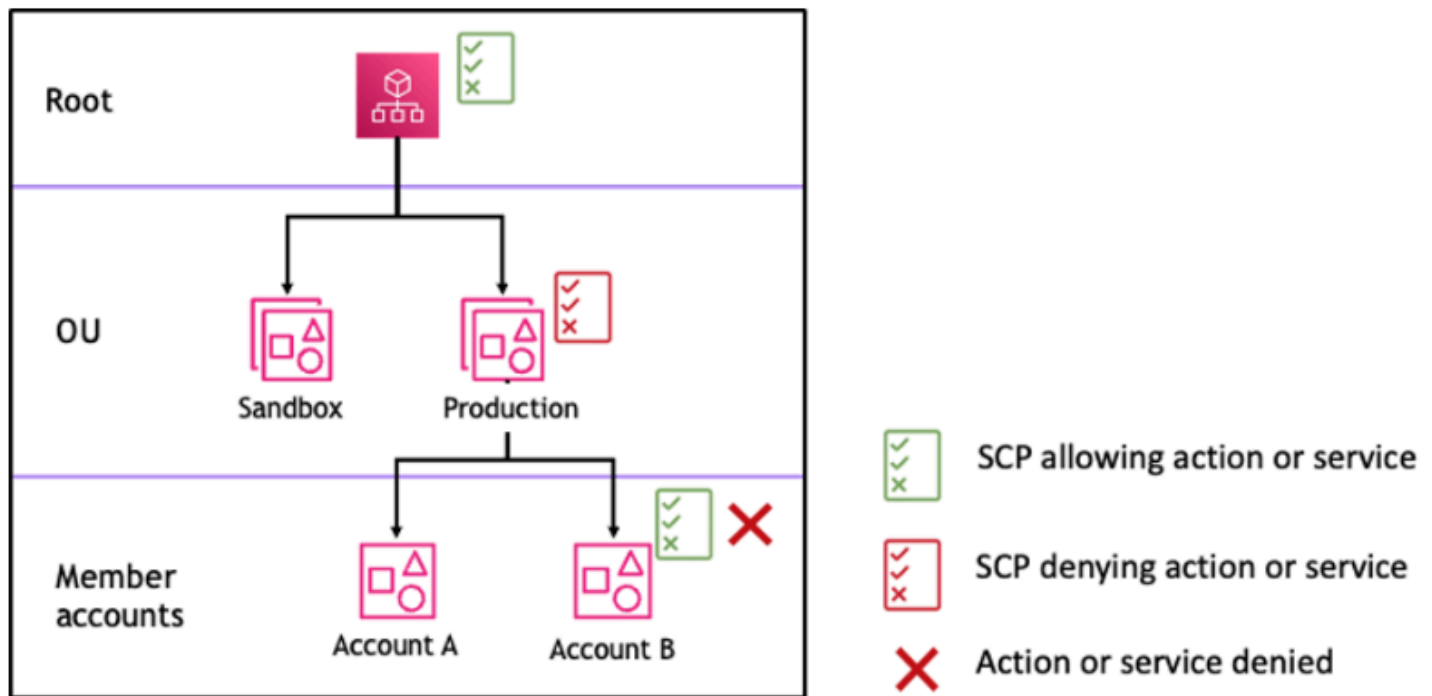


그림 3: 프로덕션 OU에 Deny 문이 연결된 조직 구조의 예와 이것이 계정 B에 미치는 영향

SCP 사용 전략

SCP를 작성할 때 Allow 및 Deny 문을 조합하여 조직에서 의도한 조치와 서비스를 허용할 수 있습니다. Deny 문은 루트 수준이나 OU 수준에서 적용되면 그 아래 있는 모든 계정에 적용되기 때문에 조직 또는 OU의 더 넓은 부분에 적용되어야 하는 제한을 구현할 수 있는 강력한 방법입니다.

Tip

IAM에서 [서비스가 마지막으로 액세스한 데이터](#)를 사용하여 필요한 AWS 서비스 로만 액세스를 제한하도록 SCP를 업데이트할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [Organizations에서 서비스가 마지막으로 액세스한 데이터 보기](#)를 참조하세요.

AWS Organizations 는 생성 시 모든 루트, OU 및 계정에 [FullAWSAccess](#)라는 AWS 관리형 SCP를 연결합니다. 이 정책은 모든 서비스와 작업을 허용합니다. SCP를 업데이트하여 명시적으로 허용되지 않는 한 새 AWS 서비스 가 허용되지 않도록 FullAWSAccess를 서비스 세트만 허용하는 정책으로 바꿀 수 있습니다. SCPs 예를 들어 조직에서 사용자 환경의 하위 집합 서비스만 사용하도록 허용하려는 경우 Allow 명령문을 사용하여 특정 서비스만 허용할 수 있습니다. 루트 수준 또는 모든 수준에서 FullAWSAccess를 교체하도록 선택할 수 있습니다. 루트에 서비스별 허용 목록 SCP를 연결하면 루트 아래의 모든 OUs 및 계정에 자동으로 적용됩니다. 즉, 단일 루트 수준 정책이 시나리오 7과 같이 전체

조직에 걸쳐 효과적인 서비스 허용 목록을 결정합니다. 또는 각 OU 및 계정에서 FullAWSAccess를 제거하고 교체하여 조직 단위 또는 개별 계정마다 다른 보다 세분화된 서비스 허용 목록을 구현할 수 있습니다.

참고: 허용 문과 암시적 deny-by-default 모델에만 의존하면 더 넓거나 중첩되는 허용 문이 더 제한적인 문을 재정의할 수 있으므로 의도하지 않은 액세스로 이어질 수 있습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "cloudwatch:*",
        "organizations:*"
      ],
      "Resource": "*"
    }
  ]
}
```

두 명령문을 조합한 정책은 멤버 계정이 조직을 떠나는 것을 방지하고 원하는 AWS 서비스의 사용을 허용하는 다음 예와 유사할 수 있습니다. 조직 관리자는 FullAWSAccess 정책을 분리하고 대신에 이 정책을 연결하면 됩니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "cloudwatch:*",
        "organizations:*"
      ],

```

```

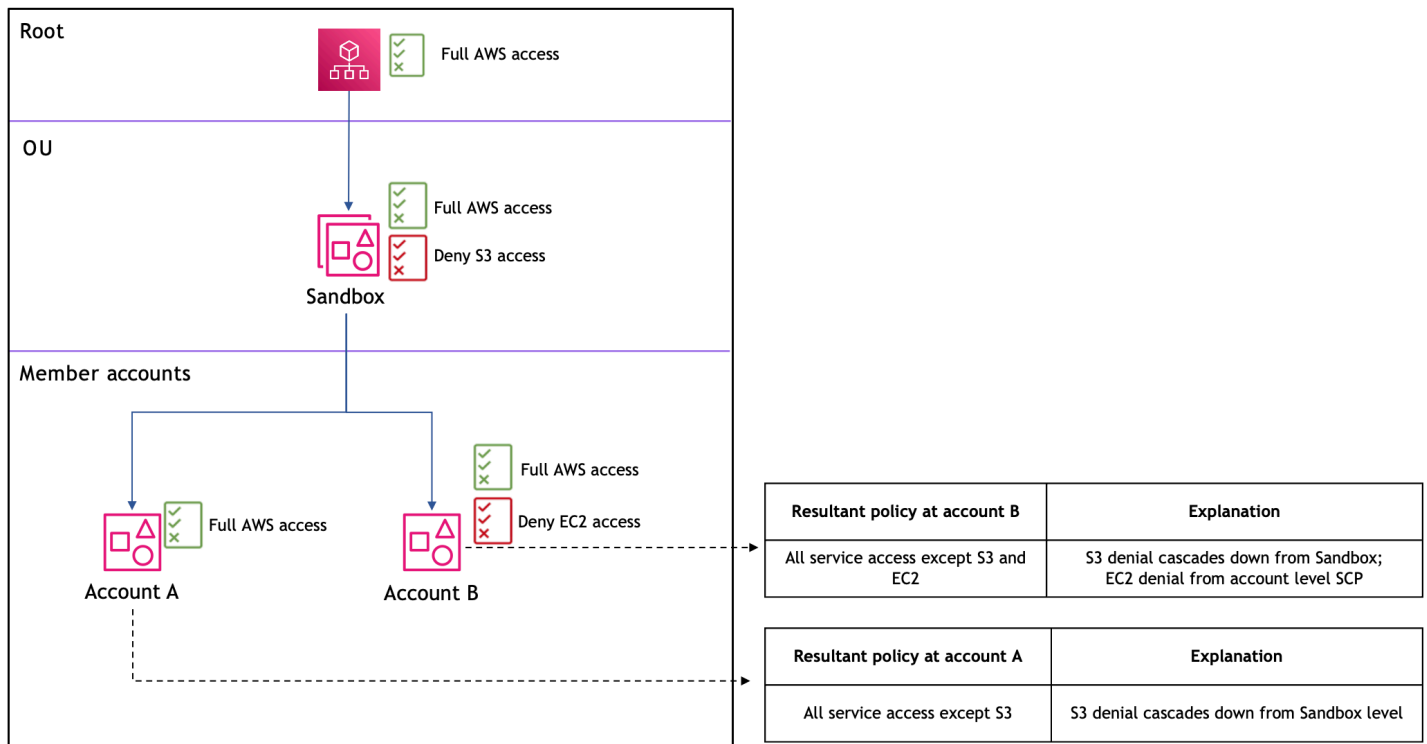
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": "organizations:LeaveOrganization",
    "Resource": "*"
  }
]
}

```

AWS 조직에서 여러 서비스 제어 정책(SCP)을 적용하는 방법을 보여주려면 다음 조직 구조 및 시나리오를 고려하세요.

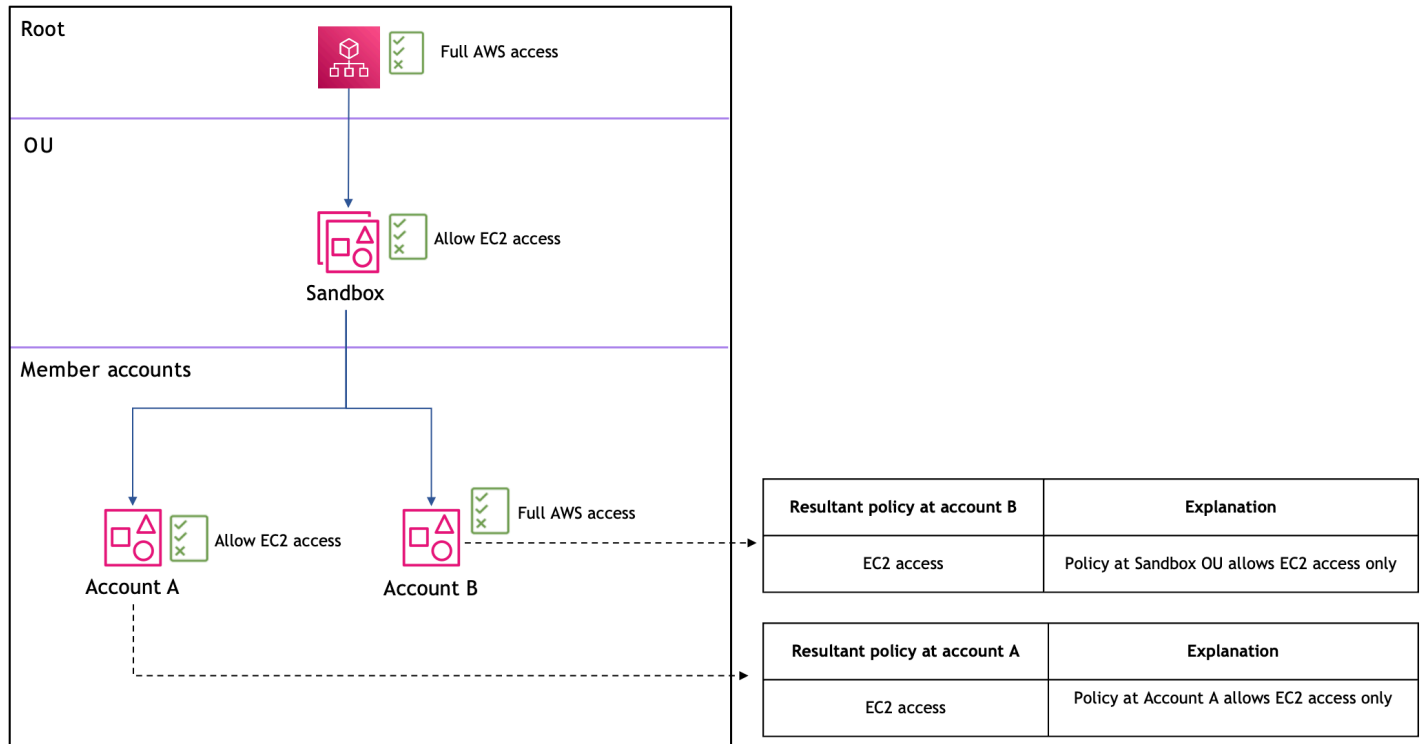
시나리오 1: 거부 정책의 영향

이 시나리오는 조직 내 상위 수준의 거부 정책이 아래의 모든 계정에 미치는 영향을 보여줍니다. 샌드박스 OU에 "전체 AWS 액세스" 및 "S3 액세스 거부" 정책이 모두 있고 계정 B에 "EC2 액세스 거부" 정책이 있는 경우 결과적으로 계정 B는 S3(OU 수준 거부) 및 EC2(계정 수준 거부)에 액세스할 수 없습니다. 계정 A에는 S3 액세스 권한이 없습니다(OU 수준 거부에서).



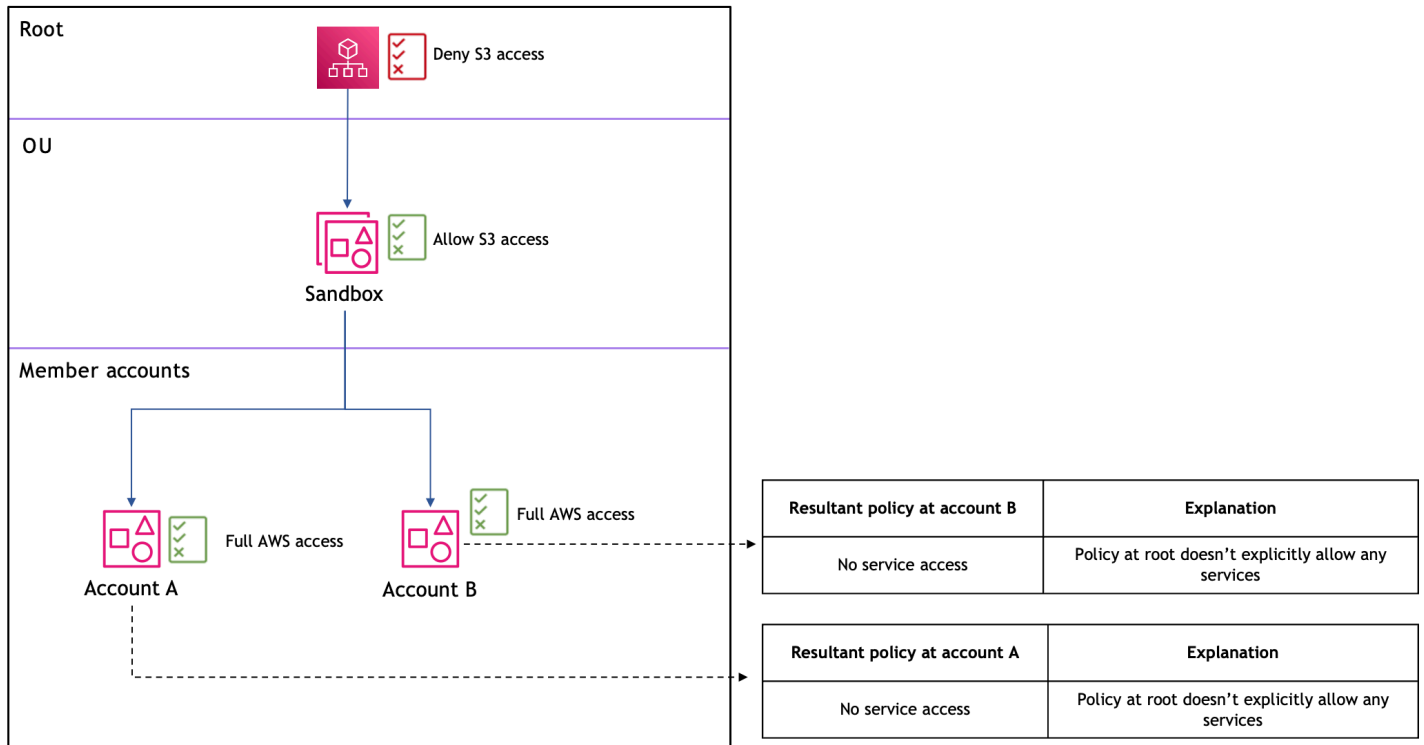
시나리오 2: 모든 수준에서 허용 정책이 존재해야 함

이 시나리오는 SCP에서 허용 정책이 작동하는 방식을 보여줍니다. 서비스에 액세스하려면 루트에서 계정까지 모든 수준에서 명시적인 허용이 있어야 합니다. 여기서 샌드박스 OU에는 EC2 서비스 액세스만 명시적으로 허용하는 'EC2 액세스 허용' 정책이 있으므로 계정 A와 B에는 EC2 액세스 권한만 있습니다.



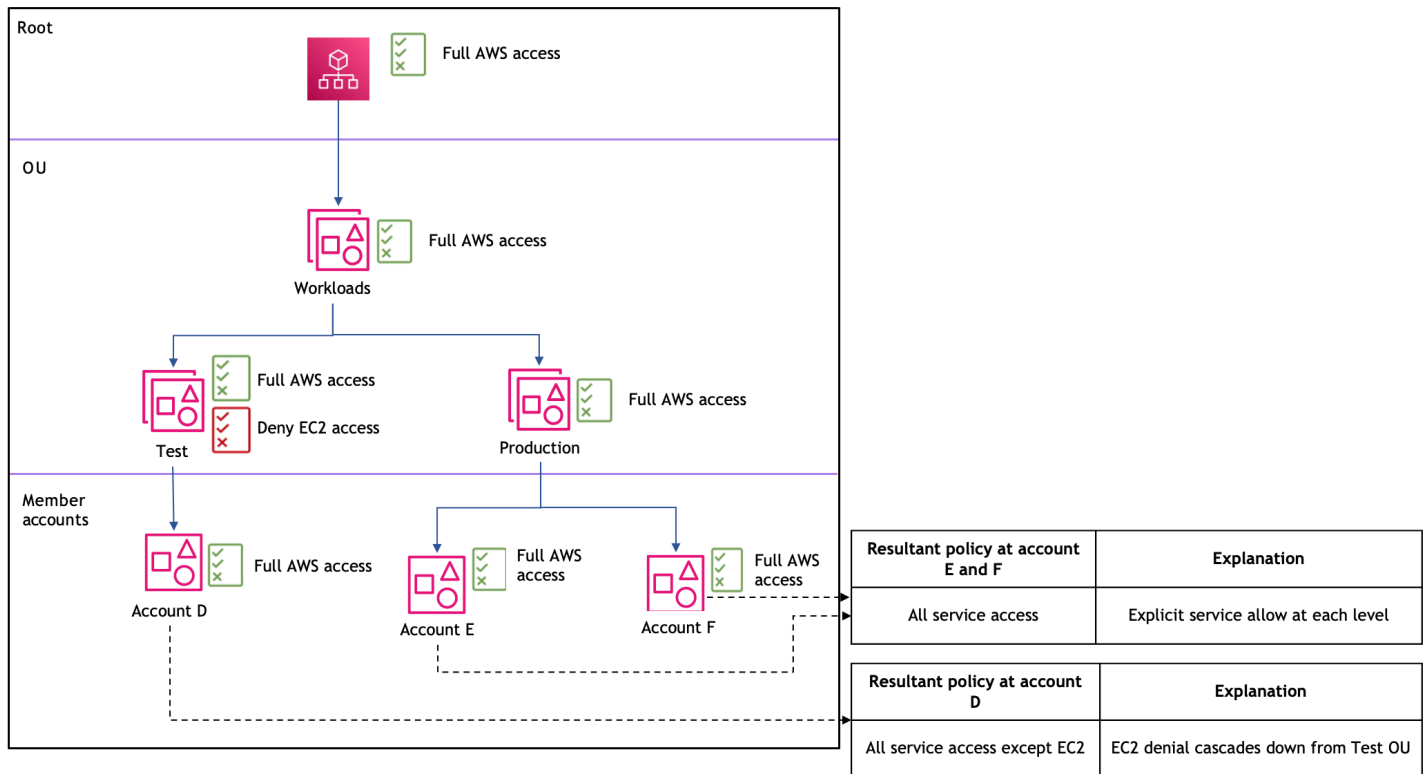
시나리오 3: 루트 수준에서 허용(Allow) 문 누락의 영향

SCP의 루트 수준에서 "허용" 문이 누락된 것은 조직의 모든 멤버 계정에 대한 AWS 서비스 및 작업에 대한 모든 액세스를 효과적으로 차단하는 중요한 잘못된 구성입니다.



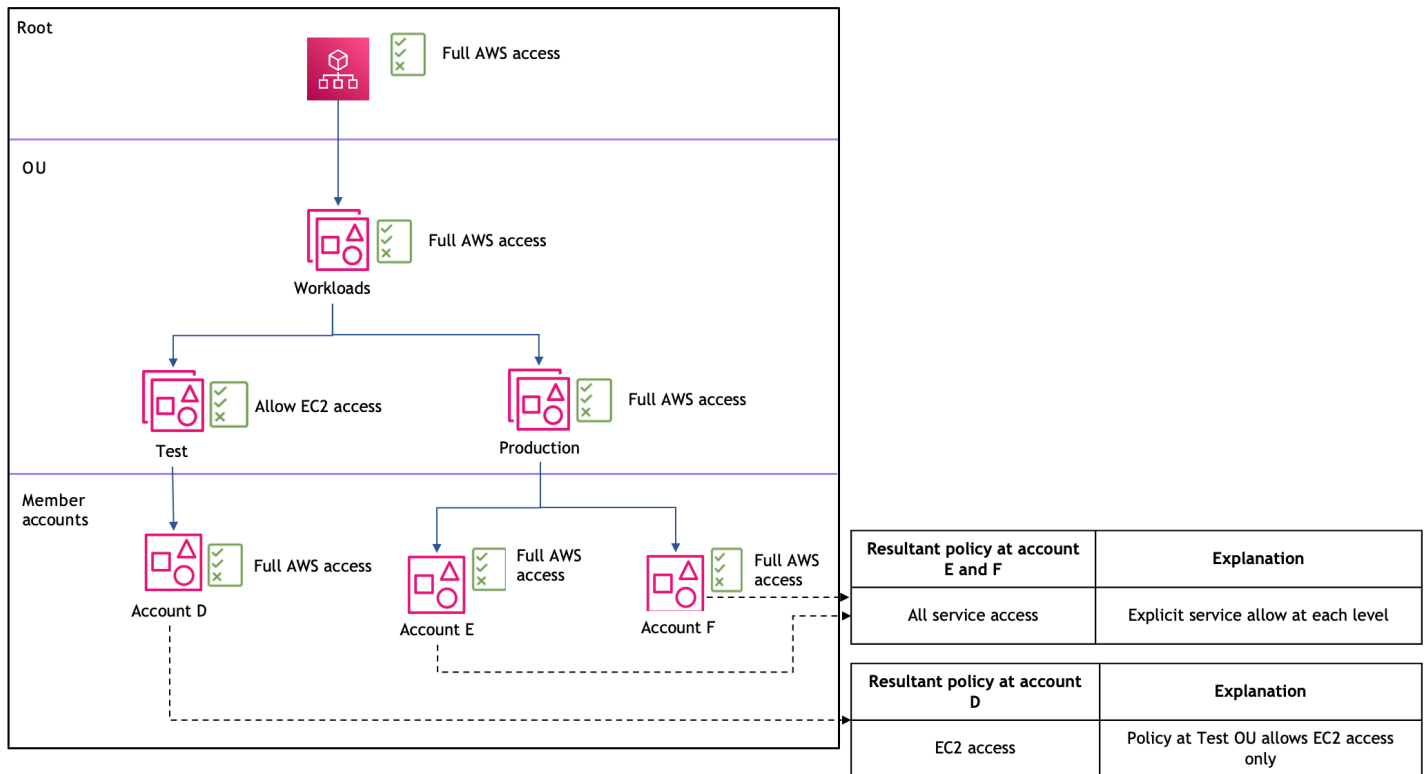
시나리오 4: 계층화된 거부(Deny) 문 및 결과 권한

이 시나리오는 2단계 심층 OU 구조를 보여줍니다. 루트 및 워크로드 OU에는 모두 "전체 AWS 액세스"가 있고, 테스트 OU에는 "EC2 AWS 액세스 거부"가 있는 "전체 액세스"가 있으며, 프로덕션 OU에는 "전체 AWS 액세스"가 있습니다. 결과적으로, 계정 D는 EC2를 제외한 모든 서비스에 대한 액세스 권한을 가지며, 계정 E와 F는 모든 서비스에 대한 액세스 권한을 가집니다.



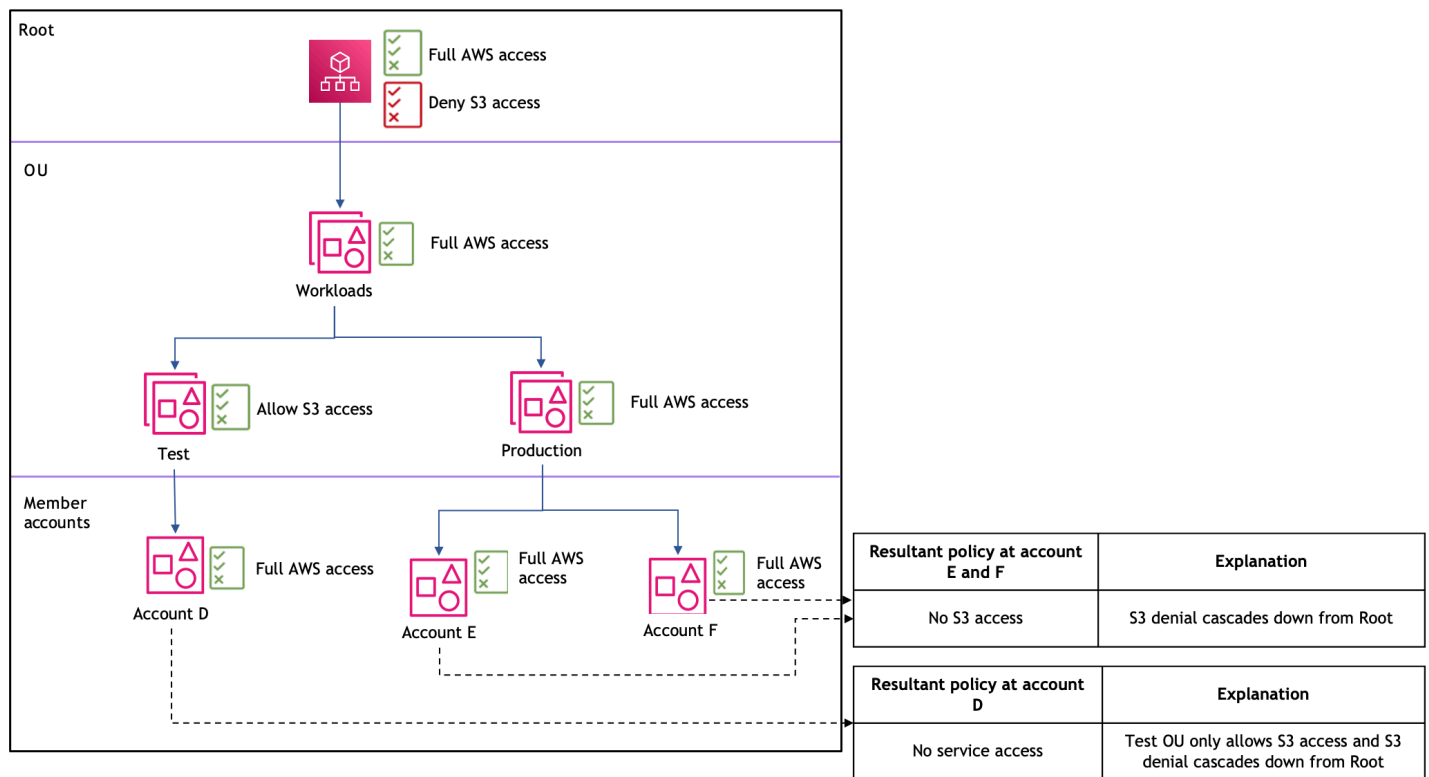
시나리오 5: OU 수준의 정책이 서비스 액세스를 제한하도록 허용

이 시나리오에서는 허용 정책을 사용하여 특정 서비스에 대한 액세스를 제한하는 방법을 보여줍니다. 테스트 OU에는 'EC2 액세스 허용' 정책이 있습니다. 즉, 계정 D에는 EC2 서비스만 허용됩니다. 프로덕션 OU는 '전체 AWS 액세스'를 유지하므로 계정 E와 F는 모든 서비스에 액세스할 수 있습니다. 이는 어떻게 루트 수준에서는 더 광범위한 허용 정책을 유지하면서 OU 수준에서는 더 제한적인 허용 정책을 구현할 수 있는지 보여줍니다.



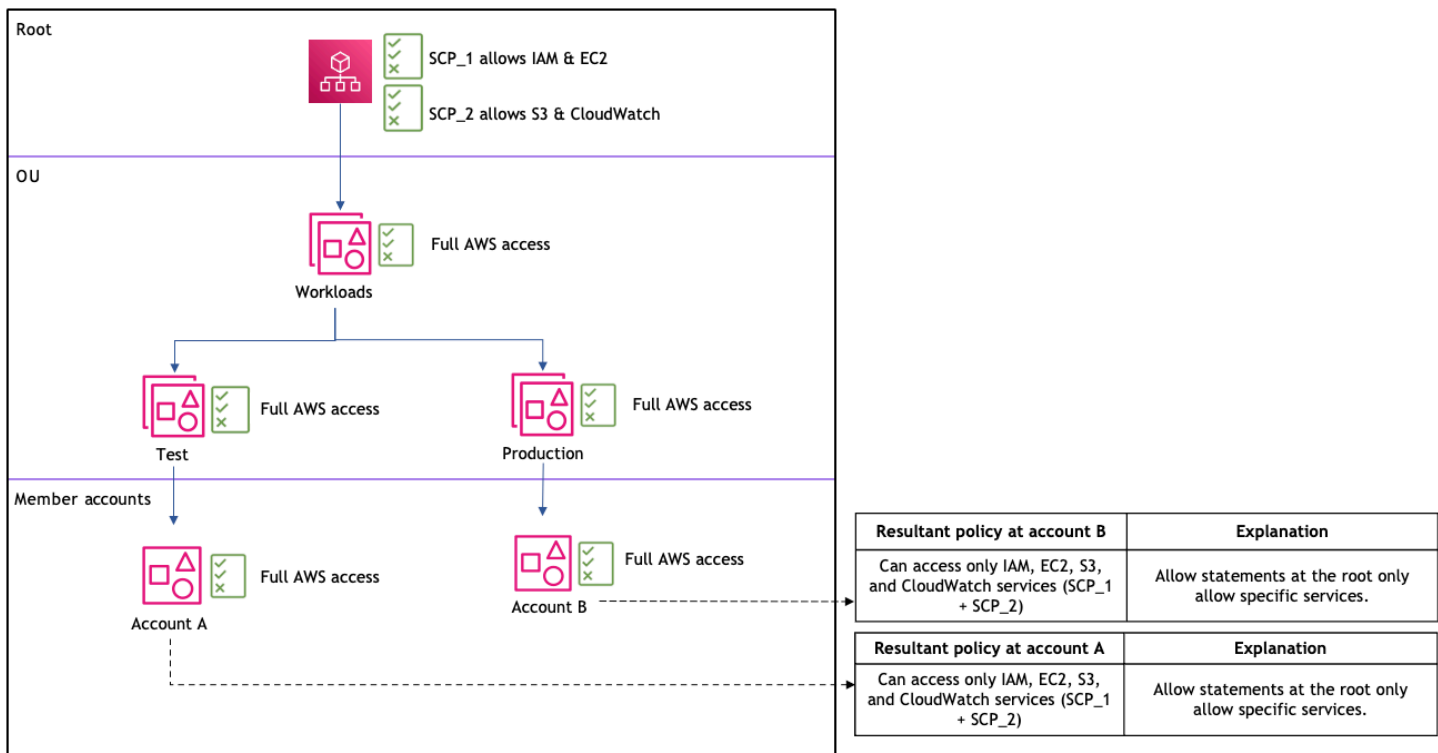
시나리오 6: 하위 수준 허용과 관계없이 루트 수준 거부가 모든 계정에 영향을 미칩니다

이 시나리오는 하위 수준의 정책 허용에 관계없이 루트 수준의 거부 정책이 조직의 모든 계정에 영향을 미친다는 것을 보여줍니다. 루트에는 "전체 AWS 액세스" 및 "S3 액세스 거부" 정책이 모두 있습니다. 테스트 OU에 'S3 액세스 허용' 정책이 있더라도 루트 수준 S3 거부가 우선합니다. 테스트 OU는 S3 액세스만 허용하지만 루트 수준에서는 S3가 거부되므로 계정 D에는 서비스 액세스 권한이 없습니다. 계정 E와 F는 루트 수준에서 명시적 거부로 인해 S3를 제외한 다른 서비스에 액세스할 수 있습니다.



시나리오 7: OU 수준 액세스를 제한하는 루트 수준 사용자 지정 허용 정책

이 시나리오는 명시적 서비스가 있는 SCPs 내에서 루트 수준에서 적용될 때 어떻게 작동하는지 보여줍니다. AWS Organizations. 조직 루트 수준에서는 제한된 AWS 서비스 세트에 대한 액세스를 명시적으로 허용하는 두 개의 사용자 지정 "서비스 허용" SCPs가 연결됩니다. SCP_1은 IAM 및 Amazon EC2를 허용하고, SCP_2는 Amazon S3 및 Amazon CloudWatch를 허용합니다. 조직 단위(OU) 수준에서 기본 FullAWSAccess 정책은 연결된 상태로 유지됩니다. 그러나 교차 동작으로 인해 이러한 OUs의 계정 A와 B는 루트 수준 SCP가 명시적으로 허용하는 서비스에만 액세스할 수 있습니다. 더 제한적인 루트 정책이 우선하므로 더 낮은 조직 수준에서 부여된 광범위한 권한과 관계없이 IAM, EC2, S3 및 CloudWatch 서비스에 대한 액세스만 효과적으로 제한합니다.



SCP 구문

서비스 제어 정책(SCPs AWS Identity and Access Management (IAM) 권한 정책 및 [리소스 기반 정책](#)(예: Amazon S3 버킷 정책)에서 사용하는 구문과 유사한 구문을 사용합니다. IAM 정책과 그 구문에 대한 자세한 내용은 [IAM 사용 설명서](#)의 IAM 정책 개요를 참조하세요.

SCP는 [JSON](#) 규칙에 따라 구성된 일반 텍스트 파일입니다. SCP는 이번 주제에서 설명하는 요소를 사용합니다.

Note

SCP 내 모든 문자는 [최대 크기](#)를 기준으로 계수됩니다. 이 설명서의 예제는 가독성을 높이기 위한 추가 공백으로 포맷된 SCP를 보여 줍니다. 하지만 정책 크기가 최대 크기에 근접한 경우 공백을 저장하려면 인용 부호 바깥에 있는 공백 문자(예: 공백 및 줄 바꿈)를 모두 삭제할 수 있습니다.

SCP에 대한 일반적인 내용은 [서비스 제어 정책\(SCP\)](#) 단원을 참조하세요.

요소 요약

다음 표에는 SCP에서 사용할 수 있는 정책 요소가 요약되어 있습니다. 일부 정책 요소는 작업을 거부하는 SCP에서만 사용할 수 있습니다. 지원되는 효과(Supported effects) 열에는 SCP에서 각 정책 요소와 함께 사용할 수 있는 효과 유형이 나열되어 있습니다.

요소	용도	지원되는 효과
작업	SCP가 허용하거나 거부하는 AWS 서비스 및 작업을 지정합니다.	Allow, Deny
효과	SCP 문이 계정의 IAM 사용자 및 역할에 대해 액세스를 허용 하는지, 아니면 거부 하는지를 정의합니다.	Allow, Deny
Statement	정책 요소 컨테이너의 역할을 합니다. SCP에 여러 문을 포함할 수 있습니다.	Allow, Deny

요소	용도	지원되는 효과
Statement ID(Sid)	(선택 사항) 문의 표시 이름을 제공합니다.	Allow, Deny
버전	정책을 처리하는 데 사용할 언어 구문 규칙을 지정합니다.	Allow, Deny
조건	문이 효력을 발휘하는 조건을 지정합니다.	Allow, Deny
NotAction	SCP에서 제외되는 AWS 서비스 및 작업을 지정합니다. Action 요소 대신 사용합니다.	Allow, Deny
리소스	SCP가 적용되는 AWS 리소스를 지정합니다.	Allow, Deny

요소	용도	지원되는 효과
NotResource	SCP에서 제외되는 AWS 리소스를 지정합니다. Resource 요소 대신 사용합니다.	Allow, Deny

다음 섹션에서는 SCP에서 정책 요소가 사용되는 방식에 대한 자세한 설명 및 예제를 제공합니다.

주제

- [Action 및 NotAction 요소](#)
- [Condition 요소](#)
- [Effect 요소](#)
- [Resource 및 NotResource 요소](#)
- [Statement 요소](#)
- [Statement ID\(Sid\) 요소](#)
- [Version 요소](#)
- [지원되지 않는 요소](#)

Action 및 NotAction 요소

Action 또는 NotAction 요소의 값은 문에 의해 허용되거나 거부되는 AWS 서비스 및 작업을 식별하는 문자열 목록(JSON 배열)입니다.

각 문자열은 서비스의 소문자 약자("s3", "ec2", "iam" 또는 "organizations" 등) 뒤에 콜론이 오고 그 뒤에 해당 서비스의 작업이 붙는 형태로 구성됩니다. Action 및 NotAction은 대/소문자를 구분하지 않습니다. 일반적으로 각 단어는 첫 글자만 대문자로, 나머지는 소문자로 입력합니다. 예를 들어 "s3:ListAllMyBuckets"입니다.

SCP에서 별표(*) 또는 물음표(?) 와 같은 와일드카드 문자도 사용할 수도 있습니다.

- 이름의 일부를 공유하는 여러 작업을 일치시키려면 별표(*)를 와일드카드로 사용하십시오. "s3:*" 값은 Amazon S3 서비스의 모든 작업을 의미합니다. "ec2:Describe*" 값은 "Describe"로 시작하는 EC2 작업에만 대응합니다.
- 단일 문자를 일치시키려면 물음표(?) 와일드카드를 사용하십시오.

AWS Organizations SCPs 및 IAM 권한 정책 모두에서 지원하는 모든 서비스 및 작업 목록은 IAM 사용 설명서의 [AWS 서비스에 사용되는 작업, 리소스 및 조건 키를 참조하세요](#).

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: Action](#) 및 [IAM JSON 정책 요소: NotAction](#)을 참조하세요.

Action 요소 예제

다음은 계정 관리자가 계정의 EC2 인스턴스에 대한 권한 설명, 시작, 중단, 중지를 위임하게 하는 문이 포함된 SCP를 보여주는 예제입니다. 이 예제는 [허용 목록](#)의 예입니다. 허용 목록은 기본 Allow * 정책이 연결되지 않아 기본적으로 권한이 묵시적으로 거부되는 때에 유용합니다. 기본 Allow * 정책이 다음과 같은 정책이 연결된 루트, OU 또는 계정에 여전히 연결돼 있다면, 해당 정책은 영향을 주지 못하게 됩니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
      "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
      "ec2:RunInstances",
      "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
    ],
    "Resource": "*"
  }
}
```

다음 예제는 연결된 계정에서 사용하지 않으려는 서비스에 대해 [액세스를 거부](#)하는 방법을 보여 줍니다. 기본 "Allow *" SCP가 모든 OU와 루트에 여전히 연결돼 있다고 가정합니다. 이 예제 정책은 연결 계정에 있는 계정 관리자가 IAM, Amazon EC2, Amazon RDS 서비스에 대해 어떤 권한도 위임하지

못하게 합니다. 이러한 권한을 거부하는 다른 연결된 정책이 없는 한, 다른 서비스의 모든 작업을 위임할 수 있습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [ "iam:*", "ec2:*", "rds:*" ],
    "Resource": "*"
  }
}
```

NotAction 요소 예제

다음 예제에서는 NotAction 요소를 사용하여 정책의 효과에서 AWS 서비스를 제외하는 방법을 보여줍니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
      }
    }
  ]
}
```

이 문에서 영향을 받는 계정은 IAM 작업을 사용하는 경우를 AWS 리전제외하고 지정된에서 작업을 수행하는 것으로 제한됩니다.

Condition 요소

SCP에서 허용 및 거부 문에 Condition 요소를 지정할 수 있습니다.

다음 예제에서는 SCP에서 허용 문과 함께 조건 요소를 사용하여 특정 보안 주체가 AWS 서비스에 액세스하도록 허용하는 방법을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServicesForSpecificPrincipal",
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "s3:*",
        "rds:*",
        "lambda:*",
        "cloudformation:*",
        "iam:*",
        "cloudwatch:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalArn": [
            "arn:aws:iam::123456789012:role/specific-role"
          ]
        }
      }
    }
  ]
}
```

다음 예제에서는 SCP에서 거부 문이 있는 조건 요소를 사용하여 지정된 서비스의 작업을 제외하고 eu-central-1 및 eu-west-1 리전 외부의 모든 작업에 대한 액세스를 제한하는 방법을 보여줍니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutsideEU",
      "Effect": "Deny",
      "NotAction": [
        "cloudfront:*",
        "iam:*",
        "route53:*",
        "support:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "eu-central-1",
            "eu-west-1"
          ]
        }
      }
    }
  ]
}
```

자세한 정보는 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.

Effect 요소

각 문에는 Effect 요소 하나가 있어야 합니다. 이때 값은 Allow 또는 Deny가 될 수 있습니다. 이것은 같은 문에서 나열하는 모든 작업에 영향을 줍니다.

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 효과](#)를 참조하세요.

"Effect": "Allow"

다음 예제는 계정 사용자가 Amazon S3 서비스를 위한 작업을 수행하도록 허용하는 Allow 값을 갖는 Effect 요소를 포함한 문이 있는 SCP를 보여줍니다. 이 예제는 [허용 목록 전략](#)을 사용하는 조직에서 유용하게 활용할 수 있습니다(기본 FullAWSAccess 정책이 모두 분리되어 있어 기본적으로 권한이

묵시적으로 거부되는 전략). 결과적으로 이 문은 연결된 모든 계정에 대해 Amazon S3 권한을 [허용](#)합니다.

```
{
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

이 문은 IAM 권한 정책과 동일한 Allow 값 키워드를 사용하지만, SCP에서는 실제로 사용자에게 특정 작업을 수행할 수 있는 권한을 부여하지 않습니다. 대신에 SCP가 조직 내 계정, 조직 단위(OU) 또는 계정에 대한 최대 권한을 지정하는 필터 역할을 합니다. 이전 예제에서, 계정의 사용자에게 AdministratorAccess 관리형 정책이 연결돼 있다 하더라도 이 SCP는 영향받는 계정의 모든 사용자가 Amazon S3 작업만 할 수 있게 합니다.

"Effect": "Deny"

Effect 요소의 값이 Deny인 문에서는 특정 리소스에 대한 액세스를 제한하거나 SCP가 효력을 발휘하는 조건을 정의할 수도 있습니다.

다음 예제는 거부 문에서 조건 키를 사용하는 방법을 보여줍니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:InstanceType": "t2.micro"
      }
    }
  }
}
```

SCP에서 이 문은 Amazon EC2 인스턴스가 t2.micro로 설정되지 않은 경우 영향받는 계정(SCP가 계정 자체에 연결된 계정 또는 계정을 포함한 조직 루트 또는 OU에 연결된 계정)이 Amazon EC2 인스턴스를 시작하는 것을 금지하는 가드레일을 설정합니다. 이 작업을 허용하는 IAM 정책이 계정에 연결되어 있더라도 SCP에 의해 생성된 가드레일이 이를 금지합니다.

Resource 및 NotResource 요소

Effect 요소의 값이 Allow인 문에서는 SCP의 Resource 요소에 "*"만 지정할 수 있습니다. 개별 Amazon 리소스 이름(ARN) 리소스를 지정할 수 없습니다.

리소스 요소에서 별표(*) 또는 물음표(?)와 같은 와일드카드 문자를 사용할 수 있습니다.

- 이름의 일부를 공유하는 여러 작업을 일치시키려면 별표(*)를 와일드카드로 사용하세요.
- 단일 문자를 일치시키려면 물음표(?) 와일드카드를 사용하십시오.

Effect 요소의 값이 Deny인 문에서는 다음 예제와 같이 개별 ARN을 지정하는 것이 가능합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

```
]
}
```

이 SCP는 영향받는 계정의 IAM 사용자 및 역할이 조직 내 모든 계정에 생성된 공통 관리 IAM 역할을 변경하지 못하게 제한합니다.

다음 예에서는 NotResource 요소를 사용하여 정책 효과에서 특정 Amazon Bedrock 모델을 제외하는 방법을 보여줍니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "NotResource": [
        "arn:aws:bedrock:*::foundation-model/model-to-permit"
      ]
    }
  ]
}
```

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 리소스](#)를 참조하세요.

Statement 요소

SCP는 하나 이상의 Statement 요소로 구성됩니다. 정책은 Statement 키워드 하나만 가질 수 있지만, 값은 ([] 문자로 구분한) JSON 문 어레이가 될 수 있습니다.

다음 예제는 하나의 Effect, Action 및 Resource 요소로 구성된 한 문을 보여줍니다.

```
"Statement": {
  "Effect": "Allow",
  "Action": "*",
  "Resource": "*"
}
```

다음 예제는 하나의 Statement 요소 안에 어레이 목록으로 존재하는 문 2개를 보여줍니다. 첫 번째 문은 모든 작업을 허용하지만 두 번째 문은 모든 EC2 작업을 거부합니다. 그 결과 계정 관리자는 Amazon Elastic Compute Cloud(Amazon EC2)를 제외한 모든 출처의 권한을 위임할 수 있습니다.

```
"Statement": [
  {
    "Effect": "Allow",
    "Action": "*",
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": "ec2:*",
    "Resource": "*"
  }
]
```

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 문](#)을 참조하세요.

Statement ID(Sid) 요소

Sid는 정책 문에 입력되는 식별자(옵션)입니다. Sid 값은 문 배열에서 각 문에 할당할 수 있습니다. 다음 예제 SCP는 샘플 Sid 문을 보여줍니다.

```
{
  "Statement": {
    "Sid": "AllowsAllActions",
    "Effect": "Allow",
    "Action": "*",
    "Resource": "*"
  }
}
```

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: ID](#)를 참조하세요.

Version 요소

모든 SCP에는 값이 "2012-10-17"인 Version 요소가 있어야 합니다. 이 버전 값은 IAM 권한 정책의 최신 버전과 같습니다.

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 버전](#)을 참조하세요.

지원되지 않는 요소

다음 요소는 SCP에서 지원되지 않습니다.

- NotPrincipal
- Principal

서비스 제어 정책 예

이 주제에 나온 예제 [서비스 제어 정책\(SCP\)](#)은 정보 제공용입니다.

이 예제를 사용하기 전에

조직에서 이러한 예제 SCPs 사용하기 전에 다음 사항을 고려하세요.

- [서비스 제어 정책\(SCPs\)](#)은 대략적인 가드레일로 사용하기 위한 것이며 액세스를 직접 부여하지 않습니다. 실제로 권한을 부여하려면 관리자가 여전히 계정의 IAM 보안 주체 또는 리소스에 자격 [증명 기반 또는 리소스 기반 정책을](#) 연결해야 합니다. 유효 권한은 서비스 제어 정책/리소스 제어 정책과 자격 증명 정책 또는 서비스 제어 정책/리소스 제어 정책과 리소스 정책 간의 논리적 교집합입니다. 권한에 대한 SCP 효과에 대한 자세한 내용은 여기에서 확인할 수 [있습니다](#).
- 조직, 조직 단위 또는 계정에 연결된 경우 [서비스 제어 정책\(SCP\)](#)은 조직, 조직 단위 또는 계정의 모든 계정에 대해 사용 가능한 최대 권한을 중앙에서 제어합니다. 조직의 여러 수준에서 SCP를 적용할 수 있으므로 [SCPs 평가](#) 방법을 이해하면 올바른 결과를 산출하는 SCPs를 작성하는 데 도움이 될 수 있습니다.
- 이 리포지토리의 서비스 제어 정책은 예제로 표시됩니다. 정책이 계정에 미치는 영향을 철저히 테스트하지 않고 SCPs를 연결해서는 안 됩니다. 구현하려는 정책이 준비되면 프로덕션 환경을 나타낼 수 있는 별도의 조직 또는 OU에서 테스트하는 것이 좋습니다. 테스트를 마치면 더 구체적인 OUs에 변경 사항을 배포한 다음 시간이 지남에 따라 더 광범위하고 더 광범위한 OUs에 변경 사항을 천천히 배포해야 합니다.
- 이 리포지토리의 SCP 예제는 [거부 목록 전략](#)을 사용합니다. 즉, [FullAWSAccess](#) 정책 또는 조직 엔터티에 연결된 액세스가 작업을 허용하도록 허용하는 기타 정책도 필요합니다. 또한 자격 증명 기반 또는 리소스 기반 정책을 사용하여 보안 주체에게 적절한 권한을 부여해야 합니다.

i Tip

[IAM](#)에서 [서비스가 마지막으로 액세스한 데이터](#)를 사용하여 필요한 AWS 서비스 로만 액세스를 제한하도록 SCP를 업데이트할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [Organizations에서 서비스가 마지막으로 액세스한 데이터 보기](#)를 참조하세요.

GitHub 리포지토리

- [서비스 제어 정책 예제](#) -이 GitHub 리포지토리에는 AWS SCPs 있습니다.

를 사용하여 서비스 제어 정책(SCPs) 문제 해결 AWS Organizations

여기에 있는 정보를 사용하여 서비스 제어 정책(SCP)에서 발견되는 일반적인 오류를 진단하고 해결하세요.

의 서비스 제어 정책(SCPs) AWS Organizations 은 IAM 정책과 유사하며 공통 구문을 공유합니다. 이 구문은 [JavaScript Object Notation\(JSON\)](#) 규칙으로 시작합니다. JSON은 객체를 구성하는 이름과 값 쌍으로 객체를 설명합니다. [IAM 정책 문법](#)은 정책을 사용하여 권한을 부여하는 AWS 서비스 에서 어떤 이름과 값이 의미를 가지며 어떤 의미로 이해되는지를 정의함으로써 JSON을 기반으로 생성됩니다.

AWS Organizations 는 IAM 구문 및 문법의 하위 집합을 사용합니다. 자세한 내용은 [SCP 구문](#)을 참조하세요.

공통 정책 오류

- [정책 객체가 하나 이상인 경우](#)
- [Statement 요소가 하나 이상인 경우](#)
- [정책 문서가 최대 크기를 초과함](#)

정책 객체가 하나 이상인 경우

SCP는 단 하나의 JSON 객체로 구성되어야 합니다. 객체는 중괄호 { }로 묶어 표시합니다. 대괄호 [] 안에 중괄호 { }를 추가로 삽입하여 JSON 객체 내에 다른 객체를 중첩시킬 수도 있지만 정책에 따라 중괄호 { }를 묶는 대괄호 []는 하나로 제한됩니다. 다음 예제는 올바르지 않은데, 최상위 레벨에 (###으로 호출한) 객체 2개가 있기 때문입니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

하지만 올바른 정책 문법을 사용하여 이전 예제의 의도를 만족하는 방법도 있습니다. 2개의 정책 객체에 Statement 요소를 각각 추가하지 않고 두 블록을 단일 Statement 요소로 결합하면 됩니다. 그러면 다음 예제와 같이 Statement 요소가 두 객체 배열을 값으로 인식합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

이 예제는 서로 효과가 다른 요소 2개가 있어 요소가 하나인 Statement로 추가 압축할 수 없습니다. 일반적으로 각 문의 Effect와 Resource 요소가 같을 때만 문을 결합할 수 있습니다.

Statement 요소가 하나 이상인 경우

이 오류는 처음에는 이전 섹션에 나온 오류의 변형처럼 보일지도 모릅니다. 하지만 구문으로 보면 다른 유형의 오류입니다. 다음 예제를 보면 중괄호 {} 한 쌍이 최상위 레벨로 정책 객체 하나만 표시하고 있습니다. 하지만 객체에 포함된 Statement 요소는 2개입니다.

SCP는 콜론 왼쪽의 이름(Statement)과 오른쪽의 값으로 구성된 Statement 요소 1개만 포함해야 합니다. 그리고, Statement 요소의 값은 Effect 요소 1개와 Action 요소 1개, 그리고 Resource 요소 1개가 중괄호 {}로 묶여 구성된 객체가 되어야 합니다. 다음은 예제는 올바르지 않은데, 정책 객체에 Statement 요소 2개가 있기 때문입니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

값 객체는 다수의 값 객체 배열이 될 수 있으므로 이 문제는 다음 예제와 같이 Statement 요소 2개를 객체 배열을 통해 하나의 요소로 결합하여 해결할 수 있습니다.

JSON

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



```

"Statement": [
  {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
]
}

```

Statement 요소 값이 객체 배열이 되었습니다. 예제의 배열은 두 객체로 구성되며, 각 객체 자체가 정확한 Statement 요소 값으로 인식됩니다. 배열을 구성하는 각 객체는 쉼표로 구분합니다.

정책 문서가 최대 크기를 초과함

SCP 문서의 최대 크기는 5,120자입니다. 이 최대 크기는 공백을 포함하여 모든 문자를 포함합니다. SCP의 크기를 줄이려면 인용 부호 바깥에 있는 공백 문자(예: 공백 및 줄 바꿈)를 모두 제거할 수 있습니다.

Note

를 사용하여 정책을 저장하면 JSON 요소와 인용 부호 외부 사이의 AWS Management Console 추가 공백이 제거되고 계산되지 않습니다. SDK 작업 또는 를 사용하여 정책을 저장하면 제공된 대로 AWS CLI 정책이 정확히 저장되며 문자가 자동으로 제거되지 않습니다.

리소스 제어 정책(RCP)

Note

서비스 제어 정책(SCP) 및 리소스 제어 정책(RCP)
조직의 멤버 계정 내에서 IAM 위탁자의 권한을 제한해야 하는 경우 SCP를 사용합니다.
조직의 멤버 계정 내 리소스에 액세스하도록 요청하는 조직 계정 외부의 IAM 위탁자를 제한해야 하는 경우 RCP를 사용합니다.
자세한 내용은 [SCP 및 RCP 이해](#)를 참조하세요.

리소스 제어 정책(RCP)은 조직의 권한을 관리하는 데 사용할 수 있는 조직 정책 유형입니다. RCP는 조직의 모든 리소스에 사용 가능한 최대 권한을 중앙에서 제어합니다. RCP는 계정의 리소스가 조직의 액세스 제어 지침을 준수하도록 보장하는 데 도움을 줍니다. RCP는 [활성화된 모든 기능을 가진](#) 조직에서만 사용할 수 있습니다. 조직이 통합 결제 기능만 지원한다면 RCP를 이용할 수 없습니다. RCP를 활성화하는 데 대한 지침은 [정책 유형 활성화](#) 섹션을 참조하세요.

RCP만으로는 조직 내 리소스에 권한을 부여하기에 충분하지 않습니다. RCP는 어떤 권한도 부여하지 않습니다. RCP는 자격 증명에 조직의 리소스에 대해 수행할 수 있는 작업에 대한 권한 가이드라인을 정의하거나 제한을 설정합니다. 관리자는 실제로 권한을 부여하기 위해 여전히 자격 증명 기반 정책을 IAM 사용자 또는 역할에 연결하거나 리소스 기반 정책을 계정의 리소스에 연결해야 합니다. 자세한 내용은 IAM 사용 설명서에서 [자격 증명 기반 정책 및 리소스 기반 정책](#)을 참조하세요.

[유효 권한](#)은 RCP와 [서비스 제어 정책\(SCP\)](#)이 허용하는 권한과 ID 및 리소스 기반 정책이 허용하는 권한 간의 논리적 교집합입니다.

 RCP는 관리 계정의 리소스에 영향을 주지 않습니다.

RCP는 관리 계정의 리소스에 영향을 주지 않습니다. 조직 내 멤버 계정의 리소스에만 영향을 줍니다. 이는 또한 RCP가 위임된 관리자로 지정된 멤버 계정에도 적용됨을 의미합니다.

이 페이지의 주제

- [RCPs AWS 서비스 지원하는 목록](#)
- [RCP의 효과 테스트](#)
- [RCP의 최대 크기](#)
- [조직 내 여러 수준에 RCP 연결하기](#)
- [권한에 대한 RCP 효과](#)
- [RCP로 제한받지 않는 리소스 및 엔터티](#)
- [RCP 평가](#)
- [RCP 구문](#)
- [리소스 제어 정책 예제](#)

RCPs AWS 서비스 지원하는 목록

RCPs AWS 서비스다음에 대한 작업에 적용됩니다.

- [Amazon S3](#)
- [AWS Security Token Service](#)
- [AWS Key Management Service](#)
- [Amazon SQS](#)
- [AWS Secrets Manager](#)
- [Amazon Cognito](#)
- [Amazon CloudWatch Logs](#)
- [Amazon DynamoDB](#)
- [Amazon Elastic 컨테이너 레지스트리](#)
- [Amazon OpenSearch Serverless](#)

RCP의 효과 테스트

AWS에서는 정책이 계정의 리소스에 미치는 영향을 철저히 테스트하지 않고 RCPs를 조직의 루트에 연결하지 않을 것을 강력히 권장합니다. 먼저 개별 테스트 계정에 RCP를 연결하고 계층 구조에서 가장 낮은 OU로 이동시킨 다음 필요에 따라 조직 구조를 따라 작업할 수 있습니다. 영향을 확인하는 한 가지 방법은 액세스 거부 오류에 대한 AWS CloudTrail 로그를 검토하는 것입니다.

RCP의 최대 크기

RCP 내 모든 문자는 [최대 크기](#)를 기준으로 계수됩니다. 이 설명서의 예제는 가독성을 높이기 위한 추가 공백으로 포맷된 RCP를 보여 줍니다. 하지만 정책 크기가 최대 크기에 근접한 경우 공백을 저장하려면 인용 부호 바깥에 있는 공백 문자(예: 공백 및 줄 바꿈)를 모두 삭제할 수 있습니다.

Tip

시각적 편집기를 사용하여 RCP를 작성합니다. 편집기가 자동으로 불필요한 공백을 제거합니다.

조직 내 여러 수준에 RCP 연결하기

RCP를 개별 계정, OU 또는 조직 루트에 직접 연결할 수 있습니다. RCP가 작동하는 방식에 대한 자세한 설명은 [RCP 평가](#) 섹션을 참조하세요.

권한에 대한 RCP 효과

RCPs는 AWS Identity and Access Management (IAM) 정책의 한 유형입니다. [리소스 기반 정책과](#) 가장 밀접하게 관련이 있습니다. 그러나 RCP는 권한을 부여하지는 않습니다. 대신 RCP는 조직의 리소스에 대해 사용할 수 있는 최대 권한을 지정하는 액세스 제어입니다. 자세한 내용은 IAM 사용자 안내서의 [정책 평가 로직](#)을 참조하세요.

- RCPs의 하위 집합에 대한 리소스에 적용됩니다 AWS 서비스. 자세한 내용은 [RCPs AWS 서비스 지원하는 목록](#) 단원을 참조하십시오.
- RCP는 RCP를 연결한 조직에 속하는 계정에서 관리하는 리소스에만 영향을 미칩니다. 조직 외부 계정의 리소스에는 영향을 주지 않습니다. 예를 들어 조직의 A 계정이 소유하는 Amazon S3 버킷을 가정해 보겠습니다. 버킷 정책(리소스 기반 정책)은 조직 외부의 B 계정에 속한 사용자에게 액세스 권한을 부여합니다. A 계정에는 RCP가 연결되어 있습니다. RCP는 계정 B의 사용자가 액세스한 경우에도 계정 A의 S3 버킷에 적용됩니다. 그러나 계정 A의 사용자가 액세스 시 계정 B의 리소스에는 해당 RCP가 적용되지 않습니다.
- RCP는 멤버 계정의 리소스에 대한 권한을 제한합니다. 각 계정의 모든 리소스는 각 상위 계정이 허용하는 권한만 갖게 됩니다. 해당 계정 위의 어떤 수준에서든 권한이 차단된 경우 리소스 소유자가 사용자에게 전체 액세스를 허용하는 리소스 기반 정책을 연결하더라도 영향을 받는 계정의 리소스에는 해당 권한이 없습니다.
- RCP는 작업 요청의 일부로 승인된 리소스에 적용됩니다. 이러한 리소스는 [서비스 권한 부여 참조](#) 내 작업 테이블의 '리소스 유형' 열에서 찾을 수 있습니다. '리소스 유형' 열에 리소스가 지정되면 직접적으로 호출하는 위탁자의 RCP가 적용됩니다. 예를 들어 s3:GetObject이 객체 리소스를 승인합니다. GetObject 요청이 이루어질 때마다 해당 RCP가 적용되어 요청 위탁자가 GetObject 작업을 간접적으로 호출할 수 있는지 여부를 결정합니다. 적용 가능한 RCP는 계정, 조직 단위(OU) 또는 액세스 중인 리소스를 소유한 조직의 루트에 연결된 RCP입니다.
- RCP는 조직의 멤버 계정에만 영향을 미칩니다. 관리 계정의 리소스에는 영향을 미치지 않습니다. 이는 또한 RCP가 위임된 관리자로 지정된 멤버 계정도 적용됨을 의미합니다. 자세한 내용은 [관리 계정의 모범 사례](#) 단원을 참조하십시오.
- 위탁자가 RCP가 연결된 계정 내의 리소스(적용 가능한 RCP가 있는 리소스)에 접근 요청을 할 때, 해당 RCP는 정책 평가 논리에 포함되어 위탁자의 접근을 허용 또는 거부할지 결정하는 데 사용됩니다.
- RCP는 위탁자가 동일한 조직에 속하는지 여부에 관계없이 적용 가능한 RCP를 사용하여 멤버 계정의 리소스에 액세스하려는 해당 위탁자의 유효 권한에 영향을 미칩니다. 여기에는 루트 사용자가 포함됩니다. RCP는 서비스 연결 역할이 수행한 호출에는 적용되지 않으므로 위탁자가 서비스 연결 역할인 경우는 예외입니다. 서비스 연결 역할을 사용하면 AWS 서비스 가 사용자를 대신하여 필요한 작업을 수행할 수 있으며 RCPs 의해 제한될 수 없습니다.

- 사용자 및 역할에는 여전히 자격 증명 기반 정책 및 리소스 기반 정책을 포함해 적절한 IAM 권한 정책을 통해 권한이 부여되어야 합니다. IAM 권한 정책이 없는 사용자 또는 역할은 RCP가 모든 서비스, 모든 작업 및 모든 리소스를 허용하더라도 액세스할 수 없습니다.

RCP로 제한받지 않는 리소스 및 엔터티

다음 작업은 RCP를 사용해 제한할 수 없습니다.

- 관리 계정의 리소스에 대한 모든 작업.
- RCP는 어떤 서비스 연결 역할의 유효 권한에도 영향을 주지 않습니다. 서비스 연결 역할은 AWS 서비스에 직접 연결된 고유한 유형의 IAM 역할로, 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. 서비스 연결 역할의 권한은 RCP로 제한할 수 없습니다. 또한 RCPs AWS 서비스 연결 역할을 수입하는 서비스의 기능에 영향을 주지 않습니다. 즉, 서비스 연결 역할의 신뢰 정책도 RCPs의 영향을 받지 않습니다.
- RCPs [AWS 관리형 키 for AWS Key Management Service](#). AWS 관리형 키 are에서 사용자를 대신하여 생성, 관리 및 사용하는 데는 적용되지 않습니다 AWS 서비스. 이들의 권한은 변경하거나 관리할 수 없습니다.
- RCP 다음의 권한에 영향을 주지 않습니다.

서비스	API	RCP에서 승인하지 않은 리소스
AWS Key Management Service	kms:RetireGrant	RCP는 kms:RetireGrant 권한에 영향을 주지 않습니다. kms:RetireGrant 에 대한 권한 결정 방법에 관한 자세한 내용은 AWS KMS 개발자 안내서의 권한 부여 중지 및 취소 를 참조하세요.

RCP 평가

Note

이 섹션의 정보는 백업 정책, 태그 정책, 채팅 애플리케이션 정책 또는 AI 서비스 옵트아웃 정책을 비롯한 관리 정책 유형에 적용되지 않습니다. 자세한 내용은 [관리 정책 상속에 대한 이해](#) 단원을 참조하십시오.

AWS Organizations에서 여러 수준의 다양한 리소스 제어 정책(RCP)을 연결할 수 있으므로 RCP가 평가되는 방식을 이해하면 올바른 결과를 산출하는 RCP를 작성하는 데 도움이 될 수 있습니다.

RCP 사용 전략

RCPFu11AWSAccess 정책은 AWS 관리형 정책입니다. 리소스 제어 정책(RCP)을 활성화하면 조직 루트, 모든 OU 및 조직의 모든 계정에 자동으로 연결됩니다. 이 정책은 분리할 수 없습니다. 이 기본 RCP를 사용하면 모든 위탁자와 작업이 RCP 평가를 통과할 수 있습니다. 즉, RCP를 생성하고 연결하기 시작할 때까지는 기존 IAM 권한이 모두 그대로 작동합니다. 이 AWS 관리형 정책은 액세스 권한을 부여하지 않습니다.

Deny 문을 사용하여 조직의 리소스에 대한 액세스를 차단할 수 있습니다. 특정 계정의 리소스에 대한 권한이 거부되는 경우, 루트에서 각 OU를 거쳐 계정의 직접 경로(대상 계정 자체 포함)에 있는 모든 RCP가 해당 권한을 거부할 수 있습니다.

Deny 문은 조직의 더 광범위한 부분에 적용되어야 하는 제한을 구현하는 강력한 방법입니다. 예를 들어, 조직 외부의 자격 증명이 리소스 루트 수준에 접근하는 것을 방지하는 정책을 적용할 수 있으며, 이는 조직 내 모든 계정에 효과적으로 적용됩니다. AWS에서는 조직 루트에 RCP를 적용하기 전에 해당 정책이 계정 내 리소스에 미치는 영향을 철저히 테스트할 것을 강력히 권장합니다. 자세한 내용은 [RCP의 효과 테스트](#) 단원을 참조하십시오.

그림 1에서는 프로덕션 OU에 연결된 RCP가 있으며, 특정 서비스에 대해 명시적 Deny 선언이 지정되어 있습니다. 따라서 조직의 모든 수준에 연결된 거부 정책을 모든 OU 및 해당 계정 아래에 있는 멤버 계정에서 평가하므로 계정 A와 계정 B 모두 서비스에 대한 액세스가 거부됩니다.

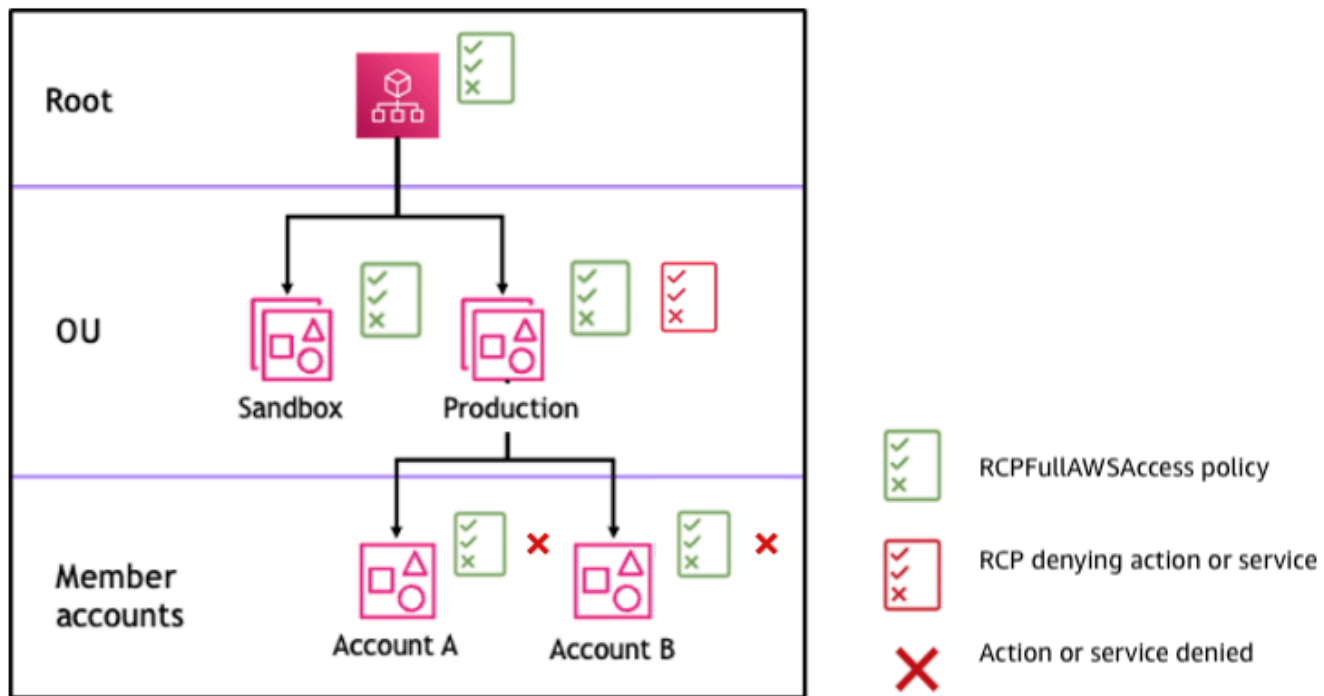


그림 1: 프로덕션 OU에 *Deny* 문이 연결된 조직 구조 예시 및 이것이 계정 A와 계정 B에 미치는 영향

RCP 구문

리소스 제어 정책(RCP)은 [리소스 기반 정책](#)에서 사용하는 구문과 유사한 구문을 사용합니다. IAM 정책과 그 구문에 대한 자세한 내용은 IAM 사용 설명서의 [IAM 정책 개요](#)를 참조하세요.

RCP는 [JSON](#) 규칙에 따라 구성됩니다. SCP는 이번 주제에서 설명하는 요소를 사용합니다.

Note

RCP 내 모든 문자는 [최대 크기](#)를 기준으로 계수됩니다. 이 설명서의 예제는 가독성을 높이기 위한 추가 공백으로 포맷된 RCP를 보여 줍니다. 하지만 정책 크기가 최대 크기에 근접한 경우 공백을 저장하려면 인용 부호 바깥에 있는 공백 문자(예: 공백 및 줄 바꿈)를 모두 삭제할 수 있습니다.

RCP에 대한 일반적인 정보는 [리소스 제어 정책\(RCP\)](#) 섹션을 참조하세요.

요소 요약

다음 표에는 RCP에서 사용할 수 있는 정책 요소가 요약되어 있습니다.

Note

Allow의 효과는 **RCPFullAWSAccess** 정책에 대해서만 지원됩니다.

Allow의 효과는 RCPFullAWSAccess 정책에 대해서만 지원됩니다. 이 정책은 리소스 제어 정책(RCP)을 활성화하면 조직 루트, 모든 OU 및 조직의 모든 계정에 자동으로 연결됩니다. 이 정책은 분리할 수 없습니다. 이 기본 RCP를 사용하면 모든 위탁자와 작업이 RCP 평가를 통과할 수 있습니다. 즉, RCP를 생성하고 연결하기 시작할 때까지는 기존 IAM 권한이 모두 그대로 작동합니다. 이것이 액세스 권한을 부여하지는 않습니다.

요소	용도
버전	정책을 처리하는 데 사용할 언어 구문 규칙을 지정합니다.
Statement	정책 요소 컨테이너의 역할을 합니다. RCP에 여러 문을 포함할 수 있습니다.
Statement ID(Sid)	(선택 사항) 문의 표시 이름을 제공합니다.
효과	RCP 문이 계정의 리소스에 대한 액세스를 거부할지 여부를 정의합니다.
보안 주체	계정 내 리소스에 대한 접근이 허용되거나 거부되는 위탁자를 지정합니다.
작업	RCP가 허용하거나 거부하는 AWS 서

요소	용도	
	비스 및 작업을 지정합니다.	
리소스	RCP가 적용되는 AWS 리소스를 지정합니다.	
NotResource	RCP에서 제외되는 AWS 리소스를 지정합니다. Resource 요소 대신 사용합니다.	
조건	문이 효력을 발휘하는 조건을 지정합니다.	

주제

- [Version 요소](#)
- [Statement 요소](#)
- [Statement ID\(Sid\) 요소](#)
- [Effect 요소](#)
- [Principal 요소](#)
- [Action 요소](#)
- [Resource 및 NotResource 요소](#)
- [Condition 요소](#)
- [지원되지 않는 요소](#)

Version 요소

모든 RCP에는 값이 **"2012-10-17"**인 Version 요소가 있어야 합니다. 이 버전 값은 IAM 권한 정책의 최신 버전과 같습니다.

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 버전](#)을 참조하세요.

Statement 요소

RCP는 하나 이상의 Statement 요소로 구성됩니다. 정책은 Statement 키워드 하나만 가질 수 있지만, 값은 ([] 문자로 구분한) JSON 문 어레이가 될 수 있습니다.

다음 예제는 하나의 Effect, Principal, Action 및 Resource 요소로 구성된 한 문을 보여줍니다.

```
{
  "Statement": {
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutBucketPublicAccessBlock",
    "Resource": "*"
  }
}
```

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 문](#)을 참조하세요.

Statement ID(Sid) 요소

Sid는 정책 문에 입력되는 식별자(옵션)입니다. Sid 값은 문 배열에서 각 문에 할당할 수 있습니다. 다음 예제 RCP는 샘플 Sid 문을 보여줍니다.

```
{
  "Statement": {
    "Sid": "DenyBPAConfigurations",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutBucketPublicAccessBlock",
    "Resource": "*"
  }
}
```

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: Sid](#)를 참조하세요.

Effect 요소

각 문에는 Effect 요소 하나가 있어야 합니다. Effect 요소의 Deny 값을 사용하여 특정 리소스에 대한 액세스를 제한하거나 RCP가 효과를 발휘하는 조건을 정의할 수 있습니다. 생성하는 RCP의 경우 값은 Deny여야 합니다. 자세한 내용은 IAM 사용 설명서의 [RCP 평가](#)과 [IAM JSON 정책 요소: Effect](#)를 참조하세요.

Principal 요소

각 문에는 Principal 요소가 있어야 합니다. RCP의 Principal 요소에서만 '*'을 지정할 수 있습니다. Conditions 요소를 사용하여 특정 위탁자 제한합니다.

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: Principal](#)를 참조하세요.

Action 요소

각 문에는 Action 요소가 있어야 합니다.

Action 요소의 값은 문에 의해 허용되거나 거부되는 AWS 서비스 및 작업을 식별하는 문자열 또는 문자열 목록(JSON 배열)입니다.

각 문자열은 서비스의 소문자 약자('s3', 'sqs' 또는 'sts' 등) 뒤에 콜론이 오고 그 뒤에 해당 서비스의 작업이 붙는 형태로 구성됩니다. 일반적으로 각 단어는 첫 글자만 대문자로, 나머지는 소문자로 입력합니다. 예를 들어 "s3:ListAllMyBuckets"입니다.

RCP에서 다음과 같이 별표(*) 또는 물음표(?)와 같은 와일드카드 문자를 사용할 수도 있습니다.

- 이름의 일부를 공유하는 여러 작업을 일치시키려면 별표(*)를 와일드카드로 사용하세요. "s3:*" 값은 Amazon S3 서비스의 모든 작업을 의미합니다. 값은 "Get"으로 시작하는 AWS STS 작업과만 "sts:Get*" 일치합니다.
- 단일 문자를 일치시키려면 물음표(?) 와일드카드를 사용하세요.

Note

와일드카드(*) 및 물음표(?)는 작업 이름의 어느 곳에서나 사용할 수 있습니다. 고객 관리형 RCP의 작업 요소에 '*'를 사용할 수 없으며 액세스를 제한하려는 서비스의 약어(예: 's3', 'sqs' 또는 'sts')를 지정해야 합니다.

RCP 지원 서비스 목록은 [RCPs AWS 서비스 지원하는 목록](#) 단원을 참조하세요. 에서 AWS 서비스 지원하는 작업 목록은 서비스 승인 참조의 [AWS 서비스에 사용되는 작업, 리소스 및 조건 키를 참조하세요](#).

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: Action](#)을 참조하세요.

Resource 및 NotResource 요소

각 문에는 Resource 또는 NotResource 요소가 있어야 합니다.

리소스 요소에서 별표(*) 또는 물음표(?)와 같은 와일드카드 문자를 사용할 수 있습니다.

- 이름의 일부를 공유하는 여러 리소스를 일치시키려면 별표(*)를 와일드카드로 사용하십시오.
- 단일 문자를 일치시키려면 물음표(?) 와일드카드를 사용하세요.

자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: Resource](#) 및 [IAM JSON 정책 요소: NotResource](#)를 참조하세요.

Condition 요소

RCP에서 거부 문에 Condition 요소를 지정할 수 있습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}
```

이 RCP는 요청이 보안 전송(TLS를 통해 전송된 요청)을 통해 이루어지지 않는 한 Amazon S3 작업 및 리소스에 대한 접근을 허용하지 않습니다.

자세한 정보는 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.

지원되지 않는 요소

다음 요소는 RCP에서 지원되지 않습니다.

- NotPrincipal

- NotAction

리소스 제어 정책 예제

이 주제에 나온 예제 [리소스 제어 정책\(RCP\)](#)은 정보 제공용입니다.

이 예제를 사용하기 전에

조직에서 이러한 예제 RCPs 사용하기 전에 다음 사항을 고려하세요.

- [리소스 제어 정책\(RCPs\)](#)은 대략적인 예방 제어로 사용하기 위한 것이며 액세스 권한을 부여하지 않습니다. 실제로 권한을 부여하려면 계정의 IAM 보안 주체 또는 리소스에 [ID 기반 또는 리소스 기반 정책을](#) 연결해야 합니다. 유효 권한은 SCP/RCP와 자격 증명 정책 또는 SCP/RCP와 리소스 정책 간의 논리적 교집합입니다. RCP가 권한에 미치는 영향에 대한 자세한 내용은 여기에서 확인할 수 [있습니다](#).
- 이 리포지토리의 리소스 제어 정책은 예제로 표시됩니다. 정책이 계정의 리소스에 미치는 영향을 철저히 테스트하지 않고 RCPs를 연결해서는 안 됩니다. 구현하려는 정책이 준비되면 프로덕션 환경을 나타낼 수 있는 별도의 조직 또는 OU에서 테스트하는 것이 좋습니다. 테스트가 완료되면 변경 사항을 배포하여 OUs를 테스트한 다음 시간이 지남에 따라 변경 사항을 더 광범위한 OUs 집합에 점진적으로 배포해야 합니다.
- 리소스 제어 정책(RCPs)을 활성화하면 [RCPFullAWSAccess](#) 정책이 조직 루트, 모든 OU 및 조직의 모든 계정에 자동으로 연결됩니다. 이 기본 RCP를 사용하면 모든 보안 주체 및 작업에 대한 액세스 권한이 RCP 평가를 통과할 수 있습니다. 거부 문을 사용하여 조직의 리소스에 대한 액세스를 제한할 수 있습니다. 또한 자격 증명 기반 또는 리소스 기반 정책을 사용하여 보안 주체에게 적절한 권한을 부여해야 합니다.
- [리소스 제어 정책\(RCP\)](#)은 조직 루트, 조직 단위 또는 계정에 연결된 경우 조직, 조직 단위 또는 계정의 리소스에 대해 사용 가능한 최대 권한을 중앙에서 제어합니다. 조직의 여러 수준에서 RCP를 적용할 수 있으므로 [RCPs가 평가되는](#) 방법을 이해하면 예상 결과를 산출하는 RCPs를 작성하는 데 도움이 될 수 있습니다.

이 단원의 정책 예제는 RCP의 구현과 사용을 보여줍니다. 그러나 제시된 그대로 실행할 수 있는 공식적인 AWS 권장 사항 또는 모범 사례로 해석해서는 안 됩니다. 고객은 자신의 환경이 가진 비즈니스 요구 사항을 해결하기 위해 모든 정책의 적합성을 신중하게 테스트할 책임이 있습니다. 거부 기반 리소스 제어 정책은 정책에 필요한 예외를 추가하지 않는 한 AWS 서비스 사용을 의도하지 않게 제한하거나 차단할 수 있습니다.

i Tip

RCPs 구현하기 전에 [AWS CloudTrail 로그](#)를 검토하는 것 외에도 [IAM Access Analyzer 외부 액세스 조사 결과](#)를 평가하면 현재 퍼블릭이거나 외부에서 공유되는 리소스를 이해하는 데 도움이 될 수 있습니다.

GitHub 리포지토리

- [리소스 제어 정책 예제](#) -이 GitHub 리포지토리에는 AWS RCPs 사용을 시작하거나 성숙시키기 위한 예제 정책이 포함되어 있습니다.

의 관리 정책 AWS Organizations

관리 정책을 사용하면 AWS 서비스 및 해당 기능을 중앙에서 구성하고 관리할 수 있습니다. 정책이 해당 정책을 상속하는 OU 및 계정에 미치는 영향은 AWS Organizations에 적용되는 관리 정책 유형에 따라 달라집니다. 이 섹션의 주제를 검토하여 관리 정책에 대한 관련 용어 및 개념을 이해하세요.

주제

- [에 대한 관리 정책의 사전 조건 및 권한 AWS Organizations](#)
- [관리 정책 상속에 대한 이해](#)
- [유효 관리 정책 보기](#)
- [잘못된 유효 정책 알림 정보](#)
- [선언적 정책](#)
- [백업 정책](#)
- [- 태그 정책](#)
- [채팅 애플리케이션 정책](#)
- [AI 서비스 옵트아웃 정책](#)
- [Security Hub 정책](#)
- [Amazon Bedrock 정책](#)
- [Amazon Inspector 정책](#)
- [롤아웃 정책 업그레이드](#)
- [Amazon S3 정책](#)
- [AWS Shield Network Security Director 정책](#)

에 대한 관리 정책의 사전 조건 및 권한 AWS Organizations

이 페이지에서는 AWS Organizations의 관리 정책에 대한 사전 조건 및 필수 권한에 대해 설명합니다.

주제

- [관리 정책의 사전 조건](#)
- [관리 정책에 대한 권한](#)

관리 정책의 사전 조건

조직에 대한 관리 정책을 사용하려면 다음이 필요합니다.

- 조직의 [모든 기능을 활성화](#)해야 합니다.
- 조직의 관리 계정에 로그인하거나 위임된 관리자여야 합니다.
- AWS Identity and Access Management (IAM) 사용자 또는 역할에는 다음 섹션에 나열된 권한이 있어야 합니다.

관리 정책에 대한 권한

다음 IAM 정책 예는 조직에서 관리 정책의 모든 측면을 사용할 수 있는 권한을 제공합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationPolicies",
      "Effect": "Allow",
      "Action": [
        "organizations:AttachPolicy",
        "organizations:CreatePolicy",
        "organizations>DeletePolicy",
        "organizations:DescribeAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
```

```

        "organizations:DescribePolicy",
        "organizations:DetachPolicy",
        "organizations:DisableAWSServiceAccess",
        "organizations:DisablePolicyType",
        "organizations:EnableAWSServiceAccess",
        "organizations:EnablePolicyType",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListCreateAccountStatus",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTargetsForPolicy",
        "organizations:UpdatePolicy"
    ],
    "Resource": "*"
}
]
}

```

IAM 정책 및 권한에 대한 자세한 내용은 [IAM 사용 설명서](#)를 참조하세요.

관리 정책 상속에 대한 이해

Important

이 섹션의 정보는 서비스 제어 정책(SCP) 및 리소스 제어 정책(RCP)과 같은 권한 부여 정책에는 적용되지 않습니다. AWS Organizations 계층 구조에서 SCPs 및 RCPs 작동하는 방식에 대한 자세한 내용은 [SCP 평가](#) 및 섹션을 참조하세요 [RCP 평가](#).

조직에 속한 조직 엔터티(조직 루트, OU(조직 단위) 또는 계정)에 관리 정책을 연결할 수 있습니다.

- 정책을 조직 루트에 연결하면 조직의 모든 OU 및 계정이 해당 정책을 상속합니다.
- 정책을 특정 OU에 연결하면 해당 OU 또는 하위 OU 바로 아래에 있는 계정이 관리 정책을 상속합니다.
- 관리 정책을 특정 계정에 연결하면 해당 계정에만 영향을 미칩니다.

조직의 여러 수준에 관리 정책을 연결할 수 있으므로 계정은 여러 정책을 상속할 수 있습니다.

다음 주제에서는 상위 정책과 하위 정책이 계정의 유효 정책으로 처리되는 방법을 설명합니다.

주제

- [상속 용어](#)
- [관리 정책 유형에 대한 정책 구문 및 상속](#)
- [상속 연산자](#)
- [상속 사례](#)

상속 용어

이 주제에서는 관리 정책 상속을 설명할 때 다음 용어를 사용합니다.

정책 상속

조직의 최상위 루트에서 OU(조직 단위) 계층 그리고 개별 계정으로 이동하며 조직의 서로 다른 수준에서 이루어지는 정책의 상호 작용입니다.

조직 루트, OU, 개별 계정 및 이러한 조직 엔터티의 조합에 정책을 연결할 수 있습니다. 관리 정책 상속은 조직 루트 또는 OU에 연결된 정책을 말합니다. 관리 정책이 연결된 조직 루트 또는 OU의 멤버인 모든 계정은 해당 정책을 상속 합니다.

예를 들어 관리 정책이 조직 루트에 연결되면 조직의 모든 계정이 해당 정책을 상속합니다. 조직의 모든 계정이 항상 조직 루트 아래에 있기 때문입니다. 정책을 특정 OU에 연결하면 해당 OU 또는 하위 OU 바로 아래에 있는 계정이 정책을 상속합니다. 조직의 여러 수준에 정책을 연결할 수 있으므로 계정은 단일 정책 유형에 대해 여러 정책 문서를 상속할 수 있습니다.

상위 정책

조직 트리에서 트리 아래쪽에 있는 엔터티에 연결된 정책보다 높은 수준에 연결된 정책입니다.

예를 들어 관리 정책 A를 조직 루트에 연결하는 경우 단지 정책일 뿐입니다. 정책 B도 해당 루트 아래 OU에 연결하는 경우 정책 A는 정책 B의 상위 정책입니다. 정책 B는 정책 A의 하위 정책입니다. 정책 A와 정책 B는 병합되어 OU의 계정에 대한 유효 태그 정책을 생성합니다.

하위 정책

조직 트리에서 상위 정책보다 하위 수준에 연결된 정책입니다.

유효 정책

계정에 적용되는 규칙을 지정하는 최종 단일 정책 문서입니다. 유효 정책은 계정이 상속하는 모든 정책과 계정에 직접 연결된 정책을 집계한 것입니다. 자세한 내용은 [유효 관리 정책 보기](#) 단원을 참조하십시오.

상속 연산자

상속된 정책이 단일 유효 정책으로 병합되는 방법을 제어하는 연산자입니다. 이러한 연산자는 고급 기능으로 간주됩니다. 숙련된 정책 작성자는 이러한 연산자를 사용하여 하위 정책이 변경할 수 있는 내용과 정책의 설정이 병합되는 방법을 제한할 수 있습니다. 자세한 내용은 [상속 연산자](#) 단원을 참조하십시오.

관리 정책 유형에 대한 정책 구문 및 상속

정책이 해당 정책을 상속하는 OU 및 계정에 미치는 영향은 선택한 관리 정책 유형에 따라 달라집니다. 관리 정책 유형은 다음과 같습니다.

- [선언적 정책](#)
- [백업 정책](#)
- [- 태그 정책](#)
- [채팅 애플리케이션 정책](#)
- [AI 서비스 옵트아웃 정책](#)
- [Security Hub 정책](#)
- [Bedrock 정책](#)
- [검사기 정책](#)
- [롤아웃 정책 업그레이드](#)
- [S3 정책](#)
- [AWS Shield Network Security Director 정책](#)

관리 정책 유형의 구문에는 [상속 연산자](#)이(가) 포함되어 있습니다. 이 연산자를 사용하면 상위 정책의 어떤 요소가 적용되는지, 그리고 요소가 하위 OU 및 계정에 의해 상속될 때 어떤 요소가 무시되거나 수정될 수 있는지 세밀하게 지정할 수 있습니다.

유효 정책은 조직 루트 및 OU에서 상속되는 규칙과 계정에 직접 연결된 규칙의 집합입니다. 유효 정책은 계정에 적용되는 최종 규칙 집합을 지정합니다. 적용되는 정책의 모든 상속 연산자가 미치는 영향을 포함한 계정의 유효 정책을 볼 수 있습니다. 자세한 내용은 [유효 관리 정책 보기](#) 단원을 참조하십시오.

상속 연산자

상속 연산자는 상속된 정책과 계정 정책이 계정의 유효 정책으로 병합되는 방법을 제어합니다. 이러한 연산자에는 값 설정 연산자와 하위 제어 연산자가 포함됩니다.

AWS Organizations 콘솔에서 시각적 편집기를 사용하는 경우 `@@assign` 연산자만 사용할 수 있습니다. 기타 연산자는 고급 기능으로 간주됩니다. 기타 연산자를 사용하려면 JSON 정책을 수동으로 작성해야 합니다. 숙련된 정책 작성자는 상속 연산자를 사용하여 유효 정책에 적용되는 값을 제어하고 하위 정책에 따라 변경할 수 있는 내용을 제한할 수 있습니다.

조직에서 정책 상속이 작동하는 방식에 대한 자세한 내용은 [상속 사례](#) 섹션을 참조하세요.

값 설정 연산자

다음 값 설정 연산자를 사용하여 정책이 상위 정책과 상호 작용하는 방식을 제어할 수 있습니다.

- `@@assign` – 상속된 정책 설정을 지정된 설정으로 덮어씁니다. 지정된 설정이 상속되지 않은 경우 이 연산자는 해당 설정을 유효 정책에 추가합니다. 이 연산자는 모든 유형의 정책 설정에 적용할 수 있습니다.
 - 단일 값 설정의 경우 이 연산자는 상속된 값을 지정된 값으로 바꿉니다.
 - 다중 값 설정(JSON 배열)의 경우 이 연산자는 상속된 값을 모두 제거하고 이 정책에 지정된 값으로 바꿉니다.
- `@@append` – 지정된 설정을 제거하지 않고 상속된 설정에 추가합니다. 지정된 설정이 상속되지 않은 경우 이 연산자는 해당 설정을 유효 정책에 추가합니다. 이 연산자는 다중 값 설정에서만 사용할 수 있습니다.
 - 이 연산자는 상속된 배열의 값에 지정된 값을 추가합니다.
- `@@remove` – 상속된 지정된 설정(있는 경우)을 유효 정책에서 제거합니다. 이 연산자는 다중 값 설정에서만 사용할 수 있습니다.
 - 이 연산자는 상위 정책에서 상속된 값 배열에서 지정된 값만 제거합니다. 다른 값은 배열에 계속 존재할 수 있으며 하위 정책이 상속할 수 있습니다.

하위 제어 연산자

하위 제어 연산자를 사용하는 것은 선택 사항입니다.

`@@operators_allowed_for_child_policies` 연산자를 사용하여 하위 정책에서 사용할 수 있는 값 설정 연산자를 제어할 수 있습니다. 모든 연산자를 허용하거나, 일부 특정 연산자를 허용하거나, 연산자를 허용하지 않을 수 있습니다. 기본적으로 모든 연산자(`@@all`)가 허용됩니다.

- `"@operators_allowed_for_child_policies":["@all"]` – 하위 OU와 계정은 정책에서 어떤 연산자든지 사용할 수 있습니다. 기본적으로 모든 연산자가 하위 정책에서 허용됩니다.
- `"@operators_allowed_for_child_policies":["@assign", "@append", "@remove"]` – 하위 OU 및 계정은 하위 정책에서 지정된 연산자만 사용할 수 있습니다. 이 하위 제어 연산자에서 값 설정 연산자를 하나 이상 지정할 수 있습니다.
- `"@operators_allowed_for_child_policies":["@none"]` – 하위 OU와 계정은 정책에서 연산자를 사용할 수 없습니다. 이 연산자를 사용하여 하위 정책에서 해당 값을 추가, 첨부 또는 제거할 수 없도록 상위 정책에서 정의된 값을 효과적으로 잠글 수 있습니다.

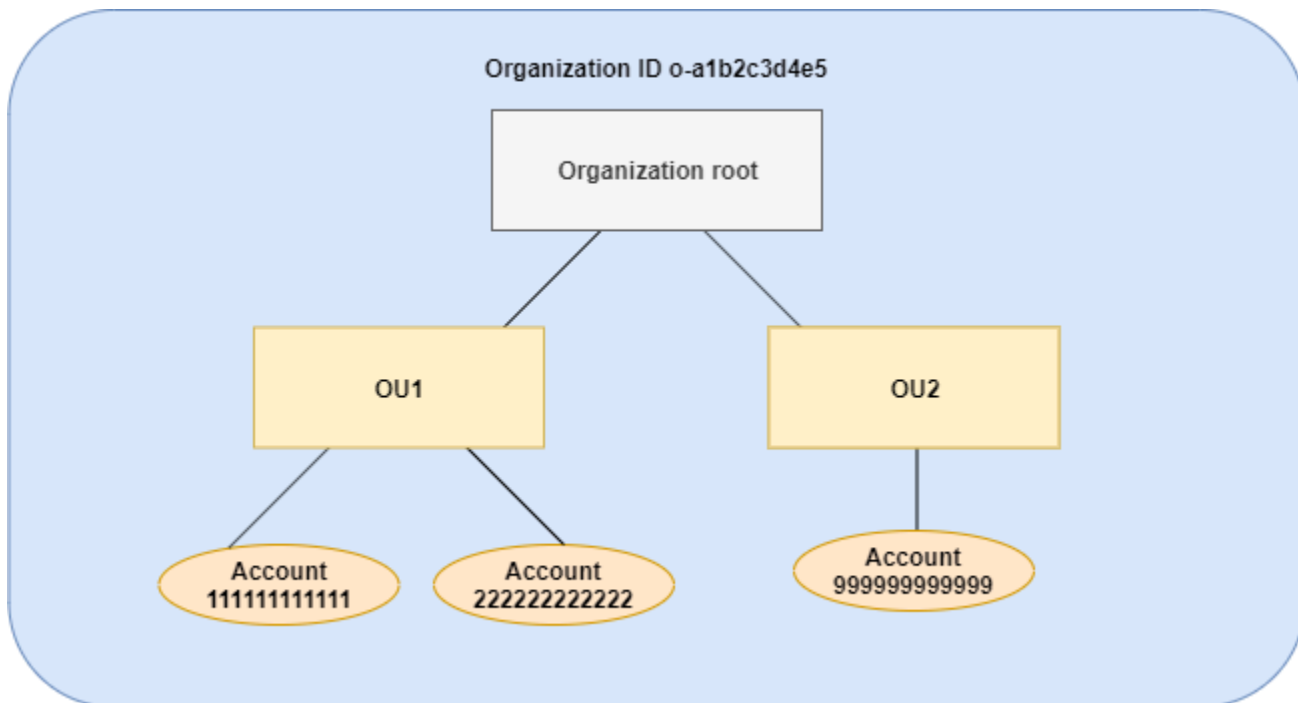
Note

상속된 하위 제어 연산자가 연산자 사용을 제한하는 경우 하위 정책에서 해당 규칙을 되돌릴 수 없습니다. 상위 정책에 하위 제어 연산자를 포함하면 이러한 연산자는 모든 하위 정책에서 값 설정 연산자를 제한합니다.

상속 사례

다음 예제에서는 상위 및 하위 태그 정책이 계정의 유효 태그 정책으로 병합되는 과정을 설명하여 정책 상속이 작동하는 방식을 보여 줍니다.

이 예에서는 다음 다이어그램에 표시된 조직 구조가 있다고 가정합니다.



예제

- [예제 1: 하위 정책이 태그 값만 덮어쓰도록 허용](#)
- [예제 2: 상속된 태그에 새 값 추가](#)
- [예제 3: 상속된 태그에서 값 제거](#)
- [예제 4: 하위 정책의 변경 제한](#)
- [예제 5: 하위 제어 연산자와 충돌](#)
- [예제 6: 동일한 계층 수준에서 값 추가와 충돌](#)

예제 1: 하위 정책이 태그 값만 덮어쓰도록 허용

다음 태그 정책은 CostCenter 태그 키와 허용 가능한 두 값 Development 및 Support를 정의합니다. 이 태그 정책을 조직 루트에 연결하면 태그 정책은 조직의 모든 계정에 적용됩니다.

정책 A - 조직 루트 태그 정책

```
{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "Development",
          "Support"
        ]
      }
    }
  }
}
```

OU1의 사용자가 키에 다른 태그 값을 사용하도록 하고 특정 리소스 유형에 대해 해당 태그 정책을 적용하려고 한다고 가정합니다. 정책 A는 어떤 하위 제어 연산자가 허용되는지를 지정하지 않으므로 모든 연산자가 허용됩니다. @@assign 연산자를 사용하고 다음과 같은 태그 정책을 생성하여 OU1에 연결할 수 있습니다.

정책 B - OU1 태그 정책

```
{
```

```

    "tags": {
      "costcenter": {
        "tag_key": {
          "@@assign": "CostCenter"
        },
        "tag_value": {
          "@@assign": [
            "Sandbox"
          ]
        },
        "enforced_for": {
          "@@assign": [
            "redshift:*",
            "dynamodb:table"
          ]
        }
      }
    }
  }
}

```

태그에 대해 @@assign 연산자를 지정하면 정책 A와 정책 B가 병합되어 계정의 유효 태그 정책을 형성할 때 다음이 수행됩니다.

- 정책 B는 상위 정책에서 지정된 두 개의 태그 값을 덮어씁니다. 따라서 Sandbox는 CostCenter 태그 키의 유일한 정책 준수 값입니다.
- enforced_for를 추가하면 CostCenter 태그가 모든 Amazon Redshift 리소스와 Amazon DynamoDB 테이블에서 지정된 태그 값을 사용해야 합니다.

그림과 같이 OU1에는 111111111111 및 222222222222라는 두 개의 계정이 포함되어 있습니다.

계정 111111111111 및 222222222222에 대해 생성된 유효 태그 정책

Note

표시된 유효 정책의 내용을 새 정책의 내용으로 직접 사용할 수는 없습니다. 구문에는 다른 하위 및 상위 정책과의 병합을 제어하는 데 필요한 연산자가 포함되지 않습니다. 유효 정책을 표시하는 이유는 오직 병합 결과의 이해를 돕기 위한 것입니다.

```
{
```

```

    "tags": {
      "costcenter": {
        "tag_key": "CostCenter",
        "tag_value": [
          "Sandbox"
        ],
        "enforced_for": [
          "redshift:*",
          "dynamodb:table"
        ]
      }
    }
  }
}

```

예제 2: 상속된 태그에 새 값 추가

조직의 모든 계정에서 허용 가능한 값의 짧은 목록이 있는 태그 키를 지정하려는 경우가 있을 수 있습니다. 한 OU에 있는 계정의 경우 리소스를 생성할 때 해당 계정만 지정할 수 있는 추가 값을 허용하려고 할 수 있습니다. 이 예제에서는 @@append 연산자를 사용하여 이 작업을 수행하는 방법을 설명합니다. @@append 연산자는 고급 기능입니다.

예제 1과 마찬가지로, 이 예제는 조직 루트 태그 정책에 대한 정책 A로 시작합니다.

정책 A - 조직 루트 태그 정책

```

{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "Development",
          "Support"
        ]
      }
    }
  }
}

```

이 예제에서는 정책 C를 OU2에 연결합니다. 이 예제의 차이점은 정책 C에서 @@append 연산자를 사용할 경우 허용 값 목록과 enforced_for 규칙을 덮어쓰지 않고 해당 항목에 추가한다는 것입니다.

정책 C - 값을 추가하기 위한 OU2 태그 정책

```
{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@append": [
          "Marketing"
        ]
      },
      "enforced_for": {
        "@@append": [
          "redshift:*",
          "dynamodb:table"
        ]
      }
    }
  }
}
```

정책 C를 OU2에 연결하면 정책 A와 정책 C가 병합되어 계정의 유효 태그 정책을 형성할 때 다음과 같은 효과가 발생합니다.

- 정책 C에는 @@append 연산자가 포함되어 있으므로 이 정책은 정책 A에서 지정된 허용 가능한 태그 값의 목록을 덮어쓰지 않고 이 목록에 값을 추가하도록 허용 합니다.
- 정책 B와 같이, enforced_for를 추가하면 CostCenter 태그가 모든 Amazon Redshift 리소스와 Amazon DynamoDB 테이블에서 지정된 태그 값으로 사용되어야 합니다. 상위 정책에 하위 정책이 지정할 수 있는 항목을 제한하는 하위 제어 연산자가 포함되지 않으면 덮어쓰기(@@assign)와 추가(@@append)는 동일한 효과를 나타냅니다.

다이어그램과 같이 OU2에는 999999999999라는 계정 하나가 포함되어 있습니다. 정책 A와 정책 C가 병합되어 계정 999999999999에 대한 유효 태그 정책을 생성합니다.

계정 999999999999에 대한 유효 태그 정책

Note

표시된 유효 정책의 내용을 새 정책의 내용으로 직접 사용할 수는 없습니다. 구문에는 다른 하위 및 상위 정책과의 병합을 제어하는 데 필요한 연산자가 포함되지 않습니다. 유효 정책을 표시하는 이유는 오직 병합 결과의 이해를 돕기 위한 것입니다.

```
{
  "tags": {
    "costcenter": {
      "tag_key": "CostCenter",
      "tag_value": [
        "Development",
        "Support",
        "Marketing"
      ],
      "enforced_for": [
        "redshift:*",
        "dynamodb:table"
      ]
    }
  }
}
```

예제 3: 상속된 태그에서 값 제거

조직에 연결된 태그 정책이 계정에서 사용하려는 것보다 더 많은 태그 값을 정의하는 경우가 있을 수 있습니다. 이 예에서는 @@remove 연산자를 사용하여 태그 정책을 수정하는 방법을 설명합니다. @@remove는 고급 기능입니다.

다른 예제와 마찬가지로, 이 예제는 조직 루트 태그 정책에 대한 정책 A로 시작합니다.

정책 A - 조직 루트 태그 정책

```
{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
```

```

        "@@assign": [
            "Development",
            "Support"
        ]
    }
}
}
}

```

이 예제에서는 계정 999999999999에 정책 D를 연결합니다.

정책 D - 값을 제거하는 계정 999999999999 태그 정책

```

{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@remove": [
          "Development",
          "Marketing"
        ],
        "enforced_for": {
          "@@remove": [
            "redshift:*",
            "dynamodb:table"
          ]
        }
      }
    }
  }
}
}
}

```

정책 D를 계정 999999999999에 연결하면 정책 A, 정책 C 및 정책 D가 병합되어 유효 태그 정책을 형성할 때 다음과 같은 효과가 발생합니다.

- 이전의 예제를 모두 수행했다고 가정하면 정책 B, C 및 C는 A의 하위 정책입니다. 정책 B는 OU1에만 연결되므로 계정 999999999999에 영향을 미치지 않습니다.
- 계정 999999999999의 경우 CostCenter 태그 키에 허용 가능한 유일한 값은 Support입니다.
- 정책 준수는 CostCenter 태그 키에 적용되지 않습니다.

계정 999999999999에 대한 새로운 유효 태그 정책

Note

표시된 유효 정책의 내용을 새 정책의 내용으로 직접 사용할 수는 없습니다. 구문에는 다른 하위 및 상위 정책과의 병합을 제어하는 데 필요한 연산자가 포함되지 않습니다. 유효 정책을 표시하는 이유는 오직 병합 결과의 이해를 돕기 위한 것입니다.

```
{
  "tags": {
    "costcenter": {
      "tag_key": "CostCenter",
      "tag_value": [
        "Support"
      ]
    }
  }
}
```

나중에 OU2에 계정을 더 추가하는 경우 해당 계정의 유효 태그 정책은 계정 999999999999와 다릅니다. 더 제한적인 정책 D는 계정 수준에서만 연결되고 OU에는 연결되지 않기 때문입니다.

예제 4: 하위 정책의 변경 제한

하위 정책의 변경을 제한하려는 경우가 있을 수 있습니다. 이 예제에서는 하위 제어 연산자를 사용하여 이 작업을 수행하는 방법에 대해 설명합니다.

이 예제에서는 새 조직 루트 태그 정책으로 시작하며 태그 정책이 조직 엔터티에 아직 연결되어 있지 않다고 가정합니다.

정책 E - 하위 정책의 변경을 제한하는 조직 루트 태그 정책

```
{
  "tags": {
    "project": {
      "tag_key": {
        "@operators_allowed_for_child_policies": ["@none"],
        "@assign": "Project"
      },
      "tag_value": {
```

```

        "@operators_allowed_for_child_policies": ["@append"],
        "@assign": [
            "Maintenance",
            "Escalations"
        ]
    }
}
}
}

```

조직 루트에 정책 E를 연결하면 하위 정책이 Project 태그 키를 변경할 수 없습니다. 하지만 하위 정책은 태그 값을 덮어쓰거나 추가할 수 있습니다.

그런 다음 OU에 다음과 같은 정책 F를 연결한다고 가정합니다.

정책 F - OU 태그 정책

```

{
  "tags": {
    "project": {
      "tag_key": {
        "@assign": "PROJECT"
      },
      "tag_value": {
        "@append": [
          "Escalations - research"
        ]
      }
    }
  }
}

```

정책 E와 정책 F를 병합하면 OU의 계정에 다음과 같은 영향을 미칩니다.

- 정책 F는 정책 E의 하위 정책입니다.
- 정책 F는 사례 처리를 변경하려고 시도하지만 그렇게 할 수 없습니다. 정책 E에는 태그 키에 대한 "@operators_allowed_for_child_policies": ["@none"] 연산자가 포함되어 있기 때문입니다.
- 하지만 정책 F는 키의 태그 값을 추가할 수 있습니다. 정책 E에는 태그 값에 대한 "@operators_allowed_for_child_policies": ["@append"]가 포함되어 있기 때문입니다.

OU의 계정에 대한 유효 정책

Note

표시된 유효 정책의 내용을 새 정책의 내용으로 직접 사용할 수는 없습니다. 구문에는 다른 하위 및 상위 정책과의 병합을 제어하는 데 필요한 연산자가 포함되지 않습니다. 유효 정책을 표시하는 이유는 오직 병합 결과의 이해를 돕기 위한 것입니다.

```
{
  "tags": {
    "project": {
      "tag_key": "Project",
      "tag_value": [
        "Maintenance",
        "Escalations",
        "Escalations - research"
      ]
    }
  }
}
```

예제 5: 하위 제어 연산자와 충돌

하위 제어 연산자는 조직 계층의 동일한 수준에서 연결된 태그 정책에 존재할 수 있습니다. 이러한 경우 정책이 병합되어 계정의 유효 정책을 형성할 때 허용된 연산자의 교집합이 사용됩니다.

정책 G와 정책 H가 조직 루트에 연결되어 있다고 가정합니다.

정책 G - 조직 루트 태그 정책 1

```
{
  "tags": {
    "project": {
      "tag_value": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "@@assign": [
          "Maintenance"
        ]
      }
    }
  }
}
```

```
}

```

정책 H - 조직 루트 태그 정책 2

```
{
  "tags": {
    "project": {
      "tag_value": {
        "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
      }
    }
  }
}
```

이 예제에서 조직 루트에 있는 한 정책은 태그 키의 값을 추가만 할 수 있도록 정의합니다. 조직 루트에 연결된 다른 정책은 하위 정책이 값을 추가하고 제거할 수 있도록 허용합니다. 이러한 두 가지 권한의 교집합이 하위 정책에 사용됩니다. 결과적으로 하위 정책은 값을 추가할 수 있지만 값을 제거할 수 없습니다. 따라서 하위 정책은 태그 값 목록에 값을 추가할 수 있지만 Maintenance 값을 제거할 수 없습니다.

예제 6: 동일한 계층 수준에서 값 추가와 충돌

각 조직 엔터티에 여러 태그 정책을 연결할 수 있습니다. 이렇게 하면 동일한 조직 엔터티에 연결된 태그 정책에 충돌하는 정보가 포함될 수 있습니다. 정책은 조직 엔터티에 연결된 순서를 기준으로 평가됩니다. 어떤 정책이 먼저 평가되는지를 변경하려면 정책을 분리한 다음 다시 연결하면 됩니다.

정책 J가 조직 루트에 먼저 연결된 다음, 정책 K가 조직 루트에 연결된다고 가정합니다.

정책 J - 조직 루트에 연결된 첫 번째 태그 정책

```
{
  "tags": {
    "project": {
      "tag_key": {
        "@@assign": "PROJECT"
      },
      "tag_value": {
        "@@append": ["Maintenance"]
      }
    }
  }
}
```

정책 K - 조직 루트에 연결된 두 번째 태그 정책

```
{
  "tags": {
    "project": {
      "tag_key": {
        "@@assign": "project"
      }
    }
  }
}
```

이 예제에서는 태그 키를 정의한 정책이 조직 루트에 먼저 연결되었기 때문에 유효 태그 정책에서 태그 키 PROJECT가 사용됩니다.

정책 JK - 계정의 유효 태그 정책

계정의 유효 정책은 다음과 같습니다.

Note

표시된 유효 정책의 내용을 새 정책의 내용으로 직접 사용할 수는 없습니다. 구문에는 다른 하위 및 상위 정책과의 병합을 제어하는 데 필요한 연산자가 포함되지 않습니다. 유효 정책을 표시하는 이유는 오직 병합 결과의 이해를 돕기 위한 것입니다.

```
{
  "tags": {
    "project": {
      "tag_key": "PROJECT",
      "tag_value": [
        "Maintenance"
      ]
    }
  }
}
```

유효 관리 정책 보기

조직의 계정에 대한 유효 관리 정책을 결정합니다.

효과적인 관리 정책이란 무엇인가요?

유효 정책은 관리 정책 유형에 대해 AWS 계정에 적용되는 최종 규칙을 지정합니다. 이는 계정이 상속하는 모든 관리 정책과 계정에 직접 연결된 관리 정책을 집계한 것입니다. 관리 정책을 조직 루트에 연결하면 해당 정책은 조직의 모든 계정에 적용됩니다. 태관리 그 정책을 조직 단위(OU)에 연결하면 해당 정책은 OU에 속한 모든 계정 및 OU에 적용됩니다. 관리 정책을 계정에 직접 연결하면 해당 계정에만 적용됩니다 AWS 계정.

AI 서비스 옵트아웃 정책이 최종 유효 정책으로 결합되는 방식에 대한 자세한 내용은 [관리 정책 상속에 대한 이해](#) 단원을 참조하세요.

백업 정책 예제

조직 루트에 연결된 백업 정책은 조직의 모든 계정이 기본 백업 빈도인 일주일에 한 번씩 모든 Amazon DynamoDB 테이블을 백업하도록 지정할 수 있습니다. 테이블에 중요한 정보가 있는 한 멤버 계정에 직접 연결된 별도의 백업 정책은 하루에 한 번으로 빈도를 재정의할 수 있습니다. 이러한 백업 정책의 조합이 유효 백업 정책을 구성합니다. 이 유효 백업 정책은 조직의 각 계정에 대해 개별적으로 결정됩니다. 이 예제를 실행하면 결과적으로 DynamoDB 테이블을 매일 백업하는 한 계정을 제외하고 조직의 모든 계정이 일주일에 한 번씩 테이블을 백업합니다.

태그 정책 예제

조직 루트에 연결된 태그 정책은 4개의 정책 준수 값이 있는 CostCenter 태그를 정의할 수 있습니다. 계정에 연결된 별도의 태그 정책은 CostCenter 키를 4개의 정책 준수 값 중 두 개로만 제한할 수 있습니다. 이러한 태그 정책의 조합으로 유효 태그 정책이 구성됩니다. 결과적으로 조직 루트 태그 정책에 정의된 4개의 정책 준수 태그 값 중 두 개만 계정에 대해 호환됩니다.

채팅 애플리케이션 정책 예제

채팅 애플리케이션의 Amazon Q Developer는 기존에 생성된 모든 채팅 애플리케이션의 Amazon Q Developer 구성 설정을 유효한 채팅 애플리케이션 정책에 따라 재평가하며, 이전에 허용되었던 작업이 유효 정책의 허용된 설정 및 가드레일과 일치하는 경우 이를 거부합니다. 멤버 계정에 대한 유효 정책은 허용되는 설정 및 가드레일을 정의합니다. 예를 들어 퍼블릭 Slack 채널에 대한 액세스 거부가 포함된 채팅 애플리케이션 정책이 멤버 계정에 적용되는 경우 멤버 계정의 퍼블릭 Slack 채널에 대한 기존 채팅 애플리케이션의 Amazon Q Developer 구성이 비활성화됩니다. 채팅 애플리케이션의 Amazon Q Developer는 알림을 전송하지 않으며 채널 멤버는 차단된 채널에서 태스크를 실행할 수 없습니다. 채팅 애플리케이션의 Amazon Q Developer 콘솔은 영향을 받는 채널을 비활성화된 것으로 표시하고 옆에 적절한 오류 메시지를 표시합니다.

AI 서비스 옵트아웃 예제

조직 루트에 연결된 AI 서비스 옵트아웃 정책은 조직의 모든 계정이 모든 AWS 기계 학습 서비스에서 콘텐츠를 사용하지 않도록 지정할 수 있습니다. 여기서, 한 멤버 계정에 직접 연결된 개별적 AI 서비스 옵트아웃 정책이 Amazon Rekognition에 대해서만 콘텐츠 사용을 옵트인하도록 지정되어 있습니다. 이 AI 서비스 옵트아웃 정책들의 조합이 유효 AI 서비스 옵트아웃 정책을 구성하고 있습니다. 결과적으로 Amazon Rekognition에 옵트인하는 계정 하나를 AWS 서비스제외하고 조직의 모든 계정이 모두 옵트아웃됩니다.

유효 관리 정책을 보는 방법

, AWS Management Console AWS API 또는에서 계정에 대한 관리 정책 유형의 유효 정책을 볼 수 있습니다 AWS Command Line Interface.

최소 권한

계정에 대한 관리 정책 유형의 유효 정책을 보려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

계정에 대한 관리 정책 유형의 유효 정책을 보려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 유효 정책을 보려는 계정의 이름을 선택합니다. 원하는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 정책 탭에서 유효한 정책을 보려는 관리 정책 유형을 선택합니다.
4. 이 AWS 계정에 대한 유효 정책 보기를 선택합니다.

지정한 계정에 적용되는 유효 정책이 콘솔에 표시됩니다.

Note

중요한 변경 없이 유효 정책을 복사하여 붙여넣은 후 다른 정책의 JSON으로 사용할 수는 없습니다. 정책 문서에는 각 설정이 최종 유효 정책으로 병합되는 방법을 지정하는 [상속 연산자](#)가 포함되어야 합니다.

AWS CLI & AWS SDKs

계정에 대한 관리 정책 유형의 유효 정책을 보려면

다음 중 하나를 사용하여 유효 정책을 볼 수 있습니다.

- AWS CLI: [describe-effective-policy](#)

다음 예제에서는 계정에 대한 유효 AI 서비스 옵트아웃 정책을 보여 줍니다.

```
$ aws organizations describe-effective-policy \
  --policy-type AISERVICES_OPT_OUT_POLICY \
  --target-id 123456789012
{
  "EffectivePolicy": {
    "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":\
    \"optOut\"}}, ....TRUNCATED FOR BREVITY.... \"opt_out_policy\":{\"optIn\"}}}\",
    "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
    "TargetId": "123456789012",
    "PolicyType": "AISERVICES_OPT_OUT_POLICY"
  }
}
```

- AWS SDKs [DescribeEffectivePolicy](#)

유효 정책이 무효화될 수 있는 상황에 대한 자세한 내용은 [잘못된 정책 알림 보기](#)를 참조하세요.

잘못된 유효 정책 알림 정보

정책 알림이 잘못되면 잘못된 유효 정책에 대해 알리고 정책이 잘못된 계정을 식별하는 메커니즘(APIs)을 제공합니다. 계정 중 하나에 잘못된 유효 정책이 있는 경우 비동기적으로 AWS Organizations 알림이 발생합니다. 알림은 AWS Organizations 콘솔 페이지에 배너로 표시되며 이벤트로 AWS CloudTrail 기록됩니다.

조직에서 잘못된 유효 관리 정책 감지

조직에서 잘못된 유효 관리 정책을 볼 수 있는 방법에는 AWS 관리 콘솔, AWS API, AWS 명령줄 인터페이스(CLI) 또는 AWS CloudTrail 이벤트와 같은 여러 가지가 있습니다.

최소 권한

조직 내 관리 정책 유형의 잘못된 유효 정책과 관련된 정보를 찾으려면 다음 작업을 실행할 권한이 있어야 합니다.

- `organizations:ListAccountsWithInvalidEffectivePolicy`
- `organizations:ListEffectivePolicyValidationErrors`
- `organizations:ListRoots` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

콘솔에서 잘못된 유효 관리 정책 보기

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 조직에 잘못된 유효 정책이 있는 경우 페이지 상단에 경고 배너가 표시됩니다.
3. 배너에서 감지된 문제 보기를 클릭하여 잘못된 유효 정책이 있는 조직의 모든 계정 목록을 봅니다.
4. 목록의 각 계정에 대해 문제 보기를 선택하여 이 페이지의 유효 정책 문제 섹션에 표시된 각 계정의 자세한 오류 정보를 가져옵니다.

AWS CLI & AWS SDKs

계정에 대한 관리 정책 유형의 유효 정책을 보려면

다음 명령은 유효하지 않은 유효 정책이 있는 계정을 보는 데 도움이 됩니다.

- AWS CLI: [list-accounts-with-invalid-effective-policy](#)
- AWS SDKs: [ListAccountsWithInvalidEffectivePolicy](#)

다음 명령은 계정의 유효 정책 오류를 보는 데 도움이 됩니다

- AWS CLI: [list-effective-policy-validation-errors](#)
- AWS SDKs: [ListEffectivePolicyValidationErrors](#)

AWS CloudTrail

AWS CloudTrail 이벤트를 사용하여 조직의 계정에 잘못된 유효 관리 정책이 있는 경우와 정책이 수정되는 경우를 모니터링할 수 있습니다. 자세한 내용은 [AWS Organizations 로그 파일 항목 이해](#)의 효과적인 정책 예제를 참조하세요.

유효하지 않은 유효 정책 알림을 받은 경우 AWS Organizations 콘솔을 탐색하거나 관리 또는 위임된 관리자 계정에서 이러한 APIs를 호출하여 특정 계정 및 정책의 상태에 대한 자세한 내용을 찾을 수 있습니다.

- `ListAccountsWithInvalidEffectivePolicy` – 지정된 유형의 잘못된 유효 정책이 있는 조직의 계정 목록을 반환합니다.
- `ListEffectivePolicyValidationErrors` – 지정된 계정 및 관리 정책 유형에 대한 검증 오류 목록을 반환합니다. 검증 오류에는 오류 코드, 오류 설명, 유효 정책을 무효화한 기여 정책을 포함한 세부 정보가 포함됩니다.

유효 관리 정책이 잘못된 것으로 간주될 수 있는 경우

특정 정책 유형에 대해 정의된 제약 조건을 위반하면 계정에 대한 유효 정책이 무효화될 수 있습니다. 예를 들어 정책에 최종 유효 정책의 필수 파라미터가 없거나 정책 유형에 정의된 특정 할당량을 초과할 수 있습니다.

백업 정책 예제

9개의 백업 규칙이 포함된 백업 정책을 생성하여 조직의 루트에 연결한다고 가정해 보겠습니다. 나중에 두 개의 추가 규칙을 사용하여 동일한 백업 계획에 대한 다른 백업 정책을 생성하고 조직의 모든 계정에 연결합니다. 이 경우 계정에 잘못된 유효 정책이 있습니다. 두 정책의 집계가 백업 계획에 대한 11개의 규칙을 정의하므로 유효하지 않습니다. 계획의 백업 규칙은 10개로 제한됩니다.

⚠ Warning

조직의 계정에 잘못된 유효 정책이 있는 경우 해당 계정은 특정 정책 유형에 대한 유효 정책 업데이트를 받지 않습니다. 모든 오류가 수정되지 않는 한 계정에 마지막으로 적용된 유효한 정책으로 계속됩니다.

유효 정책에 발생할 수 있는 오류의 예

- **ELEMENTS_T00_MANY** – 백업 계획에 10개 이상의 규칙이 주어지는 경우와 같이 유효 정책의 특정 속성이 허용 한도를 초과할 때 발생합니다.
- **ELEMENTS_T00_FEW** – 백업 계획에 정의된 리전이 없는 경우와 같이 유효 정책의 특정 속성이 최소 제한을 충족하지 않는 경우에 발생합니다.
- **KEY_REQUIRED** – 백업 계획에 백업 규칙이 누락된 경우와 같이 유효 정책에서 필수 구성이 누락된 경우에 발생합니다.

AWS Organizations 는 조직의 계정에 적용하기 전에 유효 정책을 검증합니다. 이 감사 프로세스는 조직 구조가 크고 조직의 정책을 둘 이상의 팀에서 관리하는 경우에 특히 유용합니다.

선언적 정책

선언적 정책을 사용하면 조직 전체에서 지정된에 대해 원하는 구성을 중앙 AWS 서비스 에서 선언하고 적용할 수 있습니다. 연결되면 서비스가 새 기능 또는 API를 추가할 때 구성이 항상 유지됩니다. 선언적 정책을 사용하여 규정 미준수 작업을 방지합니다. 예를 들어 조직 전체에서 Amazon VPC 리소스에 대한 퍼블릭 인터넷 액세스를 차단할 수 있습니다.

선언적 정책 사용의 주요 이점은 다음과 같습니다.

- **사용 편의성:** AWS Organizations 및 AWS Control Tower 콘솔에서 AWS 서비스 몇 가지를 선택하거나 AWS CLI & AWS SDKs.
- **한 번 설정하고 잊어버림:** 서비스에 새 기능 또는 APIs가 도입되더라도의 기존 구성 AWS 서비스 은 항상 유지됩니다. 새 계정이 조직에 추가되거나 새 위탁자 및 리소스가 생성될 때도 기존 구성이 유지됩니다.
- **투명성:** 계정 상태 보고서를 사용하여 범위 내 계정에 대한 선언적 정책에서 지원하는 모든 속성의 현재 상태를 평가할 수 있습니다. 또한 사용자 지정 가능한 오류 메시지를 생성하여 관리자가 최종 사용자를 내부 Wiki 페이지로 리디렉션하거나 최종 사용자에게 작업이 실패한 이유를 이해하는 데 도움이 되는 설명 메시지를 제공할 수 있습니다.

지원되는 AWS 서비스 및 속성의 전체 목록은 [섹션을 참조하세요](#) [지원되는 AWS 서비스 및 속성](#).

주제

- [선언적 정책 작동 방식](#)
- [선언적 정책에 대한 사용자 지정 오류 메시지](#)
- [선언적 정책에 대한 계정 상태 보고서](#)
- [지원되는 AWS 서비스 및 속성](#)
- [선언적 정책 시작하기](#)
- [선언적 정책 사용에 대한 모범 사례](#)
- [선언적 정책에 대한 계정 상태 보고서 생성](#)
- [선언적 정책 구문 및 예시](#)

선언적 정책 작동 방식

선언적 정책은 서비스의 컨트롤 플레인에서 적용되며, 이는 [서비스 제어 정책\(SCP\) 및 리소스 제어 정책\(RCP\)과 같은 권한 부여 정책과 중요한 차이점입니다](#). 권한 부여 정책은 API에 대한 액세스를 규제하지만 선언적 정책은 서비스 수준에서 직접 적용되어 지속적인 의도를 강제합니다. 이렇게 하면 서비스에 새 기능 또는 API가 도입되더라도 기존 구성이 항상 적용됩니다.

다음 표는 이러한 차이를 설명하고 몇 가지 사용 사례를 제공합니다.

	서비스 제어 정책	리소스 제어 정책	선언적 정책		
이유?	위탁자(예: IAM 사용자 및 IAM 역할)에 대한 일관된 액세스 제어를 대규모로 중앙에서 정의하고 적용합니다.	대규모 리소스에 대한 일관된 액세스 제어를 중앙에서 정의하고 적용하는 방법	대규모 AWS 서비스에 대한 기존 구성을 중앙에서 정의하고 적용합니다.		
방법?	API 수준에서 위탁자의 사	API 수준에서 리소스의 사	API 작업을 사용하지 AWS		

	서비스 제어 정책	리소스 제어 정책	선언적 정책		
	용 가능한 최대 액세스 권한을 제어합니다.	용 가능한 최대 액세스 권한을 제어합니다.	서비스 않고 의 원하는 구성을 적용합니다.		
서비스 연결 역할을 관리 하나요?	아니요	아니요	예		
피드백 메커니즘	사용자 지정할 수 없는 액세스가 SCP 오류를 거부했습니다.	사용자 지정할 수 없는 액세스가 RCP 오류를 거부했습니다.	사용자 지정 가능한 오류 메시지입니다. 자세한 내용은 선언적 정책에 대한 사용자 지정 오류 메시지 단원을 참조하십시오.		
예제 정책	멤버 계정의 조직 탈퇴 거부	리소스에 대한 HTTPS 연결에만 대한 액세스 제한	허용된 이미지 설정		

선언적 정책을 [생성하고 연결](#)하면 조직 전체에 적용되고 구현됩니다. 선언적 정책은 전체 조직, 조직 단위(OU) 또는 계정에 적용될 수 있습니다. 조직에 가입하는 계정은 조직의 선언적 정책을 자동으로 상속합니다. 자세한 내용은 [관리 정책 상속에 대한 이해](#) 단원을 참조하십시오.

유효 정책은 조직 루트 및 OU에서 상속되는 규칙과 계정에 직접 연결된 규칙의 집합입니다. 유효 정책은 계정에 적용되는 최종 규칙 집합을 지정합니다. 자세한 내용은 [유효 관리 정책 보기](#) 단원을 참조하십시오.

선언적 정책이 [분리](#)되면 속성 상태가 선언적 정책이 연결되기 전인 이전 상태로 롤백됩니다.

선언적 정책에 대한 사용자 지정 오류 메시지

선언적 정책을 사용하면 사용자 지정 오류 메시지를 생성할 수 있습니다. 예를 들어 선언적 정책으로 인해 API 작업이 실패하는 경우 오류 메시지를 설정하거나 내부 Wiki 또는 실패를 설명하는 메시지의 링크와 같은 사용자 지정 URL을 제공할 수 있습니다. 사용자 지정 오류 메시지를 지정하지 않으면에서 다음과 같은 기본 오류 메시지를 AWS Organizations 제공합니다. Example: This action is denied due to an organizational policy in effect.

선언적 정책을 생성하고, 선언적 정책을 업데이트하고, 선언적 정책을 삭제하는 프로세스를 감사할 수도 있습니다. AWS CloudTrail. CloudTrail은 선언적 정책으로 인한 API 작업 실패에 플래그를 지정할 수 있습니다. 자세한 내용은 [로깅 및 모니터링](#)을 참조하세요.

Important

사용자 지정 오류 메시지에 개인 식별 정보(PII) 또는 기타 민감 정보를 포함하지 마세요. PII에는 개인을 식별하거나 찾는 데 사용할 수 있는 일반 정보가 포함됩니다. 재무, 의료, 교육 또는 고용과 같은 기록을 다룹니다. PII의 예로는 주소, 은행 계좌 번호, 전화번호 등이 있습니다.

선언적 정책에 대한 계정 상태 보고서

계정 상태 보고서를 사용하여 범위 내 계정에 대한 선언적 정책에서 지원하는 모든 속성의 현재 상태를 평가할 수 있습니다. 보고서 범위에 포함할 계정 및 조직 단위(OU)를 선택하거나 루트를 선택하여 전체 조직을 선택할 수 있습니다.

이 보고서는 리전 분석을 제공하고 속성의 현재 상태가 계정 전반에 걸쳐 균일한지(numberOfMatchedAccounts을 통해) 또는 불일치하는지(numberOfUnmatchedAccounts을 통해)를 확인함으로써 준비 상태를 평가하는 데 도움을 줍니다. 또한 가장 빈번한 값을 확인할 수 있는데, 이는 해당 속성에 대해 가장 자주 관찰되는 구성 값입니다.

그림 1에는 생성된 계정 상태 보고서가 있으며, 이는 VPC 퍼블릭 액세스 차단 및 이미지 퍼블릭 액세스 차단 속성에 대한 계정 간 균일성을 보여줍니다. 즉, 각 속성에 대해 범위 내 모든 계정은 해당 속성에 대한 동일한 구성을 갖습니다.

생성된 계정 상태 보고서에 따르면 허용된 이미지 설정, 인스턴스 메타데이터 기본값, 직렬 콘솔 액세스 및 스냅샷 퍼블릭 액세스 차단 속성에 대한 일관되지 않은 계정이 표시됩니다. 이 예제에서 계정 불일치가 있는 각 속성은 구성 값이 다른 계정이 하나 있기 때문입니다.

가장 빈도가 높은 값이 있다면, 해당 열에 표시됩니다. 각 속성이 제어하는 항목에 대한 자세한 내용은 [선언적 정책 구문 및 예제 정책](#)을 참조하세요.

속성을 확장하여 리전 분석을 볼 수도 있습니다. 이 예제에서는 이미지 퍼블릭 액세스 차단이 확장되어 있으며, 각 리전별로 계정 간에도 일관성이 유지되고 있음을 확인할 수 있습니다.

기존 구성을 적용하기 위한 선언적 정책의 연결 여부에 대한 선택은 특정 사용 사례에 따라 달라집니다. 선언적 정책을 연결하기 전에 계정 상태 보고서를 사용하여 준비 상태를 평가할 수 있습니다.

자세한 내용은 [계정 상태 보고서 생성](#)을 참조하세요.

Account status report		Updated last Monday at 12:40 PM			Generate status report	View report in S3
Attribute	Region	Uniform across accounts	Inconsistent accounts	Most frequent value		
▶ Allowed Images Settings	All Regions	⚠ No	1			
▶ Instance Metadata Defaults	All Regions	⚠ No	1	{ "HttpTokens": "requi		
▶ Serial Console Access	All Regions	⚠ No	1	false		
▶ VPC Block Public Access	All Regions	✅ Yes	0	{ "State": "default-sta		
▶ Snapshot Block Public Access	All Regions	⚠ No	1	unblocked		
▼ Image Block Public Access	All Regions	✅ Yes	0	block-new-sharing		
	eu-west-3	✅ Yes	0			
	eu-north-1	✅ Yes	0			

그림 1: VPC 퍼블릭 액세스 차단 및 이미지 퍼블릭 액세스 차단에 대한 계정 간 균일성이 있는 계정 상태 보고서의 예.

지원되는 AWS 서비스 및 속성

EC2 선언적 정책에 대한 지원 속성

다음 표에는 Amazon EC2 관련 서비스에 지원되는 속성이 나와 있습니다.

EC2에 대한 선언적 정책

AWS 서비스	속성	정책 효과	정책 내용	추가 정보
Amazon VPC	VPC 퍼블릭 액세스 차단	Amazon VPC 및 서브넷 내 리소스가 인터넷 게이트	정책 보기	자세한 내용은 Amazon VPC 사용 설명서의 VPC

AWS 서비스	속성	정책 효과	정책 내용	추가 정보
		웨이(IGW)를 통해 인터넷에 접근할 수 있는지 제어합니다.		및 서브넷에 대한 퍼블릭 액세스 차단 을 참조하세요.
Amazon EC2	직렬 콘솔 액세스	EC2 직렬 콘솔에 액세스할 수 있는지 여부를 제어합니다.	정책 보기	자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 EC2 직렬 콘솔에 대한 액세스 구성 을 참조하세요.
	이미지 퍼블릭 액세스 차단	Amazon Machine Images(AMI)를 공개적으로 공유 가능한지 여부를 제어합니다.	정책 보기	자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 AMI에 대한 퍼블릭 액세스 차단 이해 를 참조하세요.
	허용된 이미지 설정	허용된 AMI를 통해 Amazon EC2에서 Amazon Machine Image(AMI)의 검색 및 사용을 제어합니다.	정책 보기	자세한 정보는 Amazon Elastic Compute Cloud 사용 설명서의 Amazon Machine Image(AMI) 섹션을 참조하세요.

AWS 서비스	속성	정책 효과	정책 내용	추가 정보
	인스턴스 메타데이터 기본값	모든 새 EC2 인스턴스 시작에 대한 IMDS 기본값을 제어합니다.	정책 보기	자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 새로운 인스턴스에 대한 인스턴스 메타데이터 옵션 구성 을 참조하세요.
Amazon EBS	스냅샷 퍼블릭 액세스 차단	Amazon EBS 스냅샷에 공개적으로 액세스할 수 있는지 여부를 제어합니다.	정책 보기	자세한 내용은 Amazon Elastic Block Store 사용 설명서의 Amazon EBS 스냅샷에 대한 퍼블릭 액세스 차단 을 참조하세요.

선언적 정책 시작하기

다음 단계에 따라 선언적 정책 사용을 시작합니다.

1. [선언적 정책 작업을 수행하는 데 필요한 권한에 대해 알아봅니다.](#)
2. [조직에 대해 선언적 정책을 활성화합니다.](#)

Note

신뢰 액세스를 활성화해야 합니다.

선언적 정책이 기존 구성을 적용하려면, 해당 서비스에서 신뢰할 수 있는 액세스를 활성화해야 합니다. 이는 조직 전체 계정의 기존 구성 상태를 반영한 계정 상태 보고서를 생성하는 데 사용되는 읽기 전용 서비스 연결 역할을 생성합니다.

콘솔 사용

Organizations 콘솔을 사용하는 경우 이 단계는 선언적 정책을 활성화하는 프로세스의 일부입니다.

사용 AWS CLI

를 사용하는 경우 두 AWS CLI개의 개별 APIs.

- 선언적 정책을 활성화하는 데 사용하는 것은 [EnablePolicyType](#)입니다.
- 신뢰할 수 있는 액세스를 활성화하는 데 사용하는 것은 [EnableAWSServiceAccess](#)입니다.

를 사용하여 특정 서비스에 대해 신뢰할 수 있는 액세스를 활성화하는 방법에 대한 자세한 내용은에서 사용할 수 AWS CLI 있습니다. [AWS 서비스AWS Organizations](#)

3. [계정 상태 보고서를 실행합니다.](#)
4. [선언적 정책을 생성합니다.](#)
5. [선언적 정책을 조직의 루트, OU 또는 계정에 연결합니다.](#)
6. [계정에 적용되는 결합된 유효 선언적 정책을 확인합니다.](#)

위의 모든 단계를 수행하려면 조직의 관리 계정에서 IAM 사용자로 로그인하거나, IAM 역할을 맡거나, 루트 사용자로 로그인([권장되지 않음](#))합니다.

기타 정보

- [선언적 정책 구문 알아보기 및 정책 예제 보기](#)

선언적 정책 사용에 대한 모범 사례

AWS에서는 선언적 정책 사용에 대한 다음 모범 사례를 권장합니다.

준비 상태 평가 활용

선언적 정책 계정 상태 보고서를 사용하여 범위 내 계정에 대한 선언적 정책에서 지원하는 모든 속성의 현재 상태를 평가합니다. 보고서 범위에 포함할 계정 및 조직 단위(OU)를 선택하거나 루트를 선택하여 전체 조직을 선택할 수 있습니다.

이 보고서는 리전 분석을 제공하고 속성의 현재 상태가 계정 전반에 걸쳐 균일한지(`numberOfMatchedAccounts`을 통해) 또는 불일치하는지(`numberOfUnmatchedAccounts`을 통해)를 확인함으로써 준비 상태를 평가하는 데 도움을 줍니다. 또한 가장 빈번한 값을 확인할 수 있는데, 이는 해당 속성에 대해 가장 자주 관찰되는 구성 값입니다.

기준 구성을 적용하기 위한 선언적 정책의 연결 여부에 대한 선택은 특정 사용 사례에 따라 달라집니다.

자세한 내용과 설명 예시는 [선언적 정책에 대한 계정 상태 보고서](#) 단원을 참조하세요.

작게 시작한 다음 규모 조정

디버깅을 간소화하려면 테스트 정책으로 시작합니다. 다음 변경을 수행하기 전에 각 변경의 동작 및 영향을 검증합니다. 이러한 접근 방식은 오류 또는 예기치 않은 결과가 발생할 때 고려해야 할 변수를 줄입니다.

예를 들어 중요하지 않은 테스트 환경에서 단일 계정에 연결된 테스트 정책으로 시작할 수 있습니다. 사양에 맞게 작동하는지 확인한 후에는 정책을 조직 구조 상위로 점진적으로 이동시켜 더 많은 계정과 조직 단위(OU)에 적용할 수 있습니다.

검토 프로세스 수립

새로운 선언적 속성을 모니터링하고, 정책 예외를 평가하며, 조직의 보안 및 운영 요구 사항과 일관성을 유지하기 위한 조정을 수행하는 프로세스를 구현합니다.

DescribeEffectivePolicy를 사용하여 변경 사항 검증

선언적 정책을 변경한 후 정책이 변경된 수준보다 낮은 대표 계정에 대한 유효 정책을 확인합니다. [를 사용하거나 DescribeEffectivePolicy API 작업 또는 또는 SDK 변형 중 하나를 사용하여 유효 정책을 볼 AWS Management Console](#) 수 있습니다. [DescribeEffectivePolicy](#) AWS CLI AWS 변경한 내용이 유효 정책에 의도한 영향을 미쳤는지 확인합니다.

커뮤니케이션 및 훈련

조직이 선언적 정책의 목적과 영향을 이해하고 있는지 확인합니다. 예상되는 동작과 정책 적용으로 인한 실패를 처리하는 방법에 대한 명확한 지침을 제공합니다.

선언적 정책에 대한 계정 상태 보고서 생성

계정 상태 보고서를 사용하여 범위 내 계정에 대한 선언적 정책에서 지원하는 모든 속성의 현재 상태를 평가할 수 있습니다. 보고서 범위에 포함할 계정 및 조직 단위(OU)를 선택하거나 루트를 선택하여 전체 조직을 선택할 수 있습니다.

이 보고서는 리전 분석을 제공하고 속성의 현재 상태가 계정 전반에 걸쳐 균일한지(numberOfMatchedAccounts을 통해) 또는 불일치하는지(numberOfUnmatchedAccounts을 통해)를 확인함으로써 준비 상태를 평가하는 데 도움을 줍니다. 또한 가장 빈번한 값을 확인할 수 있는데, 이는 해당 속성에 대해 가장 자주 관찰되는 구성 값입니다.

기존 구성을 적용하기 위한 선언적 정책의 연결 여부에 대한 선택은 특정 사용 사례에 따라 달라집니다.

자세한 내용과 설명 예시는 [선언적 정책에 대한 계정 상태 보고서](#) 단원을 참조하세요.

사전 조건

계정 상태 보고서를 생성하려면 먼저 다음 단계를 수행해야 합니다.

1. StartDeclarativePoliciesReport API는 조직의 관리 계정 또는 위임된 관리자만 직접 호출할 수 있습니다.
2. 보고서를 생성하기 전에 S3 버킷이 있어야 하며(새 버킷을 생성하거나 기존 버킷을 사용), 요청이 이루어진 리전과 동일한 리전에 있어야 하고, 적절한 S3 버킷 정책이 있어야 합니다. 샘플 S3 정책은 Amazon EC2 API 참조의 [예시](#)에서 샘플 Amazon S3 정책을 참조하세요.
3. 선언적 정책이 기존 구성을 적용하려면, 해당 서비스에서 신뢰할 수 있는 액세스를 활성화해야 합니다. 이는 조직 전체 계정의 기존 구성 상태를 반영한 계정 상태 보고서를 생성하는 데 사용되는 읽기 전용 서비스 연결 역할을 생성합니다.

콘솔 사용

Organizations 콘솔의 경우 이 단계는 선언적 정책을 활성화하는 프로세스의 일부입니다.

사용 AWS CLI

의 경우 [EnableAWSServiceAccess](#) API를 AWS CLI사용합니다.

를 사용하여 특정 서비스에 대해 신뢰할 수 있는 액세스를 활성화하는 방법에 대한 자세한 내용은 [AWS 서비스AWS Organizations](#)에서 사용할 수 AWS CLI 있습니다.

4. 조직당 한 번에 하나의 보고서만 생성할 수 있습니다. 다른 보고서를 생성 중인 상태에서 보고서를 생성하려고 하면 오류가 발생합니다.

규정 준수 상태 보고서에 액세스

최소 권한

규정 준수 상태 보고서를 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- ec2:StartDeclarativePoliciesReport
- ec2:DescribeDeclarativePoliciesReports
- ec2:GetDeclarativePoliciesReportSummary
- ec2:CancelDeclarativePoliciesReport

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:DescribeOrganizationalUnit`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListAWSServiceAccessForOrganization`
- `s3:PutObject`

Note

Amazon S3 버킷이 SSE-KMS 암호화를 사용하는 경우 정책에 `kms:GenerateDataKey` 권한도 포함해야 합니다.

AWS Management Console

다음 절차에 따라 계정 상태 보고서를 생성합니다.

계정 상태 보고서를 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 정책 페이지에서 EC2에 대한 선언적 정책을 선택합니다.
3. EC2에 대한 선언적 정책 페이지의 작업 드롭다운 메뉴에서 계정 상태 보고서 보기를 선택합니다.
4. 계정 상태 보고서 보기 페이지에서 상태 보고서 생성을 선택합니다.
5. 조직 구조 위젯에서 보고서에 포함할 조직 단위(OU)를 지정합니다.
6. 제출을 선택합니다.

AWS CLI & AWS SDKs

계정 상태 보고서를 생성하려면

다음 작업을 사용하여 규정 준수 상태 보고서를 생성하고, 상태를 확인하며, 보고서를 볼 수 있습니다.

- `ec2:start-declarative-policies-report`: 계정 상태 보고서를 생성합니다. 보고서는 비동기적으로 생성되며 완료되는 데 몇 시간이 걸릴 수 있습니다. 자세한 내용을 알아보려면 Amazon EC2 API 참조의 [StartDeclarativePoliciesReport](#)를 참조하세요.
- `ec2:describe-declarative-policies-report`: 보고서 상태를 포함하여 계정 상태 보고서의 메타데이터를 설명합니다. 자세한 내용은 Amazon EC2 API 참조의 [DescribeDeclarativePoliciesReports](#)를 참조하세요.
- `ec2:get-declarative-policies-report-summary`: 계정 상태 보고서의 요약を検査합니다. 자세한 내용을 알아보려면 Amazon EC2 API 참조의 [GetDeclarativePoliciesReportSummary](#)를 참조하세요.
- `ec2:cancel-declarative-policies-report`: 계정 상태 보고서 생성을 취소합니다. 자세한 내용을 알아보려면 Amazon EC2 API 참조의 [CancelDeclarativePoliciesReport](#)를 참조하세요.

보고서를 생성하기 전에, 보고서가 저장될 Amazon S3 버킷에 EC2 선언적 정책 위탁자에 대한 액세스 권한을 부여하세요. 이렇게 하려면 다음 정책을 해당 버킷에 연결하세요. `amzn-s3-demo-bucket`을 실제 Amazon S3 버킷 이름으로 바꾸고 `identity_ARN`을 `StartDeclarativePoliciesReport` API를 직접 호출하는 데 사용되는 IAM 자격 증명으로 바꿉니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DeclarativePoliciesReportDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": "identity_ARN"
      },
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "organizations.amazonaws.com"
        }
      }
    }
  ]
}
```



```
}
  ]
}
```

선언적 정책 구문 및 예시

이 페이지에서는 선언적 정책 구문에 대해 설명하고 예제를 제공합니다.

고려 사항

- 선언적 정책을 사용하여 서비스 속성을 구성하면 여러 API에 영향을 미칠 수 있습니다. 규정을 준수하지 않는 작업은 모두 실패합니다.
- 계정 관리자는 개별 계정 수준에서 서비스 속성의 값을 수정할 수 없습니다.

선언적 정책의 구문

선언적 정책은 [JSON](#) 규칙에 따라 구성된 일반 텍스트 파일입니다. 선언적 정책 구문은 모든 관리 정책 유형에 대한 구문을 따릅니다. 해당 구문에 대한 자세한 내용은 [관리 정책 유형에 대한 정책 구문 및 상속](#)을 참조하세요. 이 항목에서는 선언적 정책 유형의 특정 요구 사항에 해당 일반 구문을 적용하는 방법을 중점적으로 설명합니다.

다음 예제에서는 선언적 정책의 기본 구문을 보여줍니다.

```
{
  "ec2_attributes": {
    "exception_message": {
      "@@assign": "Your custom error message.https://myURL"
    }
  }
}
```

- ec2_attributes 필드 키 이름입니다. 선언적 정책은 항상 지정된 고정 키 이름으로 시작합니다 AWS 서비스. 위의 예제 정책에서 맨 위 줄입니다. 현재 선언적 정책은 Amazon EC2 관련 서비스만 지원합니다.
- ec2_attributes에서 exception_message를 사용하여 사용자 지정 오류 메시지를 설정할 수 있습니다. 자세한 내용은 [선언적 정책에 대한 사용자 지정 오류 메시지](#)를 참조하세요.
- ec2_attributes에서 지원되는 선언적 정책을 하나 이상 삽입할 수 있습니다. 이러한 스키마는 [지원되는 선언적 정책](#) 섹션을 참조하세요.

지원되는 선언적 정책

선언적 정책이 지원하는 AWS 서비스 및 속성은 다음과 같습니다. 다음 예제 중 일부에서는 공간을 절약하기 위해 JSON 공백 서식이 압축되었을 수 있습니다.

- VPC 퍼블릭 액세스 차단
- 직렬 콘솔 액세스
- 이미지 퍼블릭 액세스 차단
- 허용된 이미지 설정
- 인스턴스 메타데이터
- 스냅샷 퍼블릭 액세스 차단

VPC Block Public Access

정책 효과

Amazon VPC 및 서브넷 내 리소스가 인터넷 게이트웨이(IGW)를 통해 인터넷에 접근할 수 있는지 제어합니다. 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 [인터넷 액세스 구성](#)을 참조하세요.

정책 내용

```
{
  "ec2_attributes": {
    "vpc_block_public_access": {
      "internet_gateway_block": {
        "mode": {
          "@@assign": "block_ingress"
        },
        "exclusions_allowed": {
          "@@assign": "enabled"
        }
      }
    }
  }
}
```

다음은 이 속성에 사용할 수 있는 필드입니다.

- "internet_gateway":

- "mode":
 - "off": VPC BPA가 활성화되지 않았습니다.
 - "block_ingress": VPC에 대한 모든 인터넷 트래픽(제외된 VPC 또는 서브넷 제외)이 차단되었습니다. NAT 게이트웨이 및 송신 전용 인터넷 게이트웨이를 오가는 트래픽만 허용되는데, 이러한 게이트웨이는 아웃바운드 연결만 설정되도록 허용하기 때문입니다.
 - "block_bidirectional": 인터넷 게이트웨이 및 송신 전용 인터넷 게이트웨이(제외된 VPC 및 서브넷 제외)를 오가는 모든 트래픽이 차단되었습니다.
- "exclusions_allowed": 제외 항목은 계정의 VPC BPA 모드에서는 제외하고 양방향 또는 송신 전용 액세스를 허용하는 단일 VPC 또는 서브넷에 적용할 수 있는 모드입니다.
- "enabled": 계정에서 제외를 생성할 수 있습니다.
- "disabled": 계정에서 제외를 생성할 수 없습니다.

Note

속성을 사용하여 제외가 허용되는지 여부를 구성할 수 있지만 이 속성 자체로는 제외를 생성할 수 없습니다. 제외를 생성하려면 VPC를 소유한 계정에서 해당 제외를 생성해야 합니다. VPC BPA 제외 생성에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [제외 생성 및 삭제](#) 섹션을 참조하세요.

고려 사항

선언적 정책에서 이 속성을 사용하는 경우 다음 작업을 사용하여 범위 내 계정에 적용되는 구성을 수정할 수 없습니다. 단, 이 목록이 전부는 아닙니다.

- ModifyVpcBlockPublicAccessOptions
- CreateVpcBlockPublicAccessExclusion
- ModifyVpcBlockPublicAccessExclusion

Serial Console Access

정책 효과

EC2 직렬 콘솔에 액세스할 수 있는지 여부를 제어합니다. EC2 직렬 콘솔에 대한 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 [EC2 직렬 콘솔](#)을 참조하세요.

정책 내용

```
{
  "ec2_attributes": {
    "serial_console_access": {
      "status": {
        "@@assign": "enabled"
      }
    }
  }
}
```

다음은 이 속성에 사용할 수 있는 필드입니다.

- "status":
 - "enabled": EC2 직렬 콘솔 액세스가 허용됩니다.
 - "disabled": EC2 직렬 콘솔 액세스가 차단됩니다.

고려 사항

선언적 정책에서 이 속성을 사용하는 경우 다음 작업을 사용하여 범위 내 계정에 적용되는 구성을 수정할 수 없습니다. 단, 이 목록이 전부는 아닙니다.

- EnableSerialConsoleAccess
- DisableSerialConsoleAccess

Image Block Public Access

정책 효과

Amazon Machine Images(AMI)를 공개적으로 공유 가능한지 여부를 제어합니다. AMI에 대한 자세한 정보는 Amazon Elastic Compute Cloud 사용 설명서의 [Amazon Machine Image\(AMI\)](#) 섹션을 참조하세요.

정책 내용

```
{
  "ec2_attributes": {
    "image_block_public_access": {
      "state": {
        "@@assign": "block_new_sharing"
      }
    }
  }
}
```



```

    }
  }
}
}

```

다음은 이 속성에 사용할 수 있는 필드입니다.

- "state":
 - "unblocked": AMI의 퍼블릭 공유에는 제한이 없습니다.
 - "block_new_sharing": AMI의 새 퍼블릭 공유를 차단합니다. 그러나 이미 공개적으로 공유된 AMI는 계속 공개적으로 사용할 수 있습니다.

고려 사항

선언적 정책에서 이 속성을 사용하는 경우 다음 작업을 사용하여 범위 내 계정에 적용되는 구성을 수정할 수 없습니다. 단, 이 목록이 전부는 아닙니다.

- EnableImageBlockPublicAccess
- DisableImageBlockPublicAccess

Allowed Images Settings

정책 효과

허용된 AMI를 통해 Amazon EC2에서 Amazon Machine Image(AMI)의 검색 및 사용을 제어합니다. AMI에 대한 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 [허용된 AMI를 사용하여 Amazon EC2에서 AMI 검색 및 사용 제어](#)를 참조하세요.

정책 내용

다음은 이 속성에 사용할 수 있는 필드입니다.

```

{
  "ec2_attributes": {
    "allowed_images_settings": {
      "state": {
        "@@assign": "enabled"
      },
      "image_criteria": {
        "criteria_1": {

```

```

    "allowed_image_providers": {
      "@@append": [
        "amazon"
      ]
    }
  }
}

```

- "state":
 - "enabled": 속성이 활성 상태이고 적용됩니다.
 - "disabled": 속성이 비활성 상태이며 적용되지 않습니다.
 - "audit_mode": 속성이 감사 모드입니다. 즉, 규정을 준수하지 않는 이미지를 식별하지만 사용을 차단하지는 않습니다.
- "image_criteria": 기준 목록입니다. criteria_1에서 criteria_10까지의 이름으로 최대 10개의 기준 지원
 - "allowed_image_providers": amazon, aws_marketplace, aws_backup_vault의 12자리 계정 ID 또는 소유자 별칭으로 구성된 쉼표로 구분된 목록입니다.
 - "image_names": 허용되는 이미지의 이름입니다. 이름에는 와일드카드(? 및 *)가 포함될 수 있습니다. 길이는 1~128자입니다. ?를 사용할 경우, 최소 3자 이상 입력해야 합니다.
 - "marketplace_product_codes": 허용된 이미지에 대한 AWS Marketplace 제품 코드입니다. 길이: 1~25자 유효한 문자: 문자(A~Z, a~z) 및 숫자(0~9)
 - "creation_date_condition": 허용되는 이미지의 최대 경과 기간입니다.
 - "maximum_days_since_created": 이미지가 생성된 이후 경과한 최대 일수입니다. 유효 범위: 최소값은 0입니다. 최대값은 2147483647입니다.
 - "deprecation_time_condition": 허용되는 이미지의 사용 중단 이후 최대 경과 기간입니다.
 - "maximum_days_since_deprecated": 이미지의 사용 중단 이후 경과한 최대 일수입니다. 유효 범위: 최소값은 0입니다. 최대값은 2147483647입니다.

고려 사항

선언적 정책에서 이 속성을 사용하는 경우 다음 작업을 사용하여 범위 내 계정에 적용되는 구성을 수정할 수 없습니다. 단, 이 목록이 전부는 아닙니다.

- EnableAllowedImagesSettings
- ReplaceImageCriteriaInAllowedImagesSettings
- DisableAllowedImagesSettings

Instance Metadata

정책 효과

모든 새 EC2 인스턴스 시작에 대한 IMDS 기본값 및 IMDSv2 적용을 제어합니다. EC2 IMDS 기본값 및 IMDSv2 적용에 대한 자세한 내용은 Amazon [EC2 사용 설명서의 인스턴스 메타데이터를 사용하여 EC2 인스턴스 관리를 참조하세요](#). Amazon EC2

정책 내용

다음은 이 속성에 사용할 수 있는 필드입니다.

```
{
  "ec2_attributes": {
    "instance_metadata_defaults": {
      "http_tokens": {
        "@@assign": "required"
      },
      "http_put_response_hop_limit": {
        "@@assign": "4"
      },
      "http_endpoint": {
        "@@assign": "enabled"
      },
      "instance_metadata_tags": {
        "@@assign": "enabled"
      },
      "http_tokens_enforced": {
        "@@assign": "enabled"
      }
    }
  }
}
```

- "http_tokens":
 - "no_preference": 다른 기본값이 적용됩니다. 예를 들어, 해당되는 경우 AMI가 기본값으로 설정됩니다.

- "required": IMDSv2를 사용해야 합니다. IMDSv1은 허용되지 않습니다.
- "optional": IMDSv1과 IMDSv2가 모두 허용됩니다.

 Note

메타데이터 버전

http_tokens을 required(IMDSv2를 사용해야 함)로 설정하기 전에 IMDSv1 호출을 수행하는 인스턴스가 없는지 확인합니다. 자세한 내용은 [Amazon EC2 사용 설명서의 1 단계: IMDSv2=선택 사항으로 인스턴스 식별 및 IMDSv1 사용량 감사를 참조하세요.](#)

- "http_put_response_hop_limit":
 - "**Integer**": -1부터 64까지의 정수 값으로, 메타데이터 토큰이 이동할 수 있는 최대 홉 수를 나타냅니다. 기본 설정이 없음을 표시하려면 -1을 지정하십시오.

 Note

홉 제한

http_tokens이 required로 설정된 경우 http_put_response_hop_limit를 최소 2로 설정하는 것이 좋습니다. 자세한 내용을 알아보려면 Amazon Elastic Compute Cloud 사용 설명서의 [인스턴스 메타데이터 액세스 고려 사항](#)을 참조하세요.

- "http_endpoint":
 - "no_preference": 다른 기본값이 적용됩니다. 예를 들어, 해당되는 경우 AMI가 기본값으로 설정됩니다.
 - "enabled": 인스턴스 메타데이터 서비스의 엔드포인트에 액세스할 수 있습니다.
 - "disabled": 인스턴스 메타데이터 서비스의 엔드포인트에 액세스할 수 없습니다.
- "instance_metadata_tags":
 - "no_preference": 다른 기본값이 적용됩니다. 예를 들어, 해당되는 경우 AMI가 기본값으로 설정됩니다.
 - "enabled": 인스턴스 메타데이터에서 인스턴스 태그에 액세스할 수 있습니다.
 - "disabled": 인스턴스 메타데이터에서 인스턴스 태그에 액세스할 수 없습니다.
- "http_tokens_enforced":
 - "no_preference": 다른 기본값이 적용됩니다. 예를 들어, 해당되는 경우 AMI가 기본값으로 설정됩니다.

- "enabled": IMDSv2를 사용해야 합니다. IMDSv1 인스턴스를 시작하거나 기존 인스턴스에서 IMDSv1을 활성화하려는 시도는 실패합니다.
- "disabled": IMDSv1과 IMDSv2가 모두 허용됩니다.

Warning

IMDSv2 적용

IMDSv1 및 IMDSv2(토큰 선택 사항)를 허용하면서 IMDSv2 적용을 활성화하면 IMDSv1이 시작 파라미터 또는 AMI 기본값을 통해 명시적으로 비활성화되지 않는 한 시작 실패가 발생합니다. IMDSv1 자세한 내용은 Amazon EC2 사용 설명서의 [IMDSv1-enabled 인스턴스 시작 실패](#)를 참조하세요.

Snapshot Block Public Access

정책 효과

Amazon EBS 스냅샷에 공개적으로 액세스할 수 있는지 여부를 제어합니다. 스냅샷 아카이브에 대한 자세한 내용은 Amazon Elastic Block Store 사용 설명서의 [Amazon EBS 스냅샷](#)을 참조하세요.

정책 내용

```
{
  "ec2_attributes": {
    "snapshot_block_public_access": {
      "state": {
        "@@assign": "block_new_sharing"
      }
    }
  }
}
```

다음은 이 속성에 사용할 수 있는 필드입니다.

- "state":
 - "block_all_sharing": 스냅샷의 모든 퍼블릭 공유를 차단합니다. 이미 공개적으로 공유된 스냅샷은 비공개로 취급되어 더 이상 공개적으로 사용할 수 없습니다.
 - "block_new_sharing": 스냅샷의 새 퍼블릭 공유를 차단합니다. 그러나 이미 공개적으로 공유된 스냅샷은 계속 공개적으로 사용할 수 있습니다.

- "unblocked": 스냅샷의 공개 공유에는 제한이 없습니다.

고려 사항

선언적 정책에서 이 속성을 사용하는 경우 다음 작업을 사용하여 범위 내 계정에 적용되는 구성을 수정할 수 없습니다. 단, 이 목록이 전부는 아닙니다.

- EnableSnapshotBlockPublicAccess
- DisableSnapshotBlockPublicAccess

백업 정책

백업 정책을 사용하면 조직의 계정 전체에서 백업 계획을 중앙에서 관리하고 AWS 리소스에 적용할 수 있습니다.

[AWS Backup](#)를 사용하면 AWS 리소스를 백업하는 방법을 정의하는 [백업 계획](#)을 생성할 수 있습니다. 계획의 규칙에는 백업 빈도, 백업이 발생하는 기간, 백업할 리소스가 AWS 리전 포함된 , 백업을 저장할 볼트와 같은 다양한 설정이 포함됩니다. 그런 다음 태그를 사용하여 식별된 AWS 리소스 그룹에 백업 계획을 적용할 수 있습니다. 또한 사용자를 대신하여 백업 작업을 수행할 수 있는 권한을 부여하는 AWS Identity and Access Management AWS Backup (IAM) 역할을 식별해야 합니다.

의 백업 정책은 이러한 모든 부분을 [JSON](#) 텍스트 문서로 AWS Organizations 결합합니다. 정의된 백업 정책은 조직의 구조에 존재하는 모든 요소(루트, 조직 단위(OU), 개별 계정 등)에 연결할 수 있습니다. Organizations는 상속 규칙을 적용하여 조직의 루트, 상위 OU 또는 계정에 연결된 정책을 결합합니다. 이렇게 하면 각 계정에 대해 [유효 백업 정책](#)이 생성됩니다. 이 유효 정책은 리소스를 자동으로 백업 AWS 하는 AWS Backup 방법을 지시합니다.

백업 정책 작동 방식

백업 정책을 사용하면 조직에 필요한 수준의 리소스 백업을 세부적으로 제어할 수 있습니다. 예를 들어 조직의 루트에 연결된 정책에서 모든 Amazon DynamoDB 테이블을 백업하도록 지정할 수 있습니다. 이 정책에는 기본 백업 빈도가 포함될 수 있습니다. 그런 다음 각 OU의 요구 사항에 따라 백업 빈도를 재정의하는 백업 정책을 OU에 연결할 수 있습니다. 예를 들어 Developers OU는 백업 빈도를 일주일에 한 번으로 지정하고 Production OU는 하루에 한 번으로 지정할 수 있습니다.

리소스를 성공적으로 백업하는 데 필요한 정보의 일부만 개별적으로 포함하는 부분 백업 정책을 생성할 수 있습니다. 하위 수준 OU 및 계정에서 이러한 부분 정책을 상속하도록 루트 또는 상위 OU와 같은 조직 트리의 다양한 부분에 이러한 정책을 연결할 수 있습니다. Organizations가 상속 규칙을 사용하여

계정에 대한 모든 정책을 결합하는 경우 최종 유효 정책은 필수 요소를 모두 포함해야 합니다. 그렇지 않으면 정책이 유효하지 않은 것으로 AWS Backup 간주하고 영향을 받는 리소스를 백업하지 않습니다.

Important

AWS Backup 는 모든 필수 요소가 있는 완전한 유효 정책에 의해 호출되는 경우에만 성공적인 백업을 수행할 수 있습니다.

앞서 설명한 부분 정책 전략이 작동할 수 있지만 계정에 대한 유효 정책이 불완전하면 오류가 발생하거나 리소스가 백업되지 않습니다. 대체 전략으로 모든 백업 정책이 자체적으로 완전하고 유효하도록 요구하는 것이 좋습니다. 상위 계층에 연결된 정책에서 제공하는 기본값을 사용하고 [상속 하위 제어 연산자](#)를 포함하여 하위 정책에서 필요에 따라 재정의합니다.

조직의 각 AWS 계정에 대한 유효 백업 계획은 콘솔에 AWS Backup 해당 계정에 대한 변경 불가능한 계획으로 표시됩니다. 볼 수는 있지만 변경할 수는 없습니다. 그러나 [TagResource](#) 및 [UntagResource](#) API를 사용한 백업 계획 태그를 추가 또는 제거할 수 있습니다.

가 정책 생성 백업 계획을 기반으로 백업을 AWS Backup 시작하면 AWS Backup 콘솔에서 백업 작업의 상태를 볼 수 있습니다. 멤버 계정의 사용자는 해당 멤버 계정의 백업 작업에 대한 상태 및 오류를 볼 수 있습니다. 또한를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하면 조직의 관리 계정에 AWS Backup있는 사용자가 조직의 모든 백업 작업에 대한 상태 및 오류를 볼 수 있습니다. 자세한 내용은 AWS Backup 개발자 안내서의 [교차 계정 관리 활성화](#)를 참조하세요.

백업 정책 시작하기

다음 단계에 따라 백업 정책 사용을 시작합니다.

1. [백업 정책 작업을 수행하는 데 필요한 권한에 대해 알아봅니다.](#)
2. [백업 정책을 사용할 때 권장되는 몇 가지 모범 사례에 대해 알아봅니다.](#)
3. [조직에 대해 백업 정책을 활성화합니다.](#)
4. [백업 정책을 생성합니다.](#)
5. [백업 정책을 조직의 루트, OU 또는 계정에 연결합니다.](#)
6. [계정에 적용되는 결합된 유효 백업 정책을 확인합니다.](#)

위의 모든 단계를 수행하려면 조직의 관리 계정에서 IAM 사용자로 로그인하거나, IAM 역할을 맡거나, 루트 사용자로 로그인([권장되지 않음](#))합니다.

기타 정보

- [백업 정책 구문 알아보기 및 정책 예제 보기](#)

백업 정책 사용 모범 사례

AWS에서는 백업 정책 사용에 대한 다음 모범 사례를 권장합니다.

백업 정책 전략 결정

상속 및 병합되는 불완전한 부분으로 백업 정책을 생성하여 각 멤버 계정에 대해 완전한 정책을 생성할 수 있습니다. 이렇게 하면 변경 내용이 하위 수준의 모든 계정에 미치는 영향을 신중하게 고려하지 않고 특정 수준에서 정책을 변경하면 불완전한 유효 정책이 될 위험이 있습니다. 이를 방지하려면 모든 수준에서 구현하는 백업 정책이 자체적으로 완전하도록 하는 것이 좋습니다. 상위 정책을 하위 정책에 지정된 설정으로 재정의할 수 있는 기본 정책으로 취급합니다. 이렇게 하면 하위 정책이 존재하지 않더라도 상속된 정책이 완전하고 기본값을 사용합니다. [하위 제어 상속 연산자](#)를 사용하여 하위 정책에 의해 추가, 변경 또는 제거될 수 있는 설정을 제어할 수 있습니다.

GetEffectivePolicy를 사용하여 백업 정책 확인에 대한 변경 사항 유효성 검사

백업 정책을 변경한 후 정책이 변경된 수준보다 낮은 대표 계정에 대한 유효 정책을 확인합니다. [를 사용하거나 GetEffectivePolicy API 작업 또는 또는 SDK 변형 중 하나를 사용하여 유효 정책을 볼 AWS Management Console](#) 수 있습니다. [GetEffectivePolicy](#) AWS CLI AWS 변경한 내용이 유효 정책에 의도한 영향을 미쳤는지 확인합니다.

간단하게 시작하고 소규모로 변경

디버깅을 단순화하려면 간단한 정책으로 시작하여 한 번에 한 항목씩 변경합니다. 다음 변경을 수행하기 전에 각 변경의 동작 및 영향을 검증합니다. 이러한 접근 방식은 오류 또는 예기치 않은 결과가 발생할 때 고려해야 할 변수를 줄입니다.

백업 사본을 조직의 다른 AWS 리전 및 계정에 저장

재해 복구 위치를 개선하기 위해 백업의 복사본을 저장할 수 있습니다.

- 다른 리전 - 백업 사본을 추가로 저장하는 경우 원래 리전에서 실수로 손상되거나 삭제되지 않도록 백업을 보호할 수 AWS 리전있습니다. 정책의 `copy_actions` 섹션을 사용해, 백업 계획이 실행되는 해당 계정에 속한 리전 하나 이상에서 볼트를 지정합니다. 이를 위해 백업의 복사본을 저장할 백업 볼트의 ARN을 지정할 때 `$account` 변수를 사용하여 계정을 식별합니다. `$account` 변수는 실행 시점에 백업 정책이 실행되는 계정 ID로 대체됩니다.

- 다른 계정 - 백업 사본을 추가로 저장하는 경우 계정 중 하나를 손상시키는 악의적인 행위자로부터 보호하는 데 도움이 되는 보안 장벽을 AWS 계정추가합니다. 정책의 `copy_actions` 섹션을 사용해, 백업 계획이 실행되는 계정과 별도로 조직에 속한 계정 하나 이상에서 볼트를 지정합니다. 이를 위해 백업의 복사본을 저장할 백업 볼트의 ARN을 지정할 때 실제 계정 ID 번호를 사용해 계정을 식별합니다.

정책당 계획 수를 제한

여러 계획이 포함된 정책은 모두 유효성을 검사해야 하는 출력 수가 많아지기 때문에 문제를 해결하는 것이 더 복잡합니다. 대신, 각 정책에 하나의 백업 계획만 포함하여 디버깅 및 문제 해결을 단순화하도록 하세요. 그런 다음 다른 요구 사항을 충족하도록 다른 계획을 사용하여 정책을 추가할 수 있습니다. 이 방식은 특정 계획의 모든 문제를 하나의 정책으로 격리할 수 있으며 다른 정책 및 해당 계획 때문에 문제 해결이 복잡해지는 것을 방지할 수 있습니다.

스택 세트를 사용하여 필요한 백업 볼트 및 IAM 역할 생성

AWS CloudFormation 스택 세트와 Organizations의 통합을 사용하여 조직의 각 멤버 계정에 필요한 백업 볼트 및 AWS Identity and Access Management (IAM) 역할을 자동으로 생성합니다. 조직의 모든에서 자동으로 사용할 리소스가 포함된 스택 세트를 생성할 수 AWS 계정 있습니다. 이 방식을 통해 종속성이 이미 충족되었음이 보장된 상태에서 백업 계획을 실행할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 [자체 관리 권한으로 스택 세트 만들기](#)를 참조하세요.

각 계정에서 생성된 첫 번째 백업을 검토하여 결과를 확인합니다.

정책을 변경할 때 변경 이후에 생성된 다음 백업을 확인하여 변경 사항이 원하는 영향을 미치는지 확인합니다. 이 단계는 유효 정책을 살펴보는 것 그 이상이며 AWS Backup 가 정책을 해석하고 의도한 대로 백업 계획을 구현하도록 합니다.

AWS CloudTrail 이벤트를 사용하여 조직의 백업 정책 모니터링

AWS CloudTrail 이벤트를 사용하여 조직의 계정에서 백업 정책이 생성, 업데이트 또는 삭제되는 시기 또는 잘못된 조직 백업 계획이 있는 시기를 모니터링할 수 있습니다. 자세한 내용은 AWS Backup 개발자 안내서의 [교차 계정 관리 이벤트 로깅](#)을 참조하세요.

백업 정책 구문 및 예제

이 페이지에서는 백업 정책 구문에 대해 설명하고 예제를 제공합니다.

백업 정책 구문

백업 정책은 [JSON](#) 규칙에 따라 구성된 일반 텍스트 파일입니다. 백업 정책 구문은 모든 관리 정책 유형에 대한 구문을 따릅니다. 자세한 내용은 [관리 정책 유형에 대한 정책 구문 및 상속](#)을 참조하세요. 이 항목에서는 백업 정책 유형의 특정 요구 사항에 해당 일반 구문을 적용하는 방법을 중점적으로 설명합니다.

AWS Backup 계획에 대한 자세한 내용은 AWS Backup 개발자 안내서의 [CreateBackupPlan](#)을 참조하세요.

고려 사항

정책 구문

JSON에서 중복된 키 이름은 거부됩니다.

정책은 백업할 AWS 리전 및 리소스를 지정해야 합니다.

정책은가 AWS Backup 수입하는 IAM 역할을 지정해야 합니다.

동일한 수준에서 @@assign 연산자를 사용하면 기존 설정을 덮어쓸 수 있습니다. 자세한 내용은 [하위 정책이 상위 정책의 설정을 재정의](#)를 참조하세요.

상속 연산자는 상속된 정책과 계정 정책이 계정의 유효 정책으로 병합되는 방법을 제어합니다. 이러한 연산자에는 값 설정 연산자와 하위 제어 연산자가 포함됩니다.

자세한 내용은 [상속 연산자](#) 및 [백업 정책 예제](#)를 참조하세요.

IAM 역할

백업 계획을 처음 생성할 때 IAM 역할이 있어야 합니다.

IAM 역할에는 태그 쿼리로 식별된 리소스에 액세스할 수 있는 권한이 있어야 합니다.

IAM 역할에는 백업을 수행할 수 있는 권한이 있어야 합니다.

백업 저장소

백업 계획을 실행 AWS 리전 하려면 지정된 각 볼트가 있어야 합니다.

볼트는 유효 정책을 수신하는 각 AWS 계정에 대해 존재해야 합니다. 자세한 내용은 AWS Backup 개발자 안내서의 [백업 볼트 생성 및 삭제](#)를 참조하세요.

AWS CloudFormation 스택 세트 및 Organizations와의 통합을 사용하여 조직의 각 멤버 계정에 대한 백업 볼트 및 IAM 역할을 자동으로 생성하고 구성하는 것이 좋습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 [자체 관리 권한으로 스택 세트 만들기](#)를 참조하세요.

할당량:

할당량 목록은 AWS Backup 개발자 안내서의 [AWS Backup 할당량](#)을 참조하세요.

백업 구문: 개요

백업 정책 구문에는 다음 구성 요소가 포함됩니다.

```
{
  "plans": {
    "PlanName": {
      "rules": { ... },
      "regions": { ... },
      "selections": { ... },
      "advanced_backup_settings": { ... },
      "backup_plan_tags": { ... },
      "scan_settings": { ... }
    }
  }
}
```

백업 정책 요소

요소	설명	필수
규칙	백업 규칙 목록. 각 규칙은 백업이 시작되는 시기와 regions 및 selections 요소에 지정된 리소스의 실행 기간을 정의합니다.	예
리전	백업 정책이 리소스를 보호할 수 AWS 리전 있는 위치의 목록입니다.	예
선택	백업 rules이 보호하도록 지정된 regions 내에서 하나 이상의 리소스 유형.	예
advanced_backup_settings	특정 백업 시나리오에 대한 구성 옵션.	아니요

요소	설명	필수
	현재 지원되는 유일한 고급 백업 설정은 Amazon EC2 인스턴스에서 실행 중인 Windows 또는 SQL Server에 대해 Microsoft Volume Shadow Copy Service(VSS) 백업을 사용하는 것입니다.	
backup_plan_tags	백업 계획과 연결할 태그. 각 태그는 사용자 정의 키와 값으로 구성된 레이블입니다. 태그를 사용하면 백업 계획을 손쉽게 관리, 식별, 정리, 검색, 필터링할 수 있습니다.	아니요
scan_settings	스캔 설정을 위한 구성 옵션입니다. 현재 지원되는 유일한 스캔 설정은 Amazon GuardDuty 맬웨어 보호를 활성화하는 것입니다 AWS Backup.	아니요

백업 구문: 규칙

rules 정책 키는 AWS Backup 이 선택한 리소스에서 수행하는 예약된 백업 작업을 지정합니다.

백업 규칙 요소

요소	설명	필수
schedule_expression	가 백업 작업을 AWS Backup 시작하는 시기를 지정하는 UTC의 Cron 표현식입니다. Cron 표현식에 대한 자세한 정보는 Amazon EventBridge 사용 설명서의 Cron 및 rate 표현식을 사용하여 규칙 예약 을 참조하세요.	예
target_backup_vault_name	백업이 저장되는 백업 볼트입니다. 백업 저장소는 백업 저장소를 생성하는 데 사용된 계정과 백업 저장소가 생성되는 AWS 리전 계정에 고유한 이름으로 식별됩니다.	예

요소	설명	필수
target_logically_air_gapped_backup_vault_arn	백업이 저장되는 논리적 에어 갭 저장소 ARN입니다. 제공된 경우, 지원되는 완전 관리형 리소스는 논리적 에어 갭 저장소에 직접 백업되는 반면, 지원되는 다른 리소스는 백업 저장소에 임시(청구 가능한) 스냅샷을 생성한 다음 논리적 에어 갭 저장소에 복사합니다. 지원되지 않는 리소스는 지정된 백업 볼트에만 백업됩니다. ARN은 특수 자리 표시자 \$region 및를 사용하여 합칩니다 \$account. 예를 들어 이름이 인 볼트AirGappedVault 의 경우 올바른 값은 입니다arn:aws:backup:\$region:\$account:backup-vault:AirGappedVault .	아니요
start_backup_window_minutes	백업 작업이 성공적으로 시작되지 않으면 작업을 취소하기 전에 대기하는 시간(분)입니다. 이 값이 포함된 경우 오류를 방지하려면 60분 이상이어야 합니다.	아니요
complete_backup_window_minutes	백업 작업이 성공적으로 시작된 후 AWS Backup에 의해 취소되기 전에 완료되어야 하는 시간(분)입니다.	아니요

요소	설명	필수
enable_continuous_backup	가 연속 백업을 AWS Backup 생성할지 여부를 지정합니다. True AWS Backup 는 point-in-time 복원(PITR)이 가능한 연속 백업을 생성합니다. False (또는 지정되지 않음)은가 스냅샷 백업 AWS Backup 을 생성합니다. 연속 백업에 대한 자세한 내용은 AWS Backup 개발자 안내서의 특정 시점으로 복구를 참조하세요. 참고: PITR 지원 백업의 최대 보존 기간은 35일입니다.	아니요

요소	설명	필수
lifecycle	가 백업을 콜드 스토리지로 AWS Backup 전환하는 시기와 만료되는 시기를 지정합니다. 콜드 스토리지로 전환할 수 있는 리소스 유형은 AWS Backup 개발자 안내서의 리소스별 기능 가용성 테이블 리소스별 기능 가용성에 나열되어 있습니다. 각 수명 주기에는 다음 요소가 포함됩니다. • <code>move_to_cold_storage_after_days</code> : 백업이 발생한 후 복구 시점을 콜드 스토리지로 AWS Backup 이동하기까지 남은 일수입니다. • <code>delete_after_days</code> : 백업이 발생한 후 복구 시점을 AWS Backup 삭제하기 전의 일수입니다. • <code>opt_in_to_archive_for_supported_resources</code> : 값을 <code>true</code>로 지정하면 백업 계획은 지원되는 리소스를 수명 주기 설정에 따라 아카이브(콜드) 스토리지 계층으로 전환합니다. 참고: 콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 즉, <code>delete_after_days</code> 는 <code>move_to_cold_storage_after_days</code> 보다 90일 커야 합니다.	아니요

요소	설명	필수
copy_actions	가 하나 이상의 추가 위치에 백업을 AWS Backup 복사할지 여부를 지정합니다. 각 복사 작업에는 다음 요소가 포함됩니다. • <code>target_backup_vault_arn</code> : AWS Backup 이 백업의 추가 복사본을 저장할 볼트입니다. • 동일 계정 사본에 <code>\$account</code> 사용 • 교차 계정 사본에 실제 계정 ID 사용 • <code>lifecycle</code> :가 백업을 콜드 스토리지로 AWS Backup 전환하는 시기와 만료되는 시기를 지정합니다. 각 수명 주기에는 다음 요소가 포함됩니다. • <code>move_to_cold_storage_after_days</code> : AWS Backup 이 백업 후 복구 지점을 콜드 스토리지로 이동할 때까지 기간(일)입니다. • <code>delete_after_days</code> :가 복구 시점을 AWS Backup 삭제하기 전 백업이 발생한 후의 일수입니다. 참고: 콜드 스토리지로 전환된 백업은 콜드 스토리지에서 최소 90일 이상 저장되어야 합니다. 즉, <code>delete_after_days</code> 는 <code>move_to_cold_storage_after_days</code> 보다 90일 커야 합니다.	아니요

요소	설명	필수
recovery_point_tags	백업에서 복원되는 리소스에 할당하려는 태그. 각 태그에는 다음 요소가 포함됩니다. • tag_key: 이 블록 내의 필수 필드입니다. 태그 이름(대소문자 구분) • tag_value : 이 블록 내의 필수 필드입니다. 태그 값(대소문자 구분)	아니요
index_actions	가 Amazon EBS 스냅샷 및/또는 Amazon S3 백업의 백업 인덱스를 AWS Backup 생성할지 여부를 지정합니다. 백업 인덱스는 백업의 메타데이터를 검색하기 위해 생성됩니다. 백업 인덱스 생성 및 백업 검색에 대한 자세한 내용은 백업 검색을 참조하세요. 참고: Amazon EBS 스냅샷 백업 인덱스를 생성하려면 추가 IAM 역할 권한이 필요합니다. 각 인덱스 작업에는 인덱싱에 지원되는 리소스 유형이 Amazon EBS 및 Amazon S3인 요소 resource_types 가 포함되어 있습니다. 이 파라미터는 인덱싱에 옵트인할 리소스 유형을 지정합니다.	아니요

요소	설명	필수
scan_actions	지정된 규칙에 대해 스캔 작업을 활성화할지 여부를 지정합니다. 를 지정해야 합니다 ScanMode. 스캔 작업이 성공적으로 시작 scan_actions 되려면와 함께 scan_settings 백업 정책 요소에 사용해야 합니다. 또한 올바른 IAM 역할 권한이 있는지 확인하십시오. ScanMode: 백업 계획 규칙의 빈도로 실행할 스캔 유형을 지정합니다. INCREMENTAL_SCAN 또는 FULL_SCAN 중에서 선택할 수 있습니다.	아니요

백업 구문: 리전

regions 정책 키는 selections 키의 조건과 일치하는 리소스를 찾기 위해 AWS 리전 에서 AWS Backup 찾을을 지정합니다.

백업 리전 요소

요소	설명	필수
regions	AWS 리전 코드를 지정합니다. 예를 들어 ["us-east-1", "eu-north-1"] 입니다.	예

백업 구문: 선택

selections 정책 키는 백업 정책의 규칙에 의해 백업되는 리소스를 지정합니다.

상호 배타적인 요소는 tags 및 resources입니다. 유효 정책이 유효하려면 태그나 선택한 resources가 있어야합니다.

태그 조건과 리소스 조건이 모두 포함된 선택을 원하는 경우 resources 키를 사용합니다.

백업 선택 요소: 태그

요소	설명	필수
iam_role_arn	가 지정된 리전에서 리소스를 쿼리, 검색 및 백업하기 위해 AWS Backup 수임하는 IAM 역할입니다. 역할에는 태그 조건에 따라 리소스를 쿼리하고 일치하는 리소스에 대한 백업 작업을 수행할 수 있는 충분한 권한이 있어야 합니다.	예
tag_key	검색할 태그 키 이름.	예
tag_value	일치하는 tag_key와 연결되어야 하는 값. AWS Backup에는 tag_key와 tag_value가 모두 일치하는 경우에만 리소스가 포함됩니다(대소문자 구분).	예
conditions	포함하거나 제외하려는 키 및 값에 태그 지정 string_equals 또는 string_not_equals를 사용하여 정확히 일치하는 태그를 포함하거나 제외합니다. string_like 및 string_not_like를 사용하여 특정 문자를 포함하거나 포함하지 않는 태그를 포함하거나 제외합니다. 참고: 각 선택에 대해 30개의 조건으로 제한됩니다.	아니요

백업 선택 요소: 리소스

요소	설명	필수
iam_role_arn	가 지정된 리전에서 리소스를 쿼리, 검색 및 백업하기 위해 AWS Backup 수임하는 IAM 역할입니다.	예

요소	설명	필수
	역할에는 태그 조건에 따라 리소스를 쿼리하고 일치하는 리소스에 대한 백업 작업을 수행할 수 있는 충분한 권한이 있어야 합니다. 참고: 여기서 ARN에 파티션 이름을 추가해야 AWS GovCloud (US) Regions합니다. 예를 들어 "arn:aws:ec2:*:*:volume/*"는 "arn:aws-us-gov:ec2:*:*:volume/*"여야 합니다.	
resource_types	백업 계획에 포함할 리소스 유형.	예
not_resource_types	백업 계획에서 제외할 리소스 유형.	아니요
conditions	포함하거나 제외하려는 키 및 값에 태그 지정 string_equals 또는 string_not_equals를 사용하여 정확히 일치하는 태그를 포함하거나 제외합니다. string_like 및 string_not_like를 사용하여 특정 문자를 포함하거나 포함하지 않는 태그를 포함하거나 제외합니다. 참고: 각 선택에 대해 30개의 조건으로 제한됩니다.	아니요

지원되는 리소스 유형

Organizations는 resource_types 및 not_resource_types 요소에 대해 다음과 같은 리소스 유형을 지원합니다.

- AWS Backup gateway 가상 머신: "arn:aws:backup-gateway:*:*:vm/*"
- AWS CloudFormation 스택: "arn:aws:cloudformation:*:*:stack/*"
- Amazon DynamoDB 테이블: "arn:aws:dynamodb:*:*:table/*"

- Amazon EC2 인스턴스: "arn:aws:ec2:*:*:instance/*"
- Amazon EBS 볼륨: "arn:aws:ec2:*:*:volume/*"
- Amazon EFS 파일 시스템: "arn:aws:elasticfilesystem:*:*:file-system/*"
- Amazon Aurora/Amazon DocumentDB/Amazon Neptune 클러스터: "arn:aws:rds:*:*:cluster:*"
- Amazon RDS 데이터베이스: "arn:aws:rds:*:*:db:*"
- Amazon Redshift 클러스터: "arn:aws:redshift:*:*:cluster:*"
- Amazon S3: "arn:aws:s3:::*"
- AWS Systems Manager for SAP HANA 데이터베이스: "arn:aws:ssm-sap:*:*:HANA/*"
- AWS Storage Gateway 게이트웨이: "arn:aws:storagegateway:*:*:gateway/*"
- Amazon Timestream 데이터베이스: "arn:aws:timestream:*:*:database/*"
- Amazon FSx 파일 시스템: "arn:aws:fsx:*:*:file-system/*"
- Amazon FSx 볼륨: "arn:aws:fsx:*:*:volume/*"
- Amazon Elastic Kubernetes Service 볼륨: "arn:aws:eks:*:*:cluster/*"

코드 예제

자세한 내용은 [태그 블록을 사용하여 리소스 지정](#) 및 [리소스 블록을 사용하여 리소스 지정](#)을 참조하세요.

백업 구문: 고급 백업 설정

advanced_backup_settings 키는 특정 백업 시나리오에 대한 구성 옵션을 지정합니다. 각 설정은 다음 요소가 포함됩니다.

고급 백업 설정 요소

요소	설명	필수
advanced_backup_settings	특정 백업 시나리오에 대한 설정을 지정합니다. 이 키에는 하나 이상의 설정이 있습니다. 각 설정은 다음 요소를 포함하는 JSON 객체 문자열입니다.	아니요

요소	설명	필수
	현재 지원되는 유일한 고급 백업 설정은 Amazon EC2 인스턴스에서 실행 중인 Windows 또는 SQL Server에 대해 Microsoft Volume Shadow Copy Service(VSS) 백업을 사용하는 것입니다. 각 고급 백업은 다음 요소를 설정합니다. - Object key name: 다음 고급 설정이 적용되는 리소스 유형을 지정하는 문자열입니다. 키 이름은 "ec2" 리소스 유형이어야 합니다 - Object value: 연결된 리소스 유형과 관련된 하나 이상의 백업 설정을 포함하는 문자열입니다. 값은 Amazon EC2 인스턴스에서 실행되는 백업에 대해 "windows_vss" 지원이 enabled 또는 disabled인지 지정합니다.	

예시:

```
"advanced_backup_settings": {
  "ec2": {
    "windows_vss": {
      "@@assign": "enabled"
    }
  }
}
```

```

    }
  }
},

```

백업 구문: 백업 계획 태그

backup_plan_tags 정책 키는 백업 계획 자체에 연결되는 태그를 지정합니다. 이는 rules 또는 selections에 지정된 태그에는 영향을 주지 않습니다.

백업 계획 태그 요소

요소	설명	필수
backup_plan_tags	각 태그는 사용자 정의 키와 값으로 구성된 레이 붙입니다. - tag_key: 검색할 태그 키 이름. 이 블록 내의 필수 필드입니다. 이 값은 대소문자를 구분합니다. - tag_value : 백업 계획에 연결되고 tag_key와 연결되는 값. 이 블록 내의 필수 필드입니다. 이 값은 대소문자를 구분합니다.	아니요

백업 구문: 스캔 설정

scan_settings 정책 키는 Amazon GuardDuty 맬웨어 보호를 사용하여 맬웨어 스캔을 위한 구성을 지정합니다 AWS Backup. 스캔 작업이 성공적으로 시작되려면 백업 규칙scan_actions에서 scan_settings를와 함께 사용해야 합니다.

스캔 설정 요소

요소	설명	필수
scan_settings	스캔 설정을 위한 구성 옵션입니다. 현재 지원되는 유일한 스캔 설정은 Amazon GuardDuty 맬웨어 보호를 활성화하는 것입니다 AWS Backup. ResourceTypes 및를 지정해야 합니다ScannerRoleArn .	아니요

요소	설명	필수
	• ResourceTypes : 맬웨어 스캔을 선택한 리소스 선택 기준으로 필터링합니다. EBS, EC2, S3 또는 ALL를 사용할 수 있습니다. • ScannerRoleArn : 이 역할은 스캔이 시작되면 AWS Backup 에서 Amazon GuardDuty로 전달되어 백업에 대한 액세스를 제공합니다. 맬웨어 보호 액세스를 보고 필요한 전체 권한 목록을 확인합니다.	

예:

다음은 Amazon scan_actions GuardDuty 맬웨어 보호 스캔을 활성화하기 위해 백업 규칙 및 계획 수준에서 scan_settings를 구성하는 방법을 보여줍니다. Amazon GuardDuty

scan_actions 규칙에서:

```
"scan_actions": {
  "GUARDDUTY": {
    "scan_mode": {
      "@@assign": "INCREMENTAL_SCAN"
    }
  }
}
```

scan_settings 계획 수준에서:

```
"scan_settings": {
  "GUARDDUTY": {
    "resource_types": {
      "@@assign": ["EBS"]
    },
    "scanner_role_arn": {
      "@@assign": "arn:aws:iam::$account:role/MyGuardDutyScannerRole"
    }
  }
}
```


백업 정책 예제

다음 백업 정책 예제는 정보 제공 용도로만 제공됩니다. 다음 예제 중 일부에서는 공간을 절약하기 위해 JSON 공백 서식이 압축되었을 수 있습니다.

- [예제 1: 상위 노드에 할당된 정책](#)
- [예제 2: 상위 정책이 하위 정책과 병합](#)
- [예제 3: 상위 정책이 하위 정책에 의한 모든 변경을 금지](#)
- [예제 4: 상위 정책이 하위 정책에 의한 한 백업 계획의 변경을 금지](#)
- [예제 5: 하위 정책이 상위 정책의 설정을 재정의](#)
- [예제 6: 태그 블록을 사용하여 리소스 지정](#)
- [예제 7: 리소스 블록을 사용하여 리소스 지정](#)
- [예제 8: Amazon GuardDuty 맬웨어 보호 스캔을 사용한 백업 계획](#)

예제 1: 상위 노드에 할당된 정책

다음 예제에서는 계정의 상위 노드 중 하나에 할당된 백업 정책을 보여 줍니다.

상위 정책 – 이 정책은 조직의 루트 또는 모든 의도된 계정의 상위 OU에 연결할 수 있습니다.

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": {
        "@@assign": [
          "ap-northeast-2",
          "us-east-1",
          "eu-north-1"
        ]
      },
      "rules": {
        "Hourly": {
          "schedule_expression": {
            "@@assign": "cron(0 5/1 ? * * *)"
          },
          "start_backup_window_minutes": {
            "@@assign": "480"
          },
          "complete_backup_window_minutes": {
            "@@assign": "10080"
          }
        }
      }
    }
  }
}
```

```

    },
    "lifecycle": {
      "move_to_cold_storage_after_days": {
        "@@assign": "180"
      },
      "delete_after_days": {
        "@@assign": "270"
      },
      "opt_in_to_archive_for_supported_resources": {
        "@@assign": "false"
      }
    },
    "target_backup_vault_name": {
      "@@assign": "FortKnox"
    },
    "target_logically_air_gapped_backup_vault_arn": {
      "@@assign": "arn:aws:backup:$region:$account:backup-
vault:AirGappedVault"
    },
    "index_actions": {
      "resource_types": {
        "@@assign": [
          "EBS",
          "S3"
        ]
      }
    },
    "copy_actions": {
      "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
        "target_backup_vault_arn": {
          "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
        },
        "lifecycle": {
          "move_to_cold_storage_after_days": {
            "@@assign": "30"
          },
          "delete_after_days": {
            "@@assign": "120"
          },
          "opt_in_to_archive_for_supported_resources": {
            "@@assign": "false"
          }
        }
      }
    }
  }
}

```

```

        }
      },
      "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
        "target_backup_vault_arn": {
          "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
        },
        "lifecycle": {
          "move_to_cold_storage_after_days": {
            "@@assign": "30"
          },
          "delete_after_days": {
            "@@assign": "120"
          },
          "opt_in_to_archive_for_supported_resources": {
            "@@assign": "false"
          }
        }
      }
    }
  },
  "selections": {
    "tags": {
      "datatype": {
        "iam_role_arn": {
          "@@assign": "arn:aws:iam::$account:role/MyIamRole"
        },
        "tag_key": {
          "@@assign": "dataType"
        },
        "tag_value": {
          "@@assign": [
            "PII",
            "RED"
          ]
        }
      }
    }
  },
  "advanced_backup_settings": {
    "ec2": {
      "windows_vss": {

```

```

        "@@assign": "enabled"
      }
    }
  }
}

```

다른 정책이 상속되거나 계정에 연결되지 않은 경우 해당하는 각에 렌더링된 유효 정책은 다음 예제와 AWS 계정 같습니다. CRON 식은 백업을 한 시간에 한 번 실행합니다. 계정 ID 123456789012는 각 계정의 실제 계정 ID입니다.

```

{
  "plans": {
    "PII_Backup_Plan": {
      "regions": [
        "us-east-1",
        "ap-northeast-3",
        "eu-north-1"
      ],
      "rules": {
        "hourly": {
          "schedule_expression": "cron(0 0/1 ? * * *)",
          "start_backup_window_minutes": "60",
          "target_backup_vault_name": "FortKnox",
          "target_logically_air_gapped_backup_vault_arn": "arn:aws:backup:
$region:$account:backup-vault:AirGappedVault",
          "index_actions": {
            "resource_types": {
              "@@assign": [
                "EBS",
                "S3"
              ]
            }
          },
          "lifecycle": {
            "delete_after_days": "2",
            "move_to_cold_storage_after_days": "180",
            "opt_in_to_archive_for_supported_resources": "false"
          },
          "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {

```

```

        "target_backup_vault_arn": {
            "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
        },
        "lifecycle": {
            "delete_after_days": "28",
            "move_to_cold_storage_after_days": "180",
            "opt_in_to_archive_for_supported_resources": "false"
        }
    },
    "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
        "target_backup_vault_arn": {
            "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
        },
        "lifecycle": {
            "delete_after_days": "28",
            "move_to_cold_storage_after_days": "180",
            "opt_in_to_archive_for_supported_resources": "false"
        }
    }
}

},
"selections": {
    "tags": {
        "datatype": {
            "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
            "tag_key": "dataType",
            "tag_value": [
                "PII",
                "RED"
            ]
        }
    }
},
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": "enabled"
    }
}
}
}

```

```
}

```

예제 2: 상위 정책이 하위 정책과 병합

다음 예제에서는 상속된 상위 정책과 하위 정책이 상속되었거나 AWS 계정 병합에 직접 연결되어 유효 정책을 형성합니다.

상위 정책 – 이 정책은 조직의 루트 또는 모든 상위 OU에 연결할 수 있습니다.

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": { "@@append": [ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
      "rules": {
        "Hourly": {
          "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
          "start_backup_window_minutes": { "@@assign": "60" },
          "target_backup_vault_name": { "@@assign": "FortKnox" },
          "index_actions": {
            "resource_types": {
              "@@assign": [
                "EBS",
                "S3"
              ]
            }
          },
          "lifecycle": {
            "move_to_cold_storage_after_days": { "@@assign": "28" },
            "delete_after_days": { "@@assign": "180" },
            "opt_in_to_archive_for_supported_resources": { "@@assign":
"false" }
          },
          "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
              "target_backup_vault_arn" : {
                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
              },
              "lifecycle": {
                "move_to_cold_storage_after_days": { "@@assign":
"28" },
                "delete_after_days": { "@@assign": "180" },

```

```

        "opt_in_to_archive_for_supported_resources":
    { "@@assign": "false" }
    }
    }
    },
    "selections": {
        "tags": {
            "datatype": {
                "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                "tag_key": { "@@assign": "dataType" },
                "tag_value": { "@@assign": [ "PII", "RED" ] }
            }
        }
    }
}
}
}
}
}

```

하위 정책 – 이 정책은 상위 정책이 연결된 수준보다 낮은 수준에서 계정 또는 OU에 직접 연결할 수 있습니다.

```

{
    "plans": {
        "Monthly_Backup_Plan": {
            "regions": {
                "@@append": [ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "delete_after_days": { "@@assign": "365" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
"false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn" : {

```

```

    "@@assign" : "arn:aws:backup:us-east-1:$account:backup-vault:Default"
  },
  "lifecycle": {
    "move_to_cold_storage_after_days": { "@@assign":
      "30" },
    "delete_after_days": { "@@assign": "365" },
    "opt_in_to_archive_for_supported_resources":
      { "@@assign": "false" }
  }
}
}
},
"selections": {
  "tags": {
    "MonthlyDatatype": {
      "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/MyMonthlyBackupIamRole" },
      "tag_key": { "@@assign": "BackupType" },
      "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
    }
  }
}
}
}
}
}

```

최종 유효 정책 - 계정에 적용되는 유효 정책에는 각각 자체 규칙 집합과 규칙을 적용할 리소스 집합이 있는 두 개의 계획이 포함됩니다.

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
      "rules": {
        "hourly": {
          "schedule_expression": "cron(0 0/1 ? * * *)",
          "start_backup_window_minutes": "60",
          "target_backup_vault_name": "FortKnox",
          "index_actions": {
            "resource_types": {
              "@@assign": [
```



```

        "EBS",
        "S3"
    ]
}
},
"lifecycle": {
    "delete_after_days": "2",
    "move_to_cold_storage_after_days": "180",
    "opt_in_to_archive_for_supported_resources": { "@@assign":
"false" }
},
"copy_actions": {
    "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
        "target_backup_vault_arn" : {
            "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
        },
        "lifecycle": {
            "move_to_cold_storage_after_days": "28",
            "delete_after_days": "180",
            "opt_in_to_archive_for_supported_resources":
{ "@@assign": "false" }
        }
    }
}
},
"selections": {
    "tags": {
        "datatype": {
            "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
            "tag_key": "dataType",
            "tag_value": [ "PII", "RED" ]
        }
    }
}
},
"Monthly_Backup_Plan": {
    "regions": [ "us-east-1", "eu-central-1" ],
    "rules": {
        "monthly": {
            "schedule_expression": "cron(0 5 1 * ? *)",
            "start_backup_window_minutes": "480",

```

```

        "target_backup_vault_name": "Default",
        "lifecycle": {
            "delete_after_days": "365",
            "move_to_cold_storage_after_days": "30",
            "opt_in_to_archive_for_supported_resources": { "@@assign":
"false" }
        },
        "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                "target_backup_vault_arn": {
                    "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                },
                "lifecycle": {
                    "move_to_cold_storage_after_days": "30",
                    "delete_after_days": "365",
                    "opt_in_to_archive_for_supported_resources":
{ "@@assign": "false" }
                }
            }
        },
        "selections": {
            "tags": {
                "monthlydatatype": {
                    "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;role/
MyMonthlyBackupIamRole",
                    "tag_key": "BackupType",
                    "tag_value": [ "MONTHLY", "RED" ]
                }
            }
        }
    }
}

```

예제 3: 상위 정책이 하위 정책에 의한 모든 변경을 금지

다음 예제에서 상속된 상위 정책은 [하위 제어 연산자](#)를 사용하여 모든 설정을 강제 적용하고 하위 정책이 설정을 변경 또는 재정의하는 것을 금지합니다.

상위 정책 – 이 정책은 조직의 루트 또는 모든 상위 OU에 연결할 수 있습니다. 정책의 모든 노드에 "@@operators_allowed_for_child_policies": ["@none"]이 존재한다는 것은 하위 정책이 계획을 변경할 수 없음을 의미합니다. 또한 하위 정책은 유효 정책에 추가 계획을 추가할 수 없습니다. 이 정책은 연결된 OU 아래의 모든 OU 및 계정에 대해 유효한 정책이 됩니다.

```
{
  "plans": {
    "@@operators_allowed_for_child_policies": ["@none"],
    "PII_Backup_Plan": {
      "@@operators_allowed_for_child_policies": ["@none"],
      "regions": {
        "@@operators_allowed_for_child_policies": ["@none"],
        "@@append": [
          "us-east-1",
          "ap-northeast-3",
          "eu-north-1"
        ]
      },
    },
    "rules": {
      "@@operators_allowed_for_child_policies": ["@none"],
      "Hourly": {
        "@@operators_allowed_for_child_policies": ["@none"],
        "schedule_expression": {
          "@@operators_allowed_for_child_policies": ["@none"],
          "@@assign": "cron(0 0/1 ? * * *)"
        },
      },
      "start_backup_window_minutes": {
        "@@operators_allowed_for_child_policies": ["@none"],
        "@@assign": "60"
      },
      "target_backup_vault_name": {
        "@@operators_allowed_for_child_policies": ["@none"],
        "@@assign": "FortKnox"
      },
      "index_actions": {
        "@@operators_allowed_for_child_policies": ["@none"],
        "resource_types": {
          "@@assign": [
            "EBS",
            "S3"
          ]
        }
      }
    },
  },
}
```

```

        "lifecycle": {
            "@operators_allowed_for_child_policies": ["@none"],
            "move_to_cold_storage_after_days": {
                "@operators_allowed_for_child_policies": ["@none"],
                "@assign": "28"
            },
            "delete_after_days": {
                "@operators_allowed_for_child_policies": ["@none"],
                "@assign": "180"
            },
            "opt_in_to_archive_for_supported_resources": {
                "@operators_allowed_for_child_policies": ["@none"],
                "@assign": "false"
            }
        },
        "copy_actions": {
            "@operators_allowed_for_child_policies": ["@none"],
            "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                "@operators_allowed_for_child_policies": ["@none"],
                "target_backup_vault_arn": {
                    "@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault",
                    "@operators_allowed_for_child_policies": ["@none"]
                },
                "lifecycle": {
                    "@operators_allowed_for_child_policies": ["@none"],
                    "delete_after_days": {
                        "@operators_allowed_for_child_policies":
["@none"],
                        "@assign": "28"
                    },
                    "move_to_cold_storage_after_days": {
                        "@operators_allowed_for_child_policies":
["@none"],
                        "@assign": "180"
                    },
                    "opt_in_to_archive_for_supported_resources": {
                        "@operators_allowed_for_child_policies":
["@none"],
                        "@assign": "false"
                    }
                }
            }
        }
    }
}

```

```

    }
  },
  "selections": {
    "@operators_allowed_for_child_policies": ["@none"],
    "tags": {
      "@operators_allowed_for_child_policies": ["@none"],
      "datatype": {
        "@operators_allowed_for_child_policies": ["@none"],
        "iam_role_arn": {
          "@operators_allowed_for_child_policies": ["@none"],
          "@assign": "arn:aws:iam::$account:role/MyIamRole"
        },
        "tag_key": {
          "@operators_allowed_for_child_policies": ["@none"],
          "@assign": "dataType"
        },
        "tag_value": {
          "@operators_allowed_for_child_policies": ["@none"],
          "@assign": [
            "PII",
            "RED"
          ]
        }
      }
    }
  },
  "advanced_backup_settings": {
    "@operators_allowed_for_child_policies": ["@none"],
    "ec2": {
      "@operators_allowed_for_child_policies": ["@none"],
      "windows_vss": {
        "@assign": "enabled",
        "@operators_allowed_for_child_policies": ["@none"]
      }
    }
  }
}

```

최종 유효 정책 – 하위 백업 정책이 존재하면 해당 정책이 무시되고 상위 정책이 유효 정책이 됩니다.

```

{
  "plans": {
    "PII_Backup_Plan": {
      "regions": [
        "us-east-1",
        "ap-northeast-3",
        "eu-north-1"
      ],
      "rules": {
        "hourly": {
          "schedule_expression": "cron(0 0/1 ? * * *)",
          "start_backup_window_minutes": "60",
          "target_backup_vault_name": "FortKnox",
          "index_actions": {
            "resource_types": {
              "@assign": [
                "EBS",
                "S3"
              ]
            }
          },
          "lifecycle": {
            "delete_after_days": "2",
            "move_to_cold_storage_after_days": "180",
            "opt_in_to_archive_for_supported_resources": "false"
          },
          "copy_actions": {
            "target_backup_vault_arn": "arn:aws:backup:us-east-1:123456789012:backup-vault:secondary_vault",
            "lifecycle": {
              "move_to_cold_storage_after_days": "28",
              "delete_after_days": "180",
              "opt_in_to_archive_for_supported_resources": "false"
            }
          }
        }
      },
      "selections": {
        "tags": {
          "datatype": {
            "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
            "tag_key": "dataType",
            "tag_value": [

```

```

        "PII",
        "RED"
    ]
}
},
"advanced_backup_settings": {
    "ec2": {"windows_vss": "enabled"}
}
}
}
}

```

예제 4: 상위 정책이 하위 정책에 의한 한 백업 계획의 변경을 금지

다음 예제에서 상속된 상위 정책은 [하위 제어 연산자](#)를 사용하여 단일 계획의 설정을 강제 적용하고 하위 정책이 해당 설정을 변경 또는 재정의하는 것을 금지합니다. 하위 정책은 여전히 추가 계획을 추가할 수 있습니다.

상위 정책 – 이 정책은 조직의 루트 또는 모든 상위 OU에 연결할 수 있습니다. 이 예제는 plans 최상위 수준을 제외하고 모든 하위 상속 연산자가 차단된 이전 예제와 유사합니다. 이 수준에서 @@append 설정을 사용하면 하위 정책이 유효 정책의 모음에 다른 계획을 추가할 수 있습니다. 상속된 계획에 대한 변경 사항은 여전히 모두 차단됩니다.

명확성을 위해 계획 섹션은 잘렸습니다.

```

{
  "plans": {
    "@@operators_allowed_for_child_policies": ["@@append"],
    "PII_Backup_Plan": {
      "@@operators_allowed_for_child_policies": ["@none"],
      "regions": { ... },
      "rules": { ... },
      "selections": { ... }
    }
  }
}

```

하위 정책 – 이 정책은 상위 정책이 연결된 수준보다 낮은 수준에서 계정 또는 OU에 직접 연결할 수 있습니다. 이 하위 정책은 새 계획을 정의합니다.

명확성을 위해 계획 섹션은 잘렸습니다.

```
{
  "plans": {
    "MonthlyBackupPlan": {
      "regions": { ... },
      "rules": { ... },
      "selections": { ... }
    }
  }
}
```

최종 유효 정책 – 유효 정책에는 두 계획이 모두 포함됩니다.

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": { ... },
      "rules": { ... },
      "selections": { ... }
    },
    "MonthlyBackupPlan": {
      "regions": { ... },
      "rules": { ... },
      "selections": { ... }
    }
  }
}
```

예제 5: 하위 정책이 상위 정책의 설정을 재정의

다음 예제에서 하위 정책은 [값-설정\(value-setting\) 연산자](#)를 사용하여 상위 정책에서 상속된 설정 일부를 재정의합니다.

상위 정책 – 이 정책은 조직의 루트 또는 모든 상위 OU에 연결할 수 있습니다. 해당 작업을 금지하는 [하위 제어 연산자](#)가 없는 경우 기본 동작은 하위 정책에 @@assign, @@append 또는 @@remove를 허용하는 것이므로 하위 정책은 모든 설정을 재정의할 수 있습니다. 상위 정책에는 유효한 백업 계획에 필요한 모든 요소가 포함되어 있으므로 정책이 있는 그대로 상속되면 리소스가 성공적으로 백업됩니다.

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": {
        "@@append": [
```



```

        "us-east-1",
        "ap-northeast-3",
        "eu-north-1"
    ]
},
"rules": {
    "Hourly": {
        "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
        "start_backup_window_minutes": {"@@assign": "60"},
        "target_backup_vault_name": {"@@assign": "FortKnox"},
        "index_actions": {
            "resource_types": {
                "@@assign": [
                    "EBS",
                    "S3"
                ]
            }
        },
        "lifecycle": {
            "delete_after_days": {"@@assign": "2"},
            "move_to_cold_storage_after_days": {"@@assign": "180"},
            "opt_in_to_archive_for_supported_resources": {"@@assign":
false}
        },
        "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-vault:t2": {
                "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:t2"},
                "lifecycle": {
                    "move_to_cold_storage_after_days": {"@@assign": "28"},
                    "delete_after_days": {"@@assign": "180"},
                    "opt_in_to_archive_for_supported_resources":
{"@@assign": false}
                }
            }
        }
    },
    "selections": {
        "tags": {
            "datatype": {
                "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                "tag_key": {"@@assign": "dataType"},

```

```

        "tag_value": {
            "@assign": [
                "PII",
                "RED"
            ]
        }
    }
}

```

하위 정책 – 하위 정책에는 상속된 상위 정책과 달라야 하는 설정만 포함됩니다. 유효 정책으로 병합될 때 다른 필수 설정을 제공하는 상속된 상위 정책이 있어야 합니다. 그렇지 않으면 예상대로 리소스를 백업하지 않는 잘못된 백업 계획이 유효 백업 정책에 포함됩니다.

```

{
  "plans": {
    "PII_Backup_Plan": {
      "regions": {
        "@assign": [
          "us-west-2",
          "eu-central-1"
        ]
      },
      "rules": {
        "Hourly": {
          "schedule_expression": {"@assign": "cron(0 0/2 ? * * *)"},
          "start_backup_window_minutes": {"@assign": "80"},
          "target_backup_vault_name": {"@assign": "Default"},
          "lifecycle": {
            "move_to_cold_storage_after_days": {"@assign": "30"},
            "delete_after_days": {"@assign": "365"},
            "opt_in_to_archive_for_supported_resources": {"@assign":
false}
          }
        }
      }
    }
  }
}

```

최종 유효 정책 – 유효 정책에는 두 정책의 설정이 모두 포함되며 하위 정책이 제공하는 설정은 상위 정책에서 상속된 설정을 재정의합니다. 이 예제에서는 다음과 같이 변경됩니다.

- 리전 목록이 완전히 다른 목록으로 바뀝니다. 상속된 목록에 리전을 추가하려면 하위 정책에 @@assign 대신 @@append를 사용합니다.
- AWS Backup 는 시간당 대신 2시간마다를 수행합니다.
- AWS Backup 는 백업이 시작되는 데 60분이 아닌 80분을 허용합니다.
- AWS Backup 는 대신 Default 볼트를 사용합니다FortKnox.
- 백업을 콜드 스토리지로 이전 및 최종 삭제하기 위한 수명 주기가 모두 연장됩니다.

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": [
        "us-west-2",
        "eu-central-1"
      ],
      "rules": {
        "hourly": {
          "schedule_expression": "cron(0 0/2 ? * * *)",
          "start_backup_window_minutes": "80",
          "target_backup_vault_name": "Default",
          "index_actions": {
            "resource_types": {
              "@@assign": [
                "EBS",
                "S3"
              ]
            }
          },
          "lifecycle": {
            "delete_after_days": "365",
            "move_to_cold_storage_after_days": "30",
            "opt_in_to_archive_for_supported_resources": "false"
          },
          "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-vault:secondary_vault": {
```

```

    "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:secondary_vault"},
    "lifecycle": {
        "move_to_cold_storage_after_days": "28",
        "delete_after_days": "180",
        "opt_in_to_archive_for_supported_resources": "false"
    }
}
},
"selections": {
    "tags": {
        "datatype": {
            "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
            "tag_key": "dataType",
            "tag_value": [
                "PII",
                "RED"
            ]
        }
    }
}
}
}
}

```

예제 6: **tags** 블록을 사용하여 리소스 지정

다음 예제에는 tag_key = "env" 및 tag_value = "prod" 또는 인 모든 리소스가 포함됩니다. "gamma". 이 예제에서는 tag_key = "backup" 및 tag_value = "false"인 리소스를 제외합니다.

```
...
"selections":{
  "tags":{
    "selection_name":{
      "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/IAMRole"},
      "tag_key":{"@@assign": "env"},
      "tag_value":{"@@assign": ["prod", "gamma"]},
      "conditions":{
        "string_not_equals":{
          "condition_name1":{
```

```

        "condition_key": { "@@assign": "aws:ResourceTag/backup" },
        "condition_value": { "@@assign": "false" }
    }
}
},
...

```

예제 7: **resources** 블록을 사용하여 리소스 지정

다음은 **resources** 블록을 사용하여 리소스를 지정하는 예제입니다.

Example: Select all resources in my account

부울 로직은 IAM 정책에서 사용할 수 있는 것과 유사합니다. "resource_types" 블록은 부울 AND를 사용하여 리소스 유형을 결합합니다.

```

...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        }
    }
},
...

```

Example: Select all resources in my account, but exclude Amazon EBS volumes

부울 로직은 IAM 정책에서 사용할 수 있는 것과 유사합니다. "resource_types" 및 "not_resource_types" 블록은 부울을 사용하여 리소스 유형을 AND 결합합니다.

```

...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [

```

```

        "*"
      ]
    },
    "not_resource_types":{
      "@@assign": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    }
  }
},
...

```

Example: Select all resources tagged with "backup" : "true", but exclude Amazon EBS volumes

부울 로직은 IAM 정책에서 사용할 수 있는 것과 유사합니다. "resource_types" 및 "not_resource_types" 블록은 부울을 사용하여 리소스 유형을 AND 결합합니다. "conditions" 블록은 부울 AND를 사용합니다.

```

...
"resources":{
  "resource_selection_name":{
    "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
    "resource_types":{
      "@@assign": [
        "*"
      ]
    },
    "not_resource_types":{
      "@@assign": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    "conditions":{
      "string_equals":{
        "condition_name1":{
          "condition_key": { "@@assign":"aws:ResourceTag/backup"},
          "condition_value": { "@@assign":"true" }
        }
      }
    }
  }
},
...

```

Example: Select all Amazon EBS volumes and Amazon RDS DB instances tagged with both "backup" : "true" and "stage" : "prod"

부울 로직은 IAM 정책에서 사용할 수 있는 것과 유사합니다. "resource_types" 블록은 부울 AND를 사용하여 리소스 유형을 결합합니다. "conditions" 블록은 부울 AND를 사용하여 리소스 유형과 태그 조건을 결합합니다.

```
...
"resources":{
  "resource_selection_name":{
    "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
    "resource_types":{"
      "@@assign": [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:rds:*:*:db:*"
      ]
    },
    "conditions":{"
      "string_equals":{"
        "condition_name1":{
          "condition_key":{"@@assign":"aws:ResourceTag/backup"},
          "condition_value":{"@@assign":"true"}
        },
        "condition_name2":{
          "condition_key":{"@@assign":"aws:ResourceTag/stage"},
          "condition_value":{"@@assign":"prod"}
        }
      }
    }
  }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS instances tagged with "backup" : "true" but not "stage" : "test"

부울 로직은 IAM 정책에서 사용할 수 있는 것과 유사합니다. "resource_types" 블록은 부울 AND를 사용하여 리소스 유형을 결합합니다. "conditions" 블록은 부울 AND를 사용하여 리소스 유형과 태그 조건을 결합합니다.

```
...
"resources":{
```

```

    "resource_selection_name":{
      "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
      "resource_types":{
        "@@assign": [
          "arn:aws:ec2:*:*:volume/*",
          "arn:aws:rds:*:*:db:*"
        ]
      },
      "conditions":{
        "string_equals":{
          "condition_name1":{
            "condition_key":{"@@assign":"aws:ResourceTag/backup"},
            "condition_value":{"@@assign":"true"}
          }
        },
        "string_not_equals":{
          "condition_name2":{
            "condition_key":{"@@assign":"aws:ResourceTag/stage"},
            "condition_value":{"@@assign":"test"}
          }
        }
      }
    }
  },
  ...

```

Example: Select all resources tagged with "key1" and a value which begins with "include" but not with "key2" and value that contains the word "exclude"

부울 로직은 IAM 정책에서 사용할 수 있는 것과 유사합니다. "resource_types" 블록은 부울 AND를 사용하여 리소스 유형을 결합합니다. "conditions" 블록은 부울 AND를 사용하여 리소스 유형과 태그 조건을 결합합니다.

이 예제에서는 include*, *exclude*, arn:aws:rds:*:*:db:*에서 와일드카드 문자 (*)를 사용한다는 점에 유의하세요. 문자열의 시작, 끝, 중간에 와일드카드 문자 (*)를 사용할 수 있습니다.

```

...
"resources":{
  "resource_selection_name":{
    "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
    "resource_types":{
      "@@assign": [

```



```

        "*"
    ]
},
"conditions":{
    "string_like":{
        "condition_name1":{
            "condition_key":{"@@assign":"aws:ResourceTag/key1"},
            "condition_value":{"@@assign":"include*"}
        }
    },
    "string_not_like":{
        "condition_name2":{
            "condition_key":{"@@assign":"aws:ResourceTag/key2"},
            "condition_value":{"@@assign":"*exclude*"}
        }
    }
}
}
},
...

```

Example: Select all resources tagged with "backup" : "true" except Amazon FSx file systems and Amazon RDS resources

부울 로직은 IAM 정책에서 사용할 수 있는 것과 유사합니다. "resource_types" 및 "not_resource_types" 블록은 부울을 사용하여 리소스 유형을 AND 결합합니다. "conditions" 블록은 부울 AND를 사용하여 리소스 유형과 태그 조건을 결합합니다.

```

...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign":[
                "arn:aws:fsx:*:*:file-system/*",
                "arn:aws:rds:*:*:db:*"
            ]
        }
    },
    ...
}

```

```

    "conditions":{
      "string_equals":{
        "condition_name1":{
          "condition_key":{"@@assign":"aws:ResourceTag/backup"},
          "condition_value":{"@@assign":"true"}
        }
      }
    }
  },
  ...

```

예제 8: Amazon GuardDuty 맬웨어 보호 스캔을 사용한 백업 계획

다음 예제는 백업 복구 시점에서 Amazon GuardDuty 맬웨어 보호 스캔을 활성화하는 백업 정책을 보여줍니다. 이 정책은 규칙 `scan_actions`에서 사용하여 스캔을 활성화하고 계획 수준에서 `scan_settings`를 사용하여 스캐너를 구성합니다.

이 기능을 사용하려면 적절한 IAM 역할 권한이 있어야 합니다. 자세한 내용은 AWS Backup 개발자 안내서의 [액세스](#)를 참조하세요.

```

{
  "plans": {
    "Malware_Scan_Backup_Plan": {
      "regions": {
        "@@assign": [
          "us-east-1",
          "us-west-2"
        ]
      },
      "rules": {
        "Daily_With_Incremental_Scan": {
          "schedule_expression": {
            "@@assign": "cron(0 5 ? * * *)"
          },
          "start_backup_window_minutes": {
            "@@assign": "60"
          },
          "target_backup_vault_name": {
            "@@assign": "Default"
          },
          "lifecycle": {

```

```

        "delete_after_days": {
            "@@assign": "35"
        }
    },
    "scan_actions": {
        "GUARDDUTY": {
            "scan_mode": {
                "@@assign": "INCREMENTAL_SCAN"
            }
        }
    }
},
"Monthly_With_Full_Scan": {
    "schedule_expression": {
        "@@assign": "cron(0 5 1 * ? *)"
    },
    "start_backup_window_minutes": {
        "@@assign": "60"
    },
    "target_backup_vault_name": {
        "@@assign": "Default"
    },
    "lifecycle": {
        "delete_after_days": {
            "@@assign": "365"
        }
    },
    "scan_actions": {
        "GUARDDUTY": {
            "scan_mode": {
                "@@assign": "FULL_SCAN"
            }
        }
    }
},
"selections": {
    "tags": {
        "scan_selection": {
            "iam_role_arn": {
                "@@assign": "arn:aws:iam::$account:role/MyBackupRole"
            },
            "tag_key": {
                "@@assign": "backup"
            }
        }
    }
}

```

```

    },
    "tag_value": {
      "@@assign": [
        "true"
      ]
    }
  },
  "scan_settings": {
    "GUARDDUTY": {
      "resource_types": {
        "@@assign": [
          "EBS"
        ]
      },
      "scanner_role_arn": {
        "@@assign": "arn:aws:iam::${account}:role/MyGuardDutyScannerRole"
      }
    }
  }
}

```

이 예제의 핵심 사항은 다음과 같습니다.

- `scan_actions`는 각 규칙 내에 지정됩니다. 스캐너 이름은 키로 `GUARDDUTY` 사용됩니다. 일별 규칙은 `INCREMENTAL_SCAN` 사용하고 월별 규칙은 `FULL_SCAN`을 사용합니다.
- `scan_settings`는 계획 수준에서 지정됩니다(규칙 내부 아님). 스캔할 스캐너 역할과 리소스 유형을 구성합니다.
- `AWSBackupGuardDutyRolePolicyForScans` 관리형 정책이 연결된 IAM 역할과 `malware-protection.guardduty.amazonaws.com` 서비스 보안 주체가 역할을 수신히도록 허용하는 신뢰 정책을 참조해야 `scanner_role_arn` 합니다.

- 태그 정책

태그 정책을 사용하면 조직 계정의 AWS 리소스에 연결된 태그를 표준화할 수 있습니다.

태그 정책을 사용하여 태그 키와 태그 값의 기본 대소문자 처리를 포함한 태그를 일관적으로 유지 관리할 수 있습니다.

태그란 무엇입니까?

태그는 사용자가 할당하거나 AWS 리소스에 할당하는 AWS 사용자 지정 속성 레이블입니다. 각 태그는 두 부분으로 구성됩니다.

- 태그 키(예: CostCenter, Environment 또는 Project) 태그 키는 대/소문자를 구별합니다.
- 태그 값(예: 111122223333 또는 Production)으로 알려진 선택적 필드 태그 값을 생략하는 것은 빈 문자열을 사용하는 것과 같습니다. 태그 키처럼 태그 값은 대/소문자를 구별합니다.

이 페이지의 나머지 부분에서는 태그 정책에 대해 설명합니다. 태그에 대한 자세한 내용은 다음과 같은 소스를 참조하세요.

- 이름 지정 및 사용 규칙을 포함하여 태그 지정에 대한 일반적인 내용은 [AWS 리소스 태그 지정 사용 설명서를](#) 참조하세요.
- 태그 사용을 지원하는 서비스 목록은 [리소스 그룹 태깅 API 참조](#)를 참조하세요.
- 태그를 사용하여 리소스를 분류하는 방법에 대한 자세한 내용은 [AWS 리소스 태그 지정 모범 사례 백서를](#) 참조하세요.
- Organizations 리소스 태그 지정에 대한 자세한 내용은 [AWS Organizations 리소스 태그 지정](#) 단원을 참조하세요.
- 다른 리소스 태그 지정에 대한 자세한 내용은 해당 서비스의 설명서를 AWS 서비스 참조하세요.

태그 정책이란 무엇입니까?

태그 정책은 조직의 계정에 있는 리소스 전체에서 태그를 표준화하는 데 도움이 될 수 있는 정책의 한 유형입니다. 태그 정책에서 리소스에 태그를 지정할 때 리소스에 적용할 수 있는 태그 지정 규칙을 지정합니다.

예를 들어, 태그 정책은 CostCenter 태그가 리소스에 연결될 때 태그 정책에 정의된 대소문자 처리 및 태그 값을 사용해야 하도록 지정할 수 있습니다. 태그 정책은 지정된 리소스 유형에 대한 정책 미준수 태그 지정 작업이 적용되도록 지정할 수도 있습니다. 다시 말해서, 지정된 리소스 유형에 대한 정책 미준수 태그 지정 요청은 완료할 수 없습니다. 태그 없는 리소스 또는 태그 정책에서 정의되지 않은 태그는 태그 정책 준수 여부가 평가되지 않습니다.

태그 정책을 사용하려면 AWS 서비스 여러 작업을 수행해야 합니다.

- AWS Organizations를 사용하여 태그 정책을 관리합니다. 조직의 관리 계정에 로그인하고 Organizations를 사용하여 태그 정책 기능을 활성화합니다. 조직의 관리 계정에서 IAM 사용자로 로

그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다. 그런 다음 태그 정책을 생성하고 조직 엔터티에 연결하여 해당 태그 규칙을 적용할 수 있습니다.

- AWS Resource Groups를 사용하여 태그 정책 준수를 관리합니다. 조직의 계정에 로그인하고 Resource Groups를 사용하여 계정의 리소스에서 정책 미준수 태그를 찾습니다. 리소스를 생성한 AWS 서비스에서 규정 미준수 태그를 수정할 수 있습니다. [Tag Editor](#) 및 [Resource Groups Tagging API](#)를 사용하여 다중 서비스에서 리소스를 태그 지정하고 태그 해제할 수도 있습니다.

조직의 관리 계정에 로그인하면 조직의 모든 계정에 대한 정책 준수 정보를 볼 수 있습니다.

태그 정책은 [모든 기능이 활성화된](#) 조직에서만 사용할 수 있습니다. 태그 정책을 사용하는 데 필요한 항목에 대한 자세한 내용은 [에 대한 관리 정책의 사전 조건 및 권한 AWS Organizations](#) 단원을 참조하세요.

Important

태그 정책을 시작하려면 고급 태그 정책으로 이동 [태그 정책 시작하기](#)하기 전에에 설명된 예제 워크플로를 따르는 것이 AWS 좋습니다. 태그 정책을 전체 OU 또는 조직으로 확장하기 전에 간단한 태그 정책을 단일 계정에 연결하는 효과를 이해하는 것이 가장 좋습니다. 태그 정책 준수를 적용하기 전에 태그 정책의 효과를 이해하는 것이 특히 중요합니다. [태그 정책 시작하기](#) 페이지의 표에는 고급 정책 관련 작업에 대한 지침의 링크도 제공됩니다.

태그 정책 사용에 대한 모범 사례

AWS에서는 태그 정책 사용에 대한 다음 모범 사례를 권장합니다.

태그 대소문자 전략 결정

태그를 대문자로 전환하고 모든 리소스 유형에서 해당 정책을 일관적으로 구현하는 방법을 결정합니다. 예컨대, Costcenter, costcenter 또는 CostCenter를 사용할지 결정하고 모든 태그에 대해 동일한 규칙을 사용합니다. 정책 준수 보고서에서 일관된 결과를 얻으려면 일관되지 않은 대소문자 처리와 비슷한 태그를 사용하지 마세요. 이 전략은 조직의 태그 정책을 정의하는 데 도움이 됩니다.

권장 워크플로 사용

간단한 태그 정책을 생성하여 소규모로 시작합니다. 그런 다음 테스트용으로 사용할 수 있는 멤버 계정에 연결합니다. [태그 정책 시작하기](#)에서 설명하는 워크플로를 사용합니다.

태그 지정 규칙 결정

이 항목은 조직의 필요에 따라 결정됩니다. 예를 들어 CostCenter 태그가 AWS Secrets Manager 보안 암호에 연결될 때 지정된 대/소문자 처리를 사용하도록 지정할 수 있습니다. 정책 준수 태그를 정의하는 태그 정책을 생성하고 해당 태그 지정 규칙을 적용할 조직 엔터티에 태그 정책을 연결합니다.

계정 관리자 교육

태그 정책 사용을 확장할 준비가 되면 계정 관리자를 다음과 같이 교육합니다.

- 태그 지정 전략을 전달합니다.
- 관리자가 특정 리소스 유형에서 태그를 사용해야 한다는 점을 강조합니다.

태그가 없는 리소스는 정책 준수 결과에서 정책 미준수로 표시되지 않으므로 이렇게 하는 것이 중요합니다.

- 태그 정책 준수 확인에 대한 지침을 제공합니다. 리소스 태깅 사용 설명서의 계정에 [태그 지정 준수 평가에](#) 설명된 절차를 사용하여 계정의 리소스에서 규정 미준수 태그를 찾고 수정하도록 관리자에게 지시합니다. AWS 정책 준수 여부를 확인할 빈도를 관리자에게 알려줍니다.

정책 준수 적용 시 주의

정책 준수를 적용하면 조직의 계정에 있는 사용자가 필요한 리소스에 태그를 지정할 수 없습니다. [태그 지정 일관성 적용](#)의 정보를 검토합니다. [태그 정책 시작하기](#)에서 설명하는 워크플로도 참조합니다.

태그 지정 제한에 유의하세요.

AWS 서비스는 일반적으로 수정할 수 없는 사용자 정의 태그가 50개로 제한됩니다. 필수 태그 보고와 같은 기능을 사용할 때는 조직의 유효 정책이 특정 리소스 유형에 필요한 태그 50개를 초과하지 않도록 해야 합니다. 이 제한을 초과하면 두 가지 문제가 발생할 수 있습니다. 리소스는 규정 준수 요약에서 규정 준수 상태를 달성하지 못할 수 있으며, 코드형 인프라(IaC) 플랫폼은 필요에 따라 50개 이상의 태그가 정의될 때 리소스를 생성하지 못할 수 있습니다.

리소스 생성 요청에 대한 가드레일을 설정하는 SCP 생성 고려

태그가 연결되지 않은 리소스는 보고서에서 정책 미준수로 표시되지 않습니다. 계정 관리자는 여전히 태그 없는 리소스를 생성할 수 있습니다. 경우에 따라, SCP(서비스 제어 정책)를 사용하여 리소스 생성 요청에 대한 가드레일을 설정할 수 있습니다.

AWS 서비스가 태그를 사용하여 액세스 제어를 지원하는지 여부를 알아보려면 [AWS 서비스 IAM 사용 설명서의 IAM으로 작업하기를](#) 참조하세요. 태그 기반 권한 부여(ABAC) 열이 예로 표시된 서비스를 찾습니다. 서비스의 이름을 선택하여 해당 서비스에 대한 권한 부여 및 액세스 제어 문서를 봅니다.

태그 정책 시작하기

태그 정책을 사용하려면 여러 로 작업해야 합니다 AWS 서비스. 시작하려면 다음 페이지를 검토하세요. 그런 다음 이 페이지의 워크플로우에 따라 태그 정책 및 해당 효과에 대해 잘 알아두세요.

- [에 대한 관리 정책의 사전 조건 및 권한 AWS Organizations](#)
- [태그 정책 사용에 대한 모범 사례](#)

처음으로 태그 정책 사용

다음 단계에 따라 처음으로 태그 정책 사용을 시작합니다.

Task	로그인할 계정	AWS 사용할 서비스 콘솔
1단계: 조직에 대해 태그 정책을 활성화합니다.	조직의 관리 계정. ¹	AWS Organizations
2단계: 태그 정책을 생성합니다. 첫 번째 태그 정책을 간단하게 유지합니다. 사용할 대소문자 처리에 태그 키 하나를 입력하고 다른 모든 옵션은 기본값으로 둡니다.	조직의 관리 계정. ¹	AWS Organizations
3단계: 테스트에 사용할 수 있는 단일 멤버 계정에 태그 정책을 연결합니다. 다음 단계에서 이 계정에 로그인해야 합니다.	조직의 관리 계정. ¹	AWS Organizations
4단계: 정책 준수 태그가 있는 일부 리소스와 정책 미준수 태그가 있는 일부 리소스를 생성합니다.	테스트 용도로 사용하는 멤버 계정.	익숙한 모든 AWS 서비스. 예를 들어, AWS Secrets Manager 을 사용하고 기본 암호 생성 의 절차를 따라 정책 준

Task	로그인할 계정	AWS 사용할 서비스 콘솔
		수 암호 및 정책 미준수 암호를 포함한 암호를 생성합니다.
5단계: 유효 태그 정책을 보고 계정의 정책 준수 상태를 평가합니다.	테스트 용도로 사용하는 멤버 계정.	리소스 그룹 및 리소스가 생성된 AWS 서비스입니다. 정책 준수 태그와 정책 미준수 태그를 사용하여 리소스를 생성한 경우 결과에 정책 미준수 태그가 표시되어야 합니다.
6단계: 테스트 계정의 리소스가 태그 정책을 준수할 때까지 정책 준수 문제를 찾아서 수정하는 프로세스를 반복합니다.	테스트 용도로 사용하는 멤버 계정.	리소스 그룹 및 리소스가 생성된 AWS 서비스입니다.
언제든지 조직 전체의 정책 준수 여부를 평가 할 수 있습니다.	조직의 관리 계정. ¹	Resource Groups

¹ 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

태그 정책 사용 확장

다음 작업을 어떤 순서로든 수행하여 태그 정책 사용을 확장할 수 있습니다.

고급 작업	로그인할 계정	AWS 사용할 서비스 콘솔
고급 태그 정책을 생성합니다. 처음 사용자와 동일한 프로세스를 따르지만, 다른 작업을 시도해 봅니다. 예를 들어, 추가 키 또는 값을 정의하거나 태그 키에 다른 대소문자 처리를 지정합니다.	조직의 관리 계정. ¹	AWS Organizations

고급 작업	로그인할 계정	AWS 사용할 서비스 콘솔
관리 정책 상속에 대한 이해 및 태그 정책 구문 의 정보를 사용하여 더 세부적인 태그 정책을 생성할 수 있습니다.		
추가 계정 또는 OU에 태그 정책을 연결합니다. 추가 정책을 계정에 연결하거나 계정이 멤버로 속한 OU에 연결한 후 계정에 대한 유효 태그 정책 을 확인합니다.	조직의 관리 계정. ¹	AWS Organizations
다른 사람이 새 리소스를 생성할 때 태그를 반드시 사용하도록 하는 SCP를 생성합니다.	조직의 관리 계정. ¹	AWS Organizations
변경하는 동안 유효 태그 정책에 대해 계정의 정책 준수 상태를 계속 평가합니다. 정책 미준수 태그를 수정합니다.	유효한 태그 정책이 있는 멤버 계정.	리소스 그룹 및 리소스가 생성된 AWS 서비스입니다.
조직 전체의 정책 준수를 평가합니다.	조직의 관리 계정. ¹	Resource Groups

¹ 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

처음으로 태그 정책 적용

태그 정책을 처음 적용하려면 태그 정책을 처음 사용하는 것과 비슷한 워크플로우를 따르고 테스트 계정을 사용합니다.

Warning

정책 준수를 적용할 때는 주의하세요. 태그 정책 사용의 효과를 이해하고 권장 워크플로우를 따라야 합니다. 추가 계정으로 확장하기 전에 테스트 계정에서 적용이 어떻게 작동하는지 테스트

트합니다. 그렇지 않으면 조직의 계정에 있는 사용자가 필요한 리소스에 태그를 지정하지 못하도록 할 수 있습니다. 자세한 정보는 [태그 지정 일관성 적용](#) 섹션을 참조하세요.

적용 작업	로그인할 계정	AWS 사용할 서비스 콘솔
1단계: 태그 정책을 생성합니다. 첫 번째 적용된 태그 정책을 간단하게 유지합니다. 사용할 대소문자 처리에 태그 키 하나를 입력하고 이 태그에 대해 정책 미준수 작업 금지 옵션을 선택합니다. 그런 다음 적용할 리소스 유형 하나를 지정합니다. 이전의 예제를 계속 사용하여 Secrets Manager 암호에 태그 정책을 적용하도록 선택할 수 있습니다.	조직의 관리 계정. ¹	AWS Organizations
2단계: 단일 테스트 계정에 태그 정책을 연결합니다.	조직의 관리 계정. ¹	AWS Organizations
3단계: 정책 준수 태그가 있는 일부 리소스와 정책 미준수 태그가 있는 일부 리소스를 생성해 봅니다. 정책 미준수 태그를 사용하여 태그 정책에서 지정된 유형의 리소스에 태그를 생성할 수 없습니다.	테스트 용도로 사용하는 멤버 계정.	익숙한 모든 AWS 서비스. 예를 들어, AWS Secrets Manager 를 사용하고 기본 암호 생성 의 절차를 따라 정책 준수 암호 및 정책 미준수 암호를 포함한 암호를 생성합니다.
4단계: 유효 태그 정책에 대해 계정의 정책 준수 상태를 평가하고 정책 미준수 태그를 수정합니다.	테스트 용도로 사용하는 멤버 계정.	리소스 그룹 및 리소스가 생성된 AWS 서비스입니다.

적용 작업	로그인할 계정	AWS 사용할 서비스 콘솔
5단계: 테스트 계정의 리소스가 태그 정책을 준수할 때까지 정책 준수 문제를 찾아서 수정하는 프로세스를 반복합니다.	테스트 용도로 사용하는 멤버 계정.	리소스 그룹 및 리소스가 생성된 AWS 서비스입니다.
언제든지 조직 전체의 정책 준수 여부를 평가 할 수 있습니다.	조직의 관리 계정. ¹	Resource Groups

¹ 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

보고서 태그 지정 규정 준수

태그 정책은 "기본 규정 준수 규칙" 및 "필수 태그 키"에 대한 보고 모드를 제공합니다. 이 모드를 사용하여 조직의 계정이 유효한 태그 정책을 준수하는지 평가할 수 있습니다. 생성된 보고서에는 수명 주기의 어느 시점에서든 사용자 정의 태그가 하나 이상 있는 리소스만 포함됩니다.

Important

태그가 지정되지 않은 리소스는 결과에 규정 미준수로 표시되지 않습니다.

계정에서 태그가 지정되지 않은 리소스를 찾으려면 쿼리와 함께 AWS Resource Explorer를 사용합니다tag:none. 자세한 내용은 AWS Resource Explorer 사용 설명서의 [태그가 지정되지 않은 리소스 검색](#)을 참조하세요.

주제

- ["기본 규정 준수 규칙" 보고](#)
- ["필수 태그 키" 보고](#)
- [조직 전체의 정책 준수 보고서 생성](#)

"기본 규정 준수 규칙" 보고

기본 규정 준수 규칙에 대한 보고를 통해 대문자 및 허용된 태그 값에 대한 규정 준수를 확인하는 태그 지정 규정 준수 보고서를 생성할 수 있습니다.

보고하려면

시각적 편집기 탭에서 규정 준수를 보고하려는 태그 키의 값을 입력합니다. 아래 스크린샷은 "CostCenter" 태그 키에 대한 고객 규정 준수 보고서를 보여줍니다. 이 예제에서 보고서는 태그가 지정된 리소스가 "CostCenter" 태그 키의 소문자 값만 일치하는 경우 준수로 강조 표시합니다. 즉, 문자열은 "costcenter"와 같습니다.

Visual editor | JSON | Policy size: 127 / 10000 characters | [Tag policies syntax reference](#)

▼ **CostCenter** Remove tag key

Tag key

CostCenter

▼ **Basic compliance rules**

Capitalization

☒ Use the capitalization that you've specified above for the tag key.
By default, tag key capitalization is inherited from the parent policy. If the parent policy does not exist or does not specify capitalization, then an all-lowercase tag key is considered compliant. [Learn more](#)

Allowed values

☐ Specify allowed values for this tag key.
Only specified values are allowed for the tag key, including the specified capitalization. [Learn more](#)

Resource types enforcement

☐ Prevent noncompliant operations for this tag.
By default, enforcement details are inherited from the parent policy. To enforce compliance on specific resource types not listed in the parent policy, select this option and then specify the resource types. [Learn more](#)

아래 JSON은 "CostCenter" 태그 키의 소문자 값을 기준으로 리소스에 대한 규정 준수 보고서를 생성합니다.

```
{
  "tags": {
    "CostCenter": {}
  }
}
```

대소문자를 보고하려면

시각적 편집기 탭에서 규정 준수를 보고하려는 태그 키의 값을 입력하고 대문자화 옵션을 선택합니다. 아래 스크린샷은 대문자로 된 "CostCenter" 태그 키에 대한 고객 규정 준수 보고서를 보여줍니다. 이 예

제에서 보고서는 태그가 지정된 리소스가 "CostCenter" 태그 키와 정확히 일치하는 경우 규정을 준수하는 것으로 강조 표시합니다.

Visual editor
JSON
Policy size: 61 / 10000 characters
[Tag policies syntax reference](#)

▼ CostCenter
Remove tag key

Tag key

CostCenter

▼ Basic compliance rules

Capitalization

☒ Use the capitalization that you've specified above for the tag key.

By default, tag key capitalization is inherited from the parent policy. If the parent policy does not exist or does not specify capitalization, then an all-lowercase tag key is considered compliant. [Learn more](#)

Allowed values

☐ Specify allowed values for this tag key.

Only specified values are allowed for the tag key, including the specified capitalization. [Learn more](#)

Resource types enforcement

☐ Prevent noncompliant operations for this tag.

By default, enforcement details are inherited from the parent policy. To enforce compliance on specific resource types not listed in the parent policy, select this option and then specify the resource types. [Learn more](#)

아래 JSON은 대문자로 된 "CostCenter" 태그 키에 대한 리소스에 대한 규정 준수 보고서를 생성합니다.

```
{
  "tags": {
    "CostCenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      }
    }
  }
}
```

대문자로 허용된 태그 값을 보고하려면

시각적 편집기 탭에서 규정 준수를 보고하려는 태그 키의 값을 입력하고 허용된 값 옵션을 선택한 다음 허용된 태그 값의 값을 입력합니다. 아래 스크린샷은 대문자 및 허용된 태그 값이 있는 "CostCenter" 태그 키에 대한 고객 규정 준수 보고서를 보여줍니다. 이 예제에서 보고서는 태그가 지정된 리소스가

"CostCenter" 태그 키와 정확히 일치하는 문자열이고 태그 값이 "HR" 또는 "Legal"인 경우 규정을 준수하는 것으로 강조 표시합니다.

Visual editor

JSON

Policy size: 101 / 10000 characters | [Tag policies syntax reference](#)

▼ CostCenter

Remove tag key

Tag key

CostCenter

▼ Basic compliance rules

Capitalization

☒ Use the capitalization that you've specified above for the tag key.
 By default, tag key capitalization is inherited from the parent policy. If the parent policy does not exist or does not specify capitalization, then an all-lowercase tag key is considered compliant. [Learn more](#)

Allowed values

☒ Specify allowed values for this tag key.
 Only specified values are allowed for the tag key, including the specified capitalization. [Learn more](#)

Edit values

HR

Legal

Resource types enforcement

☐ Prevent noncompliant operations for this tag.
 By default, enforcement details are inherited from the parent policy. To enforce compliance on specific resource types not listed in the parent policy, select this option and then specify the resource types. [Learn more](#)

아래 JSON은 대문자와 허용된 태그 값 "HR" 및 "법적"이 있는 "CostCenter" 태그 키에 대한 리소스에 대한 규정 준수 보고서를 생성합니다.

```
{
  "tags": {
    "CostCenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "HR",
          "Legal"
        ]
      }
    }
  }
}
```

```

    }
  }
}
```

"필수 태그 키" 보고

⚠ Warning

AWS Resource Groups 콘솔은 현재 계정에 대한 규정 준수를 평가할 때 필요한 태그 키에 대한 보고를 지원하지 않습니다. 필수 태그 키가 누락된 규정 미준수 리소스는 규정 미준수 태그가 있는 리소스 섹션에 표시되지 않으며 계정을 규정 미준수로 표시하지 않습니다. 대신 조직 전체의 규정 준수 보고서를 사용하여 필수 태그 키가 누락된 규정 미준수 리소스를 찾습니다.

필수 태그 키에 대한 보고를 통해 리소스 생성 작업에 필수 또는 필수 태그 키가 누락되었는지 평가할 수 있습니다. CLI에서 다음 명령을 실행하여 계정의 유효 태그 정책에 정의된 필수 태그 키를 나열합니다. 이 정보를 사용하여 계정 관리자가 정의한 모든 필수 태그로 리소스를 생성하고 있는지 수동으로 확인할 수 있습니다.

```
$ aws resourcegroupstaggingapi list-required-tags
```

필요한 태그 키를 보고하려면

시각적 편집기 탭에서 규정 준수를 보고하려는 태그 키의 값을 입력하고 보고에 필요한 태그 표시 옵션을 선택합니다. 아래 스크린샷은 필수 태그 키에 대한 대소문자 및 보고가 포함된 "CostCenter" 태그 키에 대한 고객 규정 준수 보고서를 보여줍니다. 이 예제에서 보고서는 정확한 문자열 "CostCenter"를 태그 키로 포함하는 경우 태그가 지정된 리소스를 규정 준수로 강조 표시합니다.

⚠ Important

보고 옵션이 정확한 필수 태그가 누락된 선택한 리소스 유형에 대한 보고서를 생성하려면 필요에 따라 대문자화 및 마크 태그를 모두 선택해야 합니다. 예를 들어 "CostCenter" 태그 키와 정확히 일치하는지 확인하려고 할 때 두 옵션을 모두 사용합니다.

보고에 필요한 태그 표시 옵션만 선택하여 필수 태그가 누락된 선택한 리소스 유형의 보고서를 생성할 수 있습니다. 이 시나리오에서 생성된 보고서는 리소스에 "CostCenter", "costCenter", "Costcenter", "costcenter" 또는 이와 유사한 변형이 있는 경우 리소스를 규정 준수로 표시합니다. 이 기능을 사용하면 계정에서 태그가 지정된 모든 리소스 대신 선택한 리소스 유형에 대한 규정 준수 보고서를 생성할 수 있습니다.

대문자화만 선택하면 태그가 지정된 모든 리소스에 대한 보고서가 생성되고 태그 키의 문자열이 정확히 일치하지 않는 경우 해당 리소스가 규정 미준수로 표시됩니다.

Visual editor
JSON
Policy size: 122 / 10000 characters
[Tag policies syntax reference](#)

▼ CostCenter
Remove tag key

Tag key

CostCenter

▼ Basic compliance rules

Capitalization
☒ Use the capitalization that you've specified above for the tag key.
By default, tag key capitalization is inherited from the parent policy. If the parent policy does not exist or does not specify capitalization, then an all-lowercase tag key is considered compliant. [Learn more](#)

Allowed values
☐ Specify allowed values for this tag key.
Only specified values are allowed for the tag key, including the specified capitalization. [Learn more](#)

Resource types enforcement
☐ Prevent noncompliant operations for this tag.
By default, enforcement details are inherited from the parent policy. To enforce compliance on specific resource types not listed in the parent policy, select this option and then specify the resource types. [Learn more](#)

▼ Required tag key New
☒ Mark tag key as required for reporting.
Track compliance for this tag key across your resources. Resources missing this tag key will appear in compliance reports. Activate the CloudFormation hook 'AWS::TagPolicies::TaggingComplianceValidator' to block IaC resource creation if the specified resource types are missing this tag key.

AWS will return required tag information to validate your infrastructure deployments using infrastructure as code (IaC) tools such as CloudFormation, Terraform, and Pulumi.

Clear all

Select supported resource types

ec2:ALL_SUPPORTED ✕

아래 JSON은 보고에 필요한 대로 대문자 및 마크 태그가 있는 "CostCenter" 태그 키에 대한 리소스에 대한 규정 준수 보고서를 생성합니다.

```
{
  "tags": {
    "CostCenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "report_required_tag_for": {
        "@@assign": [
          "ec2:ALL_SUPPORTED"
        ]
      }
    }
  }
}
```

```

    }
  }
}

```

적용하려면

Terraform CloudFormation 및 Pulumi와 같은 IaC 도구와 함께 보고를 사용하여 개발자에게 경고하거나 필수 태그가 누락된 배포를 차단할 수 있습니다. 이제 CloudFormation Terraform 및 Pulumi에서 작동하는 하나의 유효 태그 정책을 사용할 수 있습니다. 자세한 내용은 [IaC로 "필수 태그 키" 적용을](#) 참조하세요.

조직 전체의 정책 준수 보고서 생성

언제든지 조직 AWS 계정 전체의에서 태그가 지정된 모든 리소스를 나열하는 보고서를 생성할 수 있습니다. 보고서에는 각 리소스가 유효 태그 정책을 준수하는지 여부가 표시됩니다. 태그 정책 또는 리소스에 대한 변경 사항이 조직 전체의 정책 준수 보고서에 반영되려면 최대 48시간까지 걸릴 수 있습니다. 예를 들어 리소스 유형에 대해 표준화된 새 태그를 정의하는 태그 정책이 있는 경우이 태그가 없는 해당 유형의 리소스는 최대 48시간 동안 보고서에 규정을 준수하는 것으로 표시됩니다.

Amazon S3 버킷에 대한 액세스 권한이 있는 경우 us-east-1 리전에 있는 조직의 관리 계정에서 보고서를 생성할 수 있습니다. 버킷에는 [보고서 저장을 위한 Amazon S3 버킷 정책](#)에 표시된 것과 같은 연결된 버킷 정책이 있어야 합니다. 보고서를 생성하려면 다음 명령을 실행합니다.

```
$ aws resourcegroupstaggingapi start-report-creation --region us-east-1
```

한 번에 하나의 보고서를 생성할 수 있습니다.

이 보고서를 완료하려면 약간 시간이 걸릴 수 있습니다. 다음 명령을 실행하여 상태를 확인할 수 있습니다.

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
  "Status": "SUCCEEDED"
}
```

위의 명령에서 SUCCEEDED가 반환되면 Amazon S3 버킷에서 보고서를 열 수 있습니다.

태그 지정 일관성 적용

태그 정책은 AWS 환경 전체에서 태그 지정 일관성을 적용하는 데 도움이 되는 "기본 규정 준수 규칙"과 "필수 태그 키"라는 두 가지 기능을 제공합니다. 적용 및 보고라는 두 가지 태그 정책 모드에서 이

러한 기능을 사용할 수 있습니다. 이 섹션에서는 두 기능에 대한 적용 모드를 강조합니다. 두 기능의 보고 모드에 대한 자세한 내용은 "태깅 규정 준수 보고"를 참조하세요.

주제

- ["기본 규정 준수 규칙"에 적용](#)
- [모범 사례](#)
- [IaC를 사용하여 "필수 태그 키" 적용](#)
- [태그 정책 구문 및 예제](#)

"기본 규정 준수 규칙"에 적용

기본 규정 준수 규칙을 적용하면 태그 정책에 지정된 요구 사항을 충족하지 않는 태그 값을 사용하여 리소스 생성을 방지할 수 있습니다. 예를 들어 제공된 'CostCenter' 태그 키에 'Business' 또는 'Legal' 태그 값이 없는 경우 Amazon EC2 생성 작업을 차단하는 정책을 정의할 수 있습니다. 기본 규정 준수 규칙을 사용하면 태그 키의 대소문자를 기준으로 적용을 적용할 수도 있습니다. 대문자를 활성화하면 태그 키가 정확히 문자열과 일치합니다. 대문자화는 "CostCenter", "costCenter" 및 "Costcenter"를 고유한 태그 키로 취급합니다. 즉, 태그 키 적용은 대/소문자를 구분합니다. 대문자 적용은 팀이 실수로 태그 변형을 생성하는 것을 방지합니다. 태그 지정 일관성은 리소스 액세스 권한을 부여하거나 거부하기 위해 정확한 태그 일치에 의존하는 비용 추적 정확도와 속성 기반 액세스 제어(ABAC) 보안 정책 모두에 중요합니다.

Important

기본 규정 준수 규칙은 태그 없이 생성된 리소스에 대해 태그 규정 준수를 적용하지 않습니다. 이 기능은 누락된 태그 키를 적용하지 않습니다. 이 기능을 사용하여 리소스 생성 시 필수 또는 필수 태그 키가 구성되어 있는지 확인할 수 없습니다. "필수 태그 키"에서 보고 모드를 사용하여 CloudFormation Terraform 및 Pulumi와 같은 IaC 도구에서 생성된 리소스에 필요한 태그 키를 적용합니다. SCPs 사용하면 요청에 지정된 태그가 포함되지 않은 경우 대상 계정의 IAM 사용자 및 역할이 특정 리소스 유형을 생성하지 못하도록 할 수 있습니다.

태그 정책에 기본 규정 준수 규칙을 적용하려면 [태그 정책을 생성할](#) 때 다음 중 하나를 수행합니다.

- 시각적 편집기 탭에서 이 태그에 대한 규정 미준수 작업 방지 옵션을 선택합니다. [태그 정책을 작성하고 연결하는 방법에 대한 단계는 태그 정책 생성](#) 섹션을 참조하세요.
- JSON 탭에서 enforced_for 필드를 사용합니다. 태그 정책 구문에 대한 자세한 내용은 [태그 정책 구문 및 예제](#) 단원을 참조하세요.

아래 이미지는 시각적 편집기 탭의 콘솔 환경을 보여줍니다. 이 예제에서 고객은 태그 정책에서 지원하는 Amazon EC2 리소스 유형에 대해서만 태그 값 검증을 적용하는 태그 정책을 정의하고 있습니다. 이 정책은 Amazon EC2 리소스 유형에 대해 제공된 태그 키가 "CostCenter"일 때 태그 값이 "Legal" 또는 "HR"인지 확인합니다. 또한 이 정책은 대문자를 적용합니다. 즉, 정책이 "CostCenter" 태그 키와 정확히 일치하는 문자열을 찾고 있음을 의미합니다.

Visual editor
JSON
Policy size: 253 / 10000 characters | [Tag policies syntax reference](#)

▼ CostCenter
Remove tag key

Tag key

CostCenter

▼ Basic compliance rules

Capitalization

☒ Use the capitalization that you've specified above for the tag key.

By default, tag key capitalization is inherited from the parent policy. If the parent policy does not exist or does not specify capitalization, then an all-lowercase tag key is considered compliant. [Learn more](#)

Allowed values

☒ Specify allowed values for this tag key.

Only specified values are allowed for the tag key, including the specified capitalization. [Learn more](#)

Edit values

HR

Legal

Resource types enforcement

☒ Prevent noncompliant operations for this tag.

By default, enforcement details are inherited from the parent policy. To enforce compliance on specific resource types not listed in the parent policy, select this option and then specify the resource types. [Learn more](#)

AWS will reject noncompliant requests to tag new resources including tagging resources upon creation.

Select all wildcards | Select all | Clear all

Select supported resource types
▼

ec2:ALL_SUPPORTED ✕

아래 JSON은 위의 "CostCenter" 예제에서 생성된 태그 정책입니다.

- 태그 정책

313

⚠ Important

태그 정책을 처음 정의할 때는 시각적 편집기를 사용하는 것이 좋습니다. 시각적 편집기는 추가 단계 없이 태그 정책 구문이 유효한지 확인하고 태그 정책을 정의할 수 있는 간소화된 클릭 환경을 제공합니다. 시각적 편집기 또는 JSON 탭을 사용하여 태그 정책을 정의할 수 있습니다.

```
{
  "tags": {
    "CostCenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "HR",
          "Legal"
        ]
      },
      "enforced_for": {
        "@@assign": [
          "ec2:ALL_SUPPORTED"
        ]
      }
    }
  }
}
```

모범 사례

태그 정책을 사용하여 "기본 규정 준수 규칙" 및 "IaC에 필수 태그 키"를 적용하려면 다음 모범 사례를 따르세요.

- 규정 준수를 적용할 때 주의 - 태그 정책 사용의 영향을 이해하고에 설명된 권장 워크플로를 따르세요 [태그 정책 시작하기](#). 더 많은 계정 또는 조직 단위로 확장하기 전에 테스트 계정에서 적용이 어떻게 작동하는지 테스트합니다. 그렇지 않으면 조직 계정의 사용자가 필요한 리소스를 생성하지 못하도록 할 수 있습니다.

- 적용할 수 있는 리소스 유형에 유의 - [지원되는 리소스 유형](#)에 대해서만 태그 정책 준수를 적용할 수 있습니다. 시각적 편집기를 사용하여 태그 정책을 빌드할 때 정책 준수 적용을 지원하는 리소스 유형이 나열됩니다.
- 일부 서비스와의 상호 작용 이해 - 일부 AWS 서비스에는 자동으로 리소스를 생성하고 한 서비스의 리소스에서 다른 서비스로 태그를 전파하는 컨테이너와 같은 리소스 그룹이 있습니다. 예를 들어 Amazon EC2 그룹 및 Amazon EMR 클러스터의 태그는 포함된 Amazon EC2 인스턴스로 자동으로 전파될 수 있습니다. 그룹 또는 Amazon EMR 클러스터보다 더 엄격한 Amazon EC2에 대한 태그 정책이 있을 수 있습니다. 적용을 활성화하면 태그 정책에 따라 리소스에 태그가 지정되지 않으며 동적 조정 및 프로비저닝이 차단될 수 있습니다.

다음 단원에서는 정책 미준수 리소스를 찾아서 올바르게 수정하는 방법을 보여 줍니다.

• [태그 지정 불일치 식별 및 해결](#)

IaC를 사용하여 "필수 태그 키" 적용

태그 정책은 코드형 인프라(IaC) 배포 전반에서 일관된 태그 지정을 유지하는 데 도움이 됩니다. "필수 태그 키"를 사용하면 Terraform CloudFormation 및 Pulumi와 같은 IaC 도구를 통해 생성된 모든 리소스에 조직에서 정의한 필수 태그가 포함되도록 할 수 있습니다.

이 기능은 리소스를 생성하기 전에 조직의 태그 정책을 기준으로 IaC 배포를 확인합니다. 배포에 필수 태그가 없는 경우 개발 팀에 경고하거나 배포를 완전히 방지하도록 IaC 설정을 구성할 수 있습니다. 이 선제적 접근 방식은 나중에 수동 수정을 요구하지 않고 리소스가 생성되는 순간부터 태그 지정 규정 준수를 유지합니다. 적용은 단일 태그 정책 정의를 사용하여 여러 IaC 도구에서 작동하므로 조직에서 사용하는 각 도구에 대해 별도의 태그 지정 규칙을 구성할 필요가 없습니다.

주제

- [를 사용하여 적용 CloudFormation](#)
- [Terraform으로 적용](#)
- [Pulumi로 적용](#)

를 사용하여 적용 CloudFormation

Note

에서 필수 태그 키를 적용하려면 태그 정책에서 리소스 유형에 필요한 태그를 지정 CloudFormation해야 합니다. 자세한 내용은 [the section called “필수 태그 키” 보고](#) 섹션을 참조하세요.

AWS다음을 위한 실행 역할 설정::TagPolicies::TaggingComplianceValidator 후크

AWS::TagPolicies::TaggingComplianceValidator 후크를 활성화하기 전에 후크가 AWS 서비스에 액세스하는 데 사용하는 실행 역할을 생성해야 합니다. 역할에는 다음과 같은 신뢰 정책이 연결되어 있어야 합니다.

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

실행 역할에는 최소한 다음 권한이 있는 역할 정책도 있어야 합니다.

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

```

        "tag:ListRequiredTags"
      ],
      "Resource": "*"
    }
  ]
}

```

퍼블릭 확장을 위한 실행 역할 설정에 대한 자세한 내용은 CloudFormation 사용 설명서의 [IAM 권한을 사용하여 실행 역할 구성 및 퍼블릭 확장 액세스를 위한 신뢰 정책을 참조](#)하세요.

AWS::TagPolicies::TaggingComplianceValidator 후크 활성화

Important

계속하기 전에 후크 작업에 필요한 권한이 있는지 확인하고 CloudFormation 콘솔에서 사전 예방적 제어를 확인합니다. 자세한 내용은 [CloudFormation 후크에 대한 IAM 권한 부여를 참조](#)하세요.

태그 정책을 업데이트한 후에는 필요한 태그 지정 규정 준수를 적용하려는 모든 AWS 계정 및 리전에서 AWS::TagPolicies::TaggingComplianceValidator 후크를 활성화해야 합니다.

이 AWS관리형 후크는 다음 두 가지 모드로 구성할 수 있습니다.

- 경고 모드: 배포를 진행하도록 허용하지만 필수 태그가 누락된 경우 경고를 생성합니다.
- 실패 모드: 필수 태그가 누락된 배포를 차단합니다.

AWS CLI를 사용하여 후크를 활성화하려면

```

aws cloudformation activate-type \
  --type HOOK \
  --type-name AWS::TagPolicies::TaggingComplianceValidator \
  --execution-role-arn arn:aws:iam::123456789012:role/MyHookExecutionRole \
  --publisher-id aws-hooks \
  --region us-east-1

```

```

aws cloudformation set-type-configuration \
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":
{"HookInvocationStatus": "ENABLED", "FailureMode": "WARN", "TargetOperations":
["STACK"], "Properties":{}}}}' \

```



```
--type-arn "arn:aws:cloudformation:us-east-1:123456789012:type/hook/AWS-TagPolicies-TaggingComplianceValidator" \
--region us-east-1
```

를 대상 AWS 리전region으로 바꾸고 경고 모드를 원하는 "FailureMode":"WARN" 경우를 "FailureMode":"FAIL"로 변경합니다.

CloudFormation StackSets를 사용하여 여러 계정 및 리전에서
AWS::TagPolicies::TaggingComplianceValidator 후크 활성화

AWS 계정이 여러 개인 조직의 경우 AWS CloudFormation StackSets를 사용하여 모든 계정과 리전에서 태깅 규정 준수 후크를 동시에 활성화할 수 있습니다.

CloudFormation StackSets를 사용하면 단일 작업으로 여러 계정 및 리전에 동일한 CloudFormation 템플릿을 배포할 수 있습니다. 이 접근 방식을 사용하면 각 계정에서 수동으로 구성할 필요 없이 AWS 조직 전체에서 일관된 태그 지정에 적용할 수 있습니다.

이를 위해 CloudFormation StackSets를 사용하려면:

1. 태그 지정 규정 준수 후크를 활성화하는 CloudFormation 템플릿 생성
2. CloudFormation StackSets를 사용하여 템플릿을 배포하여 조직 단위 또는 특정 계정을 대상으로 지정
3. 적용을 활성화하려는 모든 리전 지정

CloudFormation StackSets 배포는 지정된 모든 계정 및 리전에서 활성화 프로세스를 자동으로 처리하여 조직 전체에서 균일한 태그 지정 규정 준수를 보장합니다. 서비스 관리형StackSets를 사용하여 조직에 CloudFormation 후크를 배포하는 방법을 알아보려면 [AWS 블로그](#)를 참조하세요.

CloudFormation StackSets

CloudFormation StackSets를 사용하여 아래 CloudFormation 템플릿을 배포하여 조직의 계정에 대해 AWS::TagPolicies::TaggingComplianceValidator 후크를 활성화합니다.

Important

이 후크는 StackHook로만 작동합니다. 리소스 후크로 사용할 때는 효과가 없습니다.

Resources:

```
# Activate the AWS-managed hook type
```

```

HookTypeActivation:
  Type: AWS::CloudFormation::TypeActivation
  Properties:
    AutoUpdate: True
    PublisherId: "AWS"
    TypeName: "AWS::TagPolicies::TaggingComplianceValidator"

# Configure the hook
HookTypeConfiguration:
  Type: AWS::CloudFormation::HookTypeConfig
  DependsOn: HookTypeActivation
  Properties:
    TypeName: "AWS::TagPolicies::TaggingComplianceValidator"
    TypeArn: !GetAtt HookTypeActivation.Arn
    Configuration: !Sub |
      {
        "CloudFormationConfiguration": {
          "HookConfiguration": {
            "TargetStacks": "ALL",
            "TargetOperations": ["STACK"],
            "Properties": {},
            "FailureMode": "Warn",
            "TargetFilters": {
              "Actions": [
                "CREATE",
                "UPDATE"
              ]
            }
          }
        }
      }

```

Note

CloudFormation 후크 실행에 대한 자세한 내용은 [계정에서 사전 예방적 제어 기반 후크 활성화](#)를 참조하세요.

Terraform으로 적용

Terraform에서 필수 태그 키를 적용하려면 Terraform AWS 공급자를 6.22.0 이상으로 업데이트하고 공급자 구성에서 태그 정책 검증을 활성화해야 합니다. 구현 세부 정보 및 구성 예제는 [태그 정책 적용에 대한 Terraform AWS Provider 설명서를](#) 참조하세요.

Pulumi로 적용

Pulumi에서 필수 태그 키를 적용하려면 Pulumi Cloud에서 태그 정책 보고 정책 팩을 활성화하고 태그 정책 읽기 권한으로 IAM 역할을 구성해야 합니다. 구현 세부 정보 및 구성 예제는 [태그 정책 적용에 대한 Pulumi 설명서를](#) 참조하세요.

태그 정책 구문 및 예제

이 페이지에서는 태그 정책 구문에 대해 설명하고 예제를 제공합니다.

주제

- [태그 정책 구문](#)
- [태그 정책 예제](#)
- [예제 1: 조직 전체의 태그 키 사례 정의](#)
- [예제 2: 태그 키 사용 방지](#)
- [예제 3: 특정 AWS 서비스의 지원되는 모든 리소스 유형에 대한 태그 정책 지정](#)
- [예제 4: 규정 준수를 위해 필요한 태그 키 적용](#)

태그 정책 구문

태그 정책은 [JSON](#) 규칙에 따라 구성된 일반 텍스트 파일입니다. 태그 정책 구문은 관리 정책 유형에 대한 구문을 따릅니다. 해당 구문에 대한 자세한 내용은 [관리 정책 상속에 대한 이해](#) 단원을 참조하세요. 이 항목에서는 태그 정책 유형의 특정 요구 사항에 해당 일반 구문을 적용하는 방법을 중점적으로 설명합니다.

다음 태그 정책은 기본 태그 정책 구문을 보여줍니다.

```
{
  "tags": {
    "costcenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      },
      "tag_value": {
        "@@assign": [
          "100",
          "200",
          "300*"
        ]
      }
    }
  }
}
```

```

    ]
  },
  "enforced_for": {
    "@assign": [
      "secretsmanager:ALL_SUPPORTED"
    ]
  }
}
}
}
}

```

태그 정책 구문에는 다음 요소가 포함됩니다.

- `tags` 필드 키 이름입니다. 태그 정책은 항상 이 고정 키 이름으로 시작합니다. 위의 예제 정책에서 맨 위 줄입니다.
- 정책 설명을 고유하게 식별하는 정책 키입니다. 이 값은 대소문자 처리를 제외하고 태그 키의 값과 일치해야 합니다. 정책 값은 대소문자를 구분합니다.

이 예제에서 `costcenter`는 정책 키입니다.

- 리소스에서 준수하게 하려는 대소문자 처리 방식을 사용하여 허용된 태그 키를 지정하는 최소 하나의 태그 키입니다. 대소문자 처리가 정의되지 않은 경우 태그 키의 기본 대소문자 처리 방법은 소문자입니다. 태그 키의 값은 정책 키의 값과 일치해야 합니다. 그러나 정책 키 값은 대소문자를 구분하지 않으므로 대소문자 처리가 다를 수 있습니다.

이 예제에서 `CostCenter`는 태그 키입니다. 이는 태그 정책을 준수하는 데 필요한 대소문자 처리입니다. 이 태그 키에 대한 대체 대소문자 처리를 사용하는 리소스는 태그 정책을 준수하지 않습니다.

한 태그 정책에 여러 태그 키를 정의할 수 있습니다.

- (선택 사항) 태그 키에 대해 허용 가능한 하나 이상의 태그 값 목록입니다. 태그 정책에 따라 태그 키의 태그 값이 지정되지 않으면 모든 값(값이 전혀 없는 경우 포함)이 정책을 준수하는 것으로 간주됩니다.

이 예제에서 `CostCenter` 태그 키에 허용 가능한 값은 `100`, `200` 및 `300*`입니다.

- (선택 사항) 지정된 서비스와 리소스에서 정책 미준수 태그 지정 작업을 금지할지 여부를 나타내는 `enforced_for` 옵션입니다. 콘솔에서 이 옵션은 태그 정책 생성에 대한 시각적 편집기의 이 태그에 대한 정책 미준수 작업 금지 옵션입니다. 이 옵션의 기본 설정은 `null`입니다.

예제 태그 정책은 모든 AWS Secrets Manager 리소스에 적용된 `CostCenter` 태그가 이 정책을 준수해야 한다고 지정합니다.

⚠ Warning

태그 정책을 사용한 경험이 있는 경우에만 이 옵션을 기본값에서 변경해야 합니다. 그렇지 않으면 조직 계정의 사용자가 필요한 리소스를 생성하지 못하도록 할 수 있습니다.

- 태그 정책이 조직 트리 내의 다른 태그 정책과 병합되어 계정의 [유효 태그 정책](#)을 생성하는 방법을 지정하는 연산자입니다. 이 예제에서 @@assign은 tag_key, tag_value 및 enforced_for에 문자열을 할당하는 데 사용됩니다. 연산자에 대한 자세한 내용은 [상속 연산자](#) 단원을 참조하십시오.
- 태그 값에 * 와일드카드를 사용할 수 있습니다.
 - 태그 값당 하나의 와일드카드만 사용할 수 있습니다. 예를 들어, *@example.com은 허용되지만 *@*.com은 허용되지 않습니다.
 - enforced_for 필드의 ALL_SUPPORTED 와일드카드를 일부 서비스와 함께 사용하여 해당 서비스에 대해 지원되는 모든 리소스에 대한 적용을 활성화할 수 있습니다. enforced_for를 지원하는 서비스 및 리소스의 목록은 [적용을 지원하는 서비스 및 리소스 유형](#)을 참조하세요.
 - 와일드카드를 사용하여 모든 서비스를 지정하거나 모든 서비스에 대한 리소스를 지정할 수는 없습니다.

태그 정책 예제

다음 [태그 정책](#) 예제는 정보 제공 용도로만 제공됩니다.

i Note

조직에서 이러한 태그 정책 예제를 사용하려면 먼저 다음 사항에 주의하세요.

- 태그 정책을 시작하려면 [권장 워크플로](#)를 따라야 합니다.
- 각자 고유의 요구 사항에 맞게 이러한 태그 정책을 신중하게 검토하고 사용자 지정해야 합니다.
- 태그 정책의 모든 문자는 [최대 크기](#)가 정해져 있습니다. 이 설명서의 예제는 가독성을 높이기 위한 추가 공백으로 서식이 지정된 SCP를 보여 줍니다. 하지만 정책 크기가 최대 크기에 도달하는 경우 공간을 절약하기 위해 공백을 모두 삭제할 수 있습니다. 공백의 예에는 다음 표 밖에 있는 공백 문자와 줄 바꿈이 있습니다.
- 태그가 지정되지 않은 리소스는 결과에 정책 미준수로 나타나지 않습니다.

예제 1: 조직 전체의 태그 키 사례 정의

다음 예제에서는 두 개의 태그 키만 정의하는 태그 정책과 조직의 계정에서 표준화할 대소문자 처리만 정의하는 태그 정책을 보여 줍니다.

정책 A - 조직 루트 태그 정책

```
{
  "tags": {
    "CostCenter": {
      "tag_key": {
        "@@assign": "CostCenter",
        "@@operators_allowed_for_child_policies": ["@@none"]
      }
    },
    "Project": {
      "tag_key": {
        "@@assign": "Project",
        "@@operators_allowed_for_child_policies": ["@@none"]
      }
    }
  }
}
```

이 태그 정책은 CostCenter와 Project라는 두 가지 태그 키를 정의합니다. 이 태그 정책을 조직 루트에 연결하면 다음과 같은 효과가 발생합니다.

- 조직의 모든 계정이 이 태그 정책을 상속합니다.
- 정책을 준수하기 위해 조직의 모든 계정이 정의된 대소문자 처리를 사용해야 합니다. CostCenter 및 Project 태그가 있는 리소스는 정책을 준수합니다. 태그 키에 대한 대체 대소문자 처리를 사용하는 리소스(예: costcenter, Costcenter 또는 COSTCENTER)는 정책을 준수하지 않습니다.
- @@operators_allowed_for_child_policies: ["@@none"] 행은 태그 키를 잠급니다. 조직 트리의 아래쪽에 연결된 태그 정책(하위 정책)은 값 설정(value-setting) 연산자를 사용하여 태그 키를 변경할 수 없습니다(대소문자 처리 포함).
- 모든 태그 정책이 그렇듯이, 태그 없는 리소스 또는 태그 정책에서 정의되지 않은 태그는 태그 정책 준수 여부가 평가되지 않습니다.

AWS에서는 사용하려는 태그 키에 대해 유사한 태그 정책을 생성할 때 이 예제를 가이드로 사용할 것을 권장합니다. 이 태그 정책을 조직 루트에 연결합니다. 그런 다음 정의된 태그 키에 대해 허용 가능한 값만 정의하는 다음 예제와 비슷한 태그 정책을 생성합니다.

다음 단계: 값 정의

이전의 태그 정책을 조직 루트에 연결했다고 가정합니다. 그런 다음, 다음과 같은 태그 정책을 생성하여 계정에 연결할 수 있습니다. 이 정책은 CostCenter 및 Project 태그 키에 대해 허용 가능한 값을 정의합니다.

정책 B - 계정 태그 정책

```
{
  "tags": {
    "CostCenter": {
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    },
    "Project": {
      "tag_value": {
        "@@assign": [
          "A",
          "B"
        ]
      }
    }
  }
}
```

정책 A를 조직 루트에 연결하고 정책 B를 계정에 연결하면 정책이 결합되어 계정에 대해 다음과 같은 유효 태그 정책을 생성합니다.

정책 A + 정책 B = 계정에 대한 유효 태그 정책

```
{
  "tags": {
    "Project": {
      "tag_value": [
        "A",
        "B"
      ],
      "tag_key": "Project"
    },
  },
}
```

```

    "CostCenter": {
      "tag_value": [
        "Production",
        "Test"
      ],
      "tag_key": "CostCenter"
    }
  }
}

```

상속 연산자의 작동 방식 예제 및 유효 태그 정책 예제를 포함하여 정책 상속에 대한 자세한 내용은 [관리 정책 상속에 대한 이해](#) 섹션을 참조하세요.

예제 2: 태그 키 사용 방지

태그 키의 사용을 방지하기 위해 다음과 같은 태그 정책을 조직 엔터티에 연결할 수 있습니다.

이 예제 정책은 Color 태그 키에 어떤 값도 사용할 수 없도록 지정합니다. 또한 하위 태그 정책에서 [연산자](#)가 허용되지 않도록 지정합니다. 따라서 영향을 받는 계정의 리소스에 대한 모든 Color 태그는 미준수로 간주됩니다. 그러나 enforced_for 옵션은 영향을 받는 계정이 Amazon DynamoDB 테이블에만 Color 태그를 지정하는 것을 방지합니다.

```

{
  "tags": {
    "Color": {
      "tag_key": {
        "@operators_allowed_for_child_policies": [
          "@none"
        ],
        "@assign": "Color"
      },
      "tag_value": {
        "@operators_allowed_for_child_policies": [
          "@none"
        ],
        "@assign": []
      },
      "enforced_for": {
        "@assign": [
          "dynamodb:table"
        ]
      }
    }
  }
}

```



```
}
}
```

예제 3: 특정 AWS 서비스의 지원되는 모든 리소스 유형에 대한 태그 정책 지정

특정 AWS 서비스의 지원되는 모든 리소스 유형에 대해 태그 정책을 지정하려면 ALL_SUPPORTED 와 일드카드를 사용합니다.

이 정책은 ALL_SUPPORTED 와일드카드를 사용하여 태그 키 Environment가 있는 모든 Amazon EC2 인스턴스가 Prod 또는 Non-prod의 태그 값만 가질 수 있도록 지정합니다. 이 와일드카드는 각 Amazon EC2 인스턴스를 개별적으로 나열하는 대신 한 줄로 된 효과적인 대안을 제공합니다.

ALL_SUPPORTED 와일드카드를 지원하는 서비스 및 리소스의 목록은 [적용을 지원하는 서비스 및 리소스 유형](#) 섹션을 참조하세요.

```
{
  "tags": {
    "Environment": {
      "tag_key": {
        "@@assign": "Environment",
        "@@operators_allowed_for_child_policies": ["@none"]
      },
      "tag_value": {
        "@@assign": [
          "Prod",
          "Non-prod"
        ],
        "@@operators_allowed_for_child_policies": ["@none"]
      },
      "enforced_for": {
        "@@assign": [
          "ec2:ALL_SUPPORTED"
        ]
      }
    }
  }
}
```

예제 4: 규정 준수를 위해 필요한 태그 키 적용

이 예제에서는 모든 리소스에 필수 규정 준수 태그를 포함해야 하는 태그 정책을 정의하는 방법을 보여줍니다. 조직은 일반적으로이 패턴을 사용하여 적절한 비용 할당, 소유권 추적 및 환경 식별을 보장합니다.

```

{
  "tags": {
    "CostCenter": {
      "report_required_tag_for": {
        "@@assign": [
          "ec2:instance",
          "s3:bucket",
          "rds:db",
          "lambda:function"
        ]
      },
      "tag_key": {
        "@@assign": "CostCenter"
      }
    },
    "Environment": {
      "report_required_tag_for": {
        "@@assign": [
          "ec2:ALL_SUPPORTED",
          "rds:ALL_SUPPORTED",
          "s3:ALL_SUPPORTED"
        ]
      },
      "tag_key": {
        "@@assign": "Environment"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Staging",
          "Development",
          "Test"
        ]
      }
    },
    "Owner": {
      "report_required_tag_for": {
        "@@assign": [
          "ec2:ALL_SUPPORTED"
        ]
      },
      "tag_key": {
        "@@assign": "Owner"
      }
    }
  }
}

```

```

    }
  }
}

```

이 정책을 적용하고 태그 정책 적용으로 IaC 도구를 구성하는 경우:

- CostCenter: EC2 인스턴스, S3 버킷, RDS 데이터베이스 및 Lambda 함수에 필요합니다.
- 환경: 모든 EC2, RDS 및 S3 리소스에 필요하며 허용되는 값은 프로덕션, 스테이징, 개발 또는 테스트로 제한됩니다.
- 소유자: 조직의 모든 EC2 리소스에 필요합니다.

이 정책을 준수하는 인프라 코드의 예:

```

EC2Instance:
  Type: AWS::EC2::Instance
  Properties:
    ImageId: ami-0c02fb55956c7d316
    InstanceType: t2.micro
    Tags:
      - Key: CostCenter
        Value: CC-12345
      - Key: Environment
        Value: Test
      - Key: Owner
        Value: john.doe@company.com

```

필요한 태그 없이 리소스를 생성하려고 하면 구성에 따라 IaC 배포가 실패하거나 계획 단계에서 경고가 생성됩니다. 실패 모드로 구성하면 리소스가 생성되기 전에 배포가 차단됩니다. 경고 모드로 구성하면 배포가 진행되지만 누락된 태그를 팀에 알립니다. 검증 오류 메시지는 누락된 필수 태그와 해당 태그가 필요한 리소스를 정확하게 식별합니다.

IaC 도구에 대한 특정 구성 지침은 다음과 같습니다.

- CloudFormation: 태깅 규정 준수 후크를 활성화 [the section called “를 사용하여 적용 CloudFormation”](#) 하려면 섹션을 참조하세요.
- Terraform: AWS 공급자에서 태그 정책 검증을 활성화 [the section called “Terraform으로 적용”](#) 하려면 섹션을 참조하세요.

- Pulumi: Tag Policy Reporting 정책 팩을 활성화 [the section called “Pulumi로 적용”](#) 하려면 섹션을 참조하세요.

태그 지정 불일치 식별 및 해결

조직에서 태그 정책을 구현한 후 규정을 준수하지 않는 태그가 있는 리소스를 식별하고 이를 수정하여 AWS 환경 전반의 일관성을 보장할 수 있습니다. 이 섹션에서는 태그 지정 불일치를 찾고 수정하는 방법에 대한 지침을 제공합니다.

주제

- [Resource Explorer를 사용하여 조직의 태그가 지정되지 않고 잘못된 리소스 찾기](#)
- [리소스에서 정책 미준수 태그 수정](#)
- [Amazon EventBridge를 사용하여 정책 미준수 태그 모니터링](#)

Resource Explorer를 사용하여 조직의 태그가 지정되지 않고 잘못된 리소스 찾기

계정에서 태그가 지정되지 않은 리소스를 찾으려면 사용하는 쿼리와 AWS Resource Explorer 함께 사용합니다. `tag:none`. Resource Explorer는 적절한 태그 지정이 없거나 조직 전체에서 태그 값이 일관되지 않은 리소스를 식별할 수 있는 포괄적인 검색 기능을 제공합니다.

Resource Explorer를 사용하여 태그가 지정되지 않고 잘못된 리소스를 찾는 방법에 대한 자세한 지침은 AWS Resource Explorer 사용 설명서의 [태그가 지정되지 않은 리소스 검색](#)을 참조하세요.

리소스에서 정책 미준수 태그 수정

정책 미준수 태그를 찾은 후에는 다음 방법 중 하나를 사용하여 수정합니다. 정책 미준수 태그가 포함된 리소스가 있는 계정에 로그인해야 합니다.

- 규정을 준수하지 않는 리소스를 생성한 AWS 서비스의 콘솔 또는 태그 지정 API 작업을 사용합니다.
- AWS Resource Groups [TagResources](#) 및 [UntagResources](#) 작업을 사용해 유효 정책을 준수하는 태그를 제거하거나 미준수 태그를 제거합니다.

Amazon EventBridge를 사용하여 정책 미준수 태그 모니터링

Amazon EventBridge(이전 Amazon CloudWatch Events)를 사용하여 정책 미준수 태그가 언제 도입되는지 모니터링할 수 있습니다. 다음 예제 이벤트에서 `tag-policy-compliant`의 `"false"` 값은 새 태그가 유효 태그 정책을 준수하지 않음을 나타냅니다.

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-00000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
}
```

이벤트를 구독하고 모니터링할 문자열이나 패턴을 지정할 수 있습니다. 자세한 내용은 [Amazon EventBridge 사용 설명서](#)를 참조하세요.

적용을 지원하는 서비스 및 리소스 유형

태그 정책 적용을 지원하는 서비스 및 리소스 유형은 다음과 같습니다.

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Amplify UI Builder [amplifyu	amplify build heme	• AWS: ifyl der: e	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
[awscli]	awscli	• AWS: ifyl der: oner	Yes	Yes	No	No
	awscli	• AWS: ifyl der: oner	Yes	No	No	No
	awscli	• N/A LL_SUPPORTED	No	Yes	No	No
AWS Amplify [amplify]	amplify	• AWS: ifyl	Yes	No	Yes	Yes
AWS App Mesh [appmesh]	appmesh	• AWS: mesh:	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	appmesh/virtualgatewayroute	• AWS: appmesh:wayfinder	Yes	Yes	Yes	Yes
	appmesh/virtualgateway	• AWS: appmesh:virtualgateway	Yes	Yes	Yes	Yes
	appmesh/virtualnode	• AWS: appmesh:virtualnode	Yes	Yes	Yes	Yes
	appmesh/virtualrouter	• AWS: appmesh:virtualrouter	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	appmesh/virtualservice	• AWS: mesh:virtualservice	Yes	Yes	Yes	Yes
	appmesh/virtualnode	• AWS: mesh:virtualnode	Yes	Yes	Yes	Yes
	appmesh/virtualgateway	• AWS: mesh:virtualgateway	Yes	Yes	Yes	Yes
	appmesh/virtualnode	• N/A	No	Yes	Yes	Yes
	appmesh/virtualnode	• AWS: mesh:virtualnode	Yes	No	Yes	Yes
	appmesh/virtualnode	• AWS: mesh:virtualnode	Yes	No	Yes	Yes
AWS App Runner [apprunner]	apprunner:autoscalingconfiguration	• AWS: apprunner:autoscalingconfiguration	Yes	No	Yes	Yes
	apprunner:service	• AWS: apprunner:service	Yes	No	Yes	Yes
	apprunner:connection	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	appru :vpci sscon ion	• AWS: unne cIng onne	Yes	No	Yes	Yes
	appru :obse ility igura	• AWS: unne serv tyCo rati	Yes	No	Yes	Yes
	appru :vpcc ctor	• AWS: unne cCor r	Yes	No	Yes	Yes
AWS AppConfig [appconfi g]	appco :appl ion/ envir onmen	• AWS: onfi virc	Yes	Yes	Yes	Yes
	appco :envi ent	• AWS: onfi virc	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	appcom:configuration	• N/A	Yes	No	No	No
	appcom:external	• AWS: configuration	Yes	No	Yes	Yes
	appcom:application	• AWS: configuration	Yes	Yes	Yes	Yes
	appcom:externalassociation	• AWS: configuration, social	Yes	No	Yes	Yes
	appcom:application/configuration/profile	• AWS: configuration, onPr	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	appcom:application/environment/deployment	• AWS: onfiploy	Yes	Yes	No	No
	appcom:deploymentstrategy	• AWS: onfiploytrat	Yes	Yes	Yes	Yes
AWS AppFabric [appfabric]	appfabric:application	• N/A	Yes	No	No	No
	appfabric:application	• N/A	Yes	No	No	No
	appfabric:application/authorization	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS AppSync [appsync]	appsync:main:s	• AWS:sync:inNa	Yes	No	No	No
	appsync:pis	• AWS:sync:hQLA	Yes	No	No	No
	appsync:pis	• AWS:sync:	Yes	No	No	No
AWS Application Auto Scaling [application-autoscaling]	application-autoscaling:target	• AWS:application-autoscaling:target	Yes	No	No	No
AWS Application Migration Service [mgn]	mgn:serve	• N/A	Yes	No	No	No
	mgn:ctor	• N/A	Yes	No	No	No
	mgn:atio	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	mgn:wa	• N/A	Yes	No	No	No
	mgn:la h- confi ratio te mplat	• N/A	Yes	No	No	No
	mgn:re cation co nfigu on- templ te	• N/A	Yes	No	No	No
	mgn:jo	• N/A	Yes	No	No	No
	mgn:in t	• N/A	Yes	No	No	No
	mgn:ve er- clien	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	mgn:ent	• N/A	Yes	No	No	No
AWS Audit Manager [auditmanager]	auditmanager:assessment	• AWS: IAM:Assessment	Yes	Yes	Yes	Yes
	auditmanager:control	• N/A	Yes	Yes	No	No
	auditmanager:assessmentnetwork	• N/A	Yes	Yes	No	No
	auditmanager:APIUPPOR	• N/A	No	Yes	Yes	Yes
AWS B2B Data Interchange [b2bi]	b2bi:file	• AWS::Partner	Yes	No	Yes	Yes
	b2bi:partnership	• AWS::Partnership	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	b2bi:transform	• AWS::Transfer	Yes	No	Yes	Yes
	b2bi:capability	• AWS::Certificate	Yes	No	Yes	Yes
AWS Backup Gateway [backup-gateway]	backupgateway	• N/A	Yes	Yes	No	No
	backupgateway-aws-hypervisor	• AWS::BackupGateway	Yes	Yes	Yes	Yes
	backupgateway	• N/A	Yes	Yes	No	No
	backupgateway-SUPPORTED	• N/A	No	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Backup [backup-search]	backup-search-export-job	• N/A	Yes	No	No	No
	backup-search-job	• N/A	Yes	No	No	No
AWS Backup [backup]	backup-gal-hold	• N/A	Yes	No	No	No
	backup-ering-con-figuration	• N/A	Yes	No	No	No
	backup-port-plan	• AWS::backup::tPlan	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	backup-vault	- AWS::Backup::PVAlias - AWS::Backup::PVAlias	Yes	Yes	No	No
	backupstore-testing-plan	AWS::Backup::RestoreTestingPlan	Yes	No	Yes	Yes
	backup-amazon-workspaces	AWS::Backup::AmazonWorkspaces	Yes	No	Yes	Yes
	backup-plan	AWS::Backup::Plan	Yes	Yes	Yes	Yes
	backup-coverpoint	N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	backup-L_SUPP ED	• N/A	No	Yes	Yes	Yes
AWS Batch [batch]	batch-vice-envi ronment	• AWS:h::SEnv ent	Yes	No	No	No
	batch- defin on	• AWS:h::C init	Yes	Yes	Yes	Yes
	batch eduli p olicy	• AWS:h::S lin y	Yes	No	Yes	Yes
	batch sumab r esour	• AWS:h::C able rce	Yes	No	Yes	Yes
	batch vice- job	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	batch-compute-environment	• AWS::CloudFormation::Environment	Yes	No	Yes	Yes
	batch	• N/A	Yes	Yes	No	No
	batch-queue	• AWS::Batch::Queue	Yes	Yes	Yes	Yes
	batch-SUPPLEMENT	• N/A	No	Yes	Yes	Yes
AWS Billing And Cost Management Data Exports [bcm-data-exports]	bcm-data-exports	• AWS::BCMDataExports::DataExport	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Billing And Cost Management Pricing Calculator [bcm-pricing-calculator]	bcm-pricing-calculator:load-estimate	• N/A	Yes	No	No	No
	bcm-pricing-calculator:load-estimate	• N/A	Yes	No	No	No
	bcm-pricing-calculator:load-scenarios	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Billing Conductor [billingconductor]	billingconductor:up	• AWS: billingconductor:ingC	Yes	No	No	No
	billingconductor:pricingn	• AWS: billingconductor:ingF	Yes	No	No	No
	billingconductor:customitem	• AWS: billingconductor:omLim	Yes	No	No	No
	billingconductor:pricinge	• AWS: billingconductor:ingF	Yes	No	No	No
AWS Billing [billing]	billing:aw	• AWS: billing:ing\	Yes	No	No	No
AWS Budget Service [budgets]	budgets	• AWS: budgets:et	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	budget:action	• AWS:ets/ets/	Yes	No	Yes	Yes
AWS BugBust [bugbust]	bugbust:vent	• N/A	Yes	Yes	No	No
	bugbust:LL_SUPPORTED	• N/A	No	Yes	No	No
AWS Certificate Manager [acm]	acm:certificate	• AWS:ificnageritif	Yes	Yes	Yes	Yes
	acm:ALL_UNSUPPORTED	• N/A	No	Yes	Yes	Yes
AWS Chatbot [chatbot]	chatbot:customaction	• AWS:bot:omAc	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	chatbot-hat-configurations-microsoft-teams-channel	- AWS:bot:Kubernetes - AWS:bot:microsoft-sChannel configuration	Yes	No	No	No
	chatbot-hat-configurations-slack-channel	- AWS:bot:Kubernetes - AWS:bot:microsoft-sChannel configuration	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	chatbot-hat-configurations-chime-webhook	- AWS:bot:chatbot - AWS:chatbot:chatbot	Yes	No	No	No
AWS Clean Rooms ML [cleanrooms-ml]	cleanrooms-ml:configure-model-algorithm	N/A	Yes	No	No	No
	cleanrooms-ml:trained-model	N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	clean: s-ml:membership-trained-model	• N/A	Yes	No	No	No
	clean: s-ml:configured-model-algorithm-association	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	clean: s-ml:membership:config:model:algorithm:association	• N/A	Yes	No	No	No
	clean: s-ml:membership:trained-model-inference-job	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	clean:s-model-inference-job	• N/A	Yes	No	No	No
	clean:s-model-ancestry-model	• N/A	Yes	No	No	No
	clean:s-model-ancestry-generation-job	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	cleanrooms:training-data-set	• AWS: nRooms:TrainingData	Yes	No	Yes	Yes
	cleanrooms:configureaudiencemodel	• N/A	Yes	No	No	No
AWS Clean Rooms [cleanrooms]	cleanrooms:collaboration	• AWS: nRooms:collaboration	Yes	Yes	No	No
	cleanrooms:membership/privacybudget/employment	• AWS: nRooms:membership/privacybudget/employment	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	clean:s:member/hip/configured/association	• AWS: nRoconfiTablciat	Yes	Yes	No	No
	clean:s:connector	• AWS: nRoconfiTabl	Yes	Yes	Yes	Yes
	clean:s:member/hip/analyte	• AWS: nRoconalymp	Yes	No	No	No
	clean:s:member/hip/configured/enforcement/association	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	clean:s:membership	• AWS: nResourceEmbed	Yes	Yes	No	No
	clean:s:membership/idmappingto	• AWS: nResourceMappingable	Yes	No	No	No
	clean:s:ALLPORTABLE	• N/A	No	Yes	Yes	Yes
AWS Cloud Map [servicediscovery]	servicediscovery:namespace	• AWS: namespace • AWS: namespace	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	service-scoped service	• AWS: serviceAlias: service	Yes	No	Yes	Yes
AWS Cloud9 [cloud9]	cloud9::volumes	• AWS: cloud9::volumes	Yes	Yes	No	No
	cloud9::L_SUPPLEMENTED	• N/A	No	Yes	No	No
AWS CloudFormation [cloudformation]	cloudformation::stack	• AWS: cloudformation::stack	Yes	No	Yes	Yes
	cloudformation::stackset	• AWS: cloudformation::stackset	Yes	No	Yes	Yes
AWS CloudHSM [cloudhsm]	cloudhsm::backups	• N/A	Yes	No	No	No
	cloudhsm::clusters	• N/A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS CloudTrail [cloudtrail]	cloudtrail:cha	• AWS: dTrailhanr	Yes	No	Yes	Yes
	cloudtrail:even	• AWS: dTrailventore	Yes	No	Yes	Yes
	cloudtrail:tra	• AWS: dTrailrail	Yes	Yes	Yes	Yes
	cloudtrail:das	• AWS: dTrailasht	Yes	No	Yes	Yes
	cloudtrail:ALL	• N/A	No	Yes	Yes	Yes
AWS CloudWatch RUM [rum]	rum:anitor	• AWS: Appor	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS CodeArtifact [codeartifact]	codeartifact:repository	• AWS:ArtifactRegistry	Yes	No	Yes	Yes
	codeartifact:domain	• AWS:ArtifactDomain	Yes	No	Yes	Yes
	codeartifact:packagegroup	• AWS:ArtifactPackageGroup	Yes	No	No	No
AWS CodeBuild [codebuild]	codebuild:project	• AWS:CodeBuildProject	Yes	Yes	Yes	Yes
	codebuild:fleet	• AWS:CodeBuildFleet	Yes	No	No	No
	codebuild:reportgroup	• AWS:CodeBuildReportGroup	Yes	No	Yes	Yes
	codebuild:ALL_SUPPORTED	• N/A	No	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS CodeCommit [codecommit]	codecommit:repository	• AWS: CodeCommit repository	Yes	Yes	Yes	Yes
	codecommit:ALLPORTABLE	• N/A	No	Yes	Yes	Yes
AWS CodeConnections [codeconnections]	codeconnections:connect	• N/A	Yes	No	No	No
	codeconnections:connect:connectivity	• AWS: CodeConnections::connectivity	Yes	No	Yes	Yes
	codeconnections:position:link	• N/A	Yes	No	No	No
AWS CodeDeploy [codedeploy]	codedeploy:deployment	• AWS: CodeDeploy configuration	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	codebuild:application	• AWS: Deployment	Yes	No	Yes	Yes
	codebuild:deploymentgroup	• AWS: DeploymentGroup	Yes	No	No	No
	codebuild:instance	• N/A	Yes	No	No	No
AWS CodePipeline [codepipeline]	codepipeline:work	• AWS: Pipeline:Web	Yes	Yes	Yes	Yes
	codepipeline:putpipeline	• AWS: Pipeline:PutPipeline	Yes	Yes	Yes	Yes
	codepipeline:actiontype	• AWS: Pipeline:CustomAction	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	codepolicy:AWSUPPOR	• N/A	No	Yes	Yes	Yes
AWS CodeStar Connections [codestar-connections]	codesconnections:connection	• AWS:Starcticonne	Yes	Yes	Yes	Yes
	codesconnections:hosts	• N/A	Yes	Yes	No	No
	codesconnections:repository-link	• AWS:Starcticorepository-Link	Yes	No	Yes	Yes
	codesconnections:ALPPORT	• N/A	No	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS CodeStar Notifications [codestar-notifications]	codestarnotifications:NotificationRule	• AWS: Star	Yes	No	Yes	Yes
AWS CodeStar [codestar]	codestarproject	• AWS: StarHubFactory	Yes	No	No	No
AWS Config [config]	config:AggregateAuthorization	• AWS: Config:Authorization	Yes	Yes	Yes	Yes
	config:OrganizationConfigurationRule	• AWS: Config:OrganizationConfiguration	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	config-organization-conformance-pack	• AWS::OrganizationalConformancePack	Yes	No	No	No
	config-nfrule	• AWS::OrganizationalRule	Yes	Yes	Yes	Yes
	config-nfigure-on-record-er	• AWS::OrganizationalRecord	Yes	No	No	No
	config-ored-query	• AWS::OrganizationalQuery	Yes	No	Yes	Yes
	config-nfig-aggregator	• AWS::OrganizationalAggregator	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	config:informational:pack	• AWS:ig::rmark	Yes	No	Yes	Yes
	config:L_SUPP ED	• N/A	No	Yes	Yes	Yes
AWS Control Tower [controltower]	controltower:longzone	• AWS:roll:LargeOne	Yes	No	No	No
	controltower:enabledcontrol	• AWS:roll:EnabledControl	Yes	No	No	No
	controltower:enabledbase	• AWS:roll:EnabledBase	Yes	No	No	No
AWS Cost Explorer Service [ce]	ce:analytics	• AWS:AnonymousSubscription	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ce:costcategory	• AWS: Costory	Yes	No	Yes	Yes
	ce:anonymization	• AWS: Anonnitc	Yes	No	Yes	Yes
AWS Cost and Usage Report [cur]	cur:definition	• AWS: :Repfini	Yes	No	Yes	Yes
AWS Data Exchange [dataexchange]	dataexchange:released-revisions	• N/A	Yes	No	No	No
	dataexchange:release-action	• N/A	Yes	No	No	No
	dataexchange:released-data-sets	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	dataengine:datapipeline:grant	• N/A	Yes	No	No	No
	dataengine:datapipeline:sets	• N/A	Yes	No	No	No
AWS Data Pipeline [datapipeline]	datapipeline:datapipeline	• AWS:Pipeline	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS DataSync [datasync]	datasync:location	- AWS:Syncatic - AWS:Syncatic - AWS:Syncaticust - AWS:SyncaticNTAF - AWS:SyncaticctSt - AWS:Syncaticpen	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
		- AWS: Sync atic - AWS: Sync atic inde - AWS: Sync atic eBlc - AWS: Sync atic				
	datas task	AWS: Sync k	Yes	No	Yes	Yes
	datas task/ execution	N/ A	Yes	No	No	No
	datas agent	AWS: Sync nt	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Database Migration Service [dms]	datasystemjob	• N/A	Yes	No	No	No
	datasystemjob	• N/A	Yes	No	No	No
	dms:assessdbinstance	• N/A	Yes	No	No	No
	dms:startdbinstance	• AWS:ReplicationGroup	Yes	Yes	Yes	Yes
	dms:executeleap	• AWS:EventSubscription	Yes	Yes	Yes	Yes
	dms:restoredbinstancefroms3	• AWS:ReplicationGroup	Yes	No	Yes	Yes
	dms:createreplicationinstance	• AWS:Create	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	dms:re	• AWS: :Region	Yes	Yes	Yes	Yes
	dms:instance-profile	• AWS: :InstanceProfile	Yes	No	Yes	Yes
	dms:tag	• AWS: :Region	Yes	Yes	Yes	Yes
	dms:encrypt	• AWS: :Encryption	Yes	Yes	Yes	Yes
	dms:datamigration	• AWS: :Data	Yes	No	No	No
	dms:dataprotection	• AWS: :Data	Yes	No	Yes	Yes
	dms:migration-project	• AWS: :MigrationProject	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	dms:ALTER, dms:CREATE, dms:DELETE, dms:DROP, dms:RENAME, dms:UPDATE	• N/A	No	Yes	Yes	Yes
AWS Deadline Cloud [deadline]	deadline:license_endpoint	• AWS:license_endpoint	Yes	No	Yes	Yes
	deadline:farm	• AWS:licensefarm	Yes	No	Yes	Yes
	deadline:monitor	• AWS:license_monitor	Yes	No	No	No
AWS DeepComposer [deepcomposer]	deepcomposer:composition	• N/A	Yes	No	No	No
	deepcomposer:model	• N/A	Yes	No	No	No
AWS DeepRacer [deepracer]	deepracer:leaderboard_evaluation	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	deepresources:leader	• N/A	Yes	No	No	No
	deepresources:mode	• N/A	Yes	No	No	No
	deepresources:training_job	• N/A	Yes	No	No	No
	deepresources:evaluation_job	• N/A	Yes	No	No	No
	deepresources:car	• N/A	Yes	No	No	No
AWS Device Farm [devicefarm]	devicefarm:dev	• N/A	Yes	No	No	No
	devicefarm:test-device-project	• AWS: Device Farm test project	Yes	No	Yes	Yes
	devicefarm:instance	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	device:m:devtool	• AWS: ceFa • device	Yes	No	No	No
	device:m:project	• AWS: ceFa • project	Yes	No	Yes	Yes
	device:m:test-session	• N/A	Yes	No	No	No
	device:m:session	• N/A	Yes	No	No	No
	device:m:instance-profile	• AWS: ceFa • instance-profile	Yes	No	Yes	Yes
	device:m:network-profile	• AWS: ceFa • network-profile	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	device:m:vpce:figure:n	• AWS: ceFa PCEC urat	Yes	No	No	No
	device:m:run	• N/ A	Yes	No	No	No
AWS Diode Messaging [diode-messaging]	diode:mes saging: spond: flow	• N/ A	Yes	No	No	No
	diode:mes saging: pping	• N/ A	Yes	Yes	No	No
	diode:mes saging: quest: flow	• N/ A	Yes	No	No	No
AWS Diode [diode]	diode:nsfer	• N/ A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	diodecount-mapping	• N/A	Yes	No	No	No
AWS Direct Connect [directconnect]	directconnect:connect	• N/A	Yes	Yes	No	No
	directconnect:connect-g	• N/A	Yes	Yes	No	No
	directconnect:connect-n	• N/A	Yes	Yes	No	No
	directconnect:connect-gateway	• N/A	Yes	No	No	No
	directconnect:connect:AWS-SUPPORT	• N/A	No	Yes	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Directory Service [ds]	ds:directory	- AWS:directoryservice:sof - AWS:directoryservice:leAD	Yes	No	No	No
AWS Elastic Beanstalk [elasticbeanstalk]	elasticbeanstalk:platform	N/A	Yes	Yes	No	No
	elasticbeanstalk:configurationtemplate	AWS:elasticbeanstalk:configurationtemplate	Yes	Yes	Yes	Yes
	elasticbeanstalk:application	AWS:elasticbeanstalk:application	Yes	Yes	Yes	Yes
	elasticbeanstalk:environment	AWS:elasticbeanstalk:environment	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	elastic:application:pplication:version	• AWS: ElasticApplication:ApplicationVersion	Yes	Yes	Yes	Yes
	elastic:application:LL_SUPPORTED	• N/A	No	Yes	Yes	Yes
AWS Elastic Disaster Recovery [drs]	drs:job	• N/A	Yes	No	No	No
	drs:subnet-network	• N/A	Yes	No	No	No
	drs:region-configuration-template	• N/A	Yes	No	No	No
	drs:subnet-server	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	aws:iam::[account-id]:policy/AmazonEC2ConfigurationTemplate	• N/A	Yes	No	No	No
	aws:iam::[account-id]:policy/AmazonEC2InstanceProfile	• N/A	Yes	No	No	No
AWS Elastic Load Balancing [elasticloadbalancing]	aws:elasticloadbalancing:loadbalancer/aws:elasticloadbalancing:loadbalancer	• AWS:elasticloadbalancing::LoadBalancer	Yes	Yes	Yes	Yes
	aws:elasticloadbalancing:targetgroup	• AWS:elasticloadbalancing::TargetGroup	Yes	Yes	Yes	Yes
	aws:elasticloadbalancing:loadbalancer/aws:elasticloadbalancing:loadbalancer	• AWS:elasticloadbalancing::LoadBalancer	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	elasticloadbalancing:listener	• AWS::ElasticLoadBalancing::Listener	Yes	Yes	Yes	Yes
	elasticloadbalancing:targetgroup	• AWS::ElasticLoadBalancing::TargetGroup	Yes	No	Yes	Yes
	elasticloadbalancing:listener-rule	• AWS::ElasticLoadBalancing::ListenerRule	Yes	Yes	Yes	Yes
AWS Elemental Appliances and Software [elemental-appliances-software]	elemental-appliances-software:required	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Elemental MediaConnect [mediaconnect]	mediaconnect:routeoutput	• AWS: aCor:RouteOutput	Yes	No	No	No
	mediaconnect:source	• AWS: aCor:Flowce	Yes	No	Yes	Yes
	mediaconnect:output	• AWS: aCor:Flowut	Yes	No	Yes	Yes
	mediaconnect:elemental	• AWS: aCor:Flowtlen	Yes	No	Yes	Yes
	mediaconnect:flow	• AWS: aCor:Flow	Yes	No	Yes	Yes
	mediaconnect:routernetworkinterface	• AWS: aCor:RouterTwoInterface	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	mediaconnect:flowvpcinterface	• AWS: aCor:FlowInter	Yes	No	No	No
	mediaconnect:routerinput	• AWS: aCor:Routerput	Yes	No	No	No
AWS Elemental MediaConvert [mediaconvert]	mediaconvert:queues	• AWS: aCor:Que	Yes	No	Yes	Yes
	mediaconvert:presets	• AWS: aCor:Pre	Yes	No	Yes	Yes
	mediaconvert:jobtemplates	• AWS: aCor:Jobate	Yes	No	No	No
	mediaconvert:jobs	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Elemental MediaLive [medialive]	media:node	• N/A	Yes	No	No	No
	media:sdiscovery	• AWS:MediaLive:DiscoverySession	Yes	No	Yes	Yes
	media:reservation	• N/A	Yes	No	No	No
	media:signalingmap	• AWS:MediaLive:SignalingMap	Yes	No	Yes	Yes
	media:networktwo	• AWS:MediaLive:NetworkTwo	Yes	No	Yes	Yes
	media:cloudch-alarms-template	• AWS:MediaLive:CloudCh-alarms-template	Yes	No	Yes	Yes
	media:edge-rule-template	• AWS:MediaLive:Edge-rule-template	Yes	No	Yes	Yes
	media:rule-template	• AWS:MediaLive:Rule-template	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	media:multix	• AWS: aLiveAltip	Yes	No	Yes	Yes
	media:cloudch-alarmtemplgroup	• AWS: aLiveoudVlarnateC	Yes	No	Yes	Yes
	media:even-dge-rule-templgroup	• AWS: aLiveentERuleateC	Yes	No	Yes	Yes
	media:chan	• AWS: aLiveanne	Yes	No	No	No
	media:chanlacemroup	• AWS: aLiveanneemerp	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	mediapackage:inputsecuritypolicy	• AWS::MediaLive::InputSecurityGroup	Yes	No	Yes	Yes
	mediapackage:input	• AWS::MediaLive::Input	Yes	No	No	No
	mediapackage:input-ice	• N/A	Yes	No	No	No
AWS Elemental MediaPackage V2 [mediapackagev2]	mediapackagev2:channeloriginalpoint	• AWS::MediaPackageV2::ChannelOriginalPoint	Yes	No	Yes	Yes
	mediapackagev2:channeloriginalpoint	• AWS::MediaPackageV2::ChannelOriginalPoint	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	mediapackagev2:channelgroup	• AWS: AmazonMediaPackage2022-01-01:Group	Yes	No	Yes	Yes
	mediapackagev2:channelgroup/	• AWS: AmazonMediaPackage2022-01-01:ChannelGroup	Yes	No	Yes	Yes
	mediapackagev2:channelgroup/	• AWS: AmazonMediaPackage2022-01-01:ChannelGroup	Yes	No	Yes	Yes
AWS Elemental MediaPackage [mediapackage-vod]	mediapackage-vod:packageconfigurations	• AWS: AmazonMediaPackage2022-01-01:PackageConfiguration	Yes	No	Yes	Yes
	mediapackage-vod:assets	• AWS: AmazonMediaPackage2022-01-01:Asset	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	mediapackage:packagename	• AWS:MediaPackageGroup	Yes	No	Yes	Yes
AWS Elemental MediaPackage [mediapackage]	mediapackage:channels	• AWS:MediaPackageChannel	Yes	No	Yes	Yes
	mediapackage:origin_endpoints	• AWS:MediaPackageOriginEndpoint	Yes	No	Yes	Yes
AWS Elemental MediaStore [mediastore]	mediastore:folder	• N/A	Yes	No	No	No
	mediastore:container	• AWS:MediaStoreContainer	Yes	Yes	No	No
	mediastore:object	• N/A	Yes	No	No	No
	mediastore:ALLPORTABLE	• N/A	No	Yes	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Elemental MediaTailor or [mediatailor]	media:playbackratio	• AWS: aTailorPlayConfion	Yes	No	Yes	Yes
	media:sourcelocation	• AWS: aTailorSourceatic	Yes	No	Yes	Yes
	media:live	• AWS: aTailorLive	Yes	No	Yes	Yes
	media:voice	• AWS: aTailorVodS	Yes	No	Yes	Yes
	media:channel	• AWS: aTailorChar	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Elemental Support Cases [elemental-support-cases]	elemental-support-cases	• N/A	Yes	No	No	No
AWS End User Messaging Social [social-messaging]	social-messaging-aba	• N/A	Yes	No	No	No
	social-messaging-hone-number-id	• N/A	Yes	No	No	No
AWS Entity Resolution [entityresolution]	entityresolution-chemicaling	• AWS: EntityResolution: maMa	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	entity:arn:aws:iam::123456789012:role/role-name	• AWS: IAM::Role	Yes	Yes	Yes	Yes
	entity:arn:aws:iam::123456789012:role/role-name	• AWS: IAM::Role	Yes	No	Yes	Yes
	entity:arn:aws:iam::123456789012:role/role-name	• AWS: IAM::Role	Yes	No	Yes	Yes
	entity:arn:aws:iam::123456789012:role/role-name	• AWS: IAM::Role	Yes	No	Yes	Yes
	entity:arn:aws:iam::123456789012:role/role-name	• AWS: IAM::Role	Yes	No	Yes	Yes
AWS Fault Injection Service [fis]	fis:arn:aws:iam::123456789012:role/role-name	• N/A	Yes	No	No	No
	fis:arn:aws:iam::123456789012:role/role-name	• AWS: IAM::Role	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	fis:eni	• N/A	Yes	No	No	No
AWS Firewall Manager [fms]	fms:associationlist	• N/A	Yes	No	No	No
	fms:policylist	• N/A	Yes	No	No	No
	fms:policy	• AWS:Policy	Yes	No	No	No
	fms:resource-set	• AWS:ResourceSet	Yes	No	No	No
AWS Global Accelerator [globalaccelerator]	globalaccelerator	• AWS:GlobalAccelerator	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	global, elerac, attac, t	• AWS: alAc, ator, ssAc, Atta, t	Yes	No	Yes	Yes
AWS Glue DataBrew [databrew]	datab, job	• AWS: Brev	Yes	No	Yes	Yes
	datab, recip	• AWS: Brev, ipe	Yes	No	Yes	Yes
	datab, sched	• AWS: Brev, edu]	Yes	No	Yes	Yes
	datab, proje	• AWS: Brev, ject	Yes	No	Yes	Yes
	datab, rules	• AWS: Brev, eset	Yes	No	Yes	Yes
	datab, datas	• AWS: Brev, aset	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Glue [glue]	glue:flow	• AWS::Workflows	Yes	No	No	No
	glue:gratification:sourceproperty	• AWS::Integration::SourceProperty	Yes	No	No	No
	glue:gratification	• AWS::Integration	Yes	No	No	No
	glue:print	• N/A	Yes	No	No	No
	glue:letion	• N/A	Yes	No	No	No
	glue:eprofile	• AWS::UserProfile	Yes	No	Yes	Yes
	glue::Join	• AWS::Join	Yes	No	Yes	Yes
	glue:ion	• N/A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	glue:ger	• AWS::T	Yes	No	Yes	Yes
	glue:log	• N/A	Yes	No	No	No
	glue:ndpoint	• AWS::Deoint	Yes	No	No	No
	glue:qualileset	• AWS::Data lity et	Yes	No	Yes	Yes
	glue:ansfor	• AWS::ML form	Yes	No	Yes	Yes
	glue:ection	• AWS::Co ion	Yes	No	Yes	Yes
	glue:ler	• AWS::C	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	glue::strategy	• AWS::Resource	Yes	No	Yes	Yes
	glue::management	• AWS::Script	Yes	No	Yes	Yes
	glue::document type	• AWS::Custom	Yes	No	Yes	Yes
	glue::database	• AWS::Database	Yes	No	Yes	Yes
	glue::job	• AWS::Job	Yes	No	Yes	Yes
AWS Ground Station [groundstation]	groundstation::action	• N/A	Yes	No	No	No
	groundstation::profile	• AWS::GroundStationProfile	Yes	No	Yes	Yes
	groundstation::metric	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ground-tion:allite	• N/A	Yes	No	No	No
	ground-tion:ig	• AWS:ndSt::Co	Yes	No	Yes	Yes
	ground-tion:flow-endp oint-group	• AWS:ndSt::DawEncGrou	Yes	No	Yes	Yes
AWS HealthImaging [medical-imaging]	medical-imaging-tastoc	• AWS:thIm::Dare	Yes	No	Yes	Yes
	medical-imaging-tastoc-images	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS HealthLake [healthlake]	healthlake:dataplane	• AWS: HealthLake HIR	Yes	Yes	Yes	Yes
	healthlake:ALLPORT	• N/A	No	Yes	Yes	Yes
AWS HealthOmics [omics]	omics:otations	• AWS: omics::A	Yes	Yes	No	No
	omics:uence/reads	• N/A	Yes	Yes	No	No
	omics:erence/referen	• N/A	Yes	Yes	No	No
	omics:	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	omics cache	• N/A	Yes	No	No	No
	omics uences e	• AWS:s::Security	Yes	Yes	Yes	Yes
	omics iants	• AWS:s::VirtualStorage	Yes	Yes	No	No
	omics group	• AWS:s::Function	Yes	Yes	Yes	Yes
	omics kflow	• AWS:s::Workflow	Yes	Yes	Yes	Yes
	omics erence re	• AWS:s::Function	Yes	Yes	Yes	Yes
	omics otatio ore/ versi on	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	omics:kflow, version	• AWS::VPC::VPCFlowVe	Yes	No	No	No
	omics:_SUPPORD	• N/A	No	Yes	Yes	Yes
AWS IAM Access Analyzer [access-analyzer]	access-analyzer:analyze	• AWS::IAM::AccessAnalyzer	Yes	No	Yes	Yes
AWS IAM Identity Center [sso]	sso:permission	• AWS::IAM::PermissionSet	Yes	No	No	No
	sso:application	• AWS::IAM::Application	Yes	No	No	No
	sso:instance	• AWS::IAM::InstanceProfile	Yes	No	No	No
	sso:tokensuer	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Identity and Access Management (IAM) [iam]	iam:manage	• AWS:VirtFADe	Yes	Yes	Yes	Yes
	iam:service-registered-certificate	• AWS:ServiceCertificate	Yes	Yes	Yes	Yes
	iam:service-provider-identity	• AWS:ServiceIdentity	Yes	Yes	Yes	Yes
	iam:service-provider-identity	• AWS:ServiceIdentity	Yes	Yes	Yes	Yes
	iam:policy	• AWS:ManagedPolicy	Yes	Yes	No	No
	iam:role	• AWS:Role	Yes	No	Yes	Yes
	iam:user	• AWS:User	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iam:instance-profile	• AWS::InstanceProfile	Yes	Yes	Yes	Yes
	iam:AssumeRole	• N/A	No	Yes	Yes	Yes
AWS Identity and Access Management Roles Anywhere [nile]	nile:attest	• AWS::TrustAnchor	Yes	No	No	No
	nile:connect	• AWS::CloudFormation	Yes	No	No	No
	nile:connect	• N/A	Yes	No	No	No
	nile:connect	• AWS::P1	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Invoicing Service [invoicing]	invoice:portal-preference	• N/A	Yes	No	No	No
	invoice:invoice-unit	• AWS:invoice	Yes	No	Yes	Yes
AWS IoT Analytics [iotanalytics]	iotanalytics:channel	• AWS:iotanalytics:Channel	Yes	Yes	No	No
	iotanalytics:dataset	• AWS:iotanalytics:Dataset	Yes	Yes	No	No
	iotanalytics:dataset	• AWS:iotanalytics:Dataset	Yes	Yes	No	No
	iotanalytics:pipeline	• AWS:iotanalytics:Pipeline	Yes	Yes	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iotanalytics:ALLOPPORTED	• N/A	No	Yes	No	No
AWS IoT Core Device Advisor [iotdeviceadvisor]	iotdeviceadvisor:uitern	• N/A	Yes	No	No	No
	iotdeviceadvisor:uitern	• AWS:core[Advisory Suitability]	Yes	No	Yes	Yes
AWS IoT Events [iotevents]	iotevents:detectmodel	• AWS:venttectel	Yes	Yes	No	No
	iotevents:input	• AWS:ventput	Yes	Yes	No	No
	iotevents:alarmel	• AWS:ventarm	Yes	No	No	No
	iotevents:ALL_PORTS	• N/A	No	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS IoT Fleet Hub for Device Management [iotfleet hub]	iotfleet hub:application	• AWS: fleet Application	Yes	Yes	Yes	Yes
	iotfleet hub:ALPPORT	• N/A	No	Yes	Yes	Yes
AWS IoT FleetWise [iotfleet wise]	iotfleet wise:manifest	• AWS: fleet :Manifest	Yes	No	Yes	Yes
	iotfleet wise:vehicle	• AWS: fleet :Vehicle	Yes	No	Yes	Yes
	iotfleet wise:driver-manifest	• AWS: fleet :DriverManifest	Yes	No	Yes	Yes
	iotfleet wise:station-template	• AWS: fleet :StationPlatform	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iotfleetwise:fleetwise:Fl	• AWS: fleetwise:Fl	Yes	No	Yes	Yes
	iotfleetwise:s1-catalog	• AWS: fleetwise:Sig talc	Yes	No	Yes	Yes
	iotfleetwise:catalog:sign	• AWS: fleetwise:Can	Yes	No	Yes	Yes
AWS IoT Greengrass [greengrass]	greengrass:core:finit	• AWS: greengrass:core:lor	Yes	Yes	Yes	Yes
	greengrass:components:versions	• AWS: greengrass:Components:Ver	Yes	No	No	No
	greengrass:devicedefinition	• AWS: greengrass:device:initi	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	green:s:connection	• AWS: congruence • connection	Yes	Yes	Yes	Yes
	green:s:deployments	• N/A	Yes	No	No	No
	green:s:functiondefinition	• AWS: congruence • function	Yes	Yes	Yes	Yes
	green:s:bullet	• N/A	Yes	Yes	No	No
	green:s:resourcedefinition	• AWS: congruence • resource	Yes	Yes	Yes	Yes
	green:s:components	• N/A	Yes	No	No	No
	green:s:groups	• AWS: congruence • group	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	green:s:logs:define	• AWS:ingr ogge niti	Yes	Yes	Yes	Yes
	green:s:cores:ices	• N/A	Yes	No	No	No
	green:s:subscriptions:initi	• AWS:ingr ubsc onDe ion	Yes	Yes	Yes	Yes
	green:s:ALL:PORTE	• N/A	No	Yes	Yes	Yes
AWS IoT Managed Integrations [iotmanagedintegrations]	iotmanagedintegrations:task	• N/A	Yes	No	No	No
	iotmanagedintegrations:managed-thing	• AWS:anag egra ::Ma Thir	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iotmanaged-integrations:connect-or	• N/A	Yes	No	No	No
	iotmanaged-integrations:unt-association	• N/A	Yes	No	No	No
	iotmanaged-integrations:provision-profile	• AWS: analytics:RegistrationProfile	Yes	No	No	No
	iotmanaged-integrations:essential-locker	• AWS: analytics:RegistrationProfile	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS IoT SiteWise [iotsitewise]	iotsi se:po	• AWS: itev Port	Yes	No	Yes	Yes
	iotsi se:da ard	• AWS: itev Dash	Yes	No	Yes	Yes
	iotsi se:pro t	• AWS: itev Proj	Yes	No	Yes	Yes
	iotsi se:as	• AWS: itev Asse	Yes	Yes	Yes	Yes
	iotsi se:da t	• AWS: itev Data	Yes	No	Yes	Yes
	iotsi se:ti s eries	• N/ A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iot:se:com:ation:mod:el	• AWS:iteVComp onMc	Yes	No	No	No
	iot:se:as:model	• AWS:iteVAsse1	Yes	Yes	Yes	Yes
	iot:se:ga:y	• AWS:iteVGate	Yes	No	Yes	Yes
	iot:se:ac-policy	• AWS:iteVAcce icy	Yes	No	Yes	Yes
	iot:se:ALPPORT	• N/A	No	Yes	Yes	Yes
AWS IoT TwinMaker [iotdigit altwin]	iot:di:ltwin:kspac	• AWS:winM:Wor e	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iotdevice-ltwinspace-component-type	• AWS:winM:ComponentType	Yes	No	No	No
	iotdevice-ltwinspace-scene	• AWS:winM:Scene	Yes	No	No	No
	iotdevice-ltwinspace-sync-job	• AWS:winM:SyncJob	Yes	No	No	No
	iotdevice-ltwinspace-identity	• AWS:winM:Identity	Yes	No	No	No
AWS IoT Wireless [iotwireless]	iotwireless:signalkaccount	• AWS:wireless:Particour	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iotwireless:networkanalyticsconfiguration	• AWS:irelNetworkAnalyzerfiguration	Yes	No	Yes	Yes
	iotwireless:seeprofiling	• AWS:irelServiceofil	Yes	No	Yes	Yes
	iotwireless:multicastgroup	• AWS:irelMulticGroup	Yes	No	Yes	Yes
	iotwireless:wirelessgateway	• AWS:irelWirelessatev	Yes	No	Yes	Yes
	iotwireless:wirelessdevice	• AWS:irelWirelessdevic	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iotwireless:dedicated:destination	• AWS:irelDestination	Yes	No	Yes	Yes
	iotwireless:functional:task	• AWS:irelFunctionalTask	Yes	No	Yes	Yes
	iotwireless:improvement:task	• AWS:irelWirelessImprovementTask	Yes	No	Yes	Yes
	iotwireless:wirelessgateway:taskdefinition	• AWS:irelWirelessGatewayTaskDefinition	Yes	No	Yes	Yes
	iotwireless:device:profile	• AWS:irelDeviceProfile	Yes	No	Yes	Yes
	iotwireless:device:profile	• AWS:irelDeviceProfile	Yes	No	Yes	Yes
AWS IoT [iot]	iot:policy	• AWS:iot:SoftwarePackage	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iot:alarmrizer	• AWS:Auter	Yes	No	Yes	Yes
	iot:package/version	• AWS:SoftwarePackrsic	Yes	No	No	No
	iot:firmware	• AWS:Flexible	Yes	No	Yes	Yes
	iot:jobtemplate	• AWS:Jobate	Yes	No	Yes	Yes
	iot:billinggroup	• AWS:Billingrou	Yes	No	Yes	Yes
	iot:provisioningtemplate	• AWS:Provisioningate	Yes	No	Yes	Yes
	iot:thingtype	• AWS:Thinge	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iot:tlgroup	• AWS:Thrup	Yes	No	Yes	Yes
	iot:cficationvider	• AWS:Certificate	Yes	No	Yes	Yes
	iot:rolias	• AWS:Roles	Yes	No	Yes	Yes
	iot:ct	• AWS:CACertificate	Yes	No	Yes	Yes
	iot:cmmetric	• AWS:Custom	Yes	No	Yes	Yes
	iot:dnconfation	• AWS:Donnfiguration	Yes	No	No	No
	iot:py	• AWS:Policy	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iot:manage	• AWS: Mitigation	Yes	No	Yes	Yes
	iot:securityprofile	• AWS: Security Profile	Yes	No	Yes	Yes
	iot:rule	• AWS: Topic	Yes	No	Yes	Yes
	iot:scheduledaction	• AWS: Scheduled Action	Yes	No	Yes	Yes
	iot:topic	• N/A	Yes	No	No	No
	iot:subscription	• N/A	Yes	No	No	No
	iot:jobs	• N/A	Yes	No	No	No
	iot:ondemand	• N/A	Yes	No	No	No
	iot:connect	• AWS: Connect	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	iot:device	• AWS: :Din	Yes	No	Yes	Yes
AWS Key Management Service [kms]	kms:key	• AWS: :Key	Yes	Yes	Yes	Yes
	kms:ALUPPOR	• N/A	No	Yes	Yes	Yes
AWS Lambda [lambda]	lambda:yer/versi	• AWS: da:: Vers	Yes	No	No	No
	lambda:yer/versi	• AWS: da:: Vers	Yes	No	No	No
	lambda:yer	• N/A	Yes	No	No	No
	lambda:ction	• AWS: da:: ion	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	lambda:ent-source-e-mapping	• AWS::Source::ping	Yes	No	Yes	Yes
	lambda:de-signi-g-confi	• AWS::da::signi-g-fig	Yes	No	Yes	Yes
	lambda:L_SUPP-ED	• N/A	No	Yes	Yes	Yes
AWS Launch Wizard [launchwizard]	launchwizard:deployment	• AWS::LaunchWizard::Deployment	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS License Manager Linux Subscriptions Manager [license-manager-linux-subscriptions]	license-manager-linux-subscriptions-providers	• N/A	Yes	No	No	No
AWS License Manager User Subscriptions [license-manager-user-subscriptions]	license-manager-user-subscriptions	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	license-management:manage-user-subscription:identify-provider	• N/A	Yes	No	No	No
	license-management:manage-user-subscription:instance-user	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	license-management:aws-er-subscription:license-server-endpoint	• N/A	Yes	No	No	No
AWS License Manager [license-manager]	license-management:asset-group	• N/A	Yes	No	No	No
	license-management:license	• AWS:arn::license	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	license-manager:manage-cense-ass-et-rules	• N/A	Yes	No	No	No
	license-manager:manage-cense-con-figura-tion	• N/A	Yes	No	No	No
	license-manager:port-generator	• N/A	Yes	No	No	No
	license-manager:ant	• AWS: nseM r::C	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS MWAAS Serverless [airflow-serverless]	airflow-serverless:work	• N/A	Yes	No	No	No
AWS Mainframe Modernization Application Testing [apptest]	apptest:estsu	• N/A	Yes	No	No	No
	apptest:estco	• N/A	Yes	No	No	No
	apptest:estca	• AWS:est:Case	Yes	No	Yes	Yes
	apptest:estru	• N/A	Yes	No	No	No
AWS Mainframe Modernization Service [m2]	m2:ap	• AWS:App	Yes	No	No	No
	m2:en	• AWS:Envi	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Marketplace Vendor Insights [vendor-insights]	vendor-insights-profile	• N/A	Yes	No	No	No
	vendor-insights-source	• N/A	Yes	No	No	No
AWS Marketplace [aws-marketplace]	aws-marketplace-arames	• N/A	Yes	No	No	No
	aws-marketplace-anges	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Migration Hub Orchestrator [migrationhub-orchestrator]	migrationhub-orchestrator-workflow	• N/A	Yes	No	No	No
	migrationhub-orchestrator-template	• N/A	Yes	No	No	No
AWS Migration Hub Refactor Spaces [refactor-spaces]	refactor-spaces-environment/application	• AWS: refactor-spaces::Automatic	Yes	No	Yes	Yes
	refactor-spaces-environment/application/service	• AWS: refactor-spaces::Service	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	refactor/space/virtual	• AWS: refactor/s:Environment	Yes	No	Yes	Yes
	refactor/space/virtual/application/route	• AWS: refactor/s:Environment	Yes	No	Yes	Yes
AWS Network Firewall [network-firewall]	networkfirewall:statefulrulegroup	• AWS: networkfirewall:statefulrulegroup	Yes	Yes	Yes	Yes
	networkfirewall:pc-endpoint-association	• AWS: networkfirewall:pc-endpoint-association	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	networkfirewall:firewallpolicy	• AWS::NetworkFirewall::FirewallPolicy	Yes	Yes	Yes	Yes
	networkfirewall:statefulrulegroup	• AWS::NetworkFirewall::FirewallPolicyRuleGroup	Yes	Yes	No	No
	networkfirewall:firewallpolicy	• AWS::NetworkFirewall::FirewallPolicy	Yes	Yes	Yes	Yes
	networkfirewall:statefulrulegroup	• N/A	No	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Network Manager [networkmanager]	networkmanager	• AWS: networkmanager::tagGatewayInterface	Yes	No	No	No
	networkmanagerbal-networkark	• AWS: networkmanager::CloudNetwork	Yes	No	Yes	Yes
	networkmanagerk	• AWS: networkmanager::link	Yes	No	Yes	Yes
	networkmanager-e-network	• AWS: networkmanager::CloudNetwork	Yes	No	Yes	Yes
	networkmanagerice	• AWS: networkmanager::link	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	networkmanagerconnect-peer	AWS::NetworkManager::ConnectPeer	Yes	No	Yes	Yes
	networkmanagerachment	- AWS::NetworkManager::VpnAttachment - AWS::NetworkManager::TransitAttachment	Yes	No	No	No
	networkmanageredge	AWS::NetworkManager::SiteToSiteGateway	Yes	No	Yes	Yes
	networkmanagerconnection	N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS OpsWorks Configuration Management [opsworks-cm]	opsworks:cm:se	• N/A	Yes	No	No	No
	opsworks:cm:ba	• N/A	Yes	No	No	No
AWS OpsWorks [opsworks]	opsworks:install	• AWS::OpsWorks::InstanceProfile	Yes	No	No	No
	opsworks:stack	• AWS::OpsWorks::Stack	Yes	No	No	No
	opsworks:layer	• AWS::OpsWorks::Layer	Yes	No	No	No
AWS Organizations [organizations]	organizations:unt	• AWS::Organizations::Account	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	organizations:CreateOrganization	• AWS::Organization::Organization	Yes	Yes	Yes	Yes
	organizations:AcceptTosAndTermsOfService	• AWS::ResourceGroups::ResourceGroup	Yes	No	Yes	Yes
	organizations:AttachPolicy	• N/A	Yes	Yes	No	No
	organizations:CreatePolicy	• AWS::Policy::Policy	Yes	Yes	No	No
	organizations:DeletePolicy	• N/A	No	Yes	Yes	Yes
AWS Outposts [outposts]	outposts:CreateSite	• N/A	Yes	No	No	No
	outposts:DeleteSite	• N/A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Panorama [panorama]	panorama:package	• AWS:panorama:package	Yes	No	Yes	Yes
	panorama:applicationinstance	• AWS:panorama:applicationinstance	Yes	No	No	No
	panorama:device	• N/A	Yes	No	No	No
AWS Parallel Computing Service [pcs]	pcs:cluster	• AWS:ecs:Cluster	Yes	No	No	No
	pcs:queue	• AWS:ecs:Queue	Yes	No	No	No
	pcs:containergroup	• AWS:ecs:ContainerGroup	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Partner Central Selling [partnercentral]	partnercentral-opportunity	• N/A	Yes	No	No	No
	partnercentral-agreement-by-accepting-invitation-task	• N/A	Yes	No	No	No
	partnercentral-offer-from-opportunity-task	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Payment Cryptography [payment-cryptography]	payment-cryptography:key	• AWS: entC graph ey	Yes	No	Yes	Yes
AWS Payments [payments]	payment-instruction	• N/A	Yes	No	No	No
AWS Performance Insights [pi]	performance-report	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Private CA Connector for Active Directory [pca-connector-ad]	pca-connector-ad:connector	• AWS: Connector	Yes	No	No	No
	pca-connector-ad:connector-template	• AWS: Connector	Yes	No	No	No
	pca-connector-ad:directoryRegistration	• AWS: Connector	Yes	No	No	No
AWS Private CA Connector for SCEP [pca-connector-scep]	pca-connector-scep:connector	• AWS: Connector	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Private Certificate Authority [acm-pca]	acm-pca:certificate-authority	• AWS:CA::certificate-hierarchy	Yes	Yes	Yes	Yes
	acm-pca:ALL_SUTED	• N/A	No	Yes	Yes	Yes
AWS Proton [proton]	proton:environment-template	• AWS:Proton::onmentplat	Yes	No	Yes	Yes
	proton:environment	• N/A	Yes	No	No	No
	proton:service, service-instance	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	protocol: positive	• N/A	Yes	No	No	No
	protocol: component	• N/A	Yes	No	No	No
	protocol: environment - account connection	• AWS::IAM::Connection	Yes	No	Yes	Yes
	protocol: service	• N/A	Yes	No	No	No
	protocol: deployment	• N/A	Yes	No	No	No
	protocol: service template	• AWS::CloudFormation::Template	Yes	No	Yes	Yes
AWS Purchase Orders Console [purchase-orders]	purchase-orders: purchase-order	• N/A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS RTB Fabric [rtbfabric]	rtbfabric:required	• AWS: abriques-tewa	Yes	No	No	No
	rtbfabric:response	• AWS: abriques-tewa	Yes	No	No	No
AWS Recycle Bin [rbin]	rbin::Rule	• AWS::Rule	Yes	Yes	Yes	Yes
	rbin::SUPPORT	• N/A	No	Yes	Yes	Yes
AWS Resilience Hub [resiliencyhub]	resiliencyhub:assessment	• N/A	Yes	No	No	No
	resiliencyhub:policy	• AWS: liencyhub::Rule	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	resilience:recommended-template	• N/A	Yes	No	No	No
	resilience:application::Application	• AWS:Application	Yes	No	Yes	Yes
AWS Resource Access Manager (RAM) [ram]	ram:resource-share	• AWS:ResourceShare	Yes	Yes	Yes	Yes
	ram:resource-share-invitation	• N/A	Yes	No	No	No
	ram:permission	• N/A	Yes	No	No	No
	ram:AssociateUPPORD	• N/A	No	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Resource Groups [resource-groups]	resourcegroup:*	• AWS: resourcegroups::*	Yes	Yes	Yes	Yes
	resourcegroup:L_SUPPRESSED	• N/A	No	Yes	Yes	Yes
AWS RoboMaker [robomaker]	robomaker:worldgenerationjob	• N/A	Yes	No	No	No
	robomaker:worldgenerationjobs	• N/A	Yes	No	No	No
	robomaker:simulation-job-batch	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	robomaker:simulation-job	• N/A	Yes	No	No	No
	robomaker:world-template	• N/A	Yes	No	No	No
	robomaker:robot-makebot	• AWS: Makebot	Yes	No	No	No
	robomaker:world-export-job	• N/A	Yes	No	No	No
	robomaker:simulation-application	• AWS: Make simulation application	Yes	No	No	No
	robomaker:deploy-robot-job	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS SQL Workbench [sqlworkbench]	robomaker:robotapplication	• AWS: MakebotApplication	Yes	No	Yes	Yes
	robomaker:deployment-fleet	• AWS: Makefleet	Yes	No	No	No
	robomaker:world	• N/A	Yes	No	No	No
	sqlworkbench:query	• N/A	Yes	No	No	No
	sqlworkbench:notebook	• N/A	Yes	No	No	No
	sqlworkbench:cluster	• N/A	Yes	No	No	No
	sqlworkbench:connection	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Savings Plans [savingsplans]	savingsplans:*	• N/A	Yes	No	No	No
AWS Secrets Manager [secretsmanager]	secretsmanager:*	• AWS:SecretsManager::SecretsManager	Yes	Yes	Yes	Yes
	secretsmanager:_SUPPRESS*	• N/A	No	Yes	Yes	Yes
AWS Security Hub [securityhub]	securityhub:compliancev2	• N/A	Yes	No	No	No
	securityhub:automation-rulev2	• AWS:SecurityHub::AutomationRules	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	security:authentication-rule	• AWS: Authority AutomationRule	Yes	No	No	No
	security:aggregator	• AWS: Authority AggregatorV2	Yes	No	No	No
	security:hub	• AWS: Authority Hub	Yes	No	Yes	Yes
	security:protect-subscription	• AWS: Authority ProtectionSubscription	Yes	No	No	No
	security:hub	• AWS: Authority Hub	Yes	No	No	No
	security:compliance-policy	• AWS: Authority ConfigurationPolicy	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Service - Oracle Database@AWS [odb]	odb:cluster	• AWS: :Cluster	Yes	No	No	No
	odb:cluster-exadata-infra-structure	• AWS: :Cluster-exadata-infra-structure	Yes	No	No	No
	odb:database-node	• N/A	Yes	No	No	No
	odb:cluster-autonomous-us-vml-cluster	• AWS: :Cluster-autonomous-us-vml-cluster	Yes	No	No	No
	odb:oracle-peering-connection	• AWS: :Oracle-peering-connection	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	oddb:ondnetwork	• AWS::Odtkark	Yes	No	No	No
AWS Service Catalog [catalog]	catalogortfor	• AWS::ice(Cg::Flio	Yes	Yes	Yes	Yes
	catalogroduc	• AWS::ice(Cg::Corma rovi dProc	Yes	Yes	No	No
	catalogLL_SUITED	• N/A	No	Yes	Yes	Yes
AWS Service Catalog [servicecatalog]	servicetatalogributogr oups	• AWS::ice(CgApp try: ibut p	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	Cloud Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	servicecatalog:licata	• AWS:iceCloudApptry:ic	Yes	Yes	Yes	Yes
	servicecatalog:_SUPPORTD	• N/A	No	Yes	Yes	Yes
AWS Shield [shield]	shield:otect	• AWS:ld::ctio	Yes	No	No	No
	shield:otect:group	• AWS:ld::ctio: p	Yes	No	No	No
AWS Signer [signer]	signer:gning:pro:files	• AWS:er::ngPr	Yes	No	Yes	Yes
AWS SimSpace Weaver [simspace weaver]	simspace:weaver:ulation	• AWS:space:er::Stior	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Snow Device Management [snow-device-management]	snow-device-management:	• N/A	Yes	No	No	No
	snow-device-management:tagged-device	• N/A	Yes	No	No	No
AWS Step Functions [states]	states:execution	• N/A	Yes	No	No	No
	states:activity	• AWS::Activity	Yes	Yes	Yes	Yes
	states:state-machine	• AWS::StepFunctions::StateMachine	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	stateful-supplied	• N/A	No	Yes	Yes	Yes
AWS Storage Gateway [storagegateway]	storagegateway-ephemeral	• N/A	Yes	No	No	No
	storagegateway-association	• N/A	Yes	No	No	No
	storagegateway-e	• N/A	Yes	Yes	No	No
	storagegateway	• N/A	Yes	Yes	No	No
	storagegateway/volume	• N/A	Yes	Yes	No	No
	storagegateway-re	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS Supply Chain [scn]	scn:instance	• N/A	Yes	No	No	No
	scn:buildformat:simplified	• N/A	Yes	No	No	No
AWS Systems Manager Incident Manager Contacts [ssm-contacts]	ssm-contacts:contact	• AWS: Contact	Yes	Yes	No	No
	ssm-contacts:rotation	• AWS: Contact Rotation	Yes	No	No	No
	ssm-contacts:ALLOWED	• N/A	No	Yes	No	No
AWS Systems Manager Incident Manager [ssm-incidents]	ssm-incidents:incident-record	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ssm-incidents:replicationset	• AWS:Incidents	Yes	No	Yes	Yes
	ssm-incidents:response-plan	• AWS:Incidents:ResponsePlans	Yes	No	Yes	Yes
AWS Systems Manager Quick Setup [ssm-quicksetup]	ssm-quicksetup:figuremanagem	• AWS:QuickSetup::ConfigurationManager	Yes	No	No	No
AWS Systems Manager [ssm]	ssm:managed-instance	• N/A	Yes	Yes	No	No
	ssm:document	• AWS:Documents	Yes	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ssm:action:definition	• N/A	Yes	No	No	No
	ssm:parameter	• AWS:Parameter	Yes	No	Yes	Yes
	ssm:action:execution	• N/A	Yes	Yes	No	No
	ssm:operation	• N/A	Yes	Yes	No	No
	ssm:parameter:baseline	• AWS:Parameter	Yes	Yes	Yes	Yes
	ssm:session	• N/A	Yes	Yes	No	No
	ssm:action:association	• AWS:Association	Yes	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ssm:manageinstances:download	• AWS:Mainline	Yes	Yes	Yes	Yes
	ssm:opentadapters	• N/A	Yes	No	No	No
	ssm:AssociateUPPOR	• N/A	No	Yes	Yes	Yes
AWS Systems Manager for SAP [ssm-sap]	ssm-sap:hana/db	• N/A	Yes	No	No	No
	ssm-sap:hana	• AWS:SystemsManagerSAPlicat	Yes	No	No	No
AWS Telco Network Builder [tnb]	tnb:network-instance	• N/A	Yes	No	No	No
	tnb:function-instance	• N/A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	tnb:financial-package	• N/A	Yes	No	No	No
	tnb:network-package	• N/A	Yes	No	No	No
	tnb:network-operation	• N/A	Yes	No	No	No
AWS Transfer Family [transfer]	transfer:connect	• AWS:transfer	Yes	No	Yes	Yes
	transfer:user	• AWS:transfer	Yes	Yes	Yes	Yes
	transfer:workflows	• AWS:transfer	Yes	Yes	Yes	Yes
	transfer:webapp	• AWS:transfer App	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	trans:agree	• AWS:sfer eeme	Yes	No	Yes	Yes
	trans:host-key	• N/A	Yes	No	No	No
	trans:serve	• AWS:sfer ver	Yes	Yes	Yes	Yes
	trans:certi-te	• AWS:sfer tifi	Yes	No	Yes	Yes
	trans:profil	• AWS:sfer file	Yes	No	Yes	Yes
	trans:ALL_SRTED	• N/A	No	Yes	Yes	Yes
	trans:	• N/A	Yes	No	No	No
AWS Transform [transform]	trans:conn	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
AWS User Notifications Contacts [notifications-contacts]	notifications-contacts:notificationcontacts	• AWS: notificationcontacts:EmailContact	Yes	No	Yes	Yes
AWS User Notifications [notifications]	notifications:notificationconfiguration	• AWS: notificationconfiguration:NotificationConfiguration	Yes	No	No	No
AWS WAF Regional [waf-regional]	waf-regional:rule	• AWS: waf-regional:Rule	Yes	No	No	No
	waf-regional:rulegroup	• N/A	Yes	No	No	No
	waf-regional:rulebasedrule	• AWS: waf-regional:Rule	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	waf-regional:web-acl	• AWS: Regional WebACL	Yes	No	No	No
AWS WAF [waf]	waf:rulegroup	• N/A	Yes	No	No	No
	waf:web-acl	• AWS: WebACL	Yes	No	No	No
	waf:rulebasedrule	• N/A	Yes	No	No	No
	waf:rule:rule	• AWS: Rule	Yes	No	No	No
AWS Well-Architected Tool [wellarchitected]	wellarchitected:templates	• N/A	Yes	No	No	No
	wellarchitected:view-template	• N/A	Yes	No	No	No
	wellarchitected:workload	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	wellknown:protectedprofile	• N/A	Yes	No	No	No
	wellknown:protectedL_SUPPLIED	• N/A	No	Yes	No	No
AWS Wickr [wickr]	wickr:work	• N/A	Yes	Yes	No	No
	wickr:_SUPPORTED	• N/A	No	Yes	No	No
AWS WorkSpaces Managed Instances [workspaces-instances]	workspaces:workspaceinstance	• AWS:workspaceinstance	Yes	No	No	No
AWS X-Ray [xray]	xray:logging-rule	• AWS::SageMaker	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	xray:group	• AWS::GuardDuty	Yes	No	Yes	Yes
AWS rePost Private [repostspace]	repostspace:space	• N/A	Yes	No	No	No
AWS service providing managed private networks [private-networks]	privatenetworksite	• N/A	Yes	No	No	No
	privatenetworkorder	• N/A	Yes	No	No	No
	privatenetwork	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	private-network-network-resource	• N/A	Yes	No	No	No
	private-network-device-identification	• N/A	Yes	No	No	No
Alexa for Business [a4b]	a4b:profile	• N/A	Yes	No	No	No
	a4b:assignment-book	• N/A	Yes	No	No	No
	a4b:network-profile	• N/A	Yes	No	No	No
	a4b:usage	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	a4b:co rence pro vider	• N/ A	Yes	No	No	No
	a4b:s - group	• N/ A	Yes	No	No	No
	a4b:ro	• N/ A	Yes	No	No	No
	a4b:g ay- group	• N/ A	Yes	No	No	No
	a4b:s ule	• N/ A	Yes	No	No	No
	a4b:co ct	• N/ A	Yes	No	No	No
	a4b:de	• N/ A	Yes	No	No	No
Amazon AI Operations [aiops]	aiops estig n- group	• AWS: s::l igat oup	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon API Gateway Management [apigateway]	apigateway:users	• N/A	Yes	No	No	No
	apigateway:apikeys	• N/A	Yes	Yes	No	No
	apigateway:clientcertificates	• N/A	Yes	No	No	No
	apigateway:resources	• N/A	Yes	Yes	No	No
	apigateway:domains	• AWS: managed V2	Yes	Yes	No	No
	apigateway:domainameassociations	• AWS: managed Association	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	apigateway:vpcs	• N/A	Yes	No	No	No
	apigateway:ALL_PORTS	• N/A	No	Yes	No	No
Amazon ARC Region switch [arc-region-switch]	arc-region-switch-plan	• AWS: region::	Yes	No	No	No
Amazon AppFlow [appflow]	appflow:connections	• AWS: flow::ectd	Yes	No	No	No
	appflow:low	• AWS: low::	Yes	No	Yes	Yes
Amazon AppIntegrations [app-integrations]	app-integration-application-association	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	app-integration-ata-integration	AWS: integration	Yes	No	Yes	Yes
	app-integration-vent-integration	AWS: integration	Yes	No	Yes	Yes
	app-integration-ata-integration-as-social	N/A	Yes	No	No	No
	app-integration-application	AWS: integration	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	app-integration-vent-integration-association	• N/A	Yes	No	No	No
Amazon AppStream 2.0 [appstream]	appstream:image	• N/A	Yes	No	No	No
	appstream:application-block	• AWS:treapBlock	Yes	No	Yes	Yes
	appstream:stack	• AWS:treack	Yes	No	Yes	Yes
	appstream:application-block-builder	• AWS:treapBlock-builder	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	appstore:fleet	• AWS: treat as fleet	Yes	No	Yes	Yes
	appstore:imagebuilder	• AWS: treat as imageBuilder	Yes	No	Yes	Yes
	appstore:application	• AWS: treat as application	Yes	No	Yes	Yes
Amazon Athena [athena]	athena:attach	• AWS: Athena::attach	Yes	No	Yes	Yes
	athena:capacityreservation	• AWS: Athena::capacityreservation	Yes	No	Yes	Yes
	athena:workgroup	• AWS: Athena::workgroup	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	athena:GET_METADATA	• N/A	No	Yes	Yes	Yes
Amazon Aurora DSQL [dsql]	dsql:terminate	• AWS::DSQL::Cluster	Yes	No	Yes	Yes
Amazon Bedrock [bedrock-agentcore]	bedrock:agentcore-workload-identity	• AWS::Bedrock/AgentCore::LoadIdentity	Yes	No	No	No
	bedrock:agentcore-code-interpreter-custom	• AWS::Bedrock/AgentCore::InterpreterCustom	Yes	No	No	No
	bedrock:agentcore-gateway	• AWS::Bedrock/AgentCore::Gateway	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	bedrock-agent-tokens-vault	• N/A	Yes	No	No	No
	bedrock-agent-memory	• AWS:rock/core:ry	Yes	No	No	No
	bedrock-agent-workload-identity-direct	• N/A	Yes	No	No	No
	bedrock-agent-runtime	• AWS:rock/core:ime	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	bedrock-agent-core-browser-custom	• AWS:rock/core/serC	Yes	No	No	No
	bedrock-agent-runtime-endpoint	• AWS:rock/core/runtime	Yes	No	No	No
Amazon Bedrock [bedrock]	bedrock-model-copy-job	• N/A	Yes	No	No	No
	bedrock-custom-model-deployment	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	bedrock-prompt-router	• N/A	Yes	No	No	No
	bedrock-agent-alias	• AWS:rock:tAlias	Yes	No	Yes	Yes
	bedrock-luepr	• AWS:rock:priority	Yes	No	Yes	Yes
	bedrock-model-customization-job	• N/A	Yes	No	No	No
	bedrock-model-import-job	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	bedrock:ata-automation-invocation	• N/A	Yes	No	No	No
	bedrock:ata-automation-invocation-job	• N/A	Yes	No	No	No
	bedrock:automate-reasoning-policy	• AWS:rock:mateoniracy	Yes	No	No	No
	bedrock:odel-evaluation-job	• N/A	Yes	No	No	No
	bedrock:ession	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	bedrock:prompt	• AWS:rock:pt	Yes	No	Yes	Yes
	bedrock:guardr	• AWS:rock:drai	Yes	No	Yes	Yes
	bedrock:sync-invoke	• N/A	Yes	No	No	No
	bedrock:low/alias	• N/A	Yes	No	No	No
	bedrock:prompt-version	• AWS:rock:ptVer	Yes	No	No	No
	bedrock:ata-automation-project	• AWS:rock:AutoProc	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	bedrock-provisioned-model	• N/A	Yes	No	No	No
	bedrock-provisioned-model-v2	• N/A	Yes	No	No	No
	bedrock-application-inference-profile	• AWS:rock:inference-profile	Yes	No	Yes	Yes
	bedrock-import-model	• N/A	Yes	No	No	No
	bedrock-low	• AWS:rock:	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	bedrock-low/alias	• AWS:rock:Alias	Yes	No	No	No
	bedrock-low-alias	• AWS:rock:Alias	Yes	No	No	No
	bedrocknowledgebase	• AWS:rock:ledge	Yes	No	Yes	Yes
	bedrockgent	• AWS:rock:t	Yes	No	Yes	Yes
	bedrockodel-invo cation job	• N/A	Yes	No	No	No
	bedrockustom model	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	bedrock - job	• N/A	Yes	No	No	No
Amazon Braket [braket]	braket-antum-task	• N/A	Yes	No	No	No
	braket-b	• N/A	Yes	No	No	No
	braket-ending-limit	• N/A	Yes	No	No	No
Amazon Chime [chime]	chime-timing	• N/A	Yes	Yes	No	No
	chime-media-application	• N/A	Yes	No	No	No
	chime	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	chime - installation / bot	• N/A	Yes	No	No	No
	chime - ce-profile-domain	• N/A	Yes	No	No	No
	chime - installation / channel	• N/A	Yes	Yes	No	No
	chime - installation / user	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	chime-ia-pipeline-s-videos-streampool	• N/A	Yes	No	No	No
	chime-instances	• N/A	Yes	Yes	No	No
	chime-ia-pipeline	• N/A	Yes	Yes	No	No
	chime-ce-connector	• N/A	Yes	No	No	No
	chime	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	chime:ia-insights-pipeline-configuration	• N/A	Yes	No	No	No
	chime:_SUPPORT	• N/A	No	Yes	No	No
Amazon Cloud Directory [clouddirectory]	clouddirectory:*	• N/A	Yes	No	No	No
Amazon CloudFront [cloudfront]	cloudfront:vpcon	• AWS: CloudFront	Yes	No	No	No
	cloudfront:connection-function	• AWS: CloudFront	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	cloudformation:DistributionList	• AWS: dFromDistributionTemplate	Yes	No	No	No
	cloudformation:Distribution	• AWS: dFromDistribution	Yes	Yes	Yes	Yes
	cloudformation:AnyResourceIpList	• AWS: dFromAnyResourceIpList	Yes	No	No	No
	cloudformation:KeyValuePairStore	• AWS: dFromKeyValuePairStore	Yes	No	No	No
	cloudformation:KeyValuePairStore	• AWS: dFromKeyValuePairStore	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	cloudformation:tagging-distribution	• AWS: CloudFormation	Yes	Yes	No	No
	cloudformation:tagstore	• N/A	Yes	No	No	No
	cloudformation:connection-group	• AWS: CloudFormation Group	Yes	No	Yes	Yes
	cloudformation:PORTER	• N/A	No	Yes	Yes	Yes
Amazon CloudSearch [cloudsearch]	cloudsearch:domain	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon CloudWatch Application Insights [applicationinsights]	applicationinsights:application	• AWS: applicationinsights	Yes	No	Yes	Yes
Amazon CloudWatch Application Signals [application-signals]	application-signals:signal	• AWS: application-signals	Yes	No	Yes	Yes
Amazon CloudWatch Evidently [evidently]	evidently:segment	• AWS: evidently	Yes	No	No	No
	evidently:project	• AWS: evidently	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	evidence:project	• AWS:entl • object	Yes	No	No	No
	evidence:project features	• AWS:entl • attribute	Yes	No	No	No
	evidence:experiment	• AWS:entl • period	Yes	No	No	No
	evidence:project experiment	• AWS:entl • period	Yes	No	No	No
Amazon CloudWatch Internet Monitor	internetmonitor	• AWS:rnet • or::or	Yes	Yes	Yes	Yes
Amazon CloudWatch Internet Monitor [internetmonitor]	internetmonitor L_SUPP ED	• N/A	No	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon CloudWatch Logs [logs]	logs:CreateLogGroup	• AWS::Logs::LogGroup	Yes	Yes	Yes	Yes
	logs:CreateLogStream	• AWS::Logs::LogStream	Yes	No	Yes	Yes
	logs:PutLogEvents	• N/A	Yes	No	No	No
	logs:DescribeLogStreams	• AWS::Logs::LogStream	Yes	Yes	Yes	Yes
	logs:DescribeLogGroups	• AWS::Logs::LogGroup	Yes	No	Yes	Yes
	logs:DeleteLogStream	• AWS::Logs::LogStream	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	logs:cloudtrail:very	• AWS::Default	Yes	No	Yes	Yes
Amazon CloudWatch Network Synthetic Monitor [networkmonitors]	networkmonitors	• N/A	Yes	No	No	No
	networkmonitors:be	• N/A	Yes	No	No	No
Amazon CloudWatch Observability Access Manager [oam]	oam:logs	• AWS::Logs	Yes	Yes	No	No
	oam:services	• AWS::Service	Yes	Yes	Yes	Yes
	oam:API:UPPER	• N/A	No	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon CloudWatch Observability Admin Service [observabilityadmin]	observability:organization-telemetry-rule	• AWS: rvaAdminTernTelRule	Yes	No	No	No
	observability:s3tagintegration	• N/A	Yes	No	No	No
	observability:telemetry-rule	• AWS: rvaAdminTernTelRule	Yes	No	No	No
	observability:telemetry-pipeline	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	observability:organization-centralized-rule	• AWS: AWS::OrganizationCentralization	Yes	No	No	No
Amazon CloudWatch Synthetics [synthetics]	synthetics:groups	• AWS: AWS::Synthetics::Group	Yes	No	Yes	Yes
	synthetics:canaries	• AWS: AWS::Synthetics::Canary	Yes	No	Yes	Yes
Amazon CloudWatch [cloudwatch]	cloudwatch:metrics-stream	• AWS: AWS::CloudWatch::MetricStream	Yes	Yes	Yes	Yes
	cloudwatch:logs	• N/A	Yes	No	No	No
	cloudwatch:insights-rule	• AWS: AWS::CloudWatch::InsightsRule	Yes	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	cloudh:alarm	• AWS: CloudWatch Alarm	Yes	Yes	Yes	Yes
	cloudh:ALL_PORTS	• N/A	No	Yes	Yes	Yes
Amazon CodeCatalyst [codecatalyst]	codecat:identity-center-applications	• N/A	Yes	No	No	No
	codecat:storage	• N/A	Yes	No	No	No
	codecat:configuration	• N/A	Yes	Yes	No	No
	codecat:API_SUPPORT	• N/A	No	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon CodeGuru Profiler [codeguru-profiler]	codeguru-profiler:group	• AWS: CodeGuru Profiler: ilirp	Yes	No	Yes	Yes
Amazon CodeGuru Reviewer [codeguru-reviewer]	codeguru-reviewer:association	• AWS: CodeGuru Reviewer: sitcocial	Yes	Yes	Yes	Yes
	codeguru-reviewer:codework	• N/A	Yes	No	No	No
	codeguru-reviewer:ALL_SORTED	• N/A	No	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon CodeGuru Security [codeguru-security]	codegurusecurityscans	• N/A	Yes	Yes	No	No
	codegurusecurityscansALL_SUPPORTED	• N/A	No	Yes	No	No
Amazon CodeWhisperer [codewhisperer]	codewhispererfile	• N/A	Yes	No	No	No
	codewhisperercompliance	• N/A	Yes	No	No	No
Amazon Cognito Identity [cognito-identity]	cognitoidentityprovider	• AWS:Cognito:identityprovider	Yes	Yes	Yes	Yes
	cognitoidentityproviderALL_SUPPORTED	• N/A	No	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Cognito Identity [cognito-idp]	cognito:identityprovider:use	• AWS: Cognito: Pool	Yes	Yes	Yes	Yes
	cognito:identityprovider:ALLOWPORT	• N/A	No	Yes	Yes	Yes
Amazon Comprehend [comprehend]	comprehend:target-sentiment-detection-job	• N/A	Yes	No	No	No
	comprehend:entity-recognition-endpoint	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	compliance:send-notification-job	• N/A	Yes	No	No	No
	compliance:flywheel	• AWS:rehydrate	Yes	No	Yes	Yes
	compliance:document-classifier-endpoint	• N/A	Yes	No	No	No
	compliance:entity-recognition	• N/A	Yes	Yes	No	No
	compliance:topology-detection-job	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	compliance-detection-job	• N/A	Yes	No	No	No
	compliance-document-classifier	• AWS: reheal associated	Yes	Yes	Yes	Yes
	compliance-key-phrases-detection-job	• N/A	Yes	No	No	No
	compliance-document-classification-job	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	compliance:entitlements-detection-job	• N/A	Yes	No	No	No
	compliance:domain-translation-language-detection-job	• N/A	Yes	No	No	No
	compliance:flywheel/dataset	• N/A	Yes	No	No	No
	compliance:pii-entities-detection-job	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	compr d:ALL PORTE	• N/ A	No	Yes	Yes	Yes
Amazon Connect Cases [cases]	cases ated- item	• N/ A	Yes	No	No	No
	cases ain/ case/ relate i tem	• N/ A	Yes	No	No	No
	cases out	• N/ A	Yes	No	No	No
	cases ld	• N/ A	Yes	No	No	No
	cases plate	• N/ A	Yes	No	No	No
	cases ain/ case	• N/ A	Yes	No	No	No

Amazon Connect Customer Profiles [profile]	profile: object-types	• AWS: ome: les: ctTy	Yes	No	Yes	Yes
	profile: object-types	• N/A	Yes	No	No	No
	profile: object-types	• AWS: ome: les: in	Yes	No	Yes	Yes
	profile: object-types	• AWS: ome: les: grat	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Connect Outbound Campaigns [connect-campaigns]	connect-campaigns	• AWS: ConnectOutboundCampaigns	Yes	No	Yes	Yes
Amazon Connect Voice ID [voiceid]	voiceid	• AWS: ConnectVoiceID	Yes	No	No	No
Amazon Connect [connect]	connect-instancevaluation-form	• AWS: ConnectInstanceEvaluationForm	Yes	No	Yes	Yes
	connect-instanceattachment-state	• AWS: ConnectInstanceAttachmentState	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	connected instances exist	• N/A	Yes	No	No	No
	connected instances transferred to destination	• AWS: select: kCor	Yes	Yes	Yes	Yes
	connected instances use-case	• N/A	Yes	No	No	No
	connected instances tickcount	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	connect instance task-template	• AWS: select: Temp	Yes	No	Yes	Yes
	connect instance agent	• AWS: select:	Yes	Yes	Yes	Yes
	connect traffic distribution-group	• AWS: select: distribution-up	Yes	No	No	No
	connect instance workflow-module	• AWS: select: workflow-module	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	connection-number	• AWS: select: eNumber	Yes	No	Yes	Yes
	connection-agent-group	• AWS: select: Hier Group	Yes	No	No	No
	connection-instance-operation-hours	• AWS: select: sOfCion	Yes	No	Yes	Yes
	connection-instance-security-profile	• AWS: select: rity le	Yes	No	Yes	Yes
	connection-ildcontact	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	connect:instancequeue	• AWS:connect	Yes	Yes	Yes	Yes
	connect:instancecontactevaluation	• N/A	Yes	No	No	No
	connect:instance-rule	• AWS:connect	Yes	No	Yes	Yes
	connect:instance-integration-association	• AWS:connect:gratify:social	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	connection instance contact flow	• AWS: select active	Yes	Yes	Yes	Yes
	connection instance vocabulary	• N/A	Yes	No	No	No
	connection instance	• AWS: selectance	Yes	No	Yes	Yes
	connection instance routing profile	• AWS: selectingFile	Yes	Yes	Yes	Yes
	connection instance eue	• N/A	Yes	No	No	No
	connection instance	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	connect:connect- instances:prompt	• AWS: Connect:pt	Yes	No	Yes	Yes
	connect:connect- LL_SUPPORTED	• N/A	No	Yes	Yes	Yes
Amazon Data Lifecycle Manager [dlm]	dlm:policy	• AWS: LifecyclePolicy	Yes	Yes	Yes	Yes
	dlm:Associate- UPPERCASE	• N/A	No	Yes	Yes	Yes
Amazon DataZone [datazone]	datazone:domain	• AWS: DataZone	Yes	No	Yes	Yes
Amazon Detective [detective]	detective:graph	• AWS: DetectiveGraph	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon DocumentDB Elastic Clusters [docdb-elastic]	docdb-elastic:cluster	• AWS: BELA:Cluster	Yes	No	No	No
	docdb-elastic:ter-pg	• AWS: BELA:Cluster-pg	Yes	No	No	No
	docdb-elastic:ter-snapshot	• N/A	Yes	No	No	No
Amazon DynamoDB Accelerator (DAX) [dax]	dax:cluster	• AWS: BELA:Cluster	Yes	No	Yes	Yes
Amazon DynamoDB [dynamodb]	dynamodb:global	• AWS: BELA:Global	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	dynamic table	• AWS: mode	Yes	Yes	Yes	Yes
	dynamic index	• N/A	Yes	No	No	No
	dynamic table, stream	• N/A	Yes	No	No	No
	dynamic ALL_SORTED	• N/A	No	Yes	Yes	Yes
Amazon EC2 Auto Scaling [autoscaling]	autoscaling:policyname	• AWS: ScalingGroup	Yes	No	No	No
Amazon EC2 Image Builder [imagebuilder]	imagebuilder:configuration	• AWS: ImageBuilder:InfrastructureConfiguration	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	imagebuilder:image-recipe	• AWS:EBuilding:ImageRecipe	Yes	No	Yes	Yes
	imagebuilder:container-recipe	• AWS:EBuilding:ContainerRecipe	Yes	No	Yes	Yes
	imagebuilder:image	• AWS:EBuilding:Image	Yes	No	Yes	Yes
	imagebuilder:worklow	• AWS:EBuilding:Workflow	Yes	No	Yes	Yes
	imagebuilder:component	• AWS:EBuilding:Content	Yes	No	Yes	Yes
	imagebuilder:LifecyclePolicy	• AWS:EBuilding:LifecyclePolicy	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	image:der:discovery:configuration	• AWS: eBuild:Distribution:Image	Yes	No	Yes	Yes
	image:der:infrastructure:pipeline	• AWS: eBuild:Image	Yes	No	Yes	Yes
Amazon EC2 [ec2]	ec2:instance-usage-report	• N/A	Yes	No	No	No
	ec2:instance-resource-verification-token	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:security-group	• AWS: :SecurityGroup	Yes	Yes	Yes	Yes
	ec2:traffic-mirroring-session	• AWS: :TrafficMirroringSession	Yes	Yes	Yes	Yes
	ec2:instance-profile	• AWS: :InstanceProfile	Yes	Yes	Yes	Yes
	ec2:security-group-rule	• AWS: :SecurityGroupRule • AWS: :SecurityGroupRule	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:launch-template	• AWS: LocalGatewayVirtualInterfaceGroup	Yes	No	No	No
	ec2:network-interface	• AWS: NATGateway	Yes	Yes	Yes	Yes
	ec2:image-tasks	• N/A	Yes	Yes	No	No
	ec2:internet-gateway	• AWS: InternetGateway	Yes	Yes	Yes	Yes
	ec2:transit-gateway	• AWS: TransitGateway	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:describe-options	• AWS:DHCPOptions	Yes	Yes	Yes	Yes
	ec2:install-windows-agent	• N/A	Yes	Yes	No	No
	ec2:network-insights-access-scope-analysis	• AWS:NetworkInsightsAccessAnal	Yes	Yes	Yes	Yes
	ec2:install-windows-agent	• N/A	Yes	Yes	No	No
	ec2:transit-gateway-policy-table	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:tag:it-gateway-attachment	- AWS: :TagatevAttach - AWS: :Tagatevachn - AWS: :Tagatevringhmer	Yes	Yes	Yes	Yes
	ec2:volume	AWS: :Volume	Yes	Yes	Yes	Yes
	ec2:image:task	N/A	Yes	Yes	No	No
	ec2:subt	AWS: :Sub	Yes	Yes	Yes	Yes
	ec2:vpc	AWS: :VPC	Yes	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:vpce-endpoints	• AWS: VPCintegratedPermissions	Yes	No	Yes	Yes
	ec2:capacity-reservation	• AWS: CapacityReservation	Yes	Yes	Yes	Yes
	ec2:nat-acs	• AWS: NetworkACL	Yes	Yes	Yes	Yes
	ec2:vpce-connections-trust-provider	• AWS: VPCintegratedAccessTrustProvider	Yes	Yes	Yes	Yes
	ec2:vpce-gateways	• AWS: VPCintegratedGateway	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:configure-termination-protection	• AWS: :Configuration	Yes	Yes	Yes	Yes
	ec2:enable-gpu	• N/A	Yes	No	No	No
	ec2:enable-gpu	• N/A	Yes	No	No	No
	ec2:load-balance-table	• AWS: :LoadBalancing	Yes	Yes	Yes	Yes
	ec2:network-insights-access-scope	• AWS: :NetworkInsights	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:tag:it-gateway-connection-peer	• AWS: :TrafficGatewayConnect	Yes	Yes	Yes	Yes
	ec2:vi-ied-access-group	• AWS: :VerifiedAccessGroup	Yes	Yes	Yes	Yes
	ec2:tag:ic-mirror-target	• AWS: :TrafficMirrorTarget	Yes	Yes	Yes	Yes
	ec2:co-pool	• N/A	Yes	Yes	No	No
	ec2:f	• AWS: :EC2	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:local-gateway-route-table-association	• AWS: LocalGatewayTableVirtualInterfaceAssociation	Yes	Yes	Yes	Yes
	ec2:transit-gateway-y-multi-st-domain	• AWS: TransitGatewayAttachment	Yes	Yes	Yes	Yes
	ec2:network-interface	• AWS: NetworkInterface	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:capacity-manage-er-data-export	• AWS: :CapacityManager-Export	Yes	No	No	No
	ec2:client-vpn-endpoint	• AWS: :ClientVpnEndpoint	Yes	Yes	Yes	Yes
	ec2:system-instance-requests	• N/A	Yes	Yes	No	No
	ec2:network-insights-path	• AWS: :NetworkInsightsPath	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:instance-connect-endpoint	• AWS: :InstanceConnectEndpoint	Yes	Yes	Yes	Yes
	ec2:traffic-mirror-filerule	• AWS: :TrafficMirrorFilterRule	Yes	No	Yes	Yes
	ec2:localgatewayvirtualinterface	• AWS: :LocalGatewayVirtualInterface	Yes	No	No	No
	ec2:vpc-peeringconnection	• AWS: :VPCPeeringConnection	Yes	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:stop	• N/A	Yes	Yes	No	No
	ec2:create-gateway	• AWS:Custom Gateway	Yes	Yes	Yes	Yes
	ec2:create-block	• N/A	Yes	No	No	No
	ec2:validate-access-endpoint	• AWS:Validate Access Point	Yes	Yes	Yes	Yes
	ec2:connect	• AWS:VPN Connect	Yes	Yes	Yes	Yes
	ec2:import	• AWS:IPAM	Yes	Yes	Yes	Yes
	ec2:import	• AWS:IPAM	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:hold-reservation	• N/A	Yes	Yes	No	No
	ec2:runce-root-volume-task	• N/A	Yes	Yes	No	No
	ec2:instance	• AWS:Instance	Yes	Yes	Yes	Yes
	ec2:find-image	• N/A	Yes	Yes	No	No
	ec2:run-server-endpoint	• AWS:Route53:RouterEndpoint	Yes	No	No	No
	ec2:keep-air	• AWS:KeyPair	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:vpce- ndpoint- c onnect	• N/A	Yes	No	No	No
	ec2:dedicated-host	• AWS: :Host	Yes	Yes	Yes	Yes
	ec2:load-balancing- gateway- route-table- vpc-as social	• AWS: :LoadBalancing- TableAssociation	Yes	Yes	Yes	Yes
	ec2:vpce- ndpoint- service	• AWS: :VPCEnterprise	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:elastic-only-interne-gateway	• AWS: :Eg1lyIr tGat	Yes	Yes	Yes	Yes
	ec2:instance-resource-discovery	• AWS: :IPAurcevery	Yes	Yes	Yes	Yes
	ec2:man-modifion-task	• N/A	Yes	No	No	No
	ec2:network-insights-analysis	• AWS: :Netnsigalys	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:placement-group	• AWS:PlatGr	Yes	Yes	Yes	Yes
	ec2:instance-event-logging	• N/A	Yes	Yes	No	No
	ec2:instance-logging	• N/A	Yes	No	No	No
	ec2:prefix-list	• AWS:Prefix	Yes	Yes	Yes	Yes
	ec2:vpc-endpoint	• AWS:VPCint	Yes	Yes	Yes	Yes
	ec2:elastic-ip	• AWS:EIF	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:execute-instance-task	• N/A	Yes	Yes	No	No
	ec2:revoke-instance	• N/A	Yes	Yes	No	No
	ec2:execute-image-task	• N/A	Yes	Yes	No	No
	ec2:start-cidr-reservation	• N/A	Yes	Yes	No	No
	ec2:validate-flow-log	• AWS:Flc	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:capacity-reservationfleet	• AWS:CapacityReservationFleet	Yes	Yes	Yes	Yes
	ec2:image-resource-discovery-association	• AWS:IPAddresses-very-association	Yes	Yes	Yes	Yes
	ec2:transit-gateway-route-table-annotation	• N/A	Yes	Yes	No	No
	ec2:transit-mirror-filter	• AWS:TransitMirrorer	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:ont-st-lag	• N/A	Yes	No	No	No
	ec2:logs-gateways	• N/A	Yes	No	No	No
	ec2:launch-templates	• AWS:LaunchTemplate	Yes	Yes	Yes	Yes
	ec2:vpc-block-public-access-exclusion	• AWS:VPCPublicAccession	Yes	No	Yes	Yes
	ec2:route-tables	• AWS:RouteTable	Yes	Yes	Yes	Yes
	ec2:instances	• AWS:InstanceIPAddresses	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ec2:describe-instances-report	• N/A	Yes	No	No	No
	ec2:validate-instance-access	• AWS:VerifiedAccess	Yes	Yes	Yes	Yes
	ec2:transit-gateway-route-table	• AWS:TransitGatewayRouteTable	Yes	Yes	Yes	Yes
	ec2:spot-fleet-request	• AWS:Spot	Yes	Yes	Yes	Yes
	ec2:AssociateUPPORD	• N/A	No	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon EMR Serverless [emr-serverless]	emr-serverless	• N/A	Yes	No	No	No
	emr-serverless-application	• AWS::Application	Yes	Yes	Yes	Yes
Amazon EMR on EKS (EMR Containers) [emr-containers]	emr-containers	• N/A	Yes	No	No	No
	emr-containers-tasks/endpoints	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	emr-containers:securityprofiles	• N/A	Yes	No	No	No
	emr-containers:templates	• N/A	Yes	No	No	No
	emr-containers:virtualclusters	• AWS::EMR::VirtualClusters	Yes	No	Yes	Yes
Amazon ElastiCache [elasticsearch]	elasticache:securitygroups	• AWS::ElastiCache::SecurityGroup	Yes	No	Yes	Yes
	elasticache:parametergroups	• AWS::ElastiCache::ParameterGroup	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	elasticache:usergroup	• AWS: tiCa User	Yes	No	Yes	Yes
	elasticache:snapshot	• N/A	Yes	No	No	No
	elasticache:subgroup	• AWS: tiCa Subr up	Yes	No	Yes	Yes
	elasticache:cluster	• AWS: tiCa Cach ter	Yes	Yes	Yes	Yes
	elasticache:reserved-instance	• N/A	Yes	No	No	No
	elasticache:serverlesscache	• AWS: tiCa Serv sCac	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	elasticache:reportingpolicy	• AWS: tiCa Rep onGr	Yes	No	Yes	Yes
	elasticache:securitylesscopies	• N/A	Yes	No	No	No
	elasticache:user	• AWS: tiCa User	Yes	No	Yes	Yes
	elasticache:ALBPORT	• N/A	No	Yes	Yes	Yes
Amazon Elastic Container Registry [ecr-public]	ecr-public:repository	• AWS: Pub posi	Yes	No	Yes	Yes
Amazon Elastic Container Registry [ecr]	ecr:repository	• AWS: Rep ry	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ecr:ApplyImagePolicy	• N/A	No	Yes	Yes	Yes
Amazon Elastic Container Service [ecs]	ecs:TaskDefinition	• N/A	Yes	No	No	No
	ecs:CreateCluster	• AWS:CloudFormation	Yes	Yes	Yes	Yes
	ecs:CreateService	• N/A	Yes	No	No	No
	ecs:CreateTaskDefinition	• AWS:CloudFormation	Yes	Yes	Yes	Yes
	ecs:DeleteCluster	• N/A	Yes	No	No	No
	ecs:DeleteTaskDefinition	• N/A	Yes	No	No	No
	ecs:DescribeCluster	• AWS:CloudFormation	Yes	Yes	Yes	Yes
	ecs:DescribeTaskDefinition	• AWS:CloudFormation	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ecs:container-instance	• N/A	Yes	No	No	No
	ecs:taskset	• AWS:Task	Yes	Yes	Yes	Yes
	ecs:AUTOSCALING	• N/A	No	Yes	Yes	Yes
Amazon Elastic File System [elasticfilesystem]	elasticfilesystem:file-system	• AWS:Filesystem	Yes	Yes	Yes	Yes
	elasticfilesystem:accesspoint	• AWS:Accesspoint	Yes	No	Yes	Yes
	elasticfilesystem:ALL_SUPPORTED	• N/A	No	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Elastic Inference [amazonelasticinference]	amazonelasticinference:	• N/A	Yes	No	No	No
Amazon Elastic Kubernetes Service [eks]	eks:cluster	• AWS:Cluster	Yes	Yes	Yes	Yes
	eks:access-entry	• AWS:AccessEntry	Yes	No	Yes	Yes
	eks:access-ad	• AWS:AccessAd	Yes	No	Yes	Yes
	eks:pod-identity/association	• AWS:PodIdentity/Association	Yes	No	Yes	Yes
	eks:dashboard	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	eks:elasticache:subscri	• N/A	Yes	No	No	No
	eks:iam:identityprovidercon	• AWS: IAM:Provision	Yes	No	Yes	Yes
	eks:iam:group	• AWS: IAM:Policy	Yes	No	Yes	Yes
	eks:iam:role	• AWS: IAM:Profile	Yes	No	Yes	Yes
	eks:iam:role	• N/A	No	Yes	Yes	Yes
Amazon Elastic MapReduce [elasticmapreduce]	elasticmapreduce:cluster	• AWS: CloudFormation	Yes	Yes	Yes	Yes
	elasticmapreduce:elasticmapreduce	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	elastic:prod/elastic-notebooks-execution	• N/A	Yes	No	No	No
	elastic:prod/studio	• AWS:Studio	Yes	No	No	No
	elastic:prod/LL_SUPPORTED	• N/A	No	Yes	Yes	Yes
Amazon Elastic VMware Service [evs]	evs:environment	• AWS:Environment	Yes	No	No	No
Amazon EventBridge Pipes [pipes]	pipes:event	• AWS:Functions	Yes	Yes	Yes	Yes
	pipes:_SUPPORTED	• N/A	No	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon EventBridge Scheduler [scheduler]	schedule:schedule-group	• AWS: schedule	Yes	Yes	Yes	Yes
	schedule:ALL_SCHEDULED	• N/A	No	Yes	Yes	Yes
Amazon EventBridge Schemas [schemas]	schemas:discover	• AWS: tSchema:Discover	Yes	No	Yes	Yes
	schemas:register	• AWS: tSchema:Register	Yes	No	Yes	Yes
	schemas:chama	• AWS: tSchema:Sch	Yes	No	Yes	Yes
Amazon EventBridge [events]	event-bus	• AWS: ts::Bus	Yes	Yes	Yes	Yes
	event-le	• AWS: ts::	Yes	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	event:L_SUPPORT	• N/A	No	Yes	Yes	Yes
Amazon FSx [fsx]	fsx:backup	• N/A	Yes	Yes	No	No
	fsx:storage-virtual-machine	• AWS:StorageVirtualMachine	Yes	No	Yes	Yes
	fsx:storage-hot	• AWS:Storage	Yes	No	Yes	Yes
	fsx:filesystem	• AWS:Filesystem	Yes	Yes	Yes	Yes
	fsx:association	• AWS:DataSiteAssociation	Yes	No	Yes	Yes
	fsx:filesystem-cache	• N/A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	fsx:volume	• AWS:Volume	Yes	No	Yes	Yes
	fsx:tag	• N/A	Yes	No	No	No
	fsx:AllocationId	• N/A	No	Yes	Yes	Yes
Amazon FinSpace [finspace]	finspace:environment/kxdata/kxdata	• N/A	Yes	No	No	No
	finspace:environment/kxuser	• N/A	Yes	No	No	No
	finspace:environment	• AWS:space	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	finsp kxenv ment/ kxda tabas	• N/ A	Yes	No	No	No
	finsp kxenv ment/ kxvo lume	• N/ A	Yes	No	No	No
	finsp kxenv ment	• N/ A	Yes	No	No	No
	finsp kxenv ment/ kxsc aling p	• N/ A	Yes	No	No	No
	finsp kxenv ment/ kxcl uster	• N/ A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Forecast [forecast]	forecast-import-job	• N/A	Yes	No	No	No
	forecast-backtrack-export-job	• N/A	Yes	No	No	No
	forecast-endpoint	• N/A	Yes	No	No	No
	forecasting-group	• AWS:castaset	Yes	No	Yes	Yes
	forecast-export	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	forecast:monitor	• N/A	Yes	No	No	No
	forecast:forecastexportjob	• N/A	Yes	No	No	No
	forecast:dataset	• AWS:castaset	Yes	No	Yes	Yes
	forecast:what-if-forecast	• N/A	Yes	No	No	No
	forecast:prediction	• N/A	Yes	No	No	No
	forecast:what-if-analysis	• N/A	Yes	No	No	No
	forecast:explainability	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Fraud Detector [frauddetector]	forecast:explainability:export	• N/A	Yes	No	No	No
	forecast:forecast	• N/A	Yes	No	No	No
	frauddetector:frauddetector	• AWS::Frauddetector::Detector	Yes	Yes	Yes	Yes
	frauddetector:frauddetector-version	• N/A	Yes	Yes	No	No
	frauddetector:frauddetector-hyprediction	• N/A	Yes	No	No	No
	frauddetector:frauddetector-label	• AWS::Frauddetector::Label	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	fraud-detector-type	• AWS::CloudFormation::Event	Yes	No	Yes	Yes
	fraud-detector-arnal-model	• N/A	Yes	No	No	No
	fraud-detector-unknown-import	• N/A	Yes	No	No	No
	fraud-detector-type	• AWS::CloudFormation::Error	Yes	No	Yes	Yes
	fraud-detector-unknown	• AWS::CloudFormation::Output	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	fraudctor:1-version	• N/A	Yes	No	No	No
	fraudctor:1	• AWS::CloudDetectors::Li	Yes	No	Yes	Yes
	fraudctor:1	• N/A	Yes	Yes	No	No
	fraudctor:1able	• AWS::CloudDetectors::Value	Yes	Yes	Yes	Yes
	fraudctor:1	• N/A	Yes	Yes	No	No
	fraudctor:1SUPPORT	• N/A	No	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon FreeRTOS [freertos]	freertos:subscription	• N/A	Yes	No	No	No
	freertos:configuration	• N/A	Yes	No	No	No
Amazon GameLift Servers [gamelift]	gamelift:script	• AWS:GameLiftScript	Yes	No	Yes	Yes
	gamelift:build	• AWS:GameLiftBuild	Yes	No	Yes	Yes
	gamelift:contentgroupdefinition	• AWS:GameLiftContentGroupDefinition	Yes	No	No	No
	gamelift:gamesessionqueue	• AWS:GameLiftGameSessionQueue	Yes	No	Yes	Yes
	gamelift:fleet	• AWS:GameLiftFleet	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	gamele match ngrule	• AWS: Lift chma ules	Yes	No	Yes	Yes
	gamele locat	• AWS: Lift atic	Yes	No	Yes	Yes
	gamele alias	• AWS: Lift as	Yes	No	Yes	Yes
	gamele games rgroup	• AWS: Lift eSer oup	Yes	No	Yes	Yes
	gamele conta fleet	• AWS: Lift tair et	Yes	No	No	No
	gamele match ngcon ratio	• AWS: Lift chma onfi ion	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon GameLift Streams [gameliftstreams]	gameliftstreams:plication	• AWS::GameLift::Streams::Application	Yes	No	No	No
	gameliftstreams:reamegroup	• AWS::GameLift::Streams::ManagedGameSessionSet	Yes	No	No	No
Amazon GuardDuty [AWS]	AWS::GuardDuty::PublishFinding	• AWS::GuardDuty::PublishFinding	Yes	No	No	No
Amazon GuardDuty [guardduty]	guardduty:malwareprotection-plan	• AWS::GuardDuty::MalwareProtectionPlan	Yes	No	Yes	Yes
	guardduty:detect	• AWS::GuardDuty::Detect	Yes	Yes	Yes	Yes
	guardduty:detect/ipset	• AWS::GuardDuty::DetectSet	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	guarddetection:threatelse	• AWS:dutreatSet	Yes	Yes	Yes	Yes
	guarddetection:filter	• AWS:dutlter	Yes	Yes	Yes	Yes
Amazon Honeycode [honeycode]	honeycode:screenautomat	• N/A	Yes	No	No	No
	honeycode:workl	• N/A	Yes	No	No	No
	honeycode:table	• N/A	Yes	No	No	No
	honeycode:screen	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Inspector [inspector2]	inspector2:code-compliance	• AWS: AWSInspectorCISConfiguration	Yes	No	No	No
	inspector2:cis-conformance	• AWS: AWSInspectorCISConfiguration	Yes	No	No	No
	inspector2:filter	• AWS: AWSInspectorFilter	Yes	Yes	Yes	Yes
	inspector2:code-urality-integration	• N/A	Yes	No	No	No
	inspector2:code-urality-conformance	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Interactive Video Service [ivs]	ivs:inspect-2:ALL-PORTS	• N/A	No	Yes	Yes	Yes
	ivs:publish-key	• AWS:Public	Yes	No	Yes	Yes
	ivs:int-config-ration	• AWS:In	Yes	No	Yes	Yes
	ivs:rendering-conf-iguration	• AWS:RecgCoratic	Yes	No	Yes	Yes
	ivs:transcode-conf-iguration	• N/A	Yes	No	No	No
	ivs:chat-room	• AWS:hat	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ivs:policy-ack-restrictionpolicy	• AWS: :PlatformRestrictionPolicy	Yes	No	Yes	Yes
	ivs:channel	• AWS: :Channel	Yes	No	Yes	Yes
	ivs:policy-key	• AWS: :PlatformKeyFrame	Yes	No	Yes	Yes
	ivs:stream-key	• AWS: :StreamKey	Yes	No	Yes	Yes
	ivs:composition	• N/A	Yes	No	No	No
	ivs:stream-state	• AWS: :StreamState	Yes	No	Yes	Yes
	ivs:stream-configuration	• AWS: :StreamConfiguration	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	aws:elasticfilesystem:configuration	• AWS:Encrypted	Yes	No	Yes	Yes
Amazon Kendra Intelligent Ranking [kendra-ranking]	kendra-ranking-core-execution-plan	• AWS:KendraRanking::ExecutionPlan	Yes	No	Yes	Yes
Amazon Kendra [kendra]	kendra-index	• AWS:Kendra::Index	Yes	No	Yes	Yes
	kendra-index/thesaurus	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	kendra/dex/query-suggestions-block-list	• N/A	Yes	No	No	No
	kendra/dex/data-source	• AWS::ra::source	Yes	No	Yes	Yes
	kendra/dex/featured-results-set	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Keyspaces (for Apache Cassandra) [cassandra]	cassandra:keys	• AWS: and1 yspa	Yes	No	Yes	Yes
	cassandra:table	• AWS: and1 ble	Yes	No	No	No
Amazon Kinesis Analytics [kinesisanalytics]	kinesis:analytics:application	• AWS: sis/ ics: icat	Yes	Yes	Yes	Yes
	kinesis:analytics:application	• AWS: sis/ ics\ plic	Yes	Yes	Yes	Yes
	kinesis:analytics:LL_SUMTED	• N/ A	No	Yes	Yes	Yes
Amazon Kinesis Data Streams [kinesis]	kinesis:stream	• AWS: sis: am	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	kinesis:stream,consumer	• AWS:sis:amCcr	Yes	No	Yes	Yes
Amazon Kinesis Firehose [firehose]	firehose:deliverystream	• AWS:sis:firehose::eryS	Yes	Yes	Yes	Yes
	firehose:ALL_STREAMED	• N/A	No	Yes	Yes	Yes
Amazon Kinesis Video Streams [kinesisvideo]	kinesis:videostream	• AWS:sis:video:Stream	Yes	No	Yes	Yes
	kinesis:video:channel	• AWS:sis:video:SigningChannel	Yes	No	Yes	Yes
Amazon Lex [lex]	lex:botchannel	• N/A	Yes	No	No	No
	lex:botset	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	lex:bootstrap:alias	• AWS:Bootstrap	Yes	No	Yes	Yes
	lex:bootstrap:alias	• AWS:Bootstrap	Yes	No	Yes	Yes
Amazon Lightsail [lightsail]	lightsail:keypairs	• N/A	Yes	No	No	No
	lightsail:distribution	• AWS:LightsailDistribution	Yes	No	Yes	Yes
	lightsail:containerservice	• AWS:LightsailContainers	Yes	No	Yes	Yes
	lightsail:diskshot	• AWS:LightsailDiskSnapshot	Yes	No	No	No
	lightsail:relateddata	• AWS:LightsailRelatedData	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	lightsail:certificate	• AWS:tsaiair	Yes	No	Yes	Yes
	lightsail:buckets	• AWS:tsaiair	Yes	No	Yes	Yes
	lightsail:instances	• AWS:tsaiair	Yes	No	Yes	Yes
	lightsail:disks	• AWS:tsaiair	Yes	No	Yes	Yes
	lightsail:loadbalancers	• AWS:tsaiair	Yes	No	Yes	Yes
	lightsail:domains	• AWS:tsaiair	Yes	No	Yes	Yes
	lightsail:instancesnapshots	• AWS:tsaiair	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Location [geo]	lightweight:relationshipdataset	• N/A	Yes	No	No	No
	lightweight:static	• AWS: static	Yes	No	Yes	Yes
	geo:geofence-collection	• AWS: geofence	Yes	No	Yes	Yes
	geo:tracker	• AWS: tracker	Yes	No	Yes	Yes
	geo:apikey	• AWS: apikey	Yes	No	Yes	Yes
	geo:place-index	• AWS: place	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	geo:region-calculation	• AWS: tior teCa tor	Yes	No	Yes	Yes
	geo:region	• AWS: tior	Yes	No	Yes	Yes
Amazon Lookout for Equipment [lookoutequipment]	lookoutequipment:atase	• N/A	Yes	No	No	No
	lookoutequipment:abel-group	• N/A	Yes	No	No	No
	lookoutequipment:ference:schedule	• AWS: outE ent: renc dule	Yes	No	No	No
	lookoutequipment:odel	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Lookout for Metrics [lookoutmetrics]	lookoutmetrics	• N/A	Yes	No	No	No
	lookoutmetrics:malicious	• AWS:outM::/yDet	Yes	No	Yes	Yes
	lookoutmetrics:rt	• AWS:outM::/s::/	Yes	No	Yes	Yes
Amazon Lookout for Vision [lookoutvision]	lookoutvision:1	• N/A	Yes	No	No	No
Amazon MQ [mq]	mq:configuration	• AWS:conM::figu	Yes	Yes	Yes	Yes
	mq:broker	• AWS:conM::ker	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	mq:ALP	• N/A	No	Yes	Yes	Yes
Amazon Machine Learning [machinelearning]	machinelearning:evaluate	• N/A	Yes	No	No	No
	machinelearning:models	• N/A	Yes	No	No	No
	machinelearning:batchprediction	• N/A	Yes	No	No	No
	machinelearning:tasou	• N/A	Yes	No	No	No
Amazon Macie [macie2]	macie:classification-job	• N/A	Yes	No	No	No
	macie:L_SUPPRESSED	• N/A	No	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Macie [macie]	macie-allow-list	• AWS::Macie::AllowList	Yes	No	No	No
	macie-ber	• N/A	Yes	No	No	No
	macie-findings-filter	• AWS::Macie::FindingsFilter	Yes	No	No	No
	macie-ssifion-job	• N/A	Yes	No	No	No
	macie-com-data-identifier	• AWS::Macie::ComDataIdentifier	Yes	No	No	No
Amazon Managed Blockchain [managedblockchain]	managedblockchain-proposals	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	managedlockch members	• AWS: Yes • ManagedE • hair • ber	Yes	No	No	No
	managedlockch access	• AWS: Yes • ManagedE • hair • essc	Yes	No	Yes	Yes
	managedlockch network	• N/A	Yes	No	No	No
	managedlockch nodes	• AWS: Yes • ManagedE • hair • e	Yes	No	No	No
	managedlockch invitations	• N/A	Yes	No	No	No
Amazon Managed Grafana [grafana]	grafana workspaces	• AWS: Yes • ManagedE • hair • spac	Yes	No	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Managed Service for Prometheus [aps]	aps:service	• AWS: :Service	Yes	No	No	No
	aps:alertmanager	• AWS: :Alertmanager	Yes	No	No	No
	aps:workspace	• AWS: :Workspace	Yes	No	Yes	Yes
	aps:rulegroupspace	• AWS: :RuleGroupspace	Yes	No	Yes	Yes
Amazon Managed Streaming for Apache Kafka [kafka]	kafka-connection	• AWS: :VpcConnection	Yes	No	No	No
	kafka-cluster	• AWS: :Cluster	Yes	No	No	No
	kafka-licensing	• AWS: :Reporting	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Managed Streaming for Kafka Connect [kafkaconnect]	kafkaconnect:worker-configuration	• AWS::KafkaConnect:WorkerConfiguration	Yes	No	Yes	Yes
	kafkaconnect:connector	• AWS::KafkaConnect:Connector	Yes	No	No	No
	kafkaconnect:complianceplugin	• AWS::KafkaConnect:CompliancePlugin	Yes	No	Yes	Yes
Amazon Managed Workflows for Apache Airflow [airflow]	airflowenvironment	• AWS::EKS::EKSEnvironment	Yes	No	Yes	Yes
Amazon MemoryDB [memorydb]	memorydbcluster	• AWS::MemoryDB:Cluster	Yes	No	Yes	Yes
	memorydbacl	• AWS::MemoryDB:ClusterACL	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	memorysubnetup	• AWS: ryDEnetC	Yes	No	Yes	Yes
	memoryreservationode	• N/A	Yes	No	No	No
	memorymulticonclusion	• AWS: ryDEtiRelust	Yes	No	No	No
	memoryuser	• AWS: ryDEr	Yes	No	Yes	Yes
	memoryparamgroup	• AWS: ryDEametup	Yes	No	Yes	Yes
	memorysnapshots	• N/A	Yes	No	No	No
Amazon Nimble Studio [nimble]	nimblestudio	• AWS: leSt:Stu	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	nimbleunch-profile	• N/A	Yes	No	No	No
	nimblestreamsession	• N/A	Yes	No	No	No
	nimblestreamsessionbackup	• N/A	Yes	No	No	No
	nimblestreamimage	• N/A	Yes	No	No	No
	nimblestudio-component	• N/A	Yes	No	No	No
Amazon One Enterprise [one]	one:stream	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	one:default	• N/A	Yes	No	No	No
	one:default	• N/A	Yes	No	No	No
Amazon OpenSearch Ingestion [osis]	osis:default	• AWS::Pipes	Yes	No	Yes	Yes
Amazon OpenSearch Serverless [aoss]	aoss:default	• AWS::OpenSearch	Yes	Yes	Yes	Yes
	aoss:default	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	aoss:/*	• N/A	No	Yes	Yes	Yes
Amazon OpenSearch [es]	es:domain/*	• AWS::Docker • AWS::Elasticsearch	Yes	Yes	No	No
	es:ALB/*	• N/A	No	Yes	No	No
Amazon OpenSearch [opensearch]	opensearch:domain/*	• N/A	Yes	No	No	No
Amazon Personalize [personalize]	personalize:dataset/deletejob	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	personnel:dataset-group	• AWS: Amazon Data Group	Yes	No	Yes	Yes
	personnel:baseline-segment-job	• N/A	Yes	No	No	No
	personnel:campaign	• N/A	Yes	No	No	No
	personnel:render	• N/A	Yes	No	No	No
	personnel:baseline-inference-job	• N/A	Yes	No	No	No
	personnel:evaluation-track	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	personnel:dataset-importjob	• N/A	Yes	No	No	No
	personnel:dataset	• AWS: Amazon Data	Yes	No	Yes	Yes
	personnel:solution	• AWS: Amazon Solu	Yes	No	Yes	Yes
	personnel:file	• N/A	Yes	No	No	No
	personnel:dataset-exportjob	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Pinpoint SMS and Voice Service [sms-voice]	sms-voice:sendid	• AWS: OICE • AWS: derl	Yes	Yes	No	No
	sms-voice:protectconfiguration	• AWS: OICE • AWS: protect configuration	Yes	No	No	No
	sms-voice:opt-out-list	• AWS: OICE • AWS: Outl	Yes	Yes	No	No
	sms-voice:phonenu mber	• AWS: OICE • AWS: neNu	Yes	Yes	No	No
	sms-voice:pool1	• AWS: OICE • AWS: 1	Yes	Yes	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sms-voice:configurationset	AWS:OICEfigurationSet	Yes	Yes	No	No
	sms-voice:ALL_SUPPORTED	N/A	No	Yes	No	No
Amazon Pinpoint [mobiletargeting]	mobiletargeting	- AWS:ointTemp - AWS:ointhTen - AWS:ointppTe e - AWS:ointilTe e	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	mobile-getting-started	• AWS:oint	Yes	No	Yes	Yes
Amazon Q Business Q Apps [qapps]	qapps-licat-qapp-session	• N/A	Yes	No	No	No
	qapps-licat-qapp	• N/A	Yes	No	No	No
Amazon Q Business [qbusiness]	qbusiness:application/plugin	• AWS:inesugir	Yes	No	No	No
	qbusiness:application/retrieve	• AWS:inestrie	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	qbusi :appl ion/ index / data- sou rce	• AWS: ines taSc	Yes	No	No	No
	qbusi :appl ion	• AWS: ines plic	Yes	No	No	No
	qbusi :appl ion/ web- e xperi	• AWS: ines bExp ce	Yes	No	No	No
	qbusi :appl ion/ index	• AWS: ines dex	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Q in Connect [wisdom]	wisdom:content:associated	• N/A	Yes	No	No	No
	wisdom:content	• N/A	Yes	Yes	No	No
	wisdom:sistance	• AWS::om::tant	Yes	Yes	Yes	Yes
	wisdom:ick-response	• AWS::om::Resp	Yes	No	No	No
	wisdom-agent	• AWS::om::nt	Yes	No	Yes	Yes
	wisdom:ssage:tem:plate	• AWS::om::geTe:e	Yes	No	No	No
	wisdom:owledge:base	• AWS::om::edge	Yes	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	wisdom::session	• N/A	Yes	Yes	No	No
	wisdom::prompt	• AWS::CompliancePrompt	Yes	No	No	No
	wisdom::guardrail	• AWS::ComplianceGuardrail	Yes	No	No	No
	wisdom::social	• AWS::ComplianceInstantiation	Yes	Yes	Yes	Yes
	wisdom::L_SUPPRESSED	• N/A	No	Yes	Yes	Yes
Amazon QLDB [qldb]	qldb::er	• AWS::QLDB::Eraser	Yes	No	No	No
	qldb::sam	• AWS::QLDB::Sam	Yes	No	No	No
	qldb::er/table	• N/A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon QuickSight [quicksight]	quicksight:vpc-ec2	• AWS: QuickSight PCCo-alias	Yes	No	No	No
	quicksight:analytics	• AWS: QuickSight analytics	Yes	No	No	No
	quicksight:folders	• AWS: QuickSight folders	Yes	No	No	No
	quicksight:customer-issuances	• AWS: QuickSight customer issues	Yes	No	No	No
	quicksight:branding	• N/A	Yes	No	No	No
	quicksight:users	• N/A	Yes	No	No	No
	quicksight:datasources	• AWS: QuickSight data sources	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	quickstart:template	• AWS: QuickStart templates	Yes	No	No	No
	quickstart:topic	• AWS: QuickStart topics	Yes	No	No	No
	quickstart:email-customization-template	• N/A	Yes	No	No	No
	quickstart:themes	• AWS: QuickStart themes	Yes	No	No	No
	quickstart:customization	• N/A	Yes	No	No	No
	quickstart:flows	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	quickstart:connect	• N/A	Yes	No	No	No
	quickstart:manage	• N/A	Yes	No	No	No
	quickstart:datasignatures	• AWS: Signatures	Yes	No	No	No
	quickstart:dashboard	• AWS: Signatures	Yes	No	No	No
Amazon RDS [neptune-graph]	neptune-graph:part-task	• N/A	Yes	No	No	No
	neptune-graph:graph	• AWS: NeptuneGraph	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	neptunegraph:highlight-snapshots	• N/A	Yes	No	No	No
Amazon RDS [rds]	rds:create-snapshot	• N/A	Yes	No	No	No
	rds:delete-snapshot	• AWS: [B:] [ance] • AWS: :DBInstance	Yes	No	Yes	Yes
	rds:gluecluster	• AWS: :GlueCluster	Yes	No	No	No
	rds:glue-cluster	• AWS: :GlueCluster	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	rds:snapshot	• AWS:DBSGrou	Yes	Yes	Yes	Yes
	rds:cluster-autobackup	• N/A	Yes	No	No	No
	rds:delete	• N/A	Yes	No	No	No
	rds:promote	• AWS:uncameoup	Yes	Yes	Yes	Yes
	rds:cluster-pg	• AWS:ustemete	Yes	Yes	Yes	Yes
	rds:snapshot-hot-tenant-database	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	rds:es	• AWS: B::E subsc on	Yes	Yes	Yes	Yes
	rds:ps	• AWS: :DBF terC	Yes	Yes	Yes	Yes
	rds:tt-group	• AWS: :DBF arge p	Yes	Yes	Yes	Yes
	rds:cer	• AWS: B::[ter	Yes	No	Yes	Yes
	rds:shot	• N/A	Yes	No	No	No
	rds:proxy	• AWS: :DBF	Yes	Yes	Yes	Yes
	rds:es	• AWS: :Eve scri	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	rds:connect-endpoint	• N/A	Yes	Yes	No	No
	rds:import	• AWS:Import	Yes	No	No	No
	rds:restore	• N/A	Yes	Yes	No	No
	rds:restore-backup	• N/A	Yes	No	No	No
	rds:restore-db-instance	• AWS:DBInstance	Yes	Yes	Yes	Yes
	rds:create-custom-engine-version	• AWS:CustomEngineVersion	Yes	No	Yes	Yes
	rds:describe-proxy-endpoint	• AWS:DBProxyEndpoint	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	rds:cluster-per-pg	• AWS: :DBClusterParameterGroup	Yes	Yes	Yes	Yes
	rds:option-group	• AWS: :OptionGroup	Yes	No	No	No
	rds:option-group	• AWS: :OptionGroup	Yes	Yes	Yes	Yes
	rds:database	• AWS: :DatabaseInstance	Yes	No	Yes	Yes
	rds:subnet	• AWS: :Subnet	Yes	Yes	Yes	Yes
	rds:target-database	• N/A	Yes	No	No	No
	rds:subnet	• AWS: :Subnet	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	rds:cluster-perpg	• AWS:B::[terFterC	Yes	Yes	Yes	Yes
	rds:ALTER_INSTANCE	• N/A	No	Yes	Yes	Yes
Amazon Redshift Serverless [redshift-serverless]	redshift-serverless:recoverpoint	• N/A	Yes	No	No	No
	redshift-serverless:workup	• AWS:redshift-serverless:workup	Yes	Yes	Yes	Yes
	redshift-serverless:rename	• AWS:redshift-serverless:rename	Yes	Yes	Yes	Yes
	redshift-serverless:snapshot	• AWS:redshift-serverless:snapshot	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	redshift-serverless:ALL, PORTER	• N/A	No	Yes	Yes	Yes
Amazon Redshift [redshift]	redshift-eventsubscription	• AWS: shiftSubscription	Yes	Yes	Yes	Yes
	redshift-hsmconfiguration	• N/A	Yes	Yes	No	No
	redshift-subnetgroup	• AWS: shiftSubnetGroup	Yes	Yes	Yes	Yes
	redshift-snapshotcopygroup	• N/A	Yes	Yes	No	No
	redshift-qev2image	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	redshift:securitygrouppolicy	• AWS: ShiftsterilityControl	Yes	No	No	No
	redshift:names	• N/A	Yes	No	No	No
	redshift:snapshot	• N/A	Yes	Yes	No	No
	redshift:securitygroup	• AWS: ShiftsterilityControl	Yes	No	No	No
	redshift:iamrole	• N/A	Yes	Yes	No	No
	redshift:iamrole	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	redshift:cluster*	• AWS: hiftster	Yes	Yes	Yes	Yes
	redshift:snapshot*	• N/A	Yes	Yes	No	No
	redshift:usage*	• N/A	Yes	No	No	No
	redshift:integration*	• AWS: hiftstegra	Yes	No	Yes	Yes
	redshift:parametergroup*	• AWS: hiftsterete	Yes	Yes	Yes	Yes
	redshift:ALL_S* RTED	• N/A	No	Yes	Yes	Yes
Amazon Rekognition [rekognition]	rekognition:proct/ version	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	rekognition:project	• AWS:gnitProject	Yes	No	No	No
	rekognition:collection	• AWS:gnitCollection	Yes	No	Yes	Yes
	rekognition:streamprocess	• AWS:gnitStreamProcess	Yes	No	No	No
Amazon Route 53 Profiles [route53profiles]	route53profiles:association	• AWS:route53Profiles::Association	Yes	No	Yes	Yes
	route53profiles:le	• AWS:route53Profiles::le	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Route 53 Recovery Controls [route53-recovery-control]	route53-recovery-control/safety	• AWS::Route53RecoveryControl::Safety	Yes	No	Yes	Yes
	route53-recovery-control/cluster	• AWS::Route53RecoveryControl::Cluster	Yes	No	Yes	Yes
	route53-recovery-control/panel	• AWS::Route53RecoveryControl::Panel	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Route 53 Recovery Readiness [route53-recovery-readiness]	route53-recovery-readiness-group	• AWS::Route53RecoveryReadiness::Group	Yes	No	Yes	Yes
	route53-recovery-readiness-check	• AWS::Route53RecoveryReadiness::Check	Yes	No	Yes	Yes
	route53-recovery-readiness-cell	• AWS::Route53RecoveryReadiness::Cell	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	route53resolver:ReadResourceSet	• AWS::Route53Resolver::ResourceSet	Yes	No	Yes	Yes
Amazon Route 53 Resolver [route53resolver]	route53resolver:Rule	• AWS::Route53Resolver::Ver	Yes	Yes	Yes	Yes
	route53resolver:Rewaldomainlist	• AWS::Route53Resolver::List	Yes	No	Yes	Yes
	route53resolver:Endpoint	• AWS::Route53Resolver::Ver	Yes	Yes	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	route53::solveconflict	• AWS: e53F0000-0000-0000-0000-000000000000	Yes	No	Yes	Yes
	route53::renewalrulegroup	• AWS: e53F0000-0000-0000-0000-000000000000	Yes	No	Yes	Yes
	route53::renewalrulegroupassociation	• AWS: e53F0000-0000-0000-0000-000000000000	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	route53resolver:postresolvers	• AWS: e53F er::stRe r	Yes	No	No	No
	route53:L_SUPP ED	• N/ A	No	Yes	Yes	Yes
Amazon Route 53 [route53]	route53:healthcheck	• AWS: e53: thCh	Yes	No	Yes	Yes
	route53:omain	• N/ A	Yes	No	No	No
	route53:osted	• AWS: e53: edZc	Yes	Yes	Yes	Yes
	route53:LL_SU TED	• N/ A	No	Yes	Yes	Yes
Amazon S3 Express [s3express]	s3express:acce int	• AWS: pres cess	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	s3exp: :bucket	• AWS: pres rect cket	Yes	No	Yes	Yes
Amazon S3 Glacier [glacier]	glaci aults	• N/A	Yes	No	No	No
Amazon S3 Tables [s3tables]	s3tab: Table	• AWS: ble leBu	Yes	No	No	No
	s3tab: table	• AWS: ble le	Yes	No	No	No
Amazon S3 Vectors [s3vectors]	s3vec: :inde	• AWS: cto dex	Yes	No	No	No
	s3vec: :vecto cket	• AWS: cto cto t	Yes	No	No	No
Amazon S3 [s3]	s3:ac grant tance	• AWS: Acce nts] ce	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	s3:bucket	• AWS: Buck	Yes	Yes	Yes	Yes
	s3:job	• N/A	Yes	No	No	No
	s3:access-grants	• AWS: Access Grant	Yes	No	No	No
	s3:storage-lens	• AWS: Storage Lens	Yes	Yes	Yes	Yes
	s3:access-grants-location	• AWS: Access Grants Location	Yes	No	No	No
	s3:access-grants-attachment	• AWS: Access Grants Attachment	Yes	No	No	No
	s3:storage-lens-group	• AWS: Storage Lens Group	Yes	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon SES [ses]	s3:acpoint	• AWS: Account	Yes	No	Yes	Yes
	s3:ALPPORT	• N/A	No	Yes	Yes	Yes
	ses:identity	• AWS: Email identity • AWS: Account ID::Identity	Yes	No	Yes	Yes
	ses:dedicated-ip-pool	• AWS: DedicatedIpPool • AWS: Account ID::DedicatedIpPool	Yes	No	Yes	Yes
	ses:contact-list	• AWS: ContactList	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ses:manageinprogresspoint	• AWS:MainServerPoint	Yes	No	Yes	Yes
	ses:configureset	• AWS:Corporate • AWS:Joint::Contract	Yes	No	Yes	Yes
	ses:manageaddresslist	• AWS:MainServerAddressList	Yes	No	No	No
	ses:multi-regionendpoint	• AWS:MultiRegionEndpoint	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	ses:managearchive	• AWS:Main	Yes	No	Yes	Yes
	ses:managetrafficpolicy	• AWS:Main	Yes	No	Yes	Yes
	ses:managerule-set	• AWS:Main	Yes	No	Yes	Yes
Amazon SNS [sns]	sns:topic	• AWS:Topic	Yes	Yes	Yes	Yes
	sns:Attribute	• N/A	No	Yes	Yes	Yes
Amazon SQS [sqs]	sqs:queue	• AWS:Queue	Yes	Yes	Yes	Yes
	sqs:Attribute	• N/A	No	Yes	Yes	Yes

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon SageMaker [sagemaker]	sagemaker:image	• AWS: MakeImage	Yes	No	Yes	Yes
	sagemaker:model-quality-job-definition	• AWS: MakeModelQualityJobDefinition	Yes	No	Yes	Yes
	sagemaker:monitoring-schedule	• AWS: MakeMonitoringSchedule	Yes	No	Yes	Yes
	sagemaker:transform-job	• N/A	Yes	No	No	No
	sagemaker:code-repository	• AWS: MakeCodeRepository	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemaker:imageversion	• AWS: MakeImageVersion	Yes	No	No	No
	sagemaker:experiment	• N/A	Yes	Yes	No	No
	sagemaker:action	• N/A	Yes	Yes	No	No
	sagemaker:hypertuningparameter	• N/A	Yes	No	No	No
	sagemaker:modelsbiases-job-definition	• AWS: MakeModelBiasJobDefinition	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemaker:app-image-configuration	• AWS: MakeImagefig	Yes	Yes	Yes	Yes
	sagemaker:models	• AWS: MakeModel	Yes	No	Yes	Yes
	sagemaker:training-plan	• N/A	Yes	No	No	No
	sagemaker:workspaces	• N/A	Yes	No	No	No
	sagemaker:models-explainability-job-definition	• AWS: MakeModelExplainabilityJobDefinition	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemaker:models-card	• AWS: Make delC	Yes	No	Yes	Yes
	sagemaker:models-card-export-job	• N/A	Yes	No	No	No
	sagemaker-notebook-instance-lifecycle-e-config	• AWS: Make tebc tanc cyc] ig	Yes	No	Yes	Yes
	sagemaker-notebook-instance	• AWS: Make tebc tanc	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemanifest:compliance-job	• N/A	Yes	No	No	No
	sagemanifest:package	• AWS: MakeDefault	Yes	Yes	Yes	Yes
	sagemanifest:quality-job-definition	• AWS: MakeDefault	Yes	No	Yes	Yes
	sagemanifest:user-profile	• AWS: MakeDefault	Yes	No	Yes	Yes
	sagemanifest:domain	• AWS: MakeDefault	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemaker:mlflow:trackingserver	• AWS: MakeflowingS	Yes	No	Yes	Yes
	sagemaker:edgepackagingjob	• N/A	Yes	No	No	No
	sagemaker:clusters	• AWS: Makeuste	Yes	No	Yes	Yes
	sagemaker:devices	• AWS: Makevice	Yes	No	No	No
	sagemaker:featuregroup	• AWS: Makeaturp	Yes	No	Yes	Yes
	sagemaker:artifacts	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemaker:studio-lifecycleconfiguration	• AWS: Make lifecycle configuration	Yes	No	Yes	Yes
	sagemaker:clusterschedulernotificationsconfiguration	• N/A	Yes	No	No	No
	sagemaker:automljob	• N/A	Yes	No	No	No
	sagemaker:app	• AWS: Make p	Yes	No	Yes	Yes
	sagemaker:spaces	• AWS: Make space	Yes	No	Yes	Yes
	sagemaker:inference-component	• AWS: Make inference component	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemaker:endpoint	• AWS: Make endpoint	Yes	No	Yes	Yes
	sagemaker:workgroup	• AWS: Make market	Yes	No	Yes	Yes
	sagemaker:inference-experiment	• AWS: Make inference experiment	Yes	No	Yes	Yes
	sagemaker:optimum-job	• N/A	Yes	No	No	No
	sagemaker:algorithm	• N/A	Yes	No	No	No
	sagemaker:pipe/execution	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemaker:pipe- - execu- n	• N/A	Yes	No	No	No
	sagemaker:proj-	• AWS: Make oject	Yes	Yes	Yes	Yes
	sagemaker:mode- pa- ckage gro- up	• AWS: Make delf eGro	Yes	Yes	Yes	Yes
	sagemaker:label- - job	• N/A	Yes	No	No	No
	sagemaker:edge- dep- loyme	• N/A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemaker:training-job	• N/A	Yes	Yes	No	No
	sagemaker:compquota	• N/A	Yes	No	No	No
	sagemaker:resourcing-capacity	• N/A	Yes	No	No	No
	sagemaker:containers	• N/A	Yes	Yes	No	No
	sagemaker:partitions-app	• AWS: Make runtime	Yes	No	No	No
	sagemaker:experiment-trial	• N/A	Yes	No	No	No
	sagemaker:hub	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemaker:flowdefinition	• N/A	Yes	Yes	No	No
	sagemaker:pipeline	• AWS: Make pipeline	Yes	Yes	Yes	Yes
	sagemaker:lineargroup	• N/A	Yes	No	No	No
	sagemaker:inference-recommendationjob	• N/A	Yes	No	No	No
	sagemaker:devicefleet	• AWS: Make device	Yes	No	No	No
	sagemaker:hub-content	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	sagemaker-experiments-trials-component	• N/A	Yes	No	No	No
	sagemaker-endpoint-config	• AWS: Make endpoint configuration	Yes	No	Yes	Yes
	sagemaker-processing-job	• AWS: Make processing job	Yes	Yes	Yes	Yes
	sagemaker-human-task-ui	• N/A	Yes	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon SageMaker geospatial capabilities [sagemaker-geospatial]	sagemaker-geospatial:ras	• N/A	Yes	No	No	No
	sagemaker-geospatial:earth-observation-job	• N/A	Yes	No	No	No
	sagemaker-geospatial:visualization-job	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Security Lake [security lake]	security lake:datapoints	• AWS: security:DataPoints	Yes	Yes	No	No
	security lake:subscriber	• AWS: security:Subscriber	Yes	Yes	No	No
	security lake:ALLOWED	• N/A	No	Yes	No	No
Amazon Simple Workflow Service [swf]	swf:datapoints	• N/A	Yes	No	No	No
Amazon Textract [textract]	textract:adapt	• N/A	Yes	Yes	No	No
	textract:ALL_SORTED	• N/A	No	Yes	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon Timestream InfluxDB [timestream-influxdb]	timestream-influxdb:instance	• N/A	Yes	No	No	No
Amazon Timestream [timestream]	timestream:database	• AWS: stream-ata	Yes	No	Yes	Yes
	timestream:database/table	• AWS: stream-able	Yes	No	Yes	Yes
	timestream:scheduled-query	• AWS: stream-check-query	Yes	No	Yes	Yes
Amazon Transcribe [transcribe]	transcribe:vocabulary-filer	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	transcribe:Vocabulary	• N/A	Yes	No	No	No
	transcribe:TranscriptionJob	• N/A	Yes	No	No	No
	transcribe-medialml-transcription:TranscriptionJob	• N/A	Yes	No	No	No
	transcribe-medialml-vocabulary:Vocabulary	• N/A	Yes	No	No	No
	transcribe-medialml-scribe:TranscriptionJob	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	trans:language-model	• N/A	Yes	No	No	No
Amazon Translate [translate]	trans:parameters-data	• N/A	Yes	No	No	No
	trans:terminology	• N/A	Yes	No	No	No
Amazon VPC Lattice [vpc-lattice]	vpc-lattice:security/rule	• AWS:attitude	Yes	No	Yes	Yes
	vpc-lattice:security/networkserviceassociation	• AWS:attitude service work ceAs tior	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	vpc-lattice:security/listener	• AWS: attestation	Yes	No	Yes	Yes
	vpc-lattice:accesslogs/subscription	• AWS: attestation	Yes	No	Yes	Yes
	vpc-lattice:security/enetworkresource/social	• AWS: attestation	Yes	No	No	No
	vpc-lattice:domain/verification	• N/A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	vpc-lattice:resourceendpointassociation	• N/A	Yes	No	No	No
	vpc-lattice:serviceenetworkassociation	• AWS: attitervetworksoci	Yes	No	Yes	Yes
	vpc-lattice:service	• AWS: attiterv	Yes	No	Yes	Yes
	vpc-lattice:serviceenetwork	• AWS: attiterv	Yes	No	Yes	Yes
	vpc-lattice:resourceconfiguration	• AWS: attiresolnfigon	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	vpc-lattice:taggroup	• AWS: attitargep	Yes	No	Yes	Yes
	vpc-lattice:resourcegateway	• AWS: attiresourcegateway	Yes	No	No	No
Amazon Verified Permissions [verified permissions]	verifiedpermissions:store	• AWS: fiecssicolic	Yes	No	Yes	Yes
Amazon WorkLink [worklink]	worklink:fleet	• N/A	Yes	Yes	No	No
Amazon WorkMail [workmail]	workmail:organization	• N/A	Yes	No	No	No

Service	Tag Policy JSON syntax	CloudFormation Alias	Basic Compliance Rules		Required Tag Keys	
			Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Amazon WorkSpaces Secure Browser [workspaces-web]	workspaces-web:portal	• AWS::WorkSpaces::Portal	Yes	No	Yes	Yes
	workspaces-web:instanceaccesssettings	• AWS::WorkSpaces::InstanceAccessSettings	Yes	No	Yes	Yes
	workspaces-web:usagegathering	• AWS::WorkSpaces::UsageGathering	Yes	No	Yes	Yes
	workspaces-web:dataprotectionsettings	• AWS::WorkSpaces::DataProtectionSettings	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	works-s-web:sessionlogs	• AWS: Space :: Session Logs	Yes	No	No	No
	works-s-web:usersettings	• AWS: Space :: User Settings	Yes	No	Yes	Yes
	works-s-web:businesssettings	• AWS: Space :: Business Settings	Yes	No	Yes	Yes
	works-s-web:identityprovider	• AWS: Space :: Identity Provider	Yes	No	No	No
	works-s-web:networksettings	• AWS: Space :: Network Settings	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	works- s-web: tsto:	• AWS: Space ::Ti ore	Yes	No	Yes	Yes
Amazon WorkSpaces Secure Browser [workspacesweb]	works- sweb: tityp: der	• AWS: Space ::Ic yProc	Yes	No	No	No
Amazon WorkSpaces Thin Client [thinclient]	thinc: t:env: ment	• AWS: Space nCli Envi nt	Yes	No	No	No
	thinc: t:env: ments	• AWS: Space nCli Envi nt	Yes	No	No	No
	thinc: t:dev:	• N/A	Yes	No	No	No
	thinc: t:dev:	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	thinc t:soft reset	• N/ A	Yes	No	No	No
Amazon WorkSpaces [workspaces]	works s:dir ry	• N/ A	Yes	Yes	No	No
	works s:wor ce	• AWS: Spac orks	Yes	Yes	No	No
	works s:wor cebun	• N/ A	Yes	Yes	No	No
	works s:wor ceima	• N/ A	Yes	Yes	No	No
	works s:con ional	• AWS: Spac onne Alia	Yes	Yes	Yes	Yes
	works s:wor cespo	• AWS: Spac orks Pool	Yes	No	Yes	Yes

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
	works:workspaces:ceipg	• N/A	Yes	Yes	No	No
	works:s:ALLPORTER	• N/A	No	Yes	Yes	Yes
Deprecate d - AWS IoT 1-Click [iot1click]	iot1click:device	• N/A	Yes	No	No	No
	iot1click:project	• N/A	Yes	No	No	No
Deprecate d AWS IoT RoboRunner [iotroborunner]	iotroborunner:device	• N/A	Yes	No	No	No
	iotroborunner:device/workers/fleet	• N/A	Yes	No	No	No

			Basic Compliance Rules		Required Tag Keys	
Service	Tag Policy JSON syntax	CloudFormation Alias	Reporting Mode	Enforcement Mode	Reporting Mode	Enforce for IaC
Multi-party approval [mpa]	mpa:approval-team	• AWS: App Team	Yes	No	No	No
	mpa:identity-source	• AWS: Identity Source	Yes	No	No	No
Service Quotas [servicequotas]	servicequotas:quota	• N/A	Yes	No	No	No
route53globalresolver [route53globalresolver]	route53globalresolver:full-domain-list	• N/A	Yes	No	No	No

- [Terraform 공급자의 리소스 유형 지원은 Terraform 설명서를](#) 참조하세요. AWS
- [Pulumi 클라우드의 리소스 유형 지원은 Pulumi 설명서를](#) 참조하세요.

지원되는 리전:

태그 정책 기능은 다음 리전에서 사용할 수 있습니다.

리전 이름	리전 파라미터
미국 동부(버지니아 북부) 리전 ¹	us-east-1
US East (Ohio) Region	us-east-2
US West (N. California) Region	us-west-1
미국 서부(오리건) 리전	us-west-2
아프리카(케이프타운) 리전 ²	af-south-1
아시아 태평양(홍콩) 리전 ²	ap-east-1
아시아 태평양(타이베이) ²	ap-east-2
아시아 태평양(뭄바이) 리전	ap-south-1
아시아 태평양(하이데라바드) ²	ap-south-2
아시아 태평양(도쿄) 리전	ap-northeast-1
Asia Pacific (Seoul) Region	ap-northeast-2
Asia Pacific (Osaka) Region	ap-northeast-3
Asia Pacific (Singapore) Region	ap-southeast-1
Asia Pacific (Sydney) Region	ap-southeast-2
아시아 태평양(자카르타) 리전 ²	ap-southeast-3
아시아 태평양(멜버른) ²	ap-southeast-4
아시아 태평양(말레이시아) 리전	ap-southeast-5
아시아 태평양(뉴질랜드) ²	ap-southeast-6
아시아 태평양(태국)	ap-southeast-7
캐나다(중부) 리전	ca-central-1

리전 이름	리전 파라미터
캐나다 서부(캘거리) ²	ca-west-1
중국(베이징) 리전	cn-north-1
중국(닝샤) 리전	cn-northwest-1
유럽(프랑크푸르트) 리전	eu-central-1
유럽(취리히) 리전 ²	eu-central-2
유럽(밀라노) 리전 ²	eu-south-1
유럽(스페인) ²	eu-south-2
유럽(아일랜드) 리전	eu-west-1
Europe (London) Region	eu-west-2
유럽(파리) 리전	eu-west-3
유럽(스톡홀름) 리전	eu-north-1
멕시코(중부) 리전	mx-central-1
중동(UAE) 리전 ²	me-central-1
중동(바레인) 리전 ²	me-south-1
남아메리카(상파울루) 리전	sa-east-1
이스라엘(텔아비브) ²	il-central-1
AWS GovCloud(미국 동부)	us-gov-east-1
AWS GovCloud(미국 서부)	us-gov-west-1

¹다음 Organizations 작업을 호출할 때 **us-east-1** 리전을 지정해야 합니다.

- [DeletePolicy](#)

- [DisablePolicyType](#)
- [EnablePolicyType](#)
- [ListRoots](#)와 같은 조직 루트에 대한 다른 모든 작업.

태그 정책 기능의 일부인 다음 Resource Groups Tagging API 작업을 호출할 때도 **us-east-1** 리전을 지정해야 합니다.

- [DescribeReportCreation](#)
- [GetComplianceSummary](#)
- [StartReportCreation](#)

Note

조직 전체의 태그 정책 준수 여부를 평가하려면 보고서 저장을 위해 미국 동부(버지니아 북부) 리전의 Amazon S3 버킷에 대한 액세스 권한도 있어야 합니다. 자세한 내용은 AWS 리소스 태그 지정 사용 설명서의 [보고서 스토리지에 대한 Amazon S3 버킷 정책](#)을 참조하세요.

²이러한 리전은 수동으로 활성화해야 합니다. AWS 리전활성화 및 비활성화에 대해 자세히 알아보려면 AWS 계정 관리 참조 안내서의 [계정에서 사용할 수 있는 AWS 리전 지정](#)을 참조하세요. Resource Groups 콘솔을 이러한 리전에서 사용할 수 없습니다.

채팅 애플리케이션 정책

의 채팅 애플리케이션 정책을 AWS Organizations 사용하면 Slack 및 Microsoft Teams와 같은 채팅 애플리케이션에서 조직의 계정에 대한 액세스를 제어할 수 있습니다.

[채팅 애플리케이션의 Amazon Q Developer](#)는 DevOps 및 소프트웨어 개발 팀이 메시징 프로그램 채팅 방을 사용하여 AWS 클라우드에서 운영 이벤트를 모니터링하고 대응하는 AWS 서비스입니다. 채팅 애플리케이션의 Amazon Q Developer는 Amazon Simple Notification Service(Amazon SNS)의 AWS 서비스 알림을 처리하고 채팅룸에 전달하여 팀이 위치에 관계없이 즉시 이를 분석하고 조치를 취할 수 있도록 합니다.

채팅 애플리케이션 정책 작동 방식

채팅 애플리케이션 정책을 사용하면 조직의 관리 계정 또는 위임된 관리자가 조직 전체에서 다음을 수행할 수 있습니다.

- 지원되는 채팅 애플리케이션(Amazon Chime, Microsoft Teams, Slack)을 사용할 수 있도록 적용합니다.
- 채팅 클라이언트 액세스를 특정 워크스페이스(Slack) 및 팀(Microsoft Teams)으로 제한합니다.
- Slack 채널 가시성을 퍼블릭 또는 프라이빗 채널로 제한합니다.
- 특정 [역할 설정](#)을 설정하고 적용합니다.

채팅 애플리케이션 정책은 [역할 설정](#) 및 [채널 가드레일 정책](#)과 같은 계정 수준 설정을 제한하고 우선합니다. 채팅 애플리케이션의 Amazon Q Developer 또는 Organizations 콘솔에서 채팅 애플리케이션 정책에 액세스하고 수정할 수 있습니다.

정책이 계정 및 조직 단위(OU)에 연결되면 범위 내 계정에 대한 현재 및 미래의 모든 채팅 애플리케이션의 Amazon Q Developer 채팅 애플리케이션 구성이 자동으로 거버넌스 및 권한 설정을 준수하게 됩니다. 자세한 내용은 [관리 정책 상속 이해](#)를 참조하세요.

채팅 애플리케이션 정책에 의해 제한된 작업을 수행하려고 하면 채팅 애플리케이션 정책으로 인해 작업이 허용되지 않는다는 오류 메시지가 표시되고 조직의 관리 계정 또는 위임된 관리자에게 문의하라는 권장 사항이 표시됩니다.

Note

채팅 애플리케이션 정책은 런타임에 검증됩니다. 즉, 기존 리소스의 규정 준수 여부를 지속적으로 확인합니다. 알림을 보내거나 채팅 애플리케이션의 Amazon Q Developer와 상호 작용하기 위한 런타임 기반 IAM 권한은 현재 지원되지 않으므로 기존 IAM 권한과 중복되지 않습니다.

채팅 애플리케이션 정책 시작하기

다음 단계에 따라 채팅 애플리케이션 정책 사용을 시작합니다.

1. [채팅 애플리케이션 정책 작업을 수행하는 데 필요한 권한을 알아봅니다.](#)
2. [조직에 채팅 애플리케이션 정책을 활성화합니다.](#)
3. [채팅 애플리케이션 정책을 생성합니다.](#)
4. [채팅 애플리케이션 정책을 조직의 루트, OU 또는 계정에 연결합니다.](#)
5. [계정에 적용되는 결합된 유효 채팅 애플리케이션 정책을 확인합니다.](#)

위의 모든 단계를 수행하려면 조직의 관리 계정에서 IAM 사용자로 로그인하거나, IAM 역할을 맡거나, 루트 사용자로 로그인([권장되지 않음](#))합니다.

기타 정보

- [채팅 애플리케이션 정책 구문을 알아보고 정책 예제 보기](#)

채팅 애플리케이션 정책 구문 및 예제

이 페이지에서는 채팅 애플리케이션 정책에 대해 설명하고 예제를 제공합니다.

채팅 애플리케이션 정책에 대한 구문

채팅 애플리케이션 정책은 [JSON](#) 규칙에 따라 구성된 일반 텍스트 파일입니다. 채팅 애플리케이션 정책 구문은 관리 정책 유형에 대한 구문을 따릅니다. 해당 구문에 대한 자세한 내용은 [관리 정책 상속에 대한 이해](#) 단원을 참조하세요. 이 항목에서는 채팅 애플리케이션 정책 유형의 특정 요구 사항에 해당 일반 구문을 적용하는 방법을 중점적으로 설명합니다.

다음 예제에서는 채팅 애플리케이션 정책의 기본 구문을 보여줍니다.

```
{
  "chatbot":{
    "platforms":{
      "slack":{
        "client":{
          "@@assign":"enabled" // enabled | disabled
        },
        "workspaces": { // limit 255
          "@@assign":[
            "Slack-Workspace-Id"
          ]
        },
        "default":{
          "supported_channel_types":{
            "@@assign":[
              "private" // public | private
            ]
          },
          "supported_role_settings":{
            "@@assign":[
              "user_role" // user_role | channel_role
            ]
          }
        },
        "overrides":{ // limit 255
          "Slack-Workspace-Id":{
```



```

        "supported_channel_types":{
            "@@assign":[
                "public" // public | private
            ]
        },
        "supported_role_settings":{
            "@@assign":[
                "user_role" // user_role | channel_role
            ]
        }
    }
},
"microsoft_teams":{
    "client":{
        "@@assign":"enabled"
    },
    "tenants":{ // limit 36
        "Microsoft-Teams-Tenant-Id":{ // limit 36
            "@@assign":[
                "Microsoft-Teams-Team-Id"
            ]
        }
    },
    "default":{
        "supported_role_settings":{
            "@@assign":[
                "user_role" // user_role | channel_role
            ]
        }
    },
    "overrides":{ // limit 36
        "Microsoft-Teams-Tenant-Id":{ // limit 36
            "Microsoft-Teams-Team-Id":{
                "supported_role_settings":{
                    "@@assign":[
                        "user_role" // user_role | channel_role
                    ]
                }
            }
        }
    }
},
"chime":{

```

```

        "client":{
            "@@assign":"disabled" // enabled | disabled
        }
    },
    "default":{
        "client":{
            "@@assign":"disabled" // enabled | disabled
        }
    }
}
}

```

채팅 애플리케이션 정책에는 다음 요소가 포함됩니다.

- chatbot 필드 키 이름입니다. 채팅 애플리케이션 정책은 항상 이 고정 키 이름으로 시작합니다. 이 예제 정책에서 맨 위 줄입니다.
- chatbot에는 Slack, Microsoft Teams, Amazon Chime 등 지원되는 다양한 채팅 애플리케이션에 대한 구성이 포함된 platforms 블록이 있습니다.
- Slack의 경우 다음 필드를 사용할 수 있습니다.
 - "client":
 - "enabled": Slack 클라이언트가 활성화됩니다. Slack 통합이 허용됩니다.
 - "disabled": Slack 클라이언트가 비활성화됩니다. Slack 통합이 허용되지 않습니다.
 - "workspaces": 허용되는 Slack 워크스페이스의 심표로 구분된 목록입니다. 이 예제에서 허용되는 Slack 워크스페이스는 *Slack-Workspace-Id1* 및 *Slack-Workspace-Id2*입니다.
 - "default": Slack 워크스페이스의 기본 설정입니다.
 - "supported_channel_types":
 - "public": 범위 내 Slack 워크스페이스가 기본적으로 퍼블릭 Slack 채널을 허용합니다.
 - "private": 범위 내 Slack 워크스페이스가 기본적으로 프라이빗 Slack 채널을 허용합니다.
 - supported_role_settings:
 - "user_role": 범위 내 Slack 워크스페이스가 기본적으로 사용자 수준 IAM 역할을 허용합니다.
 - "channel_role": 범위 내 Slack 워크스페이스가 기본적으로 채널 수준 IAM 역할을 허용합니다.
 - "overrides": Slack 워크스페이스의 설정 재정의입니다.

- *Slack-Workspace-Id2*: 재정의 설정이 적용되는 Slack 워크스페이스의 쉼표로 구분된 목록입니다. 이 예제에서 Slack 워크스페이스는 *Slack-Workspace-Id2*입니다.
- "supported_channel_types":
 - "public": 범위 내 Slack 워크스페이스가 퍼블릭 Slack 채널을 허용하는지 여부를 재정의합니다.
 - "private": 범위 내 Slack 워크스페이스가 프라이빗 Slack 채널을 허용하는지 여부를 재정의합니다.
- supported_role_settings:
 - "user_role": 범위 내 Slack 워크스페이스가 사용자 수준 IAM 역할을 허용하는지 여부를 재정의합니다.
 - "channel_role": 범위 내 Slack 워크스페이스가 채널 수준 IAM 역할을 허용하는지 여부를 재정의합니다.
- Microsoft Teams의 경우 다음 필드를 사용할 수 있습니다.
- "client":
 - "enabled": Microsoft Teams 클라이언트가 활성화됩니다. Microsoft Teams 통합이 허용됩니다.
 - "disabled": Microsoft Teams 클라이언트가 비활성화됩니다. Microsoft Teams 통합이 허용되지 않습니다.
- "tenants": 허용되는 Microsoft Teams 테넌트의 쉼표로 구분된 목록입니다. 이 예제에서 허용되는 테넌트는 *Microsoft-Teams-Tenant-Id*입니다.
- *Microsoft-Teams-Tenant-Id*: 테넌트 내에서 허용되는 팀의 쉼표로 구분된 목록입니다. 이 예제에서 허용되는 팀은 *Microsoft-Teams-Team-Id*입니다.
- "default": 테넌트 내 팀의 기본 설정입니다.
- supported_role_settings:
 - "user_role": 범위 내 팀이 기본적으로 사용자 수준 IAM 역할을 허용합니다.
 - "channel_role": 범위 내 팀이 기본적으로 채널 수준 IAM 역할을 허용합니다.
- "overrides": Microsoft Teams 테넌트에 대한 재정의 설정입니다.
- *Microsoft-Teams-Tenant-Id*: 재정의 설정이 적용되는 테넌트의 쉼표로 구분된 목록입니다. 이 예제에서 테넌트는 *Microsoft-Teams-Tenant-Id*입니다.
- *Microsoft-Teams-Team-Id*: 테넌트 내 팀의 쉼표로 구분된 목록입니다. 이 예제에서 허용되는 팀은 *Microsoft-Teams-Team-Id*입니다.

- "user_role": 범위 내 팀이 사용자 수준 IAM 역할을 허용하는지 여부를 재정의합니다.
- "channel_role": 범위 내 팀이 채널 수준 IAM 역할을 허용하는지 여부를 재정의합니다.
- Amazon Chime의 경우 다음 필드를 사용할 수 있습니다.
 - "client":
 - "enabled": Amazon Chime 클라이언트가 활성화됩니다. Amazon Chime 통합이 허용됩니다.
 - "disabled": Amazon Chime 클라이언트가 비활성화됩니다. Amazon Chime 통합이 허용되지 않습니다.
- chatbot에는 더 낮은 수준에서 재정의되지 않는 한 조직 전체에서 채팅 애플리케이션의 Amazon Q Developer를 비활성화하는 default 블록이 있습니다. 이 기본값은 채팅 애플리케이션의 Amazon Q Developer에서 지원하는 모든 새 채팅 애플리케이션도 비활성화합니다. 예를 들어 채팅 애플리케이션의 Amazon Q Developer에서 새 채팅 애플리케이션을 지원하는 경우 이 기본값은 새로 지원되는 채팅 애플리케이션도 비활성화합니다.

Note

채널 수준 IAM 역할 및 사용자 수준 IAM 역할에 대한 자세한 내용은 채팅 애플리케이션의 Amazon Q Developer 관리자 안내서의 [채팅 애플리케이션의 Amazon Q Developer 권한 이해](#)를 참조하세요.

채팅 애플리케이션 정책 예제

다음 정책 예제는 정보 제공 용도로만 제공됩니다.

예제 1: 특정 워크스페이스에서 프라이빗 Slack 채널만 허용, Microsoft Teams 비활성화, 모든 인증 모드 지원

다음 정책은 Slack 및 Microsoft Teams 챗봇 통합에 허용되는 구성을 제어하는 데 중점을 둡니다.

```
{
  "chatbot": {
    "platforms": {
      "slack": {
        "client": {
```

```

        "@@assign": "enabled"
    },
    "workspaces": {
        "@@assign": [
            "Slack-Workspace-Id"
        ]
    },
    "default": {
        "supported_channel_types": {
            "@@assign": [
                "private"
            ]
        },
        "supported_role_settings": {
            "@@assign": [
                "channel_role",
                "user_role"
            ]
        }
    }
},
"microsoft_teams": {
    "client": {
        "@@assign": "disabled"
    }
},
"chime": {
    "client": {
        "@@assign": "disabled"
    }
},
"default": {
    "client": {
        "@@assign": "disabled"
    }
}
}
}
}
}

```

Slack의 경우

- Slack 클라이언트가 활성화됩니다.

- 특정 Slack 워크스페이스 *Slack-Workspace-Id*만 허용됩니다.
- 기본 설정은 프라이빗 Slack 채널, 채널 수준 IAM 역할 및 사용자 수준 IAM 역할만 허용하는 것입니다.

Microsoft Teams의 경우

- Microsoft Teams 클라이언트가 비활성화됩니다.

Amazon Chime의 경우

- Amazon Chime 클라이언트가 비활성화됩니다.

추가 세부 정보

- 하단의 default 블록은 클라이언트를 비활성화하도록 설정하며, 더 낮은 수준에서 재정의하지 않는 한 조직 전체에서 채팅 애플리케이션의 Amazon Q Developer를 비활성화합니다. 이 기본값은 채팅 애플리케이션의 Amazon Q Developer에서 지원하는 모든 새 채팅 애플리케이션도 비활성화합니다. 예를 들어 채팅 애플리케이션의 Amazon Q Developer에서 새 채팅 애플리케이션을 지원하는 경우 이 기본값은 새로 지원되는 채팅 애플리케이션도 비활성화합니다.

예제 2: 사용자 수준 IAM 역할과의 Slack 통합만 허용

다음 정책은 Slack에 대한 보다 허용적인 접근 방식을 취하여 모든 Slack 워크스페이스를 허용하지만 인증 모드를 사용자 수준 IAM 역할로만 제한합니다.

```
{
  "chatbot":{
    "platforms":{
      "slack":{
        "client":{
          "@@assign":"enabled"
        },
        "workspaces":
          {
            "@@assign":[
              "*"
            ]
          },
        "default":{
```

```

        "supported_role_settings":{
            "@@assign":[
                "user_role"
            ]
        }
    },
    "microsoft_teams":{
        "client":{
            "@@assign":"disabled"
        }
    },
    "chime":{
        "client":{
            "@@assign":"disabled"
        }
    },
    "default":{
        "client":{
            "@@assign":"disabled"
        }
    }
}

```

Slack의 경우

- Slack 클라이언트가 활성화됩니다.
- 와일드카드 "*"를 사용하여 특정 Slack 워크스페이스를 정의하지 않으므로 모든 워크스페이스가 허용됩니다.
- 기본 설정은 사용자 수준 IAM 역할만 허용하는 것입니다.

Microsoft Teams의 경우

- Microsoft Teams 클라이언트가 비활성화됩니다.

Amazon Chime의 경우

- Amazon Chime 클라이언트가 비활성화됩니다.

추가 세부 정보

- 하단의 default 블록은 클라이언트를 비활성화하도록 설정하며, 더 낮은 수준에서 재정의하지 않는 한 조직 전체에서 채팅 애플리케이션의 Amazon Q Developer를 비활성화합니다. 이 기본값은 채팅 애플리케이션의 Amazon Q Developer에서 지원하는 모든 새 채팅 애플리케이션도 비활성화합니다. 예를 들어 채팅 애플리케이션의 Amazon Q Developer에서 새 채팅 애플리케이션을 지원하는 경우 이 기본값은 새로 지원되는 채팅 애플리케이션도 비활성화합니다.

예제 3: 특정 테넌트에서 Microsoft Teams 통합만 허용

다음 예제 정책은 Slack 통합을 완전히 차단하면서 지정된 테넌트 내에서만 Microsoft Teams 챗봇 통합을 허용하도록 조직을 잠급니다.

```
{
  "chatbot":{
    "platforms":{
      "slack":{
        "client": {
          "@@assign": "disabled"
        },
      },
      "microsoft_teams":{
        "client": {
          "@@assign": "enabled"
        },
        "tenants":{
          "Microsoft-Teams-Tenant-Id":{
            "@@assign":[
              "*"
            ]
          }
        }
      },
      "chime": {
        "client":{
          "@@assign": "disabled"
        }
      }
    }
  }
}
```


Slack의 경우

- Slack 클라이언트가 비활성화됩니다.

Microsoft Teams의 경우

- 와일드카드 "*"를 사용하여 해당 테넌트 내의 모든 팀을 허용하는 특정 테넌트 *Microsoft-Teams-Tenant-Id*만 허용됩니다.

Amazon Chime의 경우

- Amazon Chime 클라이언트가 비활성화됩니다.

추가 세부 정보

- 하단의 default 블록은 클라이언트를 비활성화하도록 설정하며, 더 낮은 수준에서 재정의하지 않는 한 조직 전체에서 채팅 애플리케이션의 Amazon Q Developer를 비활성화합니다. 이 기본값은 채팅 애플리케이션의 Amazon Q Developer에서 지원하는 모든 새 채팅 애플리케이션도 비활성화합니다. 예를 들어 채팅 애플리케이션의 Amazon Q Developer에서 새 채팅 애플리케이션을 지원하는 경우 이 기본값은 새로 지원되는 채팅 애플리케이션도 비활성화합니다.

예제 4: Slack 워크스페이스 및 Microsoft Teams 테넌트에 대한 제한된 채팅 애플리케이션의 Amazon Q Developer 액세스 허용

다음 정책은 선택한 Slack 워크스페이스 및 Microsoft Teams 테넌트에 대한 제한된 채팅 애플리케이션의 Amazon Q Developer 액세스를 허용합니다.

```
{
  "chatbot":{
    "platforms":{
      "slack":{
        "client":{
          "@@assign":"enabled"
        },
        "workspaces": {
          "@@assign":[
            "Slack-Workspace-Id1",
            "Slack-Workspace-Id2"
          ]
        }
      }
    }
  }
}
```

```

    },
    "default":{
      "supported_channel_types":{
        "@@assign":[
          "private"
        ]
      },
      "supported_role_settings":{
        "@@assign":[
          "user_role"
        ]
      }
    },
    "overrides":{
      "Slack-Workspace-Id2":{
        "supported_channel_types":{
          "@@assign":[
            "public",
            "private"
          ]
        },
        "supported_role_settings":{
          "@@assign":[
            "channel_role",
            "user_role"
          ]
        }
      }
    },
    "microsoft_teams":{
      "client":{
        "@@assign":"enabled"
      },
      "tenants":{
        "Microsoft-Teams-Tenant-Id":{
          "@@assign":[
            "Microsoft-Teams-Team-Id"
          ]
        }
      }
    },
    "default":{
      "supported_role_settings":{
        "@@assign":[

```

```

        "user_role"
    ]
}
},
"overrides":{
    "Microsoft-Teams-Tenant-Id":{
        "Microsoft-Teams-Team-Id":{
            "supported_role_settings":{
                "@@assign":[
                    "channel_role",
                    "user_role"
                ]
            }
        }
    }
}
},
"default":{
    "client":{
        "@@assign":"disabled"
    }
}
}
}
}

```

Slack의 경우

- Slack 클라이언트가 활성화됩니다.
- 허용되는 Slack 워크스페이스는 *Slack-Workspace-Id1* 및 *Slack-Workspace-Id2*입니다.
- Slack의 기본 설정은 프라이빗 채널 및 사용자 수준 IAM 역할만 허용하는 것입니다.
- 퍼블릭 채널과 프라이빗 채널은 물론 채널 수준 IAM 역할과 사용자 수준 IAM 역할을 모두 허용하는 *Slack-Workspace-Id2* 워크스페이스에 대한 재정의가 있습니다.

Microsoft Teams의 경우

- Microsoft Teams가 활성화됩니다.
- 허용되는 Teams 테넌트는 *Microsoft-Teams-Tenant-Id*이고 팀은 *Microsoft-Teams-Team-Id*입니다.
- 기본 설정은 사용자 수준 IAM 역할만 허용하는 것입니다.

- 팀 *Microsoft-Teams-Team-Id*에 대한 채널 수준 IAM 역할과 사용자 수준 IAM 역할을 모두 허용하는 테넌트 *Microsoft-Teams-Tenant-Id*에 대한 재정의가 있습니다.

추가 세부 정보

- 하단의 default 블록은 클라이언트를 비활성화하도록 설정하며, 더 낮은 수준에서 재정의하지 않는 한 조직 전체에서 채팅 애플리케이션의 Amazon Q Developer를 비활성화합니다. 즉, 이 예제에서는 Amazon Chime이 비활성화됩니다. 이 기본값은 채팅 애플리케이션의 Amazon Q Developer에서 지원하는 모든 새 채팅 애플리케이션도 비활성화합니다. 예를 들어 채팅 애플리케이션의 Amazon Q Developer에서 새 채팅 애플리케이션을 지원하는 경우 이 기본값은 새로 지원되는 채팅 애플리케이션도 비활성화합니다.

AI 서비스 옵트아웃 정책

AWS AI 서비스는 운영 문제 수정, 서비스 성능 평가, 디버깅 또는 모델 훈련과 같은 서비스 개선을 위해 고객 콘텐츠를 사용하고 저장할 수 있습니다. 이를 위해 당사는 사용자가 서비스를 AWS 리전 사용하는 AWS 리전 외부의 이러한 콘텐츠를 저장할 수 있습니다. 옵트아웃 정책을 사용하여 서비스 개선을 위한 콘텐츠 사용을 AWS Organizations 옵트아웃할 수 있습니다.

개별 AI 서비스 또는 AI 서비스 옵트아웃 정책에서 지원하는 모든 서비스에 대해 옵트아웃 정책을 생성할 수 있습니다. 각 계정에 적용되는 유효 정책을 쿼리하여 설정 선택의 효과를 확인할 수 있습니다.

자세한 내용은 AWS 서비스 약관의 [AWS Machine Learning 및 인공 지능 서비스를](#) 참조하세요. AI 서비스 옵트아웃 정책에서 지원하는 서비스 목록은 [지원되는 AI 서비스 목록](#)을 참조하세요.

주제

- [AI 서비스 옵트아웃 정책 사용 시 고려 사항](#)
- [AI 서비스 옵트아웃 정책 시작하기](#)
- [지원되는 모든 AWS AI 서비스 옵트아웃](#)
- [AI 서비스 옵트아웃 정책 구문 및 예제](#)

AI 서비스 옵트아웃 정책 사용 시 고려 사항

옵트아웃하면 연결된 모든 기록 콘텐츠 삭제

AWS AI 서비스의 콘텐츠 사용을 옵트아웃하면 옵션을 설정하기 AWS 전에 공유된 모든 관련 기록 콘텐츠가 해당 서비스가 삭제됩니다. 이 삭제는 서비스 기능을 제공하는 데 필요하지 않은 저장된 데이터로 제한됩니다.

예를 들어 옵트인한 상태에서 서비스를 사용하는 경우 해당 서비스는 서비스 개선을 위해 콘텐츠 사본을 저장할 수 있습니다. 서비스 개선을 위해 서비스에서 저장한 모든 사본은 삭제되지만 서비스를 제공하는 데 사용되는 여하한 데이터는 삭제되지 않습니다.

AI 서비스 옵트아웃 정책 시작하기

다음 단계에 따라 인공 지능(AI) 서비스 옵트아웃 정책을 시작합니다.

1. [백업 정책 작업을 수행하는 데 필요한 권한에 대해 알아봅니다.](#)
2. [조직에 대해 AI 서비스 옵트아웃 정책을 활성화합니다.](#)
3. [AI 서비스 옵트아웃 정책을 만듭니다.](#)
4. [AI 서비스 옵트아웃 정책을 조직의 루트, OU 또는 계정에 연결합니다.](#)
5. [계정에 적용되는 결합된 유효 AI 서비스 옵트아웃 정책을 확인합니다.](#)

이러한 모든 단계에서 AWS Identity and Access Management 는 (IAM) 사용자로 로그인하거나, IAM 역할을 맡거나, 조직의 관리 계정에서 루트 사용자([권장되지 않음](#))로 로그인합니다.

기타 정보

- [AI 서비스 옵트아웃 정책에 대한 정책 구문 알아보기 및 정책 예제 보기](#)

지원되는 모든 AWS AI 서비스 옵트아웃

이 주제에서 수행할 작업

- AWS Organizations 콘솔에서 버튼 하나를 선택하여 옵트아웃할 수 있습니다.
- AWS CLI & AWS SDKs.
- AI 서비스 옵트아웃 정책에서 AWS 서비스 지원하는 목록을 볼 수 있습니다.

지원되는 모든 AI 서비스에서 옵트아웃

AI 서비스 옵트아웃 정책을 생성하고 연결하여 서비스 개선에 콘텐츠를 사용하지 않도록 할 수 있습니다. 이 정책은 현재 및 향후 지원되는 모든 AWS AI 서비스에 적용됩니다. 멤버 계정은 정책을 업데이트할 수 없습니다.

AWS Management Console

모든 AI 서비스에서 옵트아웃하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AI 서비스 옵트아웃 정책](#) 페이지에서 모든 서비스 옵트아웃을 선택합니다.
3. 모든 서비스에서 옵트아웃 확인 페이지에서 모든 서비스에서 옵트아웃을 선택합니다.

AWS CLI & AWS SDKs

모든 AI 서비스에서 옵트아웃하려면

1. [AI 서비스 옵트아웃 예제](#)의 “예제 1: 조직의 모든 계정에 대해 모든 AI 서비스를 옵트아웃”을 복사합니다.
2. [AI 서비스 연결 및 분리 옵트아웃](#)의 지침을 따릅니다.

Note

Amazon Monitron에서 옵트아웃하려면 추가 단계가 필요합니다. 자세한 내용은 [AWS 서비스 약관](#)을 참조하세요.

AI 서비스 옵트아웃 정책에서 지원하는 서비스 목록

다음은 AI 서비스 옵트아웃 정책에서 AWS 서비스 지원하는 목록입니다.

- [Amazon AI Operations](#)
- [Amazon Chime SDK 음성 분석](#)
- [Amazon CloudWatch](#)
- [Amazon CodeGuru Profiler](#)
- [Amazon CodeWhisperer](#)(이제 [Amazon Q Developer](#)에 속함)
- [Amazon Comprehend](#)
- [Amazon Connect](#)
- [Amazon Connect 최적화](#)

- [Amazon Connect Contact Lens](#)
- [AWS 데이터베이스 마이그레이션 서비스](#)
- [Amazon DataZone](#)(및 [Amazon SageMaker Data Agent](#))
- [AWS DevOps Agent](#)
- [AWS Entity Resolution](#)
- [Amazon Fraud Detector](#)
- [AWS Glue](#)
- [Amazon GuardDuty](#)
- [Amazon Lex](#)
- [Amazon Polly](#)
- [Amazon Q](#)
- [Amazon Quick](#)
- [Amazon Rekognition](#)
- [Amazon Security Lake](#)
- [AWS Supply Chain](#)
- [Amazon Textract](#)
- [Amazon Transcribe](#)
- [AWS 변환](#)
- [Amazon Translate](#)
- [Amazon WorkSpaces](#)
- [AWS Security Hub](#)

AI 서비스 옵트아웃 정책 구문 및 예제

이 주제에서는 AI(인공 지능) 서비스 옵트아웃 정책 구문에 대해 설명하고 예제를 제공합니다.

AI 서비스 옵트아웃 정책의 구문

AI 서비스 옵트아웃 정책은 [JSON](#) 규칙에 따라 구성된 일반 텍스트 파일입니다. AI 서비스 옵트아웃 정책 구문은 관리 정책 유형에 대한 구문을 따릅니다. 해당 구문에 대한 자세한 내용은 [관리 정책 상속에 대한 이해](#) 단원을 참조하세요. 이 주제에서는 AI 서비스 옵트아웃 정책 유형의 특정 요구 사항에 해당 일반 구문을 적용하는 방법을 중점적으로 설명합니다.

⚠ Important

이 섹션에 설명된 값의 대소문자 사용은 중요합니다. 이 주제에 제시된 대로 대문자와 소문자로 값을 입력해야 합니다. 잘못된 대소문자를 사용하면 정책이 작동하지 않습니다.

다음 정책은 기본적인 AI 서비스 옵트아웃 정책 구문을 보여 줍니다. 이 예제를 계정에 직접 연결하면 해당 계정은 한 서비스를 명시적으로 옵트아웃하고 다른 한 서비스에는 옵트인합니다. 다른 서비스들은 상위 수준(OU 또는 루트 정책)으로부터 상속된 정책에 의해 옵트인되거나 옵트아웃될 수 있습니다.

```
{
  "services": {
    "rekognition": {
      "opt_out_policy": {
        "@@assign": "optOut"
      }
    },
    "lex": {
      "opt_out_policy": {
        "@@assign": "optIn"
      }
    }
  }
}
```

다음은 조직의 루트에 연결된 정책의 예입니다. 이 예제는 조직에서 모든 AI 서비스를 옵트아웃하는 기본값을 설정합니다. 여기에는 명시적으로 제외되지 않은 한 AWS 가 향후 배포할 수 있는 모든 AI 서비스를 비롯해 모든 AI 서비스가 자동으로 포함됩니다. 하위 정책을 OU에 연결하거나 계정에 직접 연결하여 Amazon Comprehend를 제외한 모든 AI 서비스에 대해 이 설정을 재정의할 수 있습니다. 다음 예제의 두 번째 항목은 @@operators_allowed_for_child_policies를 none으로 설정하여 설정이 재정의되지 않도록 합니다. 예제의 세 번째 항목은 Amazon Rekognition에 대해 조직 전체를 제외합니다. 이에 따라 전체 조직이 해당 서비스를 옵트인합니다. 그러나 적절한 경우 해당 정책은 하위 정책의 재정의 허용합니다.

```
{
  "services": {
    "default": {
      "opt_out_policy": {
        "@@assign": "optOut"
      }
    }
  }
}
```



```

    },
    "comprehend": {
      "opt_out_policy": {
        "@operators_allowed_for_child_policies": ["@none"],
        "@assign": "optOut"
      }
    },
    "rekognition": {
      "opt_out_policy": {
        "@assign": "optIn"
      }
    }
  }
}

```

AI 서비스 옵트아웃 정책 구문에는 다음 요소가 포함됩니다.

- **services** 요소. AI 서비스 옵트아웃 정책은 이 고정 이름에 의해 가장 바깥쪽 JSON 포함 요소로 식별됩니다.

AI 서비스 옵트아웃 정책은 **services** 요소에 하나 이상의 문을 가질 수 있습니다. 각 문에는 다음 요소가 포함됩니다.

- AWS AI 서비스를 식별하는 서비스 이름 키입니다. 다음의 키 이름은 이 필드에 유효한 값입니다.
 - **default** – 현재 사용 가능한 모든 AI 서비스를 나타내며, 향후 추가될 수 있는 AI 서비스를 묵시적으로 자동 포함시킵니다.
 - aiops
 - aidevops
 - awssupplychain
 - chimesdkvoiceanalytics
 - cloudwatch
 - codeguruprofiler
 - codewhisperer
 - comprehend
 - connect
 - connectamd
 - connectoptimization
 - contactlens

- datazone
- dms
- entityresolution
- frauddetector
- glue
- guardduty
- lex
- polly
- q
- quicksightq
- rekognition
- securitylake
- textract
- transcribe
- transform
- translate
- workspaces
- securityhub

서비스 이름 키로 식별되는 각 정책 문에는 다음 요소가 포함될 수 있습니다.

- `opt_out_policy` 키. 이 키는 반드시 있어야 합니다. 이 키는 서비스 이름 키 아래에 배치할 수 있는 유일한 키입니다.

`opt_out_policy` 키는 다음 값 중 하나를 가진 `@@assign` 연산자만 포함할 수 있습니다

- `optOut` - 지정된 AI 서비스의 콘텐츠 사용을 옵트아웃하도록 선택합니다.
- `optIn` - 지정된 AI 서비스의 콘텐츠 사용을 옵트인하도록 선택합니다.

참고

- `@@append` 및 `@@remove` 상속 연산자는 AI 서비스 옵트아웃 정책에 사용할 수 없습니다.

AI 서비스 옵트아웃 정책 ~~• `@@enforced_for` 연산자는 AI 서비스 옵트아웃 정책에 사용할 수 없습니다.~~

- 어떤 레벨에서든 `@@operators_allowed_for_child_policies` 연산자를 지정하면 상위 정책에서 부과한 설정을 재정의하기 위해 하위 정책이 실행할 수 있는 동작을 제어할 수 있습니다. 다음 값 중 하나를 지정할 수 있습니다.
- `@@assign` - 해당 정책의 하위 정책이 `@@assign` 연산자를 사용하여 상속된 값을 다른 값으로 재정의할 수 있습니다.
- `@@none` - 해당 정책의 하위 정책이 값을 변경할 수 없습니다.

`@@operators_allowed_for_child_policies`가 동작하는 방식은 배치하는 위치에 따라 다릅니다. 다음의 위치를 사용할 수 있습니다.

- `services` 키 아래에 배치 - 하위 정책이 유효 정책의 서비스 목록을 추가하거나 변경할 수 있는지 여부를 제어합니다.
- 특정 AI 서비스 또는 `default` 키에 대한 키 아래에 배치 - 하위 정책이 이 특정 항목 아래의 키 목록에 키를 추가하거나 키 목록을 변경할 수 있는지 여부를 제어합니다.
- 특정 서비스에 대한 `opt_out_policies` 키 아래에 배치 - 하위 정책이 이 특정 서비스에 대한 설정만을 변경할 수 있는지 여부를 제어합니다.

AI 서비스 옵트아웃 정책 예제

다음 정책 예제는 정보 제공 용도로만 제공됩니다.

예제 1: 조직의 모든 계정에 대해 모든 AI 서비스를 옵트아웃

다음 예제에서는 조직의 루트에 연결하여 조직의 계정에 대해 AI 서비스를 옵트아웃할 수 있는 정책을 보여 줍니다.

Tip

예제의 오른쪽 위 모서리에 있는 복사 버튼을 사용하여 다음 예제를 복사하면 복사본에 행 번호가 포함되지 않습니다. 붙여 넣을 준비가 되었습니다.

```
[1] | {
    |   "services": {
    |     "@@operators_allowed_for_child_policies": ["@@none"],
    |     "default": {
    |       "@@operators_allowed_for_child_policies": ["@@none"],
    |       "opt_out_policy": {
    |         "@@operators_allowed_for_child_policies": ["@@none"],
```

```

|               "@@assign": "optOut"
|           }
|       }
|   }
| }

```

- [1] - "@@operators_allowed_for_child_policies": ["@@none"]를 services 아래에 배치하면 모든 하위 정책이 이미 존재하는 default 섹션 외에 개별 서비스의 새 섹션을 추가하지 못합니다. Default는 “모든 AI 서비스”를 나타내는 자리표시자입니다.
- [2] - "@@operators_allowed_for_child_policies": ["@@none"]를 default 아래에 배치하면 모든 하위 정책이 이미 존재하는 opt_out_policy 섹션 외에 개별 서비스에 대한 새 섹션을 추가하지 못합니다.
- [3] - "@@operators_allowed_for_child_policies": ["@@none"]를 opt_out_policy 아래에 배치하면 하위 정책이 optOut 설정의 값을 변경하거나 다른 설정을 추가하지 못합니다.

예제 2: 모든 서비스에 대해 조직 기본 설정을 설정하되 하위 정책이 개별 서비스에 대한 설정을 재정의할 수 있도록 허용

다음 정책 예제는 모든 AI 서비스에 대해 조직 전반의 기본값을 설정합니다. 값이 default이면 하위 정책이 서비스 default(모든 AI 서비스에 대한 자리표시자)의 optOut 값을 변경하지 못합니다. 이 정책을 루트 또는 OU에 연결하여 상위 정책으로 적용하더라도 하위 정책은 두 번째 정책에서처럼 개별 서비스에 대한 옵트아웃 설정을 변경할 수 있습니다.

- services 키 아래에 "@@operators_allowed_for_child_policies": ["@@none"]가 없으므로 하위 정책이 개별 서비스에 대한 새 섹션을 추가할 수 있습니다.
- "@@operators_allowed_for_child_policies": ["@@none"]를 default 아래에 배치하면 모든 하위 정책이 이미 존재하는 opt_out_policy 섹션 외에 새 섹션을 추가하지 못합니다.
- "@@operators_allowed_for_child_policies": ["@@none"]를 opt_out_policy 아래에 배치하면 하위 정책이 optOut 설정의 값을 변경하거나 다른 설정을 추가하지 못합니다.

조직 루트 사용자 AI 서비스 옵트아웃 상위 정책

```

{
  "services": {
    "default": {
      "@@operators_allowed_for_child_policies": ["@@none"],
      "opt_out_policy": {

```

```

        "@operators_allowed_for_child_policies": ["@none"],
        "@assign": "optOut"
    }
}
}
}

```

다음 정책 예제는 앞의 정책 예제가 조직 루트 또는 상위 OU에 연결되며 이 예제를 상위 정책의 영향을 받는 계정에 연결한다고 가정합니다. 이 정책은 기본 옵트아웃 설정을 재정의하고 Amazon Lex 서비스만 명시적으로 옵트인합니다.

AI 서비스 옵트아웃 하위 정책

```

{
  "services": {
    "lex": {
      "opt_out_policy": {
        "@assign": "optIn"
      }
    }
  }
}

```

에 대한 결과 유효 정책은 계정이 Amazon Lex에만 옵트인하고 상위 정책의 상속된 옵트아웃 설정으로 인해 다른 모든 AWS AI 서비스를 default옵트아웃 AWS 계정 하는 것입니다.

예제 3: 한 서비스에 대해 조직 전체의 AI 서비스 옵트아웃 정책 정의

다음 예제에서는 하나의 AI 서비스에 대해 optOut 설정을 정의하는 AI 서비스 옵트아웃 정책을 보여줍니다. 이 정책이 조직의 루트에 연결되면 하위 정책이 해당 서비스에 대한 optOut 설정을 재정의할 수 없습니다. 다른 서비스는 이 정책으로 처리되지 않지만 다른 OU 또는 계정의 하위 정책이 영향을 미칠 수 있습니다.

```

{
  "services": {
    "rekognition": {
      "opt_out_policy": {
        "@assign": "optOut",
        "@operators_allowed_for_child_policies": ["@none"]
      }
    }
  }
}

```

```
}
}
```

Security Hub 정책

AWS Security Hub 정책은 보안 팀에 보안 구성을 관리하는 중앙 집중식 접근 방식을 제공합니다 AWS Organizations. 이러한 정책을 활용하여 중앙 구성 메커니즘을 통해 일관된 보안 제어를 설정하고 유지할 수 있습니다. 이 통합을 통해 조직의 보안 요구 사항에 부합하는 정책을 생성하고 계정 및 조직 단위 (OU) 전반에 이를 중앙에서 적용함으로써 보안 적용 범위 격차를 해소할 수 있습니다.

Security Hub 정책은와 완전히 통합되어 관리 계정 또는 위임된 관리자가 보안 구성을 정의하고 적용할 수 AWS Organizations 있습니다. 계정이 조직에 가입하면 조직 계층 구조 내 위치에 따라 해당 정책을 자동으로 상속합니다. 이렇게 하면 조직이 성장함에 따라 보안 표준이 일관되게 적용됩니다. 정책은 기존 조직 구조를 존중하고 보안 구성이 배포되는 방식에 유연성을 제공하는 동시에 중요한 보안 설정에 대한 중앙 집중식 제어를 유지합니다.

주요 기능 및 이점

Security Hub 정책은 AWS 조직 전체에서 보안 구성을 관리하고 적용하는 데 도움이 되는 포괄적인 기능 세트를 제공합니다. 이러한 기능은 다중 계정 환경을 일관되게 제어하면서 보안 관리를 간소화합니다.

- 조직의 계정 및 리전 전반에 걸쳐 중앙에서 [Security Hub 활성화](#)
- 계정 및 OU에서 보안 구성을 정의하는 보안 정책 생성
- 조직에 가입할 때 새 계정에 보안 구성을 자동으로 적용
- 조직 전체에서 일관된 보안 설정 보장
- 멤버 계정이 조직 수준 보안 구성을 수정하지 못하도록 방지

Security Hub 정책이란 무엇입니까?

Security Hub 정책은 조직 계정 전반의 보안 구성을 중앙 집중식으로 제어하는 AWS Organizations 정책입니다. 이러한 정책은 AWS Organizations 와 원활하게 연동되므로 다중 계정 환경 전체에서 일관된 보안 표준을 설정하고 유지할 수 있습니다.

Security Hub 정책을 구현하면 조직 전체에 자동으로 적용되는 특정 보안 구성을 정의할 수 있는 능력을 갖게 됩니다. 이렇게 하면 새로 생성된 계정을 포함한 모든 계정이 조직의 보안 요구 사항 및 모범 사례에 맞게 조정됩니다.

또한 이러한 정책은 일관된 보안 제어를 적용하고 개별 계정이 조직 수준 보안 설정을 수정하지 못하도록 하여 규정 준수를 유지하는 데 도움이 됩니다. 이 중앙 집중식 접근 방식은 크고 복잡한 AWS 환경에서 보안 구성을 관리하는 데 드는 관리 오버헤드를 크게 줄입니다.

Security Hub 정책의 작동 방식

Security Hub 정책을 조직 또는 조직 단위에 연결하면 AWS Organizations 이(가) 해당 정책을 자동으로 평가하고 사용자가 정의한 범위에 따라 정책을 적용합니다. 이 정책 적용 프로세스는 다음과 같은 특정 충돌 해결 규칙을 따릅니다.

활성화 및 비활성화 목록 모두에 리전이 표시되면 비활성화 구성이 우선합니다. 예를 들어 리전이 활성화 및 비활성화 구성 모두에 나열된 경우 해당 리전에서 Security Hub가 비활성화됩니다.

활성화를 위해 ALL_SUPPORTED를 지정하면 명시적으로 비활성화되지 않는 한 모든 현재 및 향후 리전에서 Security Hub가 활성화됩니다. 이를 통해 새 리전으로 AWS 확장됨에 따라 포괄적인 보안 범위를 유지할 수 있습니다.

하위 정책은 상속 연산자를 사용하여 상위 정책 설정을 수정할 수 있으므로, 조직의 다양한 수준에서 세분화된 제어가 가능합니다. 이 계층적 접근 방식을 사용하면 특정 조직 단위가 기존 제어를 유지하면서 보안 설정을 사용자 지정할 수 있습니다.

용어

이 주제에서는 Security Hub 정책을 설명할 때 다음 용어를 사용합니다.

Security Hub 정책 용어

용어	정의
유효 정책	모든 상속된 정책을 결합한 후 계정에 적용되는 최종 정책입니다.
정책 상속	계정이 상위 조직 단위로부터 정책을 상속하는 프로세스입니다.
위임된 관리자	조직을 대신하여 Security Hub 정책을 관리하도록 지정된 계정입니다.
서비스 연결 역할	Security Hub가 다른 AWS 서비스와 상호 작용할 수 있도록 허용하는 IAM 역할입니다.

Security Hub 정책의 사용 사례

Security Hub 정책은 다중 계정 환경의 일반적인 보안 관리 문제를 해결합니다. 다음 사용 사례는 조직이 일반적으로 이러한 정책을 구현하여 보안 태세를 강화하는 방법을 보여줍니다.

사용 사례 예: 리전별 규정 준수 요구 사항

다국적 기업의 경우 다양한 지리적 리전에 서로 다른 Security Hub 구성이 필요합니다.

ALL_SUPPORTED를 사용하여 모든 리전에서 Security Hub를 활성화하는 상위 정책을 생성한 다음 하위 정책을 사용하여 다른 보안 제어가 필요한 특정 리전을 비활성화합니다. 이를 통해 포괄적인 보안 적용 범위를 보장하는 동시에 리전별 규정을 준수할 수 있습니다.

사용 사례 예: 개발 팀 보안 표준

소프트웨어 개발 조직은 개발 리전을 관리하지 않고 유지하면서 프로덕션 리전에서 모니터링할 수 있는 Security Hub 정책을 구현합니다. 보안 모니터링 범위에 대한 정확한 제어를 유지하기 위해 ALL_SUPPORTED보다는 정책에서 명시적 리전 목록을 사용합니다. 이 접근 방식을 사용하면 개발 영역에서 유연성을 유지하면서 프로덕션 환경에서 더 엄격한 보안 제어를 적용할 수 있습니다.

정책 상속 및 적용

정책을 상속하고 적용하는 방법을 이해하는 것은 조직 전체의 효과적인 보안 관리에 매우 중요합니다. 상속 모델은 AWS Organizations 계층 구조를 따르므로 예측 가능하고 일관된 정책 적용을 보장합니다.

- 루트 수준에서 연결된 정책은 모든 계정에 적용됩니다.
- 계정은 상위 조직 단위로부터 정책을 상속합니다.
- 단일 계정에 여러 정책을 적용할 수 있습니다.
- 보다 구체적인 정책(계층 구조상 해당 계정에 더 가까움)이 우선합니다.

정책 검증

Security Hub 정책을 생성할 때 다음과 같은 검증이 수행됩니다.

- 리전 이름은 유효한 AWS 리전 식별자여야 합니다.
- Security Hub에서 리전을 지원해야 합니다.
- 정책 구조는 AWS Organizations 정책 구문 규칙을 따라야 합니다.
- `enable_in_regions` 및 `disable_in_regions` 목록이 모두 있어야 하지만 비어 있을 수 있습니다.

리전별 고려 사항 및 지원되는 리전

Security Hub 정책은 여러 리전에서 운영되므로 글로벌 보안 요구 사항을 신중하게 고려해야 합니다. 리전별 행동을 이해하면 조직의 글로벌 사업 영역 전반에 걸쳐 효과적인 보안 제어를 구현하는 데 도움이 됩니다.

- 정책 적용은 각 리전에서 독립적으로 수행됩니다.
- 정책에 포함하거나 제외할 리전을 지정할 수 있습니다.
- ALL_SUPPORTED 옵션을 사용하면 새 리전이 자동으로 포함됩니다.
- 정책은 Security Hub를 사용할 수 있는 리전에만 적용됩니다.

다음 단계

Security Hub 정책 시작하기:

1. Security Hub 정책 시작하기의 사전 조건 검토
2. 모범 사례 가이드를 사용하여 정책 전략 계획
3. 정책 구문 알아보기 및 정책 예제 보기

Security Hub 정책 시작하기

Security Hub 정책을 구성하기 전에 사전 조건 및 구현 요구 사항을 이해해야 합니다. 이 주제에서는 조직에서 이러한 정책을 설정하고 관리하는 프로세스를 안내합니다.

시작하기 전 준비 사항

Security Hub 정책을 구현하기 전에 다음 요구 사항을 검토합니다.

- 계정은 AWS Organizations 조직의 일부여야 합니다.
- 다음 중 하나로 로그인해야 합니다.
 - 조직의 관리 계정
 - Security Hub 정책을 관리할 권한이 있는 위임된 관리자 계정
- 조직의 Security Hub에 대해 신뢰할 수 있는 액세스를 활성화해야 합니다.
- 조직의 루트에서 Security Hub 정책 유형을 활성화해야 합니다.

또한 다음을 확인하세요.

- 정책을 적용하려는 리전에서 Security Hub를 지원합니다.
- 관리 계정에 AWSServiceRoleForSecurityHubV2 서비스 연결 역할이 구성되어 있습니다. 이 역할이 존재하는지 확인하려면 `aws iam get-role --role-name AWSServiceRoleForSecurityHubV2`을(를) 실행합니다. 이 역할을 생성해야 하는 경우 관리 계정의 모든 리전에서 `aws securityhub enable-security-hub-v2`을(를) 실행하거나 `aws iam create-service-linked-role --aws-service-name securityhubv2.amazonaws.com`을(를) 실행하여 직접 생성할 수 있습니다.

구현 단계

Security Hub 정책을 효과적으로 구현하려면 다음 단계를 순서대로 따르세요. 각 단계는 적절한 구성을 보장하고 설정 중에 발생하는 일반적인 문제를 방지하는 데 도움이 됩니다. 관리 계정 또는 위임된 관리자는 AWS Organizations 콘솔, AWS 명령줄 인터페이스(AWS CLI) 또는 AWS SDKs.

1. [Security Hub에 대한 신뢰할 수 있는 액세스를 활성화합니다.](#)
2. [조직에 대해 Security Hub 정책을 활성화합니다.](#)
3. [Security Hub 정책을 생성합니다.](#)
4. [Security Hub 정책을 조직의 루트, OU 또는 계정에 연결합니다.](#)
5. [계정에 적용되는 결합된 유효 Security Hub 정책을 확인합니다.](#)

이러한 모든 단계에서 AWS Identity and Access Management 는 (IAM) 사용자로 로그인하거나, IAM 역할을 맡거나, 조직의 관리 계정에서 루트 사용자([권장되지 않음](#))로 로그인합니다.

기타 정보

- [Security Hub 정책에 대한 정책 구문 알아보기 및 정책 예제 보기](#)

Security Hub 정책 사용의 모범 사례

조직 전체에 Security Hub 정책을 구현할 때 확립된 모범 사례를 따르면 보안 구성을 성공적으로 배포하고 유지 관리하는 데 도움이 됩니다. 이러한 지침은 특히 Security Hub 정책 관리 및 적용의 고유한 측면을 다룹니다 AWS Organizations.

정책 설계 원칙

Security Hub 정책을 생성하기 전에 정책 구조에 대한 명확한 원칙을 설정합니다. 정책을 단순하게 유지하고 최종 결과를 결정하기 어렵게 만드는 복잡한 교차 속성 또는 중첩된 규칙을 피합니다. 조직 루

트 수준에서 광범위한 정책으로 시작하여 필요한 경우 하위 정책을 통해 정책을 세부적으로 조정합니다.

빈 리전 목록을 전략적으로 사용하는 것이 좋습니다. 특정 리전에서만 Security Hub를 비활성화해야 하는 경우 `enable_in_regions`을(를) 비워 두거나 정책에 따라 관리하지 않고 두려면 `disable_in_regions`을(를) 비워 둘 수 있습니다. 이러한 유연성을 통해 보안 모니터링 범위를 정확하게 제어할 수 있습니다.

리전 관리 전략

Security Hub 정책을 통해 리전을 관리할 때는 다음과 같은 검증된 접근 방식을 고려하세요. 보안 범위에 향후 리전을 자동으로 포함하려는 경우 `ALL_SUPPORTED`을(를) 사용합니다. 보다 세분화된 제어를 위해, 특히 리전마다 다른 보안 구성이 필요한 경우에 `ALL_SUPPORTED`에 의존하지 않고 리전을 명시적으로 나열합니다.

특히 다음에 대한 리전별 요구 사항을 문서화합니다.

- 특정 구성이 필요한 규정 준수 필수 리전
- 개발 환경과 프로덕션 환경의 차이점
- 특별한 고려 사항이 있는 오픈 리전
- Security Hub가 비활성화된 상태로 유지되어야 하는 리전

정책 상속 계획

정책 상속 구조를 신중하게 계획하여 필요한 유연성을 허용하면서 효과적인 보안 제어를 유지합니다. 상속된 정책을 수정할 수 있는 조직 단위와 허용되는 수정 사항을 문서화합니다. 엄격한 보안 제어를 적용해야 하는 경우 상위 수준에서 상속 연산자(`@@assign`, `@@append`, `@@remove`)를 제한하는 것이 좋습니다.

모니터링 및 검증

정책이 유효하도록 정기적인 모니터링 관행을 구현합니다. 특히 조직 변경 후 정책 첨부 파일을 정기적으로 검토합니다. 특히 `ALL_SUPPORTED`를 사용하거나 여러 리전 목록을 관리할 때 리전 구성이 의도한 보안 적용 범위와 일치하는지 확인합니다.

문제 해결 전략

Security Hub 정책의 문제를 해결할 때는 먼저 정책 우선 순위와 상속에 중점을 둡니다. 리전이 두 목록에 모두 나타나면 비활성화 구성이 활성화 구성보다 우선합니다. 정책 상속 체인을 확인하여 상위 정책과 하위 정책이 어떻게 결합하여 각 계정에 대한 유효 정책을 생성하는지 이해합니다.

Security Hub 정책 구문 및 예제

Security Hub 정책은 조직 전체에서 Security Hub를 활성화하고 구성하는 방법을 정의하는 표준화된 JSON 구문을 따릅니다. 정책 구조를 이해하면 보안 요구 사항에 맞는 효과적인 정책을 생성하는 데 도움이 됩니다.

고려 사항

Security Hub 정책을 생성하기 전에 정책 구문에 대한 다음 주요 사항을 이해합니다.

- 정책에는 `enable_in_regions` 및 `disable_in_regions` 목록이 모두 필요하지만 비어 있을 수 있습니다.
- 유효 정책을 처리할 때 `enable_in_regions`보다 `disable_in_regions`가 우선합니다.
- 명시적으로 제한되지 않는 한 하위 정책이 상속 연산자를 사용하여 상위 정책을 수정할 수 있습니다.
- `ALL_SUPPORTED` 지정에는 현재 리전과 미래 리전이 모두 포함됩니다.
- 리전 이름은 유효해야 하며 Security Hub에서 사용할 수 있어야 합니다.

기본 정책 구조

Security Hub 정책은 다음과 같은 기본 구조를 사용합니다.

```
{
  "securityhub": {
    "enable_in_regions": {
      "@append": ["ALL_SUPPORTED"],
      "@operators_allowed_for_child_policies": ["@all"]
    },
    "disable_in_regions": {
      "@append": [],
      "@operators_allowed_for_child_policies": ["@all"]
    }
  }
}
```

정책 구성 요소

Security Hub 정책에는 다음과 같은 주요 구성 요소가 포함되어 있습니다.

securityhub

정책 설정을 위한 최상위 컨테이너

모든 Security Hub 정책에 필요

enable_in_regions

Security Hub를 활성화해야 하는 리전 목록

특정 리전 이름 또는 ALL_SUPPORTED 포함 가능

필수 필드이지만 비어 있을 수 있음

ALL_SUPPORTED 사용 시 향후 리전 포함

disable_in_regions

Security Hub를 비활성화해야 하는 리전 목록

특정 리전 이름 또는 ALL_SUPPORTED 포함 가능

필수 필드이지만 비어 있을 수 있음

리전이 두 목록에 모두 나타날 enable_in_regions보다 우선함
상속 연산자

@@assign - 상속된 값을 덮어씀

@@append - 기존 값에 새 값 추가

@@remove - 상속된 설정에서 특정 값을 제거

Security Hub 정책 예제

다음 예제에서는 일반적인 Security Hub 정책 구성을 보여줍니다.

아래 예제에서는 모든 현재 및 향후 리전에서 Security Hub를 활성화합니다. enable_in_regions 목록에서 ALL_SUPPORTED을(를) 사용하고 disable_in_regions을(를) 비워 두면 새 리전을 사용할 수 있게 될 때 이 정책이 포괄적인 보안 적용 범위를 보장합니다.

```
{
  "securityhub":{
    "enable_in_regions":{
      "@@assign":[
        "ALL_SUPPORTED"
      ]
    }
  }
```

```

    },
    "disable_in_regions":{
        "@@assign":[
            ]
        }
    }
}

```

이 예제에서는 `disable_in_regions` 목록이 `enable_in_regions`보다 우선하므로 향후 리전을 포함한 모든 리전에서 Security Hub를 비활성화합니다.

```

{
  "securityhub":{
    "enable_in_regions":{
      "@@assign":[
        "us-east-1",
        "us-west-2"
      ]
    },
    "disable_in_regions":{
      "@@assign":[
        "ALL_SUPPORTED"
      ]
    }
  }
}

```

다음 예제에서는 하위 정책이 상속 연산자를 사용하여 상위 정책 설정을 수정하는 방법을 보여줍니다. 이 접근 방식을 사용하면 전체 정책 구조를 유지하면서 세부적으로 제어할 수 있습니다. 하위 정책은 `enable_in_regions`에 새 리전을 추가하고 `disable_in_regions`에서 리전을 제거합니다.

```

{
  "securityhub":{
    "enable_in_regions":{
      "@@append":[
        "eu-central-1"
      ]
    },
    "disable_in_regions":{
      "@@remove":[
        "us-west-2"
      ]
    }
  }
}

```

```

    ]
  }
}
}

```

이 예제에서는 ALL_SUPPORTED을(를) 사용하지 않고 여러 특정 리전에서 Security Hub를 활성화하는 방법을 보여줍니다. 이를 통해 Security Hub가 활성화된 리전을 정밀하게 제어할 수 있으며, 지정되지 않은 리전은 정책의 적용을 받지 않게 됩니다.

```

{
  "securityhub":{
    "enable_in_regions":{
      "@@assign":[
        "us-east-1",
        "us-west-2",
        "eu-west-1",
        "ap-southeast-1"
      ]
    },
    "disable_in_regions":{
      "@@assign":[
        ]
    }
  }
}

```

다음 예제에서는 대부분의 리전에서 Security Hub를 활성화하고 특정 위치에서는 명시적으로 비활성화하여 리전 규정 준수 요구 사항을 처리하는 방법을 보여줍니다. 이 disable_in_regions 목록이 우선하므로 다른 정책 설정에 관계없이 해당 리전에서 Security Hub가 비활성화된 상태로 유지됩니다.

```

{
  "securityhub":{
    "enable_in_regions":{
      "@@assign":[
        "ALL_SUPPORTED"
      ]
    },
    "disable_in_regions":{
      "@@assign":[
        "ap-east-1",
        "me-south-1"
      ]
    }
  }
}

```

```

    ]
  }
}
}

```

Amazon Bedrock 정책

Amazon Bedrock 정책을 사용하면 Amazon Bedrock에 대한 모든 모델 추론 호출에 대해 조직 구조의 모든 요소에 Amazon Bedrock 가드레일에 구성된 보호 기능을 자동으로 적용할 수 있습니다. 이렇게 하면 각 계정에 대해 개별 가드레일을 구성할 필요가 없습니다. Amazon Bedrock 가드레일은 Amazon Bedrock에서 지원되는 모델, 미세 조정된 모델, Amazon Bedrock 외부에서 호스팅되는 모델을 포함한 다양한 파운데이션 모델에 대한 표준 접근 방식을 통해 대규모로 생성형 AI 애플리케이션을 안전하게 구축하는 데 도움이 되는 구성 가능한 보호 장치를 제공합니다.

AWS Organizations의 Amazon Bedrock 정책을 사용하면 관리 계정에서 생성된 가드레일을 JSON 형식으로 참조할 수 있습니다. 루트, 조직 단위(OU) 및 개별 계정과 같은 조직 구조의 필수 요소에 정책을 연결할 수 있습니다. AWS 조직은 상속 규칙을 적용하여 정책을 결합하므로 생성형 AI 애플리케이션에 보호 장치가 적용되는 방법을 지정하는 각 계정에 대한 유효 정책이 생성됩니다.

작동 방식

Amazon Bedrock 정책을 사용하면 여러 계정의 가드레일 내에서 보호 기능의 자동 적용을 제어할 수 있으므로 Amazon Bedrock에 대한 추론 호출을 위해 모델의 전체 또는 하위 집합에 가드레일을 적용할 수 있습니다. 조직의 책임 있는 AI 요구 사항을 준수하여 정책 내에서 적절한 가드레일의 특정 버전을 참조해야 합니다. 이는 가드레일이 있는 AWS 리전에만 해당되며, 안전 제어를 적용하려는 각 AWS 리전마다 가드레일이 달라야 합니다. 그런 다음이 정책을 조직의 모든 노드에 연결할 수 있으며, 해당 노드 아래의 계정은 이러한 보호 조치를 자동으로 상속하고 Amazon Bedrock에 대한 모든 모델 호출에 적용합니다.

Amazon Bedrock 정책은 조직 전체에서 일관된 안전 제어를 보장하고 생성형 AI 애플리케이션을 대규모로 안전하게 구축하기 위한 중앙 집중식 접근 방식을 제공하는 데 도움이 됩니다.

Amazon Bedrock 정책 시작하기

Amazon Bedrock 정책을 구성하기 전에 사전 조건 및 구현 요구 사항을 이해해야 합니다. 이 주제에서는 조직에서 이러한 정책을 설정하고 관리하는 프로세스를 안내합니다.

시작하기 전 준비 사항

Amazon Bedrock 정책을 구현하기 전에 다음 요구 사항을 검토합니다.

- 계정은 AWS 조직의 일부여야 합니다.
- 다음 중 하나로 로그인해야 합니다.
 - 조직의 관리 계정
 - Amazon Bedrock 정책을 관리할 권한이 있는 위임된 관리자 계정
- 조직의 루트에서 Amazon Bedrock 정책 유형을 활성화해야 합니다.

구현 단계

Amazon Bedrock 정책을 효과적으로 구현하려면 다음 단계를 순서대로 따르세요. 각 단계는 적절한 구성을 보장하고 설정 중에 발생하는 일반적인 문제를 방지하는 데 도움이 됩니다. 관리 계정 또는 위임된 관리자는 AWS Organizations 콘솔, AWS 명령줄 인터페이스(AWS CLI) 또는 AWS SDKs.

1. [조직에 대해 Amazon Bedrock 정책을 활성화합니다.](#)
2. [Amazon Bedrock 정책을 생성합니다.](#)
3. [Amazon Bedrock 정책을 조직의 루트, OU 또는 계정에 연결합니다.](#)
4. [계정에 적용되는 결합된 유효 Amazon Bedrock 정책을 봅니다.](#)

Amazon Bedrock 정책 사용 모범 사례

유효한 가드레일 식별자 사용

식별자가 잘못되었거나 잘못된 경우 대상 조직 전체의 모든 Amazon Bedrock API 호출이 실패합니다. [잘못된 유효 정책 알림이 있는지 CloudTrail을 모니터링하여 잘못된 구성을 빠르게 감지합니다.](#)

자동 추론 정책 제외

자동 추론 정책이 포함된 가드레일은 조직 수준 적용에 지원되지 않습니다. 선택한 Amazon Bedrock Guardrail에이 포함되어 있지 않은지 확인합니다.

필요한 IAM 권한 부여

[Amazon Bedrock Guardrails 리소스 기반 정책](#)을 사용하여 조직과 멤버 계정에 런타임 시 적용 가드레일을 평가할 수 있는 권한을 부여합니다.

가드레일에 대한 Amazon Bedrock 서비스 제한 검토

Amazon Bedrock 정책을 사용한 멤버 계정 호출은 멤버의 Service Quotas에 포함됩니다. Service Quotas 콘솔을 검토하고 Guardrails 런타임 제한이 통화 볼륨에 충분한지 확인합니다.

작게 시작한 다음 확장

정책을 몇 개의 계정에 연결하여 정책을 예상대로 적용하고 있는지 확인합니다. 교차 계정 액세스를 허용하도록 Guardrail 권한이 구성되어 있는지 테스트해야 합니다.

DescribeEffectivePolicy를 사용하여 Amazon Bedrock 정책에 대한 변경 사항 검증

Amazon Bedrock 정책을 변경한 후 변경한 수준 미만의 대표 계정에 대한 유효 정책을 확인합니다. AWS 관리 콘솔을 사용하거나 DescribeEffectivePolicy API 작업 또는 AWS CLI 또는 AWS SDK 변형 중 하나를 사용하여 유효 정책을 볼 수 있습니다. 변경한 내용이 유효 정책에 의도한 영향을 미쳤는지 확인합니다.

커뮤니케이션 및 훈련

조직이 Amazon Bedrock 정책의 목적과 영향을 이해하고 있는지 확인합니다. Amazon Bedrock Guardrails 동작과 예상되는 사항에 대한 명확한 지침을 제공합니다.

Amazon Bedrock 정책 구문 및 예제

Amazon Bedrock 정책은 JSON 규칙에 따라 구조화된 일반 텍스트 파일입니다. Amazon Bedrock 정책의 구문은 모든 관리 정책 유형에 대한 구문을 따릅니다. 자세한 내용은 [관리 정책 유형에 대한 정책 구문 및 상속](#)을 참조하세요. 이 주제에서는 Amazon Bedrock 정책 유형의 특정 요구 사항에 해당 일반 구문을 적용하는 데 중점을 둡니다.

다음 Amazon Bedrock 정책 예제는 기본 Amazon Bedrock 정책 구문을 보여줍니다.

```
{
  "bedrock": {
    "guardrail_inference": {
      "us-east-1": {
        "config_1": {
          "identifier": {
            "@@assign": "arn:aws:bedrock:us-east-1:123456789012:guardrail/hu1d1sv9wy1d:1"
          },
          "selective_content_guarding": {
            "system": {
              "@@assign": "selective"
            },
            "messages": {
              "@@assign": "comprehensive"
            }
          }
        }
      }
    }
  }
}
```

```
    },  
    "model_enforcement": {  
      "included_models": {  
        "@@assign": ["ALL"]  
      },  
      "excluded_models": {  
        "@@assign": ["amazon.titan-embed-text-v2:0", "cohere.embed-english-v3"]  
      }  
    }  
  }  
}  
  
}
```

Amazon Bedrock 정책 구문에는 다음 요소가 포함됩니다.

"bedrock"

Amazon Bedrock 정책 문서의 최상위 키입니다.

```
"guardrail_inference"
```

가드레일 적용 구성을 정의합니다.

<region>

정책을 적용할 리전입니다. 예를 들어 "us-east-1"입니다.

```
"config_1"
```

가드레일 설정의 구성 식별자입니다.

"identifier"(필수)

가드레일 ARN 뒤에 Guardrail 버전이 :version입니다.

- 가드레일은 관리 계정이 소유해야 합니다. 다른 계정의 가드레일을 사용하여 정책을 생성할 수 없습니다.
- 가드레일에는 버전이 있어야 하며 해당 버전은 초안일 수 없습니다. 가드레일 버전을 생성하려면 Amazon Bedrock 사용 설명서 [의 가드레일 버전 생성](#)을 참조하세요.
- 가드레일에는 조직 구성원이를 호출할 수 있도록 허용하는 리소스 기반 정책이 있어야 합니다ApplyGuardrail.
- 지정된 리전에서 가드레일을 생성하고 사용해야 합니다.

"selective_content_guarding" (선택 사항)

Amazon Bedrock APIs 사용하면 호출자가 가드레일을 처리하려는 입력 내에 특정 콘텐츠를 표시할 수 있습니다. 이러한 설정을 통해 시행자는 호출자가 내린 콘텐츠 태그 지정 결정을 준수할지 여부를 제어할 수 있습니다. 지정된 경우 "system" 또는 중 하나가 "messages" 필요합니다.

"system" (선택 사항)

가드레일에서 시스템 프롬프트를 처리하는 방법을 선택합니다. 지정comprehensive하지 않으면 기본값은 입니다.

- "comprehensive": 가드 콘텐츠 태그에 관계없이 모든 콘텐츠를 평가합니다.
- "selective": 가드 콘텐츠 태그 내의 콘텐츠만 평가합니다. 태그가 지정되지 않은 경우 콘텐츠를 평가하지 않습니다.

"messages" (선택 사항)

가드레일에서 사용자 및 어시스턴트 대화가 포함된 메시지 콘텐츠를 처리하는 방법을 선택합니다. 지정comprehensive하지 않으면 기본값은 입니다.

- "comprehensive": 가드 콘텐츠 태그에 관계없이 모든 콘텐츠를 평가합니다.
- "selective": 가드 콘텐츠 태그 내의 콘텐츠만 평가합니다. 태그가 지정되지 않은 경우 메시지 내의 모든 콘텐츠를 평가합니다.

"model_enforcement" (선택 사항)

적용 가드레일 구성에 대한 모델별 정보입니다. 없는 경우 구성은 모든 모델에 적용됩니다.

"included_models"(필수)

가드레일을 적용할 모델 목록입니다. 비어 있는 경우는 모든 모델에 적용을 적용합니다. 또한 키워드 "ALL"을 수락하여 모든 모델을 명시적으로 포함합니다.

"excluded_models"(필수)

가드레일 적용에서 제외할 모델입니다. 비어 있는 경우는 적용에서 모델을 제외하지 않습니다. 포함된 모델 목록과 제외된 모델 목록에 모두 모델이 있는 경우 해당 모델은 제외됩니다.

Amazon Inspector 정책

Amazon Inspector 정책을 사용하면 AWS 조직의 여러 계정에서 Amazon Inspector를 중앙에서 활성화하고 관리할 수 있습니다. Amazon Inspector 정책을 사용하여 Amazon Inspector가 자동으로 활성화되고 Amazon Inspector 위임된 관리자 계정에 연결된 조직 엔터티(루트, OUs 또는 계정)를 지정합니다.

Amazon Inspector 정책을 사용하여 서비스 전반의 온보딩을 간소화하고 기존 계정과 새로 생성된 모든 계정에서 Amazon Inspector를 일관되게 활성화할 수 있습니다.

주요 기능 및 이점

Amazon Inspector 정책을 사용하면 조직 또는 조직의 하위 집합에 대해 활성화해야 하는 스캔 유형을 정의하여 일관된 적용 범위를 보장하고 수동 작업을 줄일 수 있습니다. 구현되면 새 계정을 자동으로 온보딩하고 조직이 확장됨에 따라 스캔 기준을 유지하는 데 도움이 됩니다.

작동 방식

Amazon Inspector 정책을 조직 엔터티에 연결하면이 정책은 해당 범위 내의 모든 멤버 계정에 대해 Amazon Inspector를 자동으로 활성화합니다. 또한 Amazon Inspector에 대한 위임된 관리자를 등록하여 Amazon Inspector 설정을 완료한 경우 해당 계정은 Amazon Inspector가 활성화된 조직의 계정에 대한 중앙 집중식 취약성 가시성을 갖게 됩니다.

Amazon Inspector 정책은 전체 조직, 특정 조직 단위(OUs) 또는 개별 계정에 적용할 수 있습니다. 조직에 가입하거나 연결된 Amazon Inspector 정책이 있는 OU로 이동하는 계정은 정책을 자동으로 상속하고 Amazon Inspector가 활성화되고 Amazon Inspector 위임된 관리자에게 연결되도록 합니다. Amazon Inspector 정책을 사용하면 Amazon EC2 스캔, Amazon ECR 스캔 또는 Lambda 표준 및 코드 스캔과 코드 보안을 활성화할 수 있습니다. 조직의 위임된 관리자 계정을 통해 특정 구성 설정 및 금지 규칙을 관리할 수 있습니다.

Amazon Inspector 정책을 조직 또는 조직 단위에 연결하면 AWS Organizations는 정책을 자동으로 평가하고 사용자가 정의한 범위에 따라 정책을 적용합니다. 이 정책 적용 프로세스는 다음과 같은 특정 충돌 해결 규칙을 따릅니다.

- 활성화 및 비활성화 목록 모두에 리전이 표시되면 비활성화 구성이 우선합니다. 예를 들어 리전이 활성화 및 비활성화 구성 모두에 나열된 경우 Amazon Inspector는 해당 리전에서 비활성화됩니다.
- 활성화를 위해 ALL_SUPPORTED를 지정하면 명시적으로 비활성화되지 않는 한 모든 현재 및 향후 리전에서 Amazon Inspector가 활성화됩니다. 이를 통해가 새 리전으로 확장됨에 따라 AWS 포괄적인 적용 범위를 유지할 수 있습니다.
- 하위 정책은 상속 연산자를 사용하여 상위 정책 설정을 수정할 수 있으므로, 조직의 다양한 수준에서 세분화된 제어가 가능합니다. 이 계층적 접근 방식을 사용하면 특정 조직 단위가 기존 제어를 유지하면서 보안 설정을 사용자 지정할 수 있습니다.

용어

이 주제에서는 Amazon Inspector 정책을 논의할 때 다음 용어를 사용합니다.

용어	정의
유효 정책	모든 상속된 정책을 결합한 후 계정에 적용되는 최종 정책입니다.
정책 상속	계정이 상위 조직 단위로부터 정책을 상속하는 프로세스입니다.
위임된 관리자	조직을 대신하여 Amazon Inspector 정책을 관리하도록 지정된 계정입니다.
서비스 연결 역할	Amazon Inspector가 다른 AWS 서비스와 상호 작용할 수 있도록 허용하는 IAM 역할입니다.

Amazon Inspector 정책의 사용 사례

여러 계정에서 대규모 워크로드를 시작하는 조직은이 정책을 사용하여 모든 계정이 올바른 스캔 유형을 즉시 활성화하고 격차를 방지할 수 있습니다. 규제 또는 규정 준수 기반 환경은 하위 정책을 사용하여 OU별로 스캔 유형을 재정의하거나 제한할 수 있습니다. 빠른 성장 환경은 새로 생성된 계정의 활성화를 자동화하여 항상 기준을 준수할 수 있습니다.

정책 상속 및 적용

정책을 상속하고 적용하는 방법을 이해하는 것은 조직 전체의 효과적인 보안 관리에 매우 중요합니다. 상속 모델은 AWS Organizations 계층 구조를 따르므로 예측 가능하고 일관된 정책 애플리케이션을 보장합니다.

- 루트 수준에서 연결된 정책은 모든 계정에 적용됩니다.
- 계정은 상위 조직 단위로부터 정책을 상속합니다.
- 단일 계정에 여러 정책을 적용할 수 있습니다.
- 보다 구체적인 정책(계층 구조상 해당 계정에 더 가까움)이 우선합니다.

정책 검증

Amazon Inspector 정책을 생성할 때 다음과 같은 검증이 수행됩니다.

- 리전 이름은 유효한 AWS 리전 식별자여야 합니다.
- 리전은 Amazon Inspector에서 지원해야 합니다.
- 정책 구조는 AWS Organizations 정책 구문 규칙을 따라야 합니다.

- `enable_in_regions` 및 `disable_in_regions` 목록이 모두 있어야 하지만 비어 있을 수 있습니다.

리전별 고려 사항 및 지원되는 리전

Amazon Inspector 정책은 Amazon Inspector 및 AWS Organizations의 신뢰할 수 있는 액세스를 사용할 수 있는 리전에만 적용됩니다. 리전별 행동을 이해하면 조직의 글로벌 사업 영역 전반에 걸쳐 효과적인 보안 제어를 구현하는 데 도움이 됩니다.

- 정책 적용은 각 리전에서 독립적으로 수행됩니다.
- 정책에 포함하거나 제외할 리전을 지정할 수 있습니다.
- `ALL_SUPPORTED` 옵션을 사용하면 새 리전이 자동으로 포함됩니다.
- 정책은 Amazon Inspector를 사용할 수 있는 리전에만 적용됩니다.

분리 동작

Amazon Inspector 정책을 분리하면 Amazon Inspector는 이전에 적용된 계정에서 활성화된 상태로 유지됩니다. 그러나 조직 구조의 향후 변경 사항(예: 새 계정 가입 또는 OU로 이전하는 기존 계정)은 더 이상 Amazon Inspector를 자동으로 활성화하지 않습니다. 추가 활성화는 수동으로 수행하거나 정책을 다시 연결하여 수행해야 합니다.

추가 세부 정보

위임된 관리자

조직의 Amazon Inspector에는 위임된 관리자 한 명만 등록할 수 있습니다. Amazon Inspector 정책을 연결하기 전에 Amazon Inspector 콘솔 또는 APIs를 통해 이를 구성해야 합니다.

사전 조건

AWS Organizations에 대해 신뢰할 수 있는 액세스를 활성화하고, Amazon Inspector에 대해 위임된 관리자가 등록되어 있으며, 모든 계정에서 서비스 연결 역할을 사용할 수 있어야 합니다.

지원되는 리전:

Amazon Inspector를 사용할 수 있는 모든 리전.

Amazon Inspector 정책 시작하기

Amazon Inspector 정책을 구성하기 전에 사전 조건 및 구현 요구 사항을 이해해야 합니다. 이 주제에서는 조직에서 이러한 정책을 설정하고 관리하는 프로세스를 안내합니다.

필요한 권한에 대해 알아보기

Amazon Inspector 정책을 활성화하거나 연결하려면 관리 계정에 다음 권한이 있어야 합니다.

- `inspector2.amazonaws.com`용 `organizations:EnableAWSServiceAccess`
- `inspector2.amazonaws.com`용 `organizations:RegisterDelegatedAdministrator`
- `organizations:AttachPolicy`, `organizations:CreatePolicy`,
`organizations:DescribeEffectivePolicy`
- `inspector2:Enable` (관리 계정 및 위임된 관리자용)

시작하기 전 준비 사항

Amazon Inspector 정책을 구현하기 전에 다음 요구 사항을 검토합니다.

- 계정은 AWS 조직의 일부여야 합니다.
- 다음 중 하나로 로그인해야 합니다.
 - 조직의 관리 계정
 - Amazon Inspector 정책을 관리할 권한이 있는 AWS Organizations 위임된 관리자
- 조직에서 Amazon Inspector에 대해 신뢰할 수 있는 액세스를 활성화해야 합니다.
- 조직의 루트에서 Amazon Inspector 정책 유형을 활성화해야 합니다.

또한 다음을 확인하세요.

- Amazon Inspector는 정책을 적용하려는 리전에서 지원됩니다.
- 관리 계정에 `AWSServiceRoleForInspectorV2` 서비스 연결 역할이 구성되어 있습니다. 이 역할이 존재하는지 확인하려면 `aws iam get-role --role-name AWSServiceRoleForInspectorV2`을(를) 실행합니다. 이 역할을 생성해야 하는 경우 관리 계정의 모든 리전에서 `aws inspector2 enable`을(를) 실행하거나 `aws iam create-service-linked-role --aws-service-name inspector2.amazonaws.com`을(를) 실행하여 직접 생성할 수 있습니다.

구현 단계

Amazon Inspector 정책을 효과적으로 구현하려면 다음 단계를 순서대로 따르세요. 각 단계는 적절한 구성을 보장하고 설정 중에 발생하는 일반적인 문제를 방지하는 데 도움이 됩니다. 관리 계정 또는 위임된 관리자는 AWS Organizations 콘솔, AWS 명령줄 인터페이스(AWS CLI) 또는 AWS SDKs.

1. [Amazon Inspector에 대해 신뢰할 수 있는 액세스를 활성화합니다.](#)
2. [조직에 대해 Amazon Inspector 정책을 활성화합니다.](#)
3. [Amazon Inspector 정책을 생성합니다.](#)
4. [Amazon Inspector 정책을 조직의 루트, OU 또는 계정에 연결합니다.](#)
5. [계정에 적용되는 결합된 유효 Amazon Inspector 정책을 봅니다.](#)

Amazon Inspector 정책 생성

최소 권한

Amazon Inspector 정책을 생성하려면 다음 권한이 필요합니다.

- `organizations:CreatePolicy`

AWS 관리 콘솔

Amazon Inspector 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. Amazon Inspector 콘솔에서 사용 중인 서비스에 대해 위임된 관리자를 설정합니다.
3. 위임된 관리자가 Amazon Inspector에 대해 설정되면 AWS 조직 콘솔을 방문하여 정책을 설정합니다. AWS 조직 콘솔에서 Amazon Inspector 정책 페이지로 이동하여 정책 생성을 선택합니다.
4. 새 Amazon Inspector 정책 생성 페이지에서 정책 이름과 선택적 정책 설명을 입력합니다.
5. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 정책에 하나 이상의 태그를 추가할 수 있습니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 내용은 [AWS Organizations 리소스 태그 지정](#) 단원을 참조하십시오.
6. JSON 코드 상자에 정책 텍스트를 입력하거나 붙여 넣습니다. Amazon Inspector 정책 구문과 시작점으로 사용할 수 있는 정책 예제에 대한 자세한 내용은 [섹션을 참조하세요](#) [Amazon Inspector 정책 구문 및 예제](#).

7. 정책 편집을 마쳤으면 페이지의 오른쪽 아래 모서리에 있는 정책 생성(Create policy)을 선택합니다.

Amazon Inspector 정책 사용 모범 사례

조직 전체에서 Amazon Inspector 정책을 구현할 때 확립된 모범 사례를 따르면 성공적인 배포 및 유지 관리를 보장하는 데 도움이 됩니다.

간단하게 시작하고 소규모로 변경

먼저 제한된 조직 단위(예: "보안 파일럿")에서 Amazon Inspector 정책을 활성화하여 모든 계정으로 롤아웃하기 전에 예상 동작을 검증합니다. 이 증분 접근 방식을 사용하면 광범위한 배포 전에 제어된 환경에서 잠재적 문제를 식별하고 해결할 수 있습니다.

검토 프로세스 수립

조직에 가입한 새 계정을 정기적으로 모니터링하고 Amazon Inspector 활성화를 자동으로 상속하는지 확인합니다. 분기별로 정책 연결 범위를 검토하여 보안 적용 범위가 조직 구조 및 보안 요구 사항에 부합하는지 확인합니다.

DescribeEffectivePolicy를 사용하여 변경 사항 검증

정책을 연결하거나 수정한 후 대표 계정에 DescribeEffectivePolicy 대해를 실행하여 Amazon Inspector 활성화가 제대로 반영되었는지 확인합니다. 이 검증 단계는 정책 변경 사항이 조직 전체에 의도한 영향을 미치는지 확인하는 데 도움이 됩니다.

커뮤니케이션 및 훈련

Amazon Inspector 위임 관리자에게 연결되면 Amazon Inspector가 자동으로 활성화되고 조사 결과가 Security Hub 또는 Amazon Inspector 대시보드에 표시될 수 있음을 계정 소유자에게 교육합니다. 명확한 커뮤니케이션은 계정 소유자가 보안 모니터링을 이해하고 결과에 적절하게 대응할 수 있도록 하는 데 도움이 됩니다.

위임된 관리자 전략 계획

보안 또는 규정 준수 계정을 Amazon Inspector의 위임된 관리자로 지정합니다. Amazon Inspector 콘솔 또는 AWS Organizations APIs를 통해 위임된 관리자를 설정합니다. 이 접근 방식을 사용하면 조직 전체에서 일관된 보안 모니터링 및 관리를 수행할 수 있습니다.

리전별 고려 사항 처리

워크로드가 실행되는 리전에서 Amazon Inspector를 활성화합니다. Amazon Inspector 적용 범위가 필요한 리전을 결정할 때는 규정 준수 요구 사항 및 운영 요구 사항을 고려하세요. 인프라 전반에서 일관된 보안 모니터링을 유지하기 위해 리전별 요구 사항을 문서화합니다.

Amazon Inspector 정책 구문 및 예제

Amazon Inspector 정책은 조직 전체에서 Amazon Inspector를 활성화하고 구성하는 방법을 정의하는 표준화된 JSON 구문을 따릅니다. Amazon Inspector 정책은 AWS Organizations 관리 정책 구문에 따라 구조화된 JSON 문서입니다. Amazon Inspector를 자동으로 활성화할 조직 엔터티를 정의합니다.

기본 정책 구조

Amazon Inspector 정책은 다음과 같은 기본 구조를 사용합니다.

```
{
  "inspector": {
    "enablement": {
      "ec2_scanning": {
        "enable_in_regions": {
          "@@assign": ["us-east-1", "us-west-2"]
        },
        "disable_in_regions": {
          "@@assign": ["eu-west-1"]
        }
      }
    }
  }
}
```

정책 구성 요소

Amazon Inspector 정책에는 다음과 같은 주요 구성 요소가 포함되어 있습니다.

inspector

모든 Amazon Inspector 정책에 필요한 Amazon Inspector 정책 문서의 최상위 키입니다.

enablement

조직 전체에서 Amazon Inspector가 활성화되는 방법을 정의하고 스캔 유형 구성을 포함합니다.

Regions (Array of Strings)

Amazon Inspector를 자동으로 활성화해야 하는 리전을 지정합니다.

Amazon Inspector 정책 예제

다음 예제에서는 일반적인 Amazon Inspector 정책 구성을 보여줍니다.

예제 1 - 조직 전체의 Amazon Inspector 활성화

다음 예시에서는 조직 루트의 모든 계정에 us-west-2 대해 us-east-1 및에서 Amazon Inspector를 활성화합니다.

inspector-policy-enable.json 파일을 생성합니다.

```
{
  "inspector": {
    "enablement": {
      "lambda_standard_scanning": {
        "enable_in_regions": {
          "@@assign": [
            "us-east-1",
            "us-west-2"
          ]
        },
      },
      "disable_in_regions": {
        "@@assign": [
          "eu-west-1"
        ]
      },
    },
    "lambda_code_scanning": {
      "enable_in_regions": {
        "@@assign": [
          "us-east-1",
          "us-west-2"
        ]
      },
      "disable_in_regions": {
        "@@assign": [
          "eu-west-1"
        ]
      },
    }
  }
}
```

```
    },
    "ec2_scanning": {
      "enable_in_regions": {
        "@@assign": [
          "us-east-1",
          "us-west-2"
        ]
      },
      "disable_in_regions": {
        "@@assign": [
          "eu-west-1"
        ]
      }
    },
    "ecr_scanning": {
      "enable_in_regions": {
        "@@assign": [
          "us-east-1",
          "us-west-2"
        ]
      },
      "disable_in_regions": {
        "@@assign": [
          "eu-west-1"
        ]
      }
    },
    "code_repository_scanning": {
      "enable_in_regions": {
        "@@assign": [
          "us-east-1",
          "us-west-2"
        ]
      },
      "disable_in_regions": {
        "@@assign": [
          "eu-west-1"
        ]
      }
    }
  }
}
```

루트에 연결되면 조직의 모든 계정이 Amazon Inspector를 자동으로 활성화하고 Amazon Inspector 위임된 관리자가 스캔 결과를 사용할 수 있습니다.

정책을 생성하고 연결합니다.

```
POLICY_ID=$(aws organizations create-policy \
  --content file://inspector-policy-enable.json \
  --name InspectorOrgPolicy \
  --type INSPECTOR_POLICY \
  --description "Inspector organization policy to enable all resources in IAD and PDX." \
  --query 'Policy.PolicySummary.Id' \
  --output text)
aws organizations attach-policy --policy-id $POLICY_ID --target-id <root-id>
```

조직에 가입하는 모든 새 계정은 자동으로 활성화를 상속합니다.

분리된 경우 기존 계정은 활성화된 상태로 유지되지만 향후 계정은 자동으로 활성화되지 않습니다.

```
aws organizations detach-policy --policy-id $POLICY_ID --target-id <root-id>
```

예제 2 - 특정 OU에 대해 Amazon Inspector 활성화

inspector-policy-eu-west-1.json 파일을 생성합니다.

```
{
  "inspector": {
    "enablement": {
      "lambda_standard_scanning": {
        "enable_in_regions": {
          "@@assign": [
            "eu-west-1"
          ]
        },
        "disable_in_regions": {
          "@@assign": [
            "eu-west-2"
          ]
        }
      },
      "lambda_code_scanning": {
        "enable_in_regions": {
          "@@assign": [
            "eu-west-1"
          ]
        }
      }
    }
  }
}
```

```

    ]
  },
  "disable_in_regions": {
    "@@assign": [
      "eu-west-2"
    ]
  }
},
"ec2_scanning": {
  "enable_in_regions": {
    "@@assign": [
      "eu-west-1"
    ]
  },
  "disable_in_regions": {
    "@@assign": [
      "eu-west-2"
    ]
  }
},
"ecr_scanning": {
  "enable_in_regions": {
    "@@assign": [
      "eu-west-1"
    ]
  },
  "disable_in_regions": {
    "@@assign": [
      "eu-west-2"
    ]
  }
},
"code_repository_scanning": {
  "enable_in_regions": {
    "@@assign": [
      "eu-west-1"
    ]
  },
  "disable_in_regions": {
    "@@assign": [
      "eu-west-2"
    ]
  }
}

```

```

    }
  }
}
}

```

의 모든 프로덕션 계정에 eu-west-1 Amazon Inspector가 활성화되고 Amazon Inspector 위임된 관리자에게 연결되도록 하려면 OU에 연결합니다.

```

aws organizations update-policy --policy-id $POLICY_ID --content file:///inspector-policy-eu-west-1.json --description "Inspector organization policy - Enable all (eu-west-1)"
aws organizations attach-policy --policy-id $POLICY_ID --target-id ou-aaaa-12345678

```

OU 외부의 계정은 영향을 받지 않습니다.

롤아웃 정책 업그레이드

AWS Organizations 업그레이드 롤아웃 정책을 사용하면 조직의 여러 AWS 리소스 및 계정에서 자동 업그레이드를 중앙에서 관리하고 시차를 지정할 수 있습니다. 이러한 정책을 사용하면 리소스가 업그레이드를 받는 순서를 정의하여 프로덕션에 도달하기 전에 덜 중요한 환경에서 변경 사항을 검증할 수 있습니다.

오늘날의 복잡한 클라우드 환경에서는 수많은 리소스와 계정에서 업그레이드를 관리하는 것이 어려울 수 있습니다. 업그레이드 롤아웃 정책은 업그레이드 구현에 대한 체계적인 접근 방식을 제공하여 문제를 해결합니다. 이러한 정책을 사용하면 업그레이드 프로세스를 조직의 변경 관리 관행에 맞게 조정하여 위험을 줄이고 운영 효율성을 개선할 수 있습니다.

업그레이드 롤아웃 정책은 계층 구조를 활용하여 전체 조직 또는 특정 조직 단위(OU)에 정책을 AWS Organizations 적용합니다. 이 통합을 통해 대규모 업그레이드를 관리할 수 있으므로 수동 조정 또는 사용자 지정 자동화 스크립트가 필요하지 않습니다.

주요 기능 및 이점

업그레이드 롤아웃 정책은 업그레이드를 관리하는 포괄적인 기능을 제공하는 동시에 여러 계정 및 환경에서 리소스를 관리하는 조직에 상당한 이점을 제공합니다. 다음 표에는 주요 기능과 관련 이점이 요약되어 있습니다.

업그레이드 롤아웃 정책의 기능 및 이점

기능	설명	주요 이점
업그레이드 주문 시스템	구성 가능한 타이밍이 있는 3계층 시스템(첫 번째, 두 번째, 마지막)	• 사전 프로덕션 환경에서 업그레이드 테스트 • 프로덕션 워크로드에 대한 위험 최소화
정책 기반 관리	를 통한 중앙 집중식 제어 AWS Organizations	• 단일 지점에서 여러 계정 관리 • 관리 오버헤드 감소
리소스 대상	태그 기반 및 OU 기반 대상 지정 옵션	• 특정 리소스 그룹을 대상으로 지정 • 대규모 정책 적용
자동 예약	기존 유지 관리 기간과 함께 작동	• 수동 조정 제거 • 일관된 업그레이드 패턴 유지
서비스 통합	AWS 서비스 업그레이드 메커니즘과 함께 작동	• Amazon EventBridge를 사용하여 이벤트 모니터링
규정 준수 제어	정책 상속 및 적용	• 조직 표준 적용 • 규정 준수 요구 사항 충족

정책 상속에 대한 자세한 내용은 섹션을 참조하세요 [관리 정책 상속에 대한 이해](#).

업그레이드 롤아웃 정책이란 무엇입니까?

업그레이드 롤아웃 정책은 AWS 리소스에 자동 업그레이드가 적용되는 방식과 시기를 결정하는 규칙 세트입니다. 이러한 정책을 사용하면 일반적으로 개발, 테스트 및 프로덕션 환경에 맞게 리소스에 대해서도 다른 업그레이드 주문을 지정할 수 있습니다. 이렇게 하면 덜 중요한 시스템에 업그레이드를 먼저 적용하여 프로덕션 워크로드에 영향을 미치기 전에 문제를 식별하고 해결할 수 있습니다.

이 정책은 첫 번째, 두 번째, 마지막의 세 가지 업그레이드 주문을 지원합니다. 이러한 주문은 업그레이드에 대한 단계적 접근 방식을 생성하며, 리소스는 처음에 "첫 번째"로 지정되어 업그레이드를 수신하고, 대기 기간 후에는 "두 번째", 마지막으로 다른 대기 기간 후에는 "마지막"으로 지정됩니다. 이 시차

를 둔 접근 방식을 사용하면 더 중요한 시스템으로 진행하기 전에 각 단계에서 업그레이드를 검증할 시간을 확보할 수 있습니다.

업그레이드 롤아웃 정책은 복잡한 다중 계정 구조 또는 엄격한 변경 관리 요구 사항이 있는 조직에 특히 유용합니다. 최신 up-to-date 시스템을 유지 관리하는 것과 중요한 서비스에 대한 업그레이드 관련 중단 위험을 최소화하는 것 사이의 균형을 제공합니다.

업그레이드 롤아웃 정책 작동 방식

업그레이드 롤아웃 정책은 기존 AWS 인프라 및 프로세스와 원활하게 통합됩니다. 업그레이드 롤아웃 정책을 생성하여 조직 단위에 연결하면 해당 OU 내의 모든 계정에 적용됩니다. 그런 다음 리소스 태그 또는 패치 주문을 사용하여 어떤 리소스를 어떤 순서로 업그레이드해야 하는지 지정할 수 있습니다.

지원되는 AWS 서비스가 업그레이드를 릴리스하면 업그레이드 롤아웃 정책을 참조하여 리소스가 업그레이드를 받아야 하는 순서를 결정합니다. 서비스는 먼저 구성된 유지 관리 기간 동안 "First"로 표시된 리소스에 업그레이드를 적용합니다. 일반적으로 약 1주일 동안 서비스별 대기 기간이 지나면 "초"로 표시된 리소스가 업그레이드 대상이 됩니다. 마지막으로 다른 대기 기간이 지나면 "Last"로 표시된 리소스가 업그레이드를 받습니다.

이 프로세스를 통해 업그레이드가 조직 전체에 제어되고 예측 가능한 방식으로 적용되도록 할 수 있습니다. 이를 통해 각 단계에서 업그레이드의 영향을 모니터링하고 변경 사항이 가장 중요한 환경에 도달하기 전에 필요한 경우 수정 조치를 취할 수 있습니다. 이 프로세스의 자동화된 특성은 업그레이드 관리의 운영 오버헤드를 줄이는 동시에 AWS 리소스의 안정성과 보안을 유지하는 데 필요한 제어 및 가시성을 제공합니다.

용어

다음은 업그레이드 롤아웃 정책을 사용할 때 이해해야 하는 주요 용어입니다.

롤아웃 정책 약관 업그레이드

용어	정의
활성 날짜	AmVU가 보류 중인 유지 관리 작업 설명 API에 표시되고 애플리케이션에 사용할 수 있게 되는 날짜입니다.
AmVU(마이너 버전 자동 업그레이드)	마이너 버전의 데이터베이스 엔진에 대한 자동 업그레이드 프로세스입니다.
유효 정책	상속되고 직접 연결된 모든 정책을 고려한 후 계정 또는 리소스에 적용되는 최종 규칙 세트입니다.

용어	정의
유지 관리 윈도우	리소스에 자동 업그레이드를 적용할 수 있는 반복 기간입니다. 업그레이드 롤아웃 정책은 이러한 구성된 유지 관리 기간 내에서 작동합니다.
조직 단위(OU)	조직의 AWS 계정에 대한 컨테이너입니다. 업그레이드 롤아웃 정책은 OU 수준에서 연결하여 OU 내의 모든 계정에 영향을 미칠 수 있습니다.
패치 순서	리소스가 업그레이드를 받는 순서(첫 번째, 두 번째, 마지막).
정책 대상	업그레이드 롤아웃 정책이 적용되는 범위로, 전체 조직, 특정 OUs 또는 개별 계정이 될 수 있습니다.
리소스 태그	정책 내에서 특정 업그레이드 순서를 따라야 하는 리소스를 식별하는 데 사용할 수 있는 키-값 페어입니다.
예약 기간	특정 패치 주문의 리소스가 업그레이드를 받는 기간입니다.
서비스별 대기 기간	서로 다른 업그레이드 주문의 리소스 업그레이드 간의 지정된 시간 간격입니다. 이 기간은 AWS 서비스 및 업그레이드 유형에 따라 다릅니다.
업그레이드 순서	리소스가 다른 리소스와 관련된 업그레이드를 수신하는 시기를 결정하는 지정입니다. 첫 번째, 두 번째 또는 마지막으로 설정할 수 있습니다.
롤아웃 정책 업그레이드	리소스 간 업그레이드 일정을 관리하는 데 사용되는 AWS Organizations 정책 유형입니다.

업그레이드 롤아웃 정책의 사용 사례

다양한 규모와 산업을 가진 조직은 업그레이드 롤아웃 정책의 이점을 누릴 수 있습니다. 다음 가상 시나리오는 일반적인 업그레이드 관리 과제와 업그레이드 롤아웃 정책이 효율적인 솔루션을 제공하는 방법을 보여줍니다. 이 예제는 일반적인 고객 경험을 기반으로 하지만 주요 이점과 구현 패턴을 강조하기 위해 간소화되었습니다.

많은 조직이 비슷한 문제에 직면합니다. 프로덕션 환경에 대한 위험을 최소화하면서 최신 버전으로 리소스를 up-to-date 유지해야 합니다. 중앙 집중식 정책 기반 접근 방식이 없으면 팀은 수동 프로세스 또는 복잡한 자동화 스크립트에 의존하는 경우가 많습니다. 다음 예제에서는 서로 다른 두 조직이 업그레이드 롤아웃 정책을 사용하여 유사한 문제를 해결하는 방법을 보여줍니다.

사용 사례 예: Global Financial Services Company

금융 서비스 회사는 여러 AWS 계정에서 수백 개의 Aurora PostgreSQL 데이터베이스를 운영합니다. 업그레이드 롤아웃 정책 전에 DevOps 팀은 매월 며칠 동안 데이터베이스 업그레이드를 수동으로 조정하여 프로덕션 시스템에 도달하기 전에 개발 환경에서 변경 사항을 테스트했는지 확인했습니다. 업그레이드 롤아웃 정책을 구현하면 다음을 수행할 수 있습니다.

- 업그레이드 순서가 "First"인 태그가 지정된 개발 데이터베이스
- "Second" 순서 업그레이드에 QA 데이터베이스 할당
- 업그레이드 주문 "Last"로 지정된 프로덕션 데이터베이스
- 업그레이드 조정을 며칠에서 몇 분으로 줄임
- 먼저 하위 환경에서 변경 사항을 자동으로 검증
- 변경 관리 요구 사항 준수 유지

사용 사례 예: IoT 디바이스 플랫폼 공급자

한 IoT 회사가 여러 Amazon RDS 데이터베이스를 사용하여 매일 수백만 개의 디바이스 이벤트를 처리합니다. 마이너 버전 자동 업그레이드로 인해 프로덕션 서비스가 중단되지 않도록 해야 했습니다. 업그레이드 롤아웃 정책을 사용하면 다음을 수행할 수 있습니다.

- 조직 구조에 적용되는 정책을 생성했습니다.
- 먼저 업그레이드를 받도록 구성된 카나리아 환경
- 조기 업그레이드 환경에서 모니터링 설정
- 프로덕션 업그레이드 전에 문제를 감지하고 대응할 시간을 확보했습니다.
- 복잡한 사용자 지정 업그레이드 자동화를 간단한 정책으로 대체
- 데이터베이스 버전을 최신 상태로 유지하면서 프로덕션 워크로드의고가용성 유지

지원되는 AWS 서비스

업그레이드 롤아웃 정책은 자동 마이너 버전 업그레이드를 지원하면서 다음 AWS 서비스와 통합됩니다.

업그레이드 롤아웃 정책에 지원되는 서비스

서비스 이름	용도
Amazon Aurora PostgreSQL 호환 에디션	자동 마이너 버전 업그레이드

서비스 이름	용도
Amazon Aurora MySQL 호환 버전	자동 마이너 버전 업그레이드
Amazon Relational Database Service for PostgreSQL	자동 마이너 버전 업그레이드
SQL Server용 Amazon 관계형 데이터베이스 서비스	자동 마이너 버전 업그레이드
Amazon Relational Database Service for Oracle	마이너 버전 자동 업그레이드
MariaDB용 Amazon Relational Database Service	자동 마이너 버전 업그레이드
Amazon Relational Database Service for MySQL	마이너 버전 자동 업그레이드
Amazon Relational Database Service for Db2	마이너 버전 자동 업그레이드

사전 조건

다음은에서 업그레이드 롤아웃 정책을 관리하는 데 필요한 사전 조건 및 필수 권한입니다 AWS Organizations.

- AWS Organizations 관리 계정 또는 위임된 관리자 액세스
- 지원되는 서비스의 리소스(현재 Amazon Aurora 및 Amazon Relational Database Service 데이터베이스 엔진)
- 업그레이드 롤아웃 정책을 관리하기 위한 적절한 IAM 권한

다음 단계

업그레이드 롤아웃 정책 사용을 시작하려면:

1. [업그레이드 롤아웃 정책 시작하기](#)를 검토하여 정책을 생성하고 관리하는 방법을 알아봅니다.
2. 업그레이드 롤아웃 정책 구현 [업그레이드 롤아웃 정책 사용 모범 사례](#) 탐색

3. 이해 [롤아웃 정책 구문 및 예제 업그레이드](#)

업그레이드 롤아웃 정책 시작하기

다음 단계에 따라 조직에서 업그레이드 롤아웃 정책을 구현합니다. 각 단계는 구현을 성공적으로 완료하는 데 도움이 되는 세부 정보로 연결됩니다.

시작하기 전 준비 사항

다음에 있는지 확인합니다.

- 예 대한 관리 액세스 AWS Organizations
- 지원되는 AWS 서비스의 리소스(예: Aurora 또는 Amazon Relational Database Service)
- 구성된 필수 IAM 권한

구현 단계

1. [조직에 대한 업그레이드 롤아웃 정책을 활성화합니다.](#)
2. [업그레이드 롤아웃 정책의 작동 방식을 이해합니다.](#)
 - 개발, 테스트 및 프로덕션 환경 식별
 - 어떤 리소스를 먼저, 두 번째, 마지막으로 업그레이드해야 하는지 결정합니다.
 - 리소스 식별을 위한 태그 지정 전략 문서화
3. [업그레이드 롤아웃 정책 생성:](#)
 - 기본 롤아웃 순서 정의(조직 단위 또는 계정 수준)
 - 태그를 사용하여 리소스 대상 지정
 - 정책 제외 구성
4. [테스트에 사용할 수 있는 단일 멤버 계정에 업그레이드 롤아웃 정책을 연결합니다.](#)
 - 테스트 조직 단위로 시작
 - 정책 상속 확인
 - 정책 연결 상태 확인
5. 업그레이드 주문 전략에 따라 리소스에 태그를 지정합니다.
 - 첫 번째 업그레이드를 위해 개발 리소스에 태그 적용
 - 2차 업그레이드를 위한 테스트 리소스에 태그 지정
 - 마지막 주문 업그레이드를 위한 프로덕션 리소스 지정

6. 정책을 모니터링하고 검증합니다.

- 업그레이드 주문 할당 검토
- 테스트 리소스에 대한 정책 영향 확인

7. 업그레이드 프로세스를 테스트합니다.

- 서비스 업그레이드를 사용할 수 있을 때까지 기다립니다.
- 환경을 통한 업그레이드 진행 상황 모니터링
- 업그레이드가 지정된 순서를 따르는지 확인

8. 필요에 따라 추가 조직 단위에 대한 업그레이드 롤아웃 정책 활성화

기타 정보

- [업그레이드 롤아웃 정책 구문 알아보기 및 정책 예제 참조](#)

업그레이드 롤아웃 정책 사용 모범 사례

AWS에서는 업그레이드 롤아웃 정책 사용에 대한 다음 모범 사례를 권장합니다.

주제

- [소규모로 시작하여 점진적으로 확장](#)
- [검토 프로세스 수립](#)
- [정책 변경 사항을 효과적으로 검증](#)
- [변경 사항 모니터링 및 전달](#)
- [규정 준수 및 보안 유지](#)
- [운영 효율성 최적화](#)

소규모로 시작하여 점진적으로 확장

중요하지 않은 환경의 단일 계정에 연결된 테스트 정책을 사용하여 구현을 시작합니다. 이 접근 방식을 사용하면 중요한 워크로드가 중단될 위험 없이 업그레이드 롤아웃 정책의 동작과 영향을 검증할 수 있습니다. 정책이 예상대로 작동하는지 확인한 후에는 더 많은 계정과 조직 단위를 포함하도록 조직 구조 위로 점진적으로 이동합니다.

이 점진적 조정은 구현 프로세스 초기에 문제를 식별하고 해결하는 데 도움이 됩니다. 환경의 다양성을 나타내지만 운영 위험은 최소화하는 리소스의 파일럿 그룹을 만드는 것이 좋습니다. 향후 정책 롤아웃 및 조정을 알리기 위해 각 확장 단계의 결과를 문서화합니다.

검토 프로세스 수립

정기 검토 프로세스를 구현하여 새 업그레이드 롤아웃 정책 속성을 모니터링하고 정책 예외를 평가합니다. 이러한 검토는 조직의 보안 및 운영 요구 사항에 부합해야 합니다. 정책 효과를 검토하기 위한 일정을 생성하고 조정 사항에 대한 문서를 유지 관리합니다.

검토 프로세스에는 정책이 적용되는 리소스에 대한 정기적인 평가, 업그레이드 주문이 의도한 전략과 일치하는지 확인, 정책 예외에 대한 평가가 포함되어야 합니다. 정책이 시간 경과에 따른 정책 변화를 추적하기 위해 변경 로그를 업데이트하고 유지 관리해야 하는 경우에 대한 기준을 설정하는 것이 좋습니다.

정책 변경 사항을 효과적으로 검증

업그레이드 롤아웃 정책을 변경한 후 조직의 각 수준에서 대표 계정에 대한 유효 정책을 확인합니다. AWS 관리 콘솔 또는 DescribeEffectivePolicy API 작업을 사용하여 변경 사항이 의도한 영향을 미치는지 확인합니다. 이 검증에는 여러 조직 단위의 리소스를 확인하고 상속이 예상대로 작동하는지 확인하는 작업이 포함되어야 합니다.

명시적 업그레이드 주문이 할당된 리소스와 기본값을 사용하는 리소스에 특히 주의하십시오. 태그 기반 대상 지정 확인, 유지 관리 기간 정렬 확인, 정책 상속 테스트가 포함된 검증 체크리스트를 설정합니다.

변경 사항 모니터링 및 전달

업그레이드 롤아웃 정책에 대한 포괄적인 모니터링을 설정하고 업그레이드 관련 정보를 공유하기 위한 명확한 통신 채널을 생성합니다. 업그레이드 실패를 처리하기 위한 명확한 절차를 문서화하고 다양한 시나리오에 대한 대응 계획을 수립합니다.

업그레이드 정책의 영향을 받는 리소스를 관리하는 팀과 정기적으로 소통합니다. 향후 업그레이드와 환경 전반의 예상 진행 상황을 파악할 수 있는 대시보드를 만드는 것이 좋습니다.

규정 준수 및 보안 유지

업그레이드 롤아웃 정책을 정기적으로 감사하여 규정 준수 요구 사항에 부합하는지 확인합니다. 모든 정책 결정을 문서화하고 업그레이드 패턴 및 예외에 대한 명확한 기록을 유지합니다. 정책 수정에 대한 보안 제어를 구현하고 이를 사용하여 정책 변경에 대한 감사 추적을 유지 관리합니다 AWS CloudTrail.

정책 관리 함수에 대한 액세스 권한을 정기적으로 검토하고 정책 관리를 위한 최소 권한 액세스를 구현합니다. 긴급 정책 수정을 위한 절차를 생성하고 보안 관련 업그레이드 요구 사항에 대한 문서를 유지 관리합니다.

운영 효율성 최적화

필요한 제어를 유지하면서 운영 오버헤드를 최소화하도록 정책을 설계합니다. 의도하지 않은 동작을 방지하려면 여러 사용 사례에서 태그를 재사용하지 마십시오. 가능한 경우 정책 규정 준수 검사를 자동화하고 일반적인 정책 관리 작업을 위한 표준 운영 절차를 생성합니다.

다양한 유형의 업그레이드 시나리오에 대한 템플릿을 생성하고 성공적인 정책 패턴에 대한 문서를 유지 관리하는 것이 좋습니다. 운영 지표를 정기적으로 검토하면 정책 최적화 및 프로세스 개선 기회를 식별하는 데 도움이 될 수 있습니다.

롤아웃 정책 구문 및 예제 업그레이드

업그레이드 롤아웃 정책은 AWS 서비스가 리소스 전체에 자동 업그레이드를 적용하는 방법을 정의합니다. 정책 구문을 이해하면 조직의 업그레이드 요구 사항에 맞는 효과적인 정책을 생성할 수 있습니다.

주제

- [고려 사항](#)
- [기본 정책 구조](#)
- [정책 구성 요소](#)
- [업그레이드 롤아웃 정책 예제](#)

고려 사항

업그레이드 롤아웃 정책을 구현할 때는 다음과 같은 중요한 요소를 고려하세요.

- 정책 이름은 조직 내에서 고유해야 하며 명확하고 설명적이어야 합니다. 정책의 목적과 범위를 반영하는 이름을 선택합니다. 자세한 내용은 [운영 효율성 최적화](#) 단원을 참조하십시오.
- 광범위한 배포 전에 테스트가 중요합니다. 먼저 비프로덕션 환경에서 새 정책을 검증하고 점진적으로 확장하여 원하는 동작을 보장합니다. 자세한 내용은 [소규모로 시작하여 점진적으로 확장](#) 단원을 참조하십시오.
- 정책 변경이 조직 전체에 전파되는 데 몇 시간이 걸릴 수 있습니다. 그에 따라 구현을 계획하고 적절한 모니터링이 이루어지도록 합니다. 자세한 내용은 [변경 사항 모니터링 및 전달](#) 단원을 참조하십시오.
- JSON 형식은 유효해야 하며 최대 정책 크기인 5,120바이트 이내로 유지되어야 합니다. 요구 사항을 충족하는 동시에 정책 구조를 최대한 단순하게 유지하세요.

- 정기적인 정책 검토는 효과를 유지하는 데 도움이 됩니다. 정책에 대한 정기 평가를 예약하여 조직의 요구 사항을 계속 충족하는지 확인합니다. 자세한 내용은 [검토 프로세스 수립](#) 단원을 참조하십시오.
- 할당된 업그레이드 순서가 없는 리소스의 기본값은 "초" 순서입니다. 기본값에 의존하지 않고 중요한 리소스에 대한 업그레이드 주문을 명시적으로 설정하는 것이 좋습니다. 자세한 내용은 [정책 변경 사항을 효과적으로 검증](#) 단원을 참조하십시오.
- 수동 업그레이드는 정책 정의 업그레이드 주문보다 우선합니다. 변경 관리 프로세스가 자동 및 수동 업그레이드 시나리오를 모두 고려하는지 확인합니다. 자세한 내용은 [검토 프로세스 수립](#) 단원을 참조하십시오.

Note

관리 계정에서 태그 기반 업그레이드 롤아웃 정책을 구현할 때 관리 계정은 멤버 계정의 리소스 수준 태그를 직접 보거나 액세스할 수 없습니다. 멤버 계정이 일관된 리소스 태그를 적용하는 프로세스를 설정한 다음 이러한 태그를 참조하는 조직 수준 정책을 생성하는 것이 좋습니다. 이렇게 하면 리소스 수준 태그 지정과 조직 정책 적용 간의 적절한 조정이 보장됩니다. 또한 [-태그 정책](#)을 사용하여 조직 전체에서 리소스에 태그를 지정할 때 일관된 태그를 유지할 수 있습니다.

기본 정책 구조

업그레이드 롤아웃 정책은 다음 주요 요소를 포함하는 JSON 구조를 사용합니다.

- 정책 메타데이터(예: 버전 정보)
- 리소스 대상 지정 규칙
- 업그레이드 주문 사양
- 선택적 예외 메시지
- 서비스별 속성

다음 예제에서는 기본 업그레이드 롤아웃 정책 구조를 보여줍니다.

```
{
  "upgrade_rollout":{
    "default":{
      "patch_order":{
        "@@assign":"last"
      }
    }
  }
}
```

```

    }
  },
  "tags":{
    "devtag":{
      "tag_values":{
        "tag1":{
          "patch_order":{
            "@@assign":"first"
          }
        },
        "tag2":{
          "patch_order":{
            "@@assign":"second"
          }
        },
        "tag3":{
          "patch_order":{
            "@@assign":"last"
          }
        }
      }
    }
  }
}

```

정책 구성 요소

업그레이드 롤아웃 정책은 리소스에 업그레이드가 적용되는 방식을 제어하기 위해 함께 작동하는 두 가지 주요 구성 요소로 구성됩니다. 이러한 구성 요소에는 기본 동작과 태그 기반 재정의의 모두에 대한 구성 옵션이 포함됩니다. 이러한 구성 요소가 상호 작용하는 방식을 이해하면 조직의 요구 사항에 맞는 효과적인 정책을 만드는 데 도움이 됩니다.

기본 패치 순서 설정

리소스별 재정의의를 지정하지 않고 업그레이드 롤아웃 정책을 생성하면 모든 리소스가 기본 업그레이드 순서로 기본 설정됩니다. 정책의 “기본값” 필드를 사용하여이 기본값을 설정할 수 있습니다. 태그를 통한 명시적 업그레이드 순서 할당이 없는 리소스는이 기본 순서를 따릅니다.

Note

현재 콘솔 환경을 사용하려면 기본 순서를 지정해야 합니다.

다음 예제에서는 태그로 재정의되지 않는 한 기본적으로 모든 리소스가 업그레이드를 받도록 설정하는 방법을 보여줍니다. 이 접근 방식은 업그레이드 주기 후반부에 대부분의 리소스가 업데이트되도록 하려는 경우에 유용합니다.

```
"upgrade_rollout": {
  "default": {
    "patch_order": "last"
  }
}
```

태그를 통한 리소스 수준 재정의

태그를 사용하여 특정 리소스의 기본 업그레이드 순서를 재정의할 수 있습니다. 이를 통해 업그레이드를 받는 리소스의 순서를 세부적으로 제어할 수 있습니다. 예를 들어 환경 유형, 개발 단계 또는 워크로드 중요도에 따라 다른 업그레이드 주문을 할당할 수 있습니다.

다음 예제에서는 먼저 업그레이드를 수신하도록 개발 리소스를 구성하고 마지막으로 수신하도록 프로덕션 리소스를 구성하는 방법을 보여줍니다. 이 구성을 사용하면 개발 환경이 프로덕션에 도달하기 전에 업그레이드를 검증할 수 있습니다.

```
"upgrade_rollout": {
  "tags": {
    "environment": {
      "tag_values": {
        "development": {
          "patch_order": "first"
        },
        "production": {
          "patch_order": "last"
        }
      }
    }
  }
}
```

업그레이드 롤아웃 정책 예제

일반적인 업그레이드 롤아웃 정책 시나리오는 다음과 같습니다.

예제 1: 개발 환경 먼저

이 예제에서는 먼저 업그레이드를 받도록 개발 환경에서 리소스를 구성하는 방법을 보여줍니다. "개발" 환경 태그로 리소스를 대상으로 지정하면 개발 환경이 새 업그레이드를 가장 먼저 수신하고 검증할 수 있습니다. 이 패턴은 업그레이드가 더 중요한 환경에 도달하기 전에 잠재적 문제를 식별하는 데 도움이 됩니다.

```
{
  "tags": {
    "environment": {
      "tag_values": {
        "development": {
          "upgrade_order": "first"
        }
      }
    }
  }
}
```

예제 2: 프로덕션 환경 마지막

이 예제에서는 프로덕션 환경이 마지막으로 업그레이드를 받도록 하는 방법을 보여줍니다. 프로덕션 태그가 지정된 리소스를 마지막 업그레이드 주문으로 명시적으로 설정하면 프로덕션 환경에서 안정성을 유지하면서 사전 프로덕션 환경에서 적절한 테스트를 수행할 수 있습니다. 이 접근 방식은 엄격한 변경 관리 요구 사항이 있는 조직에 특히 유용합니다.

```
{
  "tags": {
    "environment": {
      "tag_values": {
        "production": {
          "upgrade_order": "last"
        }
      }
    }
  }
}
```

예제 3: 태그를 사용한 여러 업그레이드 주문

다음 예제에서는 값이 다른 단일 태그 키를 사용하여 세 가지 업그레이드 주문을 모두 지정하는 방법을 보여줍니다. 이 접근 방식은 단일 태그 지정 체계를 통해 업그레이드 주문을 관리하려는 경우에 유용합니다.

```
{
  "upgrade_rollout":{
    "default":{
      "patch_order":{
        "@@assign":"last"
      }
    },
    "tags":{
      "devtag":{
        "tag_values":{
          "tag1":{
            "patch_order":{
              "@@assign":"first"
            }
          },
          "tag2":{
            "patch_order":{
              "@@assign":"second"
            }
          },
          "tag3":{
            "patch_order":{
              "@@assign":"last"
            }
          }
        }
      }
    }
  }
}
```

Amazon S3 정책

Amazon S3 정책을 사용하면 조직의 계정 전체에서 Amazon S3 리소스에 대한 구성을 대규모로 중앙에서 관리할 수 있습니다. Amazon S3 정책은 현재 퍼블릭 액세스를 차단하기 위한 설정을 지원합니다.

Amazon S3 정책을 사용하여 네 가지 퍼블릭 액세스 차단 설정을 모두 활성화 또는 비활성화할지 여부를 지정할 수 있으며, 해당 사양은 선택한 계정 내의 모든 Amazon S3 리소스에 적용됩니다. Amazon S3 정책에서 퍼블릭 액세스 차단 설정을 사용하여 조직 전체에 일관된 보안 태세를 적용하고 개별 계정 구성 관리의 운영 오버헤드를 제거할 수 있습니다.

작동 방식

Amazon S3 정책을 조직 엔터티에 연결하면 해당 범위의 계정 내 모든 Amazon S3 리소스에 적용되는 설정이 정의됩니다. 이러한 구성은 계정 수준 설정을 재정의하므로 Amazon S3 설정을 중앙에서 관리할 수 있습니다.

Amazon S3 정책은 전체 조직, 조직 단위(OU) 또는 개별 계정에 적용할 수 있습니다. 조직에 가입하는 계정은 조직 계층 구조의 위치에 따라 Amazon S3 정책을 자동으로 상속합니다.

분리 동작: Amazon S3 정책이 분리되면 계정이 자동으로 이전 계정 수준 구성으로 돌아갑니다. Amazon S3는 원래 계정 수준 설정을 보존하여 원활한 복원을 지원합니다.

주요 기능

- 통합 제어: 네 가지 퍼블릭 액세스 차단 설정(BlockPublicAcls, BlockPublicPolicy, IgnorePublicAcls, RestrictPublicBuckets)이 모두 단일 구성으로 함께 제어됩니다.
- 자동 상속: 새 계정은 조직 배치에 따라 정책을 자동으로 상속합니다.
- 보호 재정의: 조직 정책이 활성화 상태일 때 계정 수준 수정 방지
- 원활한 복원: 정책이 분리되면 원래 계정 설정이 보존되고 복원됩니다.

사전 조건

Amazon S3 정책을 사용하기 전에 다음을 충족해야 합니다.

- 모든 기능 모드의 AWS 조직
- AWS Organizations 정책을 관리할 수 있는 권한(organizations:CreatePolicy, organizations:AttachPolicy 등)
- 조직에 대해 활성화된 Amazon S3 정책 유형

Amazon S3 정책 사용 모범 사례

조직 전체에 Amazon S3 정책을 구현할 때 확립된 모범 사례를 따르면 성공적인 배포 및 유지 관리를 보장하는 데 도움이 됩니다.

간단하게 시작하고 소규모로 변경

디버깅을 단순화하려면 간단한 정책으로 시작하여 한 번에 한 항목씩 변경합니다. 다음 변경을 수행하기 전에 각 변경의 동작 및 영향을 검증합니다. 이러한 접근 방식은 오류 또는 예기치 않은 결과가 발생할 때 고려해야 할 변수를 줄입니다.

검토 프로세스 수립

새 정책 속성을 모니터링하고, 정책 예외를 평가하고, 조직 보안 및 운영 요구 사항에 맞게 조정하는 프로세스를 구현합니다.

DescribeEffectivePolicy를 사용하여 Amazon S3 정책에 대한 변경 사항 검증

Amazon S3 정책을 변경한 후 변경한 수준 미만의 대표 계정에 대한 유효 정책을 확인합니다. AWS 관리 콘솔을 사용하거나 DescribeEffectivePolicy API 작업 또는 AWS CLI 또는 AWS SDK 변형 중 하나를 사용하여 유효 정책을 볼 수 있습니다. 변경한 내용이 유효 정책에 의도한 영향을 미쳤는지 확인합니다.

커뮤니케이션 및 훈련

조직이 정책의 목적과 영향을 이해하고 있는지 확인합니다. 예상되는 동작과 정책 적용으로 인한 실패를 처리하는 방법에 대한 명확한 지침을 제공합니다.

합법적인 퍼블릭 액세스 요구 사항 계획

조직 수준 정책을 구현하기 전에 합법적인 비즈니스 목적(예: 정적 웹 사이트 호스팅)을 위해 퍼블릭 Amazon S3 버킷이 필요한 계정을 식별합니다. OU 수준 또는 계정 수준 정책 연결을 사용하여 이러한 계정을 제외하거나 퍼블릭 버킷 요구 사항을 전용 계정으로 통합하는 것이 좋습니다.

정책 적용 모니터링

AWS CloudTrail을 사용하여 정책 연결 및 적용 작업을 모니터링합니다. EventBridge 규칙을 설정하여 정책 위반 또는 변경에 대한 응답을 자동화합니다.

Amazon S3 정책 구문 및 예제

Amazon S3 정책은 [JSON](#) 규칙에 따라 구조화된 일반 텍스트 파일입니다. Amazon S3 정책의 구문은 모든 관리 정책 유형에 대한 구문을 따릅니다. 자세한 내용은 [관리 정책 상속에 대한 이해](#) 단원을 참조하십시오. 이 주제에서는 Amazon S3 정책의 특정 요구 사항과 해당 정책이 관리하는 데 도움이 되는 퍼블릭 액세스 차단 설정에 해당 일반 구문을 적용하는 데 중점을 둡니다.

다음 Amazon S3 정책 예제에서는 기본 정책 구문을 보여줍니다.


```
{
  "s3_attributes": {
    "public_access_block_configuration": {
      "@@assign": "all"
    }
  }
}
```

Amazon S3 정책 구문에는 다음 요소가 포함됩니다.

s3_attributes

Amazon S3 정책 구성을 위한 최상위 키입니다.

public_access_block_configuration

조직의 퍼블릭 액세스 차단 동작을 정의합니다.

@@assign

다음 두 값 중 하나를 수락하는 할당 연산자입니다.

- "all" - 조직 수준에서 네 가지 Amazon S3 퍼블릭 액세스 차단 설정을 모두 활성화합니다.
- "none" - 조직 수준 제어를 비활성화하여 개별 계정이 자체 퍼블릭 액세스 차단 설정을 관리할 수 있도록 허용합니다.

Amazon S3 퍼블릭 액세스 차단에는 퍼블릭 액세스를 제어하는 네 가지 설정이 있습니다.

1. BlockPublicAcls - Amazon S3는 새로 추가된 버킷 또는 객체에 적용되는 퍼블릭 액세스 권한을 차단하고 기존 버킷 및 객체에 대한 새 퍼블릭 액세스 제어 목록(ACLs) 생성을 방지합니다. 이 설정은 ACLs를 사용하여 Amazon S3 리소스에 대한 퍼블릭 액세스를 허용하는 기존 권한을 변경하지 않습니다.
2. BlockPublicPolicy - Amazon S3는 버킷 및 객체에 대한 퍼블릭 액세스 권한을 부여하는 새 버킷 및 액세스 포인트 정책을 차단합니다. 이 설정은 Amazon S3 리소스에 대한 퍼블릭 액세스를 허용하는 기존 정책을 변경하지 않습니다.
3. IgnorePublicAcls - Amazon S3는 버킷 및 객체에 대한 퍼블릭 액세스 권한을 부여하는 모든 ACLs를 무시합니다.
4. RestrictPublicBuckets - Amazon S3는 버킷 및 객체에 대한 퍼블릭 액세스 권한을 부여하는 정책을 사용하여 버킷 또는 액세스 포인트에 대한 퍼블릭 및 크로스 계정 액세스를 무시합니다.

를 @@assign로 설정하면 조직 수준에서 네 가지 설정이 "all"모두 통합되고 활성화되어 조직의 모든 계정에서 퍼블릭 액세스에 대한 포괄적인 보호를 제공합니다.

AWS Shield Network Security Director 정책

AWS Shield Network Security Director는 컴퓨팅, 네트워킹 및 네트워크 보안 리소스를 검색하여 AWS 환경을 보호하는 데 도움이 됩니다. Network Security Director는 AWS 모범 사례 및 위협 인텔리전스와 비교하여 네트워크 토폴로지 및 보안 구성을 분석하여 각 리소스의 보안 구성을 평가합니다.

AWS Shield Network Security Director 정책을 사용하면 AWS 조직의 계정 전체에서 Network Security Director를 중앙에서 활성화하고 관리할 수 있습니다. Network Security Director 정책을 사용하여 Network Security Director가 활성화된 조직 엔터티(루트, OUs 또는 계정)를 지정합니다. 계정이 조직에 가입하면 조직 계층 구조 내 위치에 따라 해당 정책을 자동으로 상속합니다. 이렇게 하면 조직이 성장함에 따라 리소스에 네트워크 보안 구성 격차가 있는지 분석할 수 있습니다. 정책은 기존 조직 구조를 존중하고 분석할 계정을 결정하는 데 유연성을 제공합니다.

AWS Shield Network Security Director는 현재 미리 보기에서 사용할 수 있습니다.

작동 방식

AWS Shield Network Security Director 정책을 조직 엔터티에 연결하면이 정책은 해당 범위 내의 모든 멤버 계정에 대해 Network Security Director를 자동으로 활성화합니다. 또한 위임된 관리자를 등록하여 AWS Shield Network Security Director 설정을 완료한 경우 해당 계정은 Network Security Director가 활성화된 조직 내 계정의 AWS Shield 네트워크 보안 태세를 중앙 집중식으로 파악할 수 있습니다.

AWS Shield Network Security Director 정책은 전체 조직, 특정 조직 단위(OUs) 또는 개별 계정에 적용할 수 있습니다. 조직에 가입하거나 정책이 연결된 OU로 이동하는 계정은 정책을 자동으로 상속하고 AWS Shield Network Security Director를 활성화하고 Network Security Director 위임된 관리자에게 연결합니다. Network Security Director 정책을 사용하면 네트워크 분석을 활성화하고, 리소스에 대한 네트워크 토폴로지 및 네트워크 보안 결과를 보고, 구성 격차를 해결하기 위한 문제 해결 권장 사항을 받을 수 있습니다. 조직의 Network Security Director 위임된 관리자 계정을 통해 특정 구성 설정 및 개별 조사 결과의 억제를 관리할 수 있습니다.

AWS Shield Network Security Director 정책을 조직 또는 조직 단위에 연결하면 AWS Organizations는 정책을 자동으로 평가하고 사용자가 정의한 범위에 따라 정책을 적용합니다. 정책 적용 로직은 특정 충돌 해결 규칙을 따릅니다.

- 활성화 및 비활성화 목록 모두에 리전이 표시되면 비활성화 구성이 우선합니다. 예를 들어 리전이 구성 활성화 및 비활성화 모두에 나열된 경우 해당 리전에서 AWS Shield Network Security Director가 비활성화됩니다.

- 활성화를 위해 ALL_SUPPORTED를 지정하면 네트워크 AWS Shield 보안 디렉터는 명시적으로 비활성화되지 않는 한 모든 현재 및 향후 리전에서 활성화됩니다. 이를 통해가 새 리전으로 AWS 확장됨에 따라 포괄적인 적용 범위를 유지할 수 있습니다.

AWS Shield Network Security Director 정책 시작하기

Network Security Director 정책을 구성하기 전에 사전 조건 및 구현 요구 사항을 이해해야 합니다. 이 주제에서는 조직에서 이러한 정책을 설정하고 관리하는 프로세스를 안내합니다.

시작하기 전 준비 사항

AWS Shield Network Security Director 정책을 구현하기 전에 다음 요구 사항을 검토합니다.

- 계정은 AWS 조직의 일부여야 합니다.
- 다음 중 하나로 로그인해야 합니다.
 - 조직의 관리 계정
 - AWS Shield Network Security Director 정책을 관리할 권한이 있는 AWS Organizations 위임된 관리자
- 조직의 Network Security Director에 대해 신뢰할 수 있는 액세스를 활성화해야 합니다.
- 조직의 루트에서 Network Security Director 정책 유형을 활성화해야 합니다.

또한 다음을 확인하세요.

- AWS Shield Network Security Director는 정책을 적용하려는 리전에서 지원됩니다.
- 관리 계정에 AWS Shield Network Security Director 서비스 연결 역할이 구성되어 있습니다. 이 역할을 생성해야 하는 경우를 실행하여 직접 생성할 수 있습니다.


```
aws iam create-service-linked-role --aws-service-name network-director.amazonaws.com.
```

구현 단계

Network Security Director 정책을 효과적으로 구현하려면 다음 단계를 순서대로 따르세요. 각 단계는 적절한 구성을 보장하고 설정 중에 발생하는 일반적인 문제를 방지하는 데 도움이 됩니다. 이러한 단계는 AWS Organizations 콘솔, AWS 명령줄 인터페이스(AWS CLI) 또는 AWS SDKs.

1. [AWS Shield Network Security Director에 대해 신뢰할 수 있는 액세스를 활성화합니다.](#)
2. [조직에 대해 AWS Shield Network Security Director 정책을 활성화합니다.](#)
3. [AWS Shield Network Security Director 정책을 생성합니다.](#)

4. [조직의 루트, OU 또는 계정에 정책을 연결합니다.](#)
5. [계정에 적용되는 결합된 유효 Network Security Director 정책을 확인합니다.](#)

AWS Shield Network Security Director 정책 구문 및 예제

Network Security Director 정책은 조직 전체에서 Network Security Director를 활성화하고 구성하는 방법을 정의하는 표준화된 JSON 구문을 따릅니다. AWS Shield Network Security Director 정책은 AWS Organizations 관리 정책 구문에 따라 구조화된 JSON 문서입니다. Network AWS Shield Security Director를 자동으로 활성화할 조직 엔터티를 정의합니다.

기본 정책 구조

AWS Shield Network Security Director 정책은 다음과 같은 기본 구조를 사용합니다.

```
{
  "network_security_director": {
    "enablement": {
      "network_security_scan": {
        "enable_in_regions": {
          "@@assign": ["us-east-1", "eu-west-1"]
        },
        "disable_in_regions": {
          "@@assign": []
        }
      }
    }
  }
}
```

정책 구성 요소

AWS Shield Network Security Director 정책에는 다음과 같은 주요 구성 요소가 포함되어 있습니다.

network_security_director

모든 Network Security Director 정책에 필요한 Network Security Director 정책 문서의 최상위 키입니다.

enablement

조직 전체에서 Network Security Director가 활성화되는 방법을 정의하고 스캔 구성을 포함합니다.

network_security_scan

네트워크 보안 스캔을 위한 적용 구성을 정의합니다.

enable_in_regions

리전 설정의 구성 식별자입니다. 네트워크 보안 스캔을 활성화해야 하는 위치를 정의합니다.

disable_in_regions

리전 설정의 구성 식별자입니다. 네트워크 보안 스캔을 비활성화할 위치를 정의합니다.

에 대한 위임된 관리자 AWS Organizations

AWS Organizations 관리 계정과 해당 사용자 및 역할은 해당 계정에서 수행해야 하는 작업에만 사용하는 것이 좋습니다. 또한 AWS 리소스를 조직의 다른 멤버 계정에 저장하고 관리 계정에는 저장하지 않는 것이 좋습니다. 이는 Organizations 서비스 제어 정책(SCP)과 같은 보안 기능이 관리 계정의 사용자나 역할을 제한하지 않기 때문입니다.

조직의 관리 계정에서, Organizations의 정책 관리를 지정된 멤버 계정에 위임하여 기본적으로 관리 계정에서만 사용할 수 있는 정책 작업을 수행할 수 있습니다.

리소스 기반 위임 정책 예제는 [에 대한 리소스 기반 정책 예제 AWS Organizations](#) 섹션을 참조하세요.

주제

- [를 사용하여 리소스 기반 위임 정책 생성 AWS Organizations](#)
- [를 사용하여 리소스 기반 위임 정책 업데이트 AWS Organizations](#)
- [를 사용하여 리소스 기반 위임 정책 보기 AWS Organizations](#)
- [를 사용하여 리소스 기반 위임 정책 삭제 AWS Organizations](#)

를 사용하여 리소스 기반 위임 정책 생성 AWS Organizations

관리 계정에서, 조직의 리소스 기반 위임 정책을 생성하고, 정책과 관련한 작업을 수행할 권한이 부여된 멤버 계정을 지정하는 문을 추가합니다. 정책에 여러 명령문을 추가하여 멤버 계정마다 다양하게 구성된 권한을 부여할 수 있습니다.

최소 권한

리소스 기반 위임 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

또한 위임된 관리자 계정의 역할과 사용자에게, 필요한 작업에 해당하는 IAM 권한을 부여해야 합니다. IAM 권한이 없으면 호출 보안 주체에게 AWS Organizations 정책을 관리하는 데 필요한 권한이 없는 것으로 간주됩니다.

AWS Management Console

AWS Management Console 에서 다음 방법 중 하나를 사용하여 리소스 기반 위임 정책에 명령문을 추가합니다.

- JSON 정책-예제 리소스 기반 위임 정책을 붙여 넣고 계정에서 사용하기에 적합하도록 수정하거나, JSON 편집기에서 직접 JSON 정책 문서를 입력합니다.
- 시각적 편집기 - 시각적 편집기에서 새 위임 정책을 구성합니다. 시각적 편집기는 사용자가 JSON 구문을 작성하지 않고도 위임 정책을 만들 수 있도록 안내합니다.

JSON 정책 편집기를 사용하여 위임 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 설정을 선택합니다.
3. Delegated administrator for AWS Organizations(의 위임된 관리자) 섹션에서 Delegate(위임)를 선택하여 Organizations 위임 정책을 생성합니다.
4. JSON 정책 문서를 입력합니다. IAM 정책 언어에 대한 자세한 내용은 [IAM JSON 정책](#) 참조를 참조하세요.
5. 정책을 검증하는 동안 생성된 모든 [보안 경고, 오류 또는 일반 경고](#)를 해결한 다음 Create policy(정책 생성)를 선택하여 작업 내용을 저장합니다.

시각적 편집기를 사용하여 위임 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 설정을 선택합니다.

3. Delegated administrator for AWS Organizations(의 위임된 관리자) 섹션에서 Delegate(위임)를 선택하여 Organizations 위임 정책을 생성합니다.
4. Create Delegation policy(위임 정책 생성) 페이지에서 Add new statement(새 명령문 추가)를 선택합니다.
5. Effect(효과)를 Allow로 설정합니다.
6. Principal을 추가하여, 작업을 위임하려는 멤버 계정을 정의합니다.
7. Actions(작업) 목록에서 위임하려는 작업을 선택합니다. Filter actions(작업 필터링)를 사용하여 선택 범위를 좁힐 수 있습니다.
8. 위임된 멤버 계정이 조직 루트 또는 조직 단위(OU)에 정책을 연결할 수 있도록 할지 여부를 지정하려면, Resources를 설정합니다. 또한 리소스 유형으로 policy를 선택해야 합니다. 다음과 같은 방법으로 리소스를 지정할 수 있습니다.
 - Add a resource(리소스 추가)를 선택하고 대화 상자에 나타나는 지시에 따라 Amazon 리소스 이름(ARN)을 구성합니다.
 - 편집기에서 리소스 ARN을 수동으로 나열합니다. ARN 구문에 대한 자세한 내용은 AWS 일반 참조 안내서의 [Amazon 리소스 이름\(ARN\)](#)을 참조하세요. 정책의 Resource 요소에 ARN을 사용하는 방법에 대한 자세한 내용은 [IAM JSON 정책 요소: Resource](#)를 참조하세요.
9. Add a condition(조건 추가)을 선택하여 위임하려는 정책 유형을 비롯한 다른 조건을 지정합니다. 조건의 Condition key(조건 키), Tag key(태그 키), Qualifier(한정어), Operator(연산자)를 선택한 후 **Value**를 입력합니다. 마치면 Add condition(조건 추가)을 선택합니다. Condition 요소에 대한 자세한 내용은 IAM JSON 정책 참조에서 [IAM JSON 정책 요소: Condition](#)을 참조하세요.
10. 권한 블록을 더 추가하려면 Add new statement(새 명령문 추가)를 선택합니다. 각 블록마다 5~9단계를 반복합니다.
11. [정책을 검증](#)하는 동안 생성된 모든 보안 경고, 오류 또는 일반 경고를 해결한 다음 Create policy(정책 생성)를 선택하여 작업 내용을 저장합니다.

AWS CLI & AWS SDKs

위임 정책 생성

위임 정책을 생성하려면 다음 명령을 사용합니다.

- AWS CLI: [put-resource-policy](#)

다음 예제에서는 위임 정책을 생성합니다.

```
$ aws organizations put-resource-policy --content
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Fully_manage_backup_policies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "135791357913"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:CreatePolicy",
        "organizations:DescribePolicy",
        "organizations:UpdatePolicy",
        "organizations>DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
      ],
      "Resource": [
        "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
        "arn:aws:organizations::246802468024:ou/o-abcdef/*",
        "arn:aws:organizations::246802468024:account/o-abcdef/*",
        "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
      ],
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": [
            "BACKUP_POLICY"
          ]
        }
      }
    }
  ]
}
```

- AWS SDK: [PutResourcePolicy](#)

지원되는 위임 정책 작업

위임 정책과 관련하여 지원되는 작업은 다음과 같습니다.

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget

- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource
- UntagResource
- UpdatePolicy

지원되는 조건 키

위임 정책에는에서 지원하는 조건 키만 사용할 AWS Organizations 수 있습니다. 자세한 내용은 서비스 권한 부여 참조의 [AWS Organizations조건 키](#)를 참조하세요.

를 사용하여 리소스 기반 위임 정책 업데이트 AWS Organizations

관리 계정에서, 조직의 리소스 기반 위임 정책을 업데이트하고, 정책과 관련한 작업을 수행할 권한이 부여된 멤버 계정을 지정하는 문을 추가합니다. 정책에 여러 명령문을 추가하여 멤버 계정마다 다양하게 구성된 권한을 부여할 수 있습니다.

최소 권한

리소스 기반 위임 정책을 업데이트하려면 다음 작업을 실행할 권한이 필요합니다.

- organizations:PutResourcePolicy
- organizations:DescribeResourcePolicy

또한 위임된 관리자 계정의 역할과 사용자에게, 필요한 작업에 해당하는 IAM 권한을 부여해야 합니다. IAM 권한이 없으면 호출 보안 주체에게 AWS Organizations 정책을 관리하는 데 필요한 권한이 없는 것으로 간주됩니다.

AWS Management Console

AWS Management Console 에서 다음 방법 중 하나를 사용하여 리소스 기반 위임 정책에 명령문을 추가합니다.

- JSON 정책-예제 리소스 기반 위임 정책을 붙여 넣고 계정에서 사용하기에 적합하도록 수정하거나, JSON 편집기에서 직접 JSON 정책 문서를 입력합니다.

- 시각적 편집기 - 시각적 편집기에서 새 위임 정책을 구성합니다. 시각적 편집기는 사용자가 JSON 구문을 작성하지 않고도 위임 정책을 만들 수 있도록 안내합니다.

JSON 정책 편집기를 사용하여 위임 정책을 업데이트하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 설정을 선택합니다.
3. AWS Organizations의 위임된 관리자 섹션에서 위임을 선택하여 Organizations 위임 정책을 업데이트합니다.
4. JSON 정책 문서를 입력합니다. IAM 정책 언어에 대한 자세한 내용은 [IAM JSON 정책 참조](#)를 참조하세요.
5. 정책 검증 동안 생성된 모든 [보안 경고, 오류 또는 일반 경고](#)를 해결한 다음 정책 생성을 선택합니다.

시각적 편집기를 사용하여 위임 정책을 업데이트하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 설정을 선택합니다.
3. AWS Organizations의 위임된 관리자 섹션에서 위임을 선택하여 Organizations 위임 정책을 업데이트합니다.
4. Create Delegation policy(위임 정책 생성) 페이지에서 Add new statement(새 명령문 추가)를 선택합니다.
5. Effect(효과)를 Allow로 설정합니다.
6. Principal을 추가하여, 작업을 위임하려는 멤버 계정을 정의합니다.
7. Actions(작업) 목록에서 위임하려는 작업을 선택합니다. Filter actions(작업 필터링)를 사용하여 선택 범위를 좁힐 수 있습니다.
8. 위임된 멤버 계정이 조직 루트 또는 조직 단위(OU)에 정책을 연결할 수 있도록 할지 여부를 지정하려면, Resources를 설정합니다. 또한 리소스 유형으로 policy를 선택해야 합니다. 다음과 같은 방법으로 리소스를 지정할 수 있습니다.
 - Add a resource(리소스 추가)를 선택하고 대화 상자에 나타나는 지시에 따라 Amazon 리소스 이름(ARN)을 구성합니다.

- 편집기에서 리소스 ARN을 수동으로 나열합니다. ARN 구문에 대한 자세한 내용은 AWS 일반 참조 안내서의 [Amazon 리소스 이름\(ARN\)](#)을 참조하세요. 정책의 Resource 요소에 ARN을 사용하는 방법에 대한 자세한 내용은 [IAM JSON 정책 요소: Resource](#)를 참조하세요.
9. Add a condition(조건 추가)을 선택하여 위임하려는 정책 유형을 비롯한 다른 조건을 지정합니다. 조건의 Condition key(조건 키), Tag key(태그 키), Qualifier(한정어), Operator(연산자)를 선택한 후 **Value**를 입력합니다. 마치면 Add condition(조건 추가)을 선택합니다. Condition 요소에 대한 자세한 내용은 IAM JSON 정책 참조에서 [IAM JSON 정책 요소: Condition](#)을 참조하세요.
 10. 권한 블록을 더 추가하려면 Add new statement(새 명령문 추가)를 선택합니다. 각 블록마다 5~9단계를 반복합니다.
 11. [정책 검증](#) 동안 생성된 모든 보안 경고, 오류 또는 일반 경고를 해결한 다음 정책 저장를 선택합니다.

AWS CLI & AWS SDKs

위임 정책 생성 또는 업데이트

위임 정책을 생성하거나 업데이트하려면 다음 명령을 사용합니다.

- AWS CLI: [put-resource-policy](#)

다음 예제에서는 위임 정책을 생성하거나 업데이트합니다.

```
$ aws organizations put-resource-policy --content
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Fully_manage_backup_policies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "135791357913"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:CreatePolicy",
        "organizations:DescribePolicy",
        "organizations:UpdatePolicy",
        "organizations>DeletePolicy",
```

```

        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
    ],
    "Resource": [
        "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
        "arn:aws:organizations::246802468024:ou/o-abcdef/*",
        "arn:aws:organizations::246802468024:account/o-abcdef/*",
        "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
    ],
    "Condition": {
        "StringLikeIfExists": {
            "organizations:PolicyType": [
                "BACKUP_POLICY"
            ]
        }
    }
}
]
}
}

```

- AWS SDK: [PutResourcePolicy](#)

지원되는 위임 정책 작업

위임 정책과 관련하여 지원되는 작업은 다음과 같습니다.

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy

- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource
- UntagResource
- UpdatePolicy

지원되는 조건 키

위임 정책에는에서 지원하는 조건 키만 사용할 AWS Organizations 수 있습니다. 자세한 내용은 서비스 권한 부여 참조의 [AWS Organizations조건 키](#)를 참조하세요.

를 사용하여 리소스 기반 위임 정책 보기 AWS Organizations

관리 계정에서, 조직의 리소스 기반 위임 정책을 보면서 위임된 관리자별로 어떤 정책 유형을 관리할 권한이 부여되어 있는지 파악합니다.

i 최소 권한

리소스 기반 위임 정책을 보려면 `organizations:DescribeResourcePolicy` 작업을 실행할 권한이 필요합니다.

AWS Management Console

위임 정책을 보려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 설정을 선택합니다.
3. Delegated administrator for AWS Organizations(의 위임된 관리자) 섹션에서 스크롤하여 전체 위임 정책을 봅니다.

AWS CLI & AWS SDKs

위임 정책 보기

위임 정책을 보려면 다음 명령을 사용합니다.

- AWS CLI: [describe-resource-policy](#)

다음 예제에서는 정책을 검색합니다.

```
$ aws organizations describe-resource-policy
```

- AWS SDK: [DescribeResourcePolicy](#)

를 사용하여 리소스 기반 위임 정책 삭제 AWS Organizations

조직의 정책 관리 작업을 더 이상 위임할 필요가 없는 경우, 조직의 관리 계정에서 리소스 기반 위임 정책을 삭제할 수 있습니다.

⚠ Important

삭제한 리소스 기반 위임 정책은 복구할 수 없습니다.

ℹ 최소 권한

리소스 기반 위임 정책을 삭제하려면 `organizations:DeleteResourcePolicy` 작업을 실행할 권한이 필요합니다.

AWS Management Console

위임 정책을 삭제하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 설정을 선택합니다.
3. Delegated administrator for AWS Organizations(의 위임된 관리자) 섹션에서 Delete(삭제)를 선택합니다.
4. Delete policy(정책 삭제) 확인 대화 상자에 **delete**를 입력합니다. 그런 다음 Delete policy(정책 삭제)를 선택합니다.

AWS CLI & AWS SDKs

위임 정책 삭제

위임 정책을 삭제하려면 다음 명령을 사용합니다.

- AWS CLI: [delete-resource-policy](#)

다음 예제에서는 정책을 삭제합니다.

```
$ aws organizations delete-resource-policy
```

- AWS SDK: [DeleteResourcePolicy](#)

정책 유형 활성화

정책을 생성하여 조직에 연결하려면 먼저 해당 정책 유형을 사용하도록 활성화해야 합니다. 정책 유형을 활성화하는 것은 조직 루트의 일회성 작업입니다. 조직의 관리 계정 또는 위임된 관리자로 지정된 멤버 계정에서만 정책 유형을 활성화할 수 있습니다.

최소 권한

정책 유형을 활성화하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- `organizations:EnablePolicyType`
- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:ListRoots` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

정책 유형을 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [정책\(Policies\)](#) 페이지에서 활성화할 정책 유형의 이름을 선택합니다.
3. 정책 유형 페이지에서 정책 유형 활성화(Enable **policy type**)를 선택합니다.

지정된 유형의 사용 가능한 정책 목록으로 페이지가 바뀝니다.

AWS CLI & AWS SDKs

정책 유형을 활성화하려면

다음 명령 중 하나를 사용하여 정책 유형을 활성화할 수 있습니다.

- AWS CLI: [enable-policy-type](#)

다음 예제에서는 조직에 백업 정책을 활성화하는 방법을 보여 줍니다. 조직의 루트 ID를 지정해야 합니다.

```
$ aws organizations enable-policy-type \
```

```

--root-id r-a1b2 \
--policy-type BACKUP_POLICY
{
  "Root": {
    "Id": "r-a1b2",
    "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
    "Name": "Root",
    "PolicyTypes": [
      {
        "Type": "BACKUP_POLICY",
        "Status": "ENABLED"
      }
    ]
  }
}

```

이제 지정한 정책 유형과 함께 ENABLED의 Status가 출력의 PolicyTypes 목록에 포함됩니다.

- AWS SDKs: [EnablePolicyType](#)

정책 유형 비활성화

조직에서 특정 정책 유형을 더 이상 사용하지 않으려면 해당 유형을 실수로 사용하지 않도록 비활성화할 수 있습니다. 조직의 관리 계정 또는 위임된 관리자로 지정된 멤버 계정에서만 정책 유형을 비활성화할 수 있습니다.

고려 사항

비활성화된 정책은 모든 엔터티에서 분리되지만 삭제되지 않음

정책 유형을 비활성화하면 지정된 유형의 모든 정책이 조직 루트의 모든 엔터티에서 자동으로 분리됩니다. 정책은 삭제되지 않습니다.

(서비스 제어 정책 유형만 해당) 루트의 모든 엔터티는 처음에 기본 **FullAWSAccess** SCP에만 연결됨

(서비스 제어 정책 유형만 해당) 나중에 SCP 정책 유형을 다시 활성화하면 조직 루트의 모든 엔터티는 처음에 기본 FullAWSAccess SCP에만 연결됩니다. 조직에서 SCP가 비활성화되면 엔터티에 대한 SCP의 연결이 손실됩니다. 나중에 SCP를 다시 활성화하려면 해당 SCP를 조직의 루트, OU, 계정에 적절히 다시 연결해야 합니다.

정책 유형 비활성화

❗ 최소 권한

SCP를 비활성화하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:ListRoots` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

AWS Management Console

정책 유형을 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [정책\(Policies\)](#) 페이지에서 비활성화하려는 정책 유형의 이름을 선택하세요.
3. 정책 유형 페이지에서 정책 유형 비활성화(Disable **policy type**)를 선택합니다.
4. 확인 대화 상자에서 **disable**이라는 단어를 입력한 다음 비활성화(Disable)를 선택합니다.

지정된 유형의 사용 가능한 정책 목록이 사라집니다.

AWS CLI & AWS SDKs

정책 유형을 비활성화하려면

다음 명령 중 하나를 사용하여 정책 유형을 비활성화할 수 있습니다.

- AWS CLI: [disable-policy-type](#)

다음 예제에서는 조직에 대해 백업 정책을 비활성화하는 방법을 보여 줍니다. 조직의 루트 ID를 지정해야 합니다.

```
$ aws organizations disable-policy-type \
  --root-id r-a1b2 \
  --policy-type BACKUP_POLICY
```

```
{
  "Root": {
    "Id": "r-a1b2",
    "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
    "Name": "Root",
    "PolicyTypes": []
  }
}
```

지정한 정책 유형이 더 이상 출력의 PolicyTypes 목록에 포함되지 않습니다.

- AWS SDKs: [DisablePolicyType](#)

를 사용하여 조직 정책 생성 AWS Organizations

조직에 대해 [정책을 활성화](#)한 후에 정책을 생성할 수 있습니다.

이 주제에서는를 사용하여 정책을 생성하는 방법을 설명합니다 AWS Organizations. 정책은 그룹에 적용할 컨트롤을 정의합니다 AWS 계정.

주제

- [서비스 제어 정책\(SCP\) 생성](#)
- [리소스 제어 정책\(RCP\) 생성](#)
- [선언적 정책 생성](#)
- [백업 정책 생성](#)
- [태그 정책 생성](#)
- [채팅 애플리케이션 정책 생성](#)
- [AI 서비스 옵트아웃 정책 생성](#)
- [업그레이드 롤아웃 정책 생성](#)
- [Security Hub 정책 생성](#)

서비스 제어 정책(SCP) 생성

최소 권한

SCP를 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- organizations:CreatePolicy

AWS Management Console

서비스 제어 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [서비스 제어 정책](#) 페이지에서 정책 생성을 선택합니다.
3. [새 서비스 제어 정책 생성 페이지](#)에서 정책 이름과 정책 설명(선택 사항)을 입력합니다.
4. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 하나 이상의 태그를 추가합니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 정보는 [AWS Organizations 리소스 태그 지정](#)을 참조하세요.

Note

이어지는 대부분의 단계에서는 JSON 편집기의 오른쪽에 있는 컨트롤을 사용하여 요소별로 정책을 구성하는 방법에 대해 설명합니다. 또는 언제든지 창 왼쪽의 JSON 편집기에 간단히 텍스트를 입력할 수 있습니다. 직접 입력하거나 복사 및 붙여넣기를 사용할 수 있습니다.

5. 정책 작성은 추가하는 문이 액세스를 [거부](#)하는지, 아니면 [허용](#)하지에 따라 그 다음 단계가 달라집니다. 자세한 내용은 [SCP 평가](#) 단원을 참조하십시오. Deny 문을 사용할 경우 특정 리소스 대한 액세스를 제한하고, SCP가 효력을 발휘하는 조건을 정의하고, [NotAction](#) 요소를 사용하는 추가 컨트롤을 사용할 수 있습니다. 구문에 대한 자세한 내용은 [SCP 구문](#) 단원을 참조하세요.

액세스를 거부하는 문을 추가하려면:

- a. 편집기의 오른쪽 문 편집 창의 작업 추가에서 AWS 서비스를 선택합니다.

오른쪽 창에서 옵션을 선택하면 JSON 편집기가 업데이트되어 왼쪽에 해당하는 JSON 정책이 표시됩니다.

- b. 서비스를 선택하면 해당 서비스에 대해 사용 가능한 작업이 포함된 목록이 열립니다. 모든 작업을 선택하거나, 거부하려는 개별 작업을 하나 이상 선택할 수 있습니다.

왼쪽의 JSON이 업데이트되면서 선택한 작업이 포함됩니다.

 Note

개별 작업을 선택한 다음 돌아가서 모든 작업을 선택하는 경우

servicename:*에 대한 예상 항목이 JSON에 추가되지만 이전에 선택한 개별 작업은 JSON에 남아 제거되지 않습니다.

- c. 추가 서비스에서 작업을 추가하려면 문 상자 상단에서 모든 서비스를 선택한 다음 필요에 따라 앞의 두 단계를 반복할 수 있습니다.
- d. 문에 포함할 리소스를 지정합니다.
 - 리소스 추가 옆에 있는 추가를 선택합니다.
 - 리소스 추가 대화 상자의 목록에서 리소스를 제어하려는 서비스를 선택합니다. 이전 단계에서 선택한 서비스 중에서만 선택할 수 있습니다.
 - 리소스 유형(Resource type)에서 제어할 리소스 유형을 선택합니다.
 - 마지막으로 액세스를 제어하려는 특정 리소스를 식별하기 위해 리소스 ARN(Resource ARN)에 Amazon 리소스 이름(ARN)을 작성합니다. 중괄호 {}로 둘러싸인 모든 자리 표시자를 교체해야 합니다. 해당 리소스 유형의 ARN 구문이 허용하는 경우 와일드카드(*)를 지정할 수 있습니다. 와일드카드를 사용할 수 있는 상황에 대한 내용은 특정 리소스 유형에 대한 설명서를 참조하세요.
 - 리소스 추가(Add resource)를 선택해 정책에 대한 추가 항목을 저장합니다. JSON의 Resource 요소는 추가 또는 변경 사항을 반영합니다. 리소스 요소는 필수입니다.

 Tip

선택한 서비스에 대한 모든 리소스를 지정하려면 목록에서 모든 리소스(All resources) 옵션을 선택하거나 "Resource": "*"를 읽는 JSON에서 Resource 문을 직접 편집합니다.

- e. (선택 사항) 정책 문이 적용되는 상황을 제한하는 조건을 지정하려면 조건 추가 옆에 있는 추가를 선택합니다.
 - 조건 키 - 목록에서 모든 AWS 서비스에 사용할 수 있는 조건 키(예: aws:SourceIp) 또는 이 문에 대해 선택한 서비스 중 하나에 대해서만 서비스별 키를 선택할 수 있습니다.

- 한정자 - (선택 사항) 요청에 다중 값 컨텍스트 키에 대한 값이 두 개 이상 있는 경우 값에 대한 요청을 테스트하기 위한 [한정자](#)를 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [단일 값 컨텍스트 키와 다중 값 컨텍스트 키](#)를 참조하세요. 요청이 여러 값을 가질 수 있는지 확인하려면 서비스 승인 참조의 AWS 서비스에 대한 [작업, 리소스 및 조건 키](#)를 참조하세요.
- 기본값 - 정책의 조건 키 값에 대해 요청의 한 값을 테스트합니다. 요청의 값이 정책의 값과 일치하면 조건이 true를 반환합니다. 정책에 둘 이상의 값이 지정되어 있으면 “or” 테스트로 처리되고, 요청 값이 임의의 정책 값과 일치하는 경우 조건이 true를 반환합니다.
- 요청의 임의의 값에 대해(For any value in a request) - 요청이 여러 값을 가질 수 있는 경우 이 옵션은 요청 값 중 하나 이상이 정책의 조건 키 값 중 하나 이상과 일치하는지 확인합니다. 요청의 키 값 중 하나가 정책의 조건 값 중 하나와 일치하면 조건이 true를 반환합니다. 일치하는 키가 없거나 null 데이터 세트의 경우 조건에서 false를 반환합니다.
- 요청의 모든 값에 대해(For all values in a request) - 요청이 여러 값을 가질 수 있는 경우 이 옵션은 모든 요청 값이 정책의 조건 키 값과 일치하는지 확인합니다. 요청의 모든 키 값이 정책에 있는 하나 이상의 값과 일치하면 조건이 true를 반환합니다. 요청에 키가 없거나 키 값이 빈 문자열과 같은 null 데이터 세트로 확인되는 경우에도 true를 반환합니다.
- 연산자(Operator) - [연산자](#)는 수행할 비교의 유형을 지정합니다. 표시되는 옵션은 조건 키의 데이터 유형에 따라 다릅니다. 예를 들어 aws:CurrentTime 전역 조건 키를 사용하면 날짜 비교 연산자 중 하나를 선택할 수 있습니다. 또는 Null을 사용하면 값이 요청에 있는지 여부를 테스트할 수 있습니다.

Null 테스트를 제외한 모든 조건 연산자에 대해 [IfExists](#) 옵션을 선택할 수 있습니다.

- 값(Value) - (선택 사항) 요청에서 테스트할 값을 하나 이상 지정합니다.

조건 추가를 선택합니다.

조건 키에 대한 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.

6. 액세스를 허용하는 문을 추가하려면:

- a. 왼쪽의 JSON 편집기에서 "Effect": "Deny" 라인을 "Effect": "Allow"로 변경합니다.

오른쪽 창에서 옵션을 선택하면 JSON 편집기가 업데이트되어 왼쪽에 해당하는 JSON 정책이 표시됩니다.

- b. 서비스를 선택하면 해당 서비스에 대해 사용 가능한 작업이 포함된 목록이 열립니다. 모든 작업(All actions)을 선택하거나, 허용하려는 개별 작업을 하나 이상 선택할 수 있습니다.

왼쪽의 JSON이 업데이트되면서 선택한 작업이 포함됩니다.

 Note

개별 작업을 선택한 다음 돌아가서 모든 작업을 선택하는 경우

servicename*:에 대한 예상 항목이 JSON에 추가되지만 이전에 선택한 개별 작업은 JSON에 남아 제거되지 않습니다.

- c. 추가 서비스에서 작업을 추가하려면 문(Statement) 상자 상단에서 모든 서비스(All services)를 선택한 다음 필요에 따라 앞의 두 단계를 반복할 수 있습니다.
7. (선택 사항) 정책에 다른 문을 추가하려면 문 추가(Add statement)를 선택하고 시각적 편집기를 사용하여 다음 문을 작성합니다.
8. 문을 모두 추가했으면 정책 생성을 선택하여 완료된 SCP를 저장합니다.

새 SCP가 조직의 정책 목록에 표시됩니다. 이제 [루트, OU 또는 계정에 SCP를 연결](#)할 수 있습니다.

AWS CLI & AWS SDKs

서비스 제어 정책을 생성하려면

다음 명령 중 하나를 사용하여 SCP를 생성할 수 있습니다.

- AWS CLI: [create-policy](#)

다음 예제에서는 JSON 정책 텍스트가 포함된 Deny-IAM.json이라는 파일을 가정합니다. 이 파일은 새 서비스 제어 정책을 생성하는 데 사용됩니다.

```
$ aws organizations create-policy \
  --content file://Deny-IAM.json \
  --description "Deny all IAM actions" \
  --name DenyIAMSCP \
  --type SERVICE_CONTROL_POLICY
{
  "Policy": {
```



```

    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/service_control_policy/p-i9j8k7l6m5",
      "Name": "DenyIAMSCP",
      "Description": "Deny all IAM actions",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n      \"Sid\": \"Statement1\",\n      \"Effect\": \"Deny\",\n      \"Action\": [\"iam:*\"],\n      \"Resource\": [\"*\"]\n    }\n  ]\n}"
  }
}

```

- AWS SDKs: [CreatePolicy](#)

Note

SCP는 관리 계정과 몇 가지 다른 상황에서는 적용되지 않습니다. 자세한 내용은 [작업 및 엔터티는 SCP로 제한할 수 없습니다](#). 단원을 참조하십시오.

리소스 제어 정책(RCP) 생성

최소 권한

RCP를 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- organizations:CreatePolicy

AWS Management Console

리소스 제어 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 리소스 제어 정책 페이지에서 정책 생성을 선택합니다.
3. [새 리소스 제어 정책 생성 페이지](#)에서 정책 이름과 정책 설명(선택 사항)을 입력합니다.

4. (선택 사항) 태그 추가를 선택한 다음 키 및 값(선택 사항)을 입력해 하나 이상의 태그를 추가합니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 정보는 [AWS Organizations 리소스 태그 지정](#)을 참조하세요.

 Note

이어지는 대부분의 단계에서는 JSON 편집기의 오른쪽에 있는 컨트롤을 사용하여 요소별로 정책을 구성하는 방법에 대해 설명합니다. 또는 언제든지 창 왼쪽의 JSON 편집기에 간단히 텍스트를 입력할 수 있습니다. 직접 입력하거나 복사 및 붙여넣기를 사용할 수 있습니다.

5. 문을 추가하려면:

- a. 편집기의 오른쪽 문 편집 창의 작업 추가에서 AWS 서비스를 선택합니다.

오른쪽 창에서 옵션을 선택하면 JSON 편집기가 업데이트되어 왼쪽에 해당하는 JSON 정책이 표시됩니다.

- b. 서비스를 선택하면 해당 서비스에 대해 사용 가능한 작업이 포함된 목록이 열립니다. 모든 작업을 선택하거나, 거부하려는 개별 작업을 하나 이상 선택할 수 있습니다.

왼쪽의 JSON이 업데이트되면서 선택한 작업이 포함됩니다.

 Note

개별 작업을 선택한 다음 돌아가서 모든 작업을 선택하는 경우

servicename:*에 대한 예상 항목이 JSON에 추가되지만 이전에 선택한 개별 작업은 JSON에 남아 제거되지 않습니다.

- c. 추가 서비스에서 작업을 추가하려면 문 상자 상단에서 모든 서비스를 선택한 다음 필요에 따라 앞의 두 단계를 반복할 수 있습니다.
- d. 문에 포함할 리소스를 지정합니다.

- 리소스 추가 옆에 있는 추가를 선택합니다.
- 리소스 추가 대화 상자의 목록에서 리소스를 제어하려는 서비스를 선택합니다. 이전 단계에서 선택한 서비스 중에서만 선택할 수 있습니다.
- 리소스 유형(Resource type)에서 제어할 리소스 유형을 선택합니다.

- 액세스를 제어하려는 특정 리소스를 식별하기 위해 리소스 ARN에 Amazon 리소스 이름(ARN)을 작성합니다. 중괄호 {}로 둘러싸인 모든 자리 표시자를 교체해야 합니다. 해당 리소스 유형의 ARN 구문이 허용하는 경우 와일드카드(*)를 지정할 수 있습니다. 와일드카드를 사용할 수 있는 상황에 대한 내용은 특정 리소스 유형에 대한 [설명서](#)를 참조하세요.
- 리소스 추가(Add resource)를 선택해 정책에 대한 추가 항목을 저장합니다. JSON의 Resource 요소는 추가 또는 변경 사항을 반영합니다. 리소스 요소는 필수입니다.

i Tip

선택한 서비스에 대한 모든 리소스를 지정하려면 목록에서 모든 리소스(All resources) 옵션을 선택하거나 "Resource": "*"를 읽는 JSON에서 Resource 문을 직접 편집합니다.

- e. (선택 사항) 정책 문이 적용되는 상황을 제한하는 조건을 지정하려면 조건 추가 옆에 있는 추가를 선택합니다.
- 조건 키 - 목록에서 모든 AWS 서비스에 사용할 수 있는 조건 키(예: aws:SourceIp) 또는 이 문에 대해 선택한 서비스 중 하나에 대해서만 서비스별 키를 선택할 수 있습니다.
 - 한정자 - (선택 사항) 요청에 다중 값 컨텍스트 키에 대한 값이 두 개 이상 있는 경우 값에 대한 요청을 테스트하기 위한 [한정자](#)를 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [단일 값 컨텍스트 키와 다중 값 컨텍스트 키](#)를 참조하세요. 요청이 여러 값을 가질 수 있는지 확인하려면 서비스 승인 참조의 AWS 서비스에 대한 [작업, 리소스 및 조건 키](#)를 참조하세요.
 - 기본값 - 정책의 조건 키 값에 대해 요청의 한 값을 테스트합니다. 요청의 값이 정책의 값과 일치하면 조건이 true를 반환합니다. 정책에 둘 이상의 값이 지정되어 있으면 "or" 테스트로 처리되고, 요청 값이 임의의 정책 값과 일치하는 경우 조건이 true를 반환합니다.
 - 요청의 임의의 값에 대해(For any value in a request) - 요청이 여러 값을 가질 수 있는 경우 이 옵션은 요청 값 중 하나 이상이 정책의 조건 키 값 중 하나 이상과 일치하는지 확인합니다. 요청의 키 값 중 하나가 정책의 조건 값 중 하나와 일치하면 조건이 true를 반환합니다. 일치하는 키가 없거나 null 데이터 세트의 경우 조건에서 false를 반환합니다.
 - 요청의 모든 값에 대해(For all values in a request) - 요청이 여러 값을 가질 수 있는 경우 이 옵션은 모든 요청 값이 정책의 조건 키 값과 일치하는지 확인합니다. 요청의 모

든 키 값이 정책에 있는 하나 이상의 값과 일치하면 조건이 true를 반환합니다. 요청에 키가 없거나 키 값이 빈 문자열과 같은 null 데이터 세트로 확인되는 경우에도 true를 반환합니다.

- 연산자(Operator) - [연산자](#)는 수행할 비교의 유형을 지정합니다. 표시되는 옵션은 조건 키의 데이터 유형에 따라 다릅니다. 예를 들어 `aws:CurrentTime` 전역 조건 키를 사용하면 날짜 비교 연산자 중 하나를 선택할 수 있습니다. 또는 `Null`을 사용하면 값이 요청에 있는지 여부를 테스트할 수 있습니다.

`Null` 테스트를 제외한 모든 조건 연산자에 대해 [IfExists](#) 옵션을 선택할 수 있습니다.

- 값(Value) - (선택 사항) 요청에서 테스트할 값을 하나 이상 지정합니다.

조건 추가를 선택합니다.

조건 키에 대한 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.

- (선택 사항) `NotAction` 요소를 사용하여 지정된 작업을 제외한 모든 작업에 대해 액세스를 거부하려면 왼쪽 창에서 `Action`을 `NotAction`으로 바꿉니다("Effect": "Deny", 요소 바로 뒤에서). 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: NotAction](#)을 참조하세요.
- (선택 사항) 정책에 다른 문을 추가하려면 문 추가(Add statement)를 선택하고 시각적 편집기를 사용하여 다음 문을 작성합니다.
 - 문을 모두 추가했으면 정책 생성을 선택하여 완료된 RCP를 저장합니다.

새 RCP가 조직의 정책 목록에 표시됩니다. 이제 [루트, OU 또는 계정에 RCP를 연결](#)할 수 있습니다.

AWS CLI & AWS SDKs

리소스 제어 정책을 생성하려면

다음 명령 중 하나를 사용하여 RCP를 생성할 수 있습니다.

- AWS CLI: [create-policy](#)

다음 예제에서는 JSON 정책 텍스트가 포함된 `Deny-IAM.json`이라는 파일을 가정합니다. 이 파일은 새 리소스 제어 정책을 생성하는 데 사용됩니다.

```
$ aws organizations create-policy \
  --content file://Deny-IAM.json \
```

```
--description "Deny all IAM actions" \
--name DenyIAMRCP \
--type RESOURCE_CONTROL_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
resource_control_policy/p-i9j8k7l6m5",
      "Name": "DenyIAMRCP",
      "Description": "Deny all IAM actions",
      "Type": "RESOURCE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\", \"Statement\": [{\"Sid\":
\\\"Statement1\\\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\"*\"]}]}\"
  }
}
```

- AWS SDKs: [CreatePolicy](#)

Note

RCP는 관리 계정과 몇 가지 다른 상황에서는 적용되지 않습니다. 자세한 내용은 [RCP로 제한 받지 않는 리소스 및 엔터티](#) 단원을 참조하십시오.

선언적 정책 생성

최소 권한

선언적 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- `organizations:CreatePolicy`

AWS Management Console

선언적 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [선언적 정책](#) 페이지에서 정책 생성을 선택합니다.
3. [EC2용 새 선언적 정책 생성 페이지](#)에서 정책 이름 및 정책 설명(선택 사항)을 입력합니다.
4. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 정책에 하나 이상의 태그를 추가할 수 있습니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 내용은 [AWS Organizations 리소스 태그 지정](#) 단원을 참조하십시오.
5. 이 절차의 설명과 같이 시각적 편집기를 사용하여 정책을 작성할 수 있습니다. JSON 탭에서 정책 텍스트를 입력하거나 붙여 넣을 수도 있습니다. 선언적 정책 구문에 대한 자세한 내용은 [선언적 정책 구문 및 예시](#) 단원을 참조하세요.

시각적 편집기를 사용하도록 선택한 경우 선언적 정책에 포함할 서비스 속성을 선택합니다. 자세한 내용은 [지원되는 AWS 서비스 및 속성](#) 단원을 참조하십시오.

6. 서비스 속성 추가를 선택하고 사양에 맞게 속성을 구성합니다. 각 효과에 대한 자세한 내용은 [선언적 정책 구문 및 예시](#) 섹션을 참조하세요.
7. 정책 편집을 마쳤으면 페이지의 오른쪽 아래 모서리에 있는 정책 생성(Create policy)을 선택합니다.

AWS CLI & AWS SDKs

선언적 정책을 생성하려면

다음 중 하나를 사용하여 선언적 정책을 생성할 수 있습니다.

- AWS CLI: [create-policy](#)

1. 다음과 같은 선언적 정책을 작성하여 텍스트 파일에 저장합니다.

```
{
  "ec2_attributes": {
    "image_block_public_access": {
      "state": {
        "@@assign": "block_new_sharing"
      }
    }
  }
}
```

```

    }
  }
}

```

이 선언적 정책은 새 Amazon Machine Image(AMI)를 공개적으로 공유할 수 없도록 정책의 영향을 받는 모든 계정을 구성해야 한다고 지정합니다. 선언적 정책 구문에 대한 자세한 내용은 [선언적 정책 구문 및 예시](#) 단원을 참조하세요.

2. JSON 정책 파일을 가져와 조직에 새 정책을 생성합니다. 이 예제에서 이전 JSON 파일의 이름은 `policy.json`이었습니다.

```

$ aws organizations create-policy \
  --type DECLARATIVE_POLICY_EC2 \
  --name "MyTestPolicy" \
  --description "My test policy" \
  --content file://policy.json
{
  "Policy": {
    "Content": "{\"ec2_attributes\":{\"image_block_public_access\":{\"state\":{\"@@assign\":\"block_new_sharing\"}}}}".
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5"
      "Arn": "arn:aws:organizations::o-aa111bb222:policy/declarative_policy_ec2/p-i9j8k7l6m5",
      "Description": "My test policy",
      "Name": "MyTestPolicy",
      "Type": "DECLARATIVE_POLICY_EC2"
    }
  }
}

```

- AWS SDKs: [CreatePolicy](#)

다음에 수행할 작업

선언적 정책을 생성한 후 [계정 상태 보고서](#)를 사용하여 준비 상태를 평가합니다. 그런 다음 기존 구성을 적용할 수 있습니다. 이를 위해 조직 루트, 조직 단위(OU), 조직 내 AWS 계정, 또는 이들의 조합에 [정책을 연결](#)할 수 있습니다.

백업 정책 생성

최소 권한

백업 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- `organizations:CreatePolicy`

AWS Management Console

다음 두 가지 방법 중 하나로 AWS Management Console 에서 백업 정책을 생성할 수 있습니다.

- 사용자가 옵션을 선택하면 자동으로 JSON 정책 텍스트를 생성하는 시각적 편집기.
- 사용자가 직접 JSON 정책 텍스트를 작성할 수 있는 텍스트 편집기.

시각적 편집기를 사용하면 프로세스를 쉽게 수행할 수 있지만 유연성은 제한됩니다. 이는 처음 정책을 생성하여 편안하게 사용할 수 있는 좋은 방법입니다. 정책이 어떻게 작동하는지 이해하고 시각적 편집기가 제공하는 기능에 의해 제한되기 시작하면 JSON 정책 텍스트를 직접 편집하여 정책에 고급 기능을 추가할 수 있습니다. 시각적 편집기는 [@@assign value-setting 연산자](#)만 사용하며, [하위 제어 연산자](#)에 대한 액세스 권한을 제공하지 않습니다. 하위 제어 연산자는 JSON 정책 텍스트를 수동으로 편집하는 경우에만 추가할 수 있습니다.

백업 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [백업 정책\(Backup policies\)](#) 페이지에서 정책 생성(Create policy)을 선택합니다.
3. 정책 생성(Create policy) 페이지에서 정책 이름과 정책 설명(선택 사항)을 입력합니다.
4. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 정책에 하나 이상의 태그를 추가할 수 있습니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요 [AWS Organizations 리소스 태그 지정](#)
5. 이 절차의 설명과 같이 시각적 편집기를 사용하여 정책을 작성할 수 있습니다. JSON 탭에서 정책 텍스트를 입력하거나 붙여 넣을 수도 있습니다. 백업 정책 구문에 대한 자세한 내용은 [백업 정책 구문 및 예제](#) 단원을 참조하세요.

시각적 편집기를 사용하기로 선택한 경우 시나리오에 적합한 백업 옵션을 선택합니다. 백업 계획은 세 부분으로 구성됩니다. 이러한 백업 계획 요소에 대한 자세한 내용은 AWS Backup 개발자 안내서의 [백업 계획 생성](#) 및 [리소스 할당](#)을 참조하세요.

a. 백업 계획 일반 세부 정보

- 백업 계획 이름은 영숫자, 하이픈, 밑줄 문자로만 구성할 수 있습니다.
- 목록에서 하나 이상의 백업 계획 영역을 선택해야 합니다. 계획은 선택한 AWS 리전에서만 리소스를 백업할 수 있습니다.

b. AWS Backup 이 작동하는 방법 및 시기를 지정하는 하나 이상의 백업 규칙이 있습니다. 각 백업 규칙은 다음 사항을 정의합니다.

- 백업 빈도 및 백업을 수행할 수 있는 기간을 포함하는 일정.
- 사용할 백업 볼트의 이름입니다. 백업 볼트 이름은 영숫자, 하이픈, 밑줄 문자로만 구성할 수 있습니다. 백업 볼트가 있어야 계획을 성공적으로 실행할 수 있습니다. AWS Backup 콘솔 또는 AWS CLI 명령을 사용하여 볼트를 생성합니다.
- (선택 사항) 하나 이상의 리전에 복사(Copy to region) 규칙을 사용하여 백업을 다른 AWS 리전의 볼트에 복사합니다.
- 이 백업 계획이 실행될 때마다 생성된 백업 복구 지점에 연결할 하나 이상의 태그 키/값 페어.
- 백업이 콜드 스토리지로 전환되는 시기와 백업이 만료되는 시기를 지정하는 수명 주기 옵션.

규칙 추가(Add rule)를 선택해 필요한 모든 규칙을 추가합니다.

백업 규칙에 대한 자세한 내용은 AWS Backup 개발자 안내서의 [백업 규칙](#)을 참조하세요.

c. AWS Backup 이 이 계획을 통해 백업해야 하는 리소스를 지정하는 리소스 할당. 할당은 리소스를 찾고 일치시키는 데 AWS Backup 사용하는 태그 페어를 지정하여 이루어집니다.

- 리소스 할당 이름은 영숫자, 하이픈, 밑줄 문자로만 구성될 수 있습니다.
- AWS Backup 이 이름을 기준으로 백업을 수행하는 데 사용할 IAM 역할을 지정합니다.

콘솔에서는 전체 Amazon 리소스 이름(ARN)을 지정하지 않습니다. 역할 이름과 역할 유형을 지정하는 접두사를 모두 포함해야 합니다. 접두사는 일반적으로 role 또는 service-role이며, 슬래시(/)로 역할 이름과 구분합니다. 예를 들어 role/MyRoleName 또는 service-role/MyManagedRoleName을 입력할 수 있습니다. 이는 기본 JSON에 저장될 때 전체 ARN으로 변환됩니다.

⚠ Important

지정된 IAM 역할은 정책이 적용되는 계정에 이미 존재해야 합니다. 그렇지 않으면 백업 계획이 백업 작업을 성공적으로 시작할 수 있지만 이러한 백업 작업은 실패합니다.

- 백업할 리소스를 식별하기 위해 하나 이상의 리소스 태그 키 및 태그 값 페어를 지정합니다. 태그 값이 두 개 이상인 경우 쉼표로 값을 구분합니다.

할당 추가(Add assignment)를 선택해, 구성된 각 리소스 할당을 백업 계획에 추가합니다.

자세한 내용은 AWS Backup 개발자 안내서의 [백업 계획에 리소스 할당](#)을 참조하세요.

6. 정책 작성을 마쳤으면 정책 생성(Create policy)을 선택합니다. 정책이 사용 가능한 백업 정책 목록에 나타납니다.

AWS CLI & AWS SDKs

백업 정책을 생성하려면

다음 중 하나를 사용하여 백업 정책을 생성할 수 있습니다.

- AWS CLI: [create-policy](#)

백업 계획을 다음과 유사한 JSON 텍스트로 생성해서 텍스트 파일에 저장합니다. 구문의 전체 규칙은 [백업 정책 구문 및 예제](#) 단원을 참조하세요.

```
{
  "plans": {
    "PII_Backup_Plan": {
      "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-north-1" ] },
      "rules": {
        "Hourly": {
          "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
          "start_backup_window_minutes": { "@@assign": "480" },
          "complete_backup_window_minutes": { "@@assign": "10080" },
          "lifecycle": {
            "move_to_cold_storage_after_days": { "@@assign": "180" },
            "delete_after_days": { "@@assign": "270" }
          }
        }
      }
    }
  }
}
```

```

        "target_backup_vault_name": { "@@assign": "FortKnox" },
        "copy_actions": {
            "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                "lifecycle": {
                    "move_to_cold_storage_after_days": { "@@assign":
"10" },
                    "delete_after_days": { "@@assign": "100" }
                }
            }
        },
        "selections": {
            "tags": {
                "datatype": {
                    "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                    "tag_key": { "@@assign": "dataType" },
                    "tag_value": { "@@assign": [ "PII" ] }
                }
            }
        }
    }
}

```

이 백업 계획은 AWS Backup이 지정된에 AWS 리전 있고 태그 값이 AWS 계정 dataType인 영향을 받는의 모든 리소스를 백업하도록 지정합니다PII.

다음으로, JSON 정책 파일 백업 계획을 가져와 조직에 새 백업 정책을 생성합니다. 출력에서 정책 ARN의 끝에 있는 정책 ID를 확인합니다.

```

$ aws organizations create-policy \
  --name "MyBackupPolicy" \
  --type BACKUP_POLICY \
  --description "My backup policy" \
  --content file://policy.json{
  "Policy": {
    "PolicySummary": {
      "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
      "Description": "My backup policy",

```

```

        "Name": "MyBackupPolicy",
        "Type": "BACKUP_POLICY"
    }
    "Content": "...a condensed version of the JSON policy document you
provided in the file...",
    }
}

```

- AWS SDKs: [CreatePolicy](#)

태그 정책 생성

최소 권한

태그 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- `organizations:CreatePolicy`

다음 두 가지 방법 중 하나로 AWS Management Console 에서 태그 정책을 생성할 수 있습니다.

- 사용자가 옵션을 선택하면 자동으로 JSON 정책 텍스트를 생성하는 시각적 편집기.
- 사용자가 직접 JSON 정책 텍스트를 작성할 수 있는 텍스트 편집기.

시각적 편집기를 사용하면 프로세스를 쉽게 수행할 수 있지만 유연성은 제한됩니다. 이는 처음 정책을 생성하여 편안하게 사용할 수 있는 좋은 방법입니다. 정책이 어떻게 작동하는지 이해하고 시각적 편집기가 제공하는 기능에 의해 제한되기 시작하면 JSON 정책 텍스트를 직접 편집하여 정책에 고급 기능을 추가할 수 있습니다. 시각적 편집기는 [@@assign value-setting 연산자](#)만 사용하며, [하위 제어 연산자](#)에 대한 액세스 권한을 제공하지 않습니다. 하위 제어 연산자는 JSON 정책 텍스트를 수동으로 편집하는 경우에만 추가할 수 있습니다.

AWS Management Console

다음 두 가지 방법 중 하나로 AWS Management Console 에서 태그 정책을 생성할 수 있습니다.

- 사용자가 옵션을 선택하면 자동으로 JSON 정책 텍스트를 생성하는 시각적 편집기.
- 사용자가 직접 JSON 정책 텍스트를 작성할 수 있는 텍스트 편집기.

시각적 편집기를 사용하면 프로세스를 쉽게 수행할 수 있지만 유연성은 제한됩니다. 이는 처음 정책을 생성하여 편안하게 사용할 수 있는 좋은 방법입니다. 정책이 어떻게 작동하는지 이해하고 시각적 편집기가 제공하는 기능에 의해 제한되기 시작하면 JSON 정책 텍스트를 직접 편집하여 정책에 고급 기능을 추가할 수 있습니다. 시각적 편집기는 [@@assign value-setting 연산자](#)만 사용하며, [하위 제어 연산자](#)에 대한 액세스 권한을 제공하지 않습니다. 하위 제어 연산자는 JSON 정책 텍스트를 수동으로 편집하는 경우에만 추가할 수 있습니다.

태그 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [태그 정책\(Tag policies\)](#) 페이지에서 정책 생성(Create policy)을 선택합니다.
3. 정책 생성(Create policy) 페이지에서 정책 이름(Policy name) 및 정책 설명(Policy description)(선택 사항)을 입력합니다.
4. (선택 사항) 정책 객체 자체에 하나 이상의 태그를 추가할 수 있습니다. 이러한 태그는 정책에 포함되지 않습니다. 이렇게 하려면 태그 추가(Add tag)를 선택한 다음 키 및 값(선택 사항)을 입력합니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 정보는 [AWS Organizations 리소스 태그 지정](#) 섹션을 참조하세요.
5. 이 절차의 설명과 같이 시각적 편집기를 사용하여 태그 정책을 빌드할 수 있습니다. JSON 탭에서 태그 정책을 입력하거나 붙여 넣을 수도 있습니다. 태그 정책 구문에 대한 자세한 내용은 [태그 정책 구문](#) 단원을 참조하세요.

시각적 편집기를 사용하도록 선택한 경우 다음을 지정합니다.

6. 새 태그 키 1(New tag key 1)에서 추가할 태그 키의 이름을 지정합니다.
7. 규정 준수 옵션에서 다음 옵션을 선택할 수 있습니다.
 - a. 태그 키에 위에서 지정한 대소문자를 사용합니다. 상속된 상위 태그 정책이 있는 경우 해당 정책이 태그 키의 대/소문자 처리를 정의하도록 지정하려면 이 옵션을 선택 취소된(기본값) 상태로 둡니다.

이 정책을 사용하여 태그 키에 특정 대소문자를 강제하려면 이 옵션을 활성화합니다. 이 옵션을 선택하면 태그 키에 대해 지정한 대소문자 처리가 상속된 상위 정책에 지정된 대소문자 처리를 재정의합니다.

상위 정책이 존재하지 않고 이 옵션을 활성화하지 않으면 모든 소문자의 태그 키만 정책을 준수하는 것으로 간주됩니다. 상위 정책으로부터의 상속에 관한 자세한 내용은 [관리 정책 상속에 대한 이해](#) 단원을 참조하세요.

 Tip

태그 키와 해당 대소문자 처리를 정의하는 태그 키를 생성할 때 [예제 1: 조직 전체의 태그 키 사례 정의](#)에 표시된 태그 정책 예제를 가이드로 사용할 수 있습니다. 이 태그 정책을 조직 루트에 연결합니다. 나중에 추가 태그 정책을 생성하고 OU 또는 계정에 연결하여 추가 태그 규칙을 생성할 수 있습니다.

- b. 이 태그 키에 허용되는 값을 지정합니다. 해당 태그 키에 허용되는 값을 상위 정책에서 상속된 모든 값에 추가하려면 이 옵션을 활성화합니다.

기본적으로 이 옵션은 선택 취소되어 있으므로 상위 정책에서 정의되고 상속된 값만 정책을 준수하는 것으로 간주됩니다. 상위 정책이 없거나 태그 값을 지정하지 않는 경우 모든 값(값 없음 포함)이 정책을 준수하는 것으로 간주됩니다.

허용 가능한 태그 값 목록을 업데이트하려면 이 태그 키에 허용되는 값 지정(Specify allowed values for this tag key)을 선택한 다음 값 지정(Specify values)을 선택합니다. 메시지가 표시되면 새 값(상자당 하나의 값)을 입력하고 변경 사항 저장(Save changes)을 선택합니다.

8. 적용할 리소스 유형에서 이 태그에 대한 정책 미준수 작업 금지를 선택할 수 있습니다.

태그 정책을 사용한 경험이 없으면 이 옵션을 선택 취소(기본값)된 상태로 두는 것이 좋습니다. [태그 지정 일관성 적용](#)에서 권장 사항을 검토했는지 확인하고 철저히 테스트합니다. 그렇지 않으면 조직의 계정에 있는 사용자가 필요한 리소스에 태그를 지정하지 못하도록 할 수 있습니다.

이 태그 키에 정책 준수를 적용하지 않으려면 확인란을 선택한 다음 리소스 유형 지정(Specify resource types)을 선택합니다. 메시지가 표시되면 정책에 포함할 리소스 유형을 선택합니다. 변경 사항 저장(Save changes)을 선택합니다.

 Important

이 옵션을 선택하면 지정된 유형의 리소스에 대한 태그를 조작하는 모든 작업은 해당 작업의 결과로 태그가 정책을 준수하게 되는 경우에만 성공합니다.

9. (선택 사항) 이 태그 정책에 다른 태그 키를 추가하려면 태그 키 추가를 선택합니다. 그런 다음 6~9단계를 수행하여 태그 키를 정의합니다.
10. 태그 정책 빌드를 완료하면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

태그 정책을 생성하려면

다음 중 하나를 사용하여 태그 정책을 생성할 수 있습니다.

- AWS CLI: [create-policy](#)

어떤 텍스트 편집기든 사용하여 태그 정책을 생성할 수 있습니다. JSON 구문을 사용하여 태그 정책을 선택한 위치에 어떤 이름과 확장명으로든 파일로 저장합니다. 태그 정책은 공백을 포함하여 최대 2,500자를 사용할 수 있습니다. 태그 정책 구문에 대한 자세한 내용은 [태그 정책 구문](#) 단원을 참조하세요.

태그 정책을 생성하려면

1. 텍스트 파일에 다음과 유사한 태그 정책을 만듭니다.

testpolicy.json의 콘텐츠:

```
{
  "tags": {
    "CostCenter": {
      "tag_key": {
        "@@assign": "CostCenter"
      }
    }
  }
}
```

이 태그 정책은 CostCenter 태그 키를 정의합니다. 태그는 어떠한 값이든 수락하거나 값을 수락하지 않을 수 있습니다. 이와 같은 정책은 값이 있거나 없는 CostCenter 태그가 연결된 리소스가 규정을 준수함을 의미합니다.

2. 파일의 정책 콘텐츠를 담은 정책을 생성합니다. 읽기 쉽도록 출력의 여분의 공백을 잘랐습니다.

```
$ aws organizations create-policy \
```

```
--name "MyTestTagPolicy" \
--description "My Test policy" \
--content file://testpolicy.json \
--type TAG_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-a1b2c3d4e5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/tag_policy/p-a1b2c3d4e5",
      "Name": "MyTestTagPolicy",
      "Description": "My Test policy",
      "Type": "TAG_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\n\":{\n\"CostCenter\"\n}\n}\n}\n}\n}"
  }
}
```

- AWS SDKs: [CreatePolicy](#)

채팅 애플리케이션 정책 생성

최소 권한

채팅 애플리케이션 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- `organizations:CreatePolicy`

AWS Management Console

다음 두 가지 방법 중 하나로 AWS Management Console 에서 채팅 애플리케이션 정책을 생성할 수 있습니다.

- 사용자가 옵션을 선택하면 자동으로 JSON 정책 텍스트를 생성하는 시각적 편집기.
- 사용자가 직접 JSON 정책 텍스트를 작성할 수 있는 텍스트 편집기.

시각적 편집기를 사용하면 프로세스를 쉽게 수행할 수 있지만 유연성은 제한됩니다. 이는 처음 정책을 생성하여 편안하게 사용할 수 있는 좋은 방법입니다. 정책이 어떻게 작동하는지 이해하고 시

각적 편집기가 제공하는 기능에 의해 제한되기 시작하면 JSON 정책 텍스트를 직접 편집하여 정책에 고급 기능을 추가할 수 있습니다. 시각적 편집기는 [@@assign value-setting 연산자](#)만 사용하며, [하위 제어 연산자](#)에 대한 액세스 권한을 제공하지 않습니다. 하위 제어 연산자는 JSON 정책 텍스트를 수동으로 편집하는 경우에만 추가할 수 있습니다.

채팅 애플리케이션 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [채팅 정책](#) 페이지에서 정책 생성을 선택합니다.
3. [새 채팅 애플리케이션 정책 생성 페이지](#)에서 정책 이름 및 정책 설명(선택 사항)을 입력합니다.
4. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 정책에 하나 이상의 태그를 추가할 수 있습니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 내용은 [AWS Organizations 리소스 태그 지정](#) 단원을 참조하십시오.
5. 이 절차의 설명과 같이 시각적 편집기를 사용하여 정책을 작성할 수 있습니다. JSON 탭에서 정책 텍스트를 입력하거나 붙여 넣을 수도 있습니다. 채팅 애플리케이션 정책 구문에 대한 자세한 내용은 [채팅 애플리케이션 정책 구문 및 예제](#) 섹션을 참조하세요.

시각적 편집기를 사용하도록 선택한 경우 채팅 클라이언트에 대한 액세스 제어를 지정하여 채팅 애플리케이션 정책을 구성합니다.

a. Amazon Chime 채팅 클라이언트 액세스 설정에서 다음 중 하나 선택

- Chime 액세스 거부
- Chime 액세스 허용

b. Microsoft Teams 채팅 클라이언트 액세스 설정에서 다음 선택

- 모든 팀에 대한 액세스 거부
- 모든 팀에 대한 액세스 허용
- 이름이 지정된 팀에 대한 액세스 제한

c. Slack 채팅 클라이언트 액세스 설정에서 다음 중 하나 선택

- 모든 Slack 워크스페이스에 대한 액세스 거부
- 모든 Slack 워크스페이스에 대한 액세스 허용
- 이름이 지정된 Slack 워크스페이스에 대한 액세스 제한

Note

또한 채팅 애플리케이션의 Amazon Q Developer의 사용을 비공개 Slack 채널로만 제한하도록 선택할 수 있습니다.

d. IAM 권한 유형 설정에서 다음 옵션 선택

- 채널 수준 IAM 역할 활성화: 모든 채널 멤버는 채널에서 작업을 실행할 수 있는 IAM 역할 권한을 공유합니다. 채널 멤버에게 동일한 권한이 필요한 경우 채널 역할이 적합합니다.
- 사용자 수준 IAM 역할 활성화: 채널 구성원은 작업을 수행할 IAM 사용자 역할을 선택해야 합니다(역할을 선택하려면 콘솔 액세스 필요). 채널 멤버에게 다른 권한이 필요하고 사용자 역할을 선택할 수 있는 경우 사용자 역할이 적합합니다.

6. 정책 작성을 마쳤으면 정책 생성(Create policy)을 선택합니다. 정책이 사용 가능한 챗봇 정책 목록에 나타납니다.

AWS CLI & AWS SDKs

채팅 애플리케이션 정책을 생성하려면

다음 중 하나를 사용하여 채팅 애플리케이션 정책을 생성할 수 있습니다.

- AWS CLI: [create-policy](#)

어떤 텍스트 편집기든 사용하여 채팅 애플리케이션 정책을 생성할 수 있습니다. JSON 구문을 사용하여 채팅 애플리케이션 정책을 선택한 위치에 임의의 이름 및 확장명을 사용하여 파일로 저장합니다. 채팅 애플리케이션 정책은 공백을 포함하여 최대 255자를 사용할 수 있습니다. 태그 정책 구문에 대한 자세한 내용은 [채팅 애플리케이션 정책 구문 및 예제](#) 단원을 참조하세요.

채팅 애플리케이션 정책을 생성하려면

1. 텍스트 파일에 다음과 유사한 채팅 애플리케이션 정책을 만듭니다.

testpolicy.json의 콘텐츠:

```
{
  "chatbot": {
    "platforms": {
      "slack": {
        "client": {
          "@@assign": "enabled"
        }
      }
    }
  }
}
```

```

    },
    "workspaces": {
      "@@assign": [
        "Slack-Workspace-Id"
      ]
    },
    "default": {
      "supported_channel_types": {
        "@@assign": [
          "private"
        ]
      }
    }
  },
  "microsoft_teams": {
    "client": {
      "@@assign": "disabled"
    }
  }
}
}
}
}

```

이 채팅 애플리케이션 정책은 특정 워크스페이스의 프라이빗 Slack 채널만 허용하고 Microsoft Teams를 비활성화하며 모든 [역할 설정](#)을 지원합니다.

2. 파일의 정책 콘텐츠를 담은 정책을 생성합니다. 읽기 쉽도록 출력의 여분의 공백을 잘랐습니다.

```

$ aws organizations create-policy \
  --name "MyTestChatbotPolicy" \
  --description "My Test policy" \
  --content file://testpolicy.json \
  --type CHATBOT_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-a1b2c3d4e5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/chatbot_policy/p-a1b2c3d4e5",
      "Name": "MyTestChatApplicationsPolicy",
      "Description": "My Test policy",
      "Type": "CHATBOT_POLICY",

```

```

    "AwsManaged": false
  },
  "Content": "{\"chatbot\":{\"platforms\":{\"slack\":{\"client\":{\"@@assign\":\"enabled\"},\"workspaces\":{\"@@assign\":[\"Slack-Workspace-Id\"]},\"supported_channel_types\":{\"@@assign\":[\"private\"]}},\"microsoft_teams\":{\"client\":{\"@@assign\":\"disabled\"}}}}}"
}
}

```

- AWS SDKs: [CreatePolicy](#)

AI 서비스 옵트아웃 정책 생성

 최소 권한

AI 서비스 옵트아웃 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- organizations:CreatePolicy

AWS Management Console

AI 서비스 옵트아웃 정책을 만들려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AI 서비스 옵트아웃 정책\(AI services opt-out policies\)](#) 페이지에서 정책 생성(Create policy)을 선택합니다.
3. [새 AI 서비스 옵트아웃 정책 생성\(Create new AI services opt-out policy\) 페이지](#)에서 정책 이름과 정책 설명을 입력합니다. 정책 설명은 선택 사항입니다.
4. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 정책에 하나 이상의 태그를 추가할 수 있습니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 정보는 [AWS Organizations 리소스 태그 지정](#)을 참조하세요.
5. JSON 탭에 정책 텍스트를 입력하거나 붙여 넣습니다. AI 서비스 옵트아웃 정책 구문에 대한 자세한 내용은 [AI 서비스 옵트아웃 정책 구문 및 예제](#) 단원을 참조하세요. 시작점으로 사용할 수 있는 정책 예제를 보려면 [AI 서비스 옵트아웃 정책 예제](#) 단원을 참조하세요.

6. 정책 편집을 마쳤으면 페이지의 오른쪽 아래 모서리에 있는 정책 생성(Create policy)을 선택합니다.

AWS CLI & AWS SDKs

AI 서비스 옵트아웃 정책을 만들려면

다음 중 하나를 사용하여 태그 정책을 생성할 수 있습니다.

- AWS CLI: [create-policy](#)

1. 다음과 같은 AI 서비스 옵트아웃 정책을 작성하여 텍스트 파일에 저장합니다. “optOut”과 “optIn”은 대소문자를 구분합니다.

```
{
  "services": {
    "default": {
      "opt_out_policy": {
        "@@assign": "optOut"
      }
    },
    "rekognition": {
      "opt_out_policy": {
        "@@assign": "optIn"
      }
    }
  }
}
```

이 AI 서비스 옵트아웃 정책은 정책의 영향을 받는 모든 계정이 Amazon Rekognition을 제외한 모든 AI 서비스에서 옵트아웃되도록 지정합니다.

2. JSON 정책 파일을 가져와 조직에 새 정책을 생성합니다. 이 예제에서 이전 JSON 파일의 이름은 policy.json이었습니다.

```
$ aws organizations create-policy \
  --type AISERVICES_OPT_OUT_POLICY \
  --name "MyTestPolicy" \
  --description "My test policy" \
  --content file://policy.json
{
  "Policy": {
```

```

    "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign\":"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn\"}}}}",
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5"
      "Arn": "arn:aws:organizations:o-aa111bb222:policy/aiservices_opt_out_policy/p-i9j8k7l6m5",
      "Description": "My test policy",
      "Name": "MyTestPolicy",
      "Type": "AISERVICES_OPT_OUT_POLICY"
    }
  }
}

```

- AWS SDKs: [CreatePolicy](#)

업그레이드 롤아웃 정책 생성

최소 권한

업그레이드 롤아웃 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- `organizations:CreatePolicy`

AWS Management Console

업그레이드 롤아웃 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [롤아웃 정책 업그레이드](#) 페이지에서 정책 생성을 선택합니다.
3. [새 업그레이드 롤아웃 정책 생성 페이지에서](#) 정책 이름과 선택적 정책 설명을 입력합니다.
4. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 정책에 하나 이상의 태그를 추가할 수 있습니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 내용은 [AWS Organizations 리소스 태그 지정](#) 단원을 참조하십시오.

- 이 절차의 설명과 같이 시각적 편집기를 사용하여 정책을 작성할 수 있습니다. JSON 탭에서 정책 텍스트를 입력하거나 붙여 넣을 수도 있습니다. 자세한 내용은 [롤아웃 정책 구문 및 예제 업그레이드](#) 단원을 참조하십시오.

시각적 편집기를 사용하도록 선택한 경우 업그레이드 롤아웃 정책에 사용할 업그레이드 순서를 선택합니다. 업그레이드 주문에 대한 자세한 내용은 섹션을 참조하세요 [업그레이드 롤아웃 정책이란 무엇입니까?](#).

- 정책 순서 및 리소스의 메뉴에서 첫 번째, 두 번째 또는 마지막을 선택합니다.
- (선택 사항)이 정책을 사용하여 개별 리소스를 대상으로 지정하려면 특정 리소스 재정의의 선택한 다음 다음을 수행합니다.
 - 키에 재정의할 리소스의 이름을 입력합니다.
 - 값에 리소스의 ARN을 입력합니다.
 - 업그레이드 순서에서이 리소스에 적용해야 하는 기본 순서를 선택합니다.
 - 추가 리소스를 지정해야 하는 경우 태그 추가를 선택한 다음 이전 단계를 반복하여 태그 키를 정의합니다.
- 정책 편집을 마쳤으면 페이지의 오른쪽 아래 모서리에 있는 정책 생성(Create policy)을 선택합니다.

업그레이드 롤아웃 정책 목록에 새 정책이 나타납니다. 이제 [정책을 루트, OUs 또는 계정에 연결할 수 있습니다](#).

AWS CLI & AWS SDKs

업그레이드 롤아웃 정책을 생성하려면

다음 중 하나를 사용하여 업그레이드 롤아웃 정책을 생성할 수 있습니다.

- AWS CLI: [create-policy](#)

- 다음과 같은 업그레이드 롤아웃 정책을 생성하고 텍스트 파일에 저장합니다.

```
{
  "upgrade_rollout": {
    "default": {
      "patch_order": {
        "@@assign": "last"
      }
    }
  },
}
```

```

    "tags": {
      "my_patch_order_tag": {
        "tag_values": {
          "tag1": {
            "patch_order": {
              "@@assign": "first"
            }
          },
          "tag2": {
            "patch_order": {
              "@@assign": "second"
            }
          },
          "tag3": {
            "patch_order": {
              "@@assign": "last"
            }
          }
        }
      }
    }
  }
}

```

이 업그레이드 롤아웃 정책은 서비스가 리소스 전체에 자동 업그레이드를 적용하는 순서를 AWS 정의합니다. 업그레이드 롤아웃 정책 구문에 대한 자세한 내용은 [섹션을 참조하세요](#) [롤아웃 정책 구문 및 예제 업그레이드](#).

2. JSON 정책 파일을 가져와 조직에 새 정책을 생성합니다. 이 예제에서 이전 JSON 파일의 이름은 `policy.json`이었습니다.

```

$ aws organizations create-policy \
  --type UPGRADE_ROLLOUT_POLICY \
  --name "MyTestPolicy" \
  --description "My test policy" \
  --content file://policy.json
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/upgrade_rollout_policy/p-i9j8k7l6m5",
      "Name": "MyTestPolicy",

```



```

        "Description": "My test policy",
        "Type": "UPGRADE_ROLLOUT_POLICY",
        "AwsManaged": false
    },
    "Content": "{\n    \"upgrade_rollout\": {\n        \"default\": {\n            \"patch_order\": {\n                \"@@assign\": \"last\"\n            }\n        },\n        \"tags\": {\n            \"my_patch_order_tag\": {\n                \"tag_values\": {\n                    \"tag1\": {\n                        \"patch_order\": {\n                            \"@@assign\": \"first\"\n                        }\n                    },\n                    \"tag2\": {\n                        \"patch_order\": {\n                            \"@@assign\": \"second\"\n                        }\n                    },\n                    \"tag3\": {\n                        \"patch_order\": {\n                            \"@@assign\": \"last\"\n                        }\n                    }\n                }\n            }\n        }\n    }\n}"
    }
}

```

- AWS SDKs: [CreatePolicy](#)

Security Hub 정책 생성

최소 권한

Security Hub 정책을 생성하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- `organizations:CreatePolicy`

AWS Management Console

Security Hub 정책을 생성하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [Security Hub 정책](#) 페이지에서 정책 생성을 선택합니다.
3. [새 Security Hub 정책 생성](#) 페이지에서 정책 이름 및 정책 설명(선택 사항)을 입력합니다.
4. (선택 사항) 태그 추가(Add tags)를 선택한 다음 키 및 값(선택 사항)을 입력해 정책에 하나 이상의 태그를 추가할 수 있습니다. 값을 공백으로 남겨두면 null이 아닌 빈 문자열로 설정됩니다.

다. 한 정책에 최대 50개의 태그를 연결할 수 있습니다. 자세한 내용은 [AWS Organizations 리소스 태그 지정](#) 단원을 참조하십시오.

5. JSON 코드 상자에 정책 텍스트를 입력하거나 붙여 넣습니다. Security Hub 정책 구문에 대한 자세한 내용은 [Security Hub 정책 구문 및 예제](#) 단원을 참조하세요. 시작점으로 사용할 수 있는 정책 예제를 보려면 [Security Hub 정책 예제](#) 단원을 참조하세요.
6. 정책 편집을 마쳤으면 페이지의 오른쪽 아래 모서리에 있는 정책 생성(Create policy)을 선택합니다.

AWS CLI & AWS SDKs

Security Hub 정책을 생성하려면

다음 중 하나를 사용하여 Security Hub 정책을 생성할 수 있습니다.

- AWS CLI: [create-policy](#)

예: 지원되는 모든 리전에서 Security Hub를 활성화하는 정책 생성

다음 예제에서는 JSON 정책 텍스트가 포함된

testPolicy_enableAllSupportedRegions.json이라는 파일을 가정합니다. 이 파일은 새 Security Hub 정책을 생성하는 데 사용됩니다.

```
$ aws organizations create-policy \
  --content file:///./testPolicy_enableAllSupportedRegions.json \
  --name "testPolicy_enableAllSupportedRegions" \
  --description "Test policy to enable securityhub in ALL_SUPPORTED Regions" \
  --type SECURITYHUB_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-66ev7hgcvj",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/securityhub_policy/p-66ev7hgcvj",
      "Name": "testPolicy_enableAllSupportedRegions",
      "Description": "Test policy to enable securityhub in ALL_SUPPORTED Regions",
      "Type": "SECURITYHUB_POLICY",
      "AwsManaged": false
    },
  }
```

```

    "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":\n{\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ],\n    },\n    \"disable_in_regions\": {\n      \"@@assign\":[\n        \"us-east-1\"\n      ]\n    }\n  }\n}"
  }
}

```

예: 지원되는 모든 리전에서 Security Hub를 활성화하지만 us-east-1 리전에서는 비활성화하는 정책 생성

다음 예제에서는 JSON 정책 텍스트가 포함된

testPolicy_enableAllSupportedRegions_Disable_us-east-1.json이라는 파일을 가정합니다. 이 파일은 새 Security Hub 정책을 생성하는 데 사용됩니다.

```

$ aws organizations create-policy \
  --content file:///testPolicy_enableAllSupportedRegions_Disable_us-east-1.json \
  --name "testPolicy_enableAllSupportedRegions_Disable_us-east-1" \
  --description "Test policy to enable securityhub in ALL_SUPPORTED Regions but\ndisable in us-east-1 Region" \
  --type SECURITYHUB_POLICY
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-66217dwpos",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/securityhub_policy/p-66217dwpos",
      "Name": "testPolicy_enableAllSupportedRegions_Disable_us-east-1",
      "Description": "Test policy to enable securityhub in ALL_SUPPORTED Regions but disable in us-east-1 Region",
      "Type": "SECURITYHUB_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":\n{\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ],\n    },\n    \"disable_in_regions\": {\n      \"@@assign\":[\n        \"us-east-1\"\n      ]\n    }\n  }\n}"
  }
}

```

- AWS SDKs: [CreatePolicy](#)

를 사용하여 조직 정책 업데이트 AWS Organizations

정책 요구 사항이 변경되면 기존 정책을 업데이트할 수 있습니다.

이 주제에서는를 사용하여 정책을 업데이트하는 방법을 설명합니다 AWS Organizations. 정책은 그룹에 적용할 컨트롤을 정의합니다 AWS 계정.

주제

- [서비스 제어 정책\(SCP\) 업데이트](#)
- [리소스 제어 정책\(RCP\) 업데이트](#)
- [선언적 정책 업데이트](#)
- [백업 정책 업데이트](#)
- [태그 정책 업데이트](#)
- [채팅 애플리케이션 정책 업데이트](#)
- [AI 서비스 옵트아웃 정책 업데이트](#)
- [Security Hub 정책 업데이트](#)

서비스 제어 정책(SCP) 업데이트

조직의 관리 계정에 로그인하면, 정책의 이름을 변경하거나 내용을 변경할 수 있습니다. SCP 내용 변경은 연결된 모든 계정의 사용자, 그룹과 역할에 즉시 영향을 줍니다.

최소 권한

SCP를 업데이트하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "**")을 포함하는 Resource 요소를 가진 `organizations:UpdatePolicy`
- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "**")을 포함하는 Resource 요소를 가진 `organizations:DescribePolicy`

AWS Management Console

정책을 업데이트하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [서비스 제어 정책](#) 페이지에서 업데이트할 정책의 이름을 선택합니다.
3. 정책의 세부 정보 페이지에서 정책 편집(Edit policy)을 선택합니다.
4. 다음 중 원하는 변경을 수행합니다.
 - 정책 이름(Policy name)에 새 이름을 입력하여 정책 이름을 변경할 수 있습니다.
 - 정책 설명(Policy description)에 새 텍스트를 입력하여 설명을 변경할 수 있습니다.
 - 왼쪽 창에서 JSON 형식의 정책을 편집하여 정책 텍스트를 편집할 수 있습니다. 또는 오른쪽 편집기에서 문을 선택하고 컨트롤을 사용하여 해당 요소를 변경할 수도 있습니다. 각 컨트롤에 대한 자세한 내용은 이 주제 앞부분의 [SCP 프로시저 생성](#)을 참조하세요.
5. 작업을 마쳤으면 변경 내용 저장을 선택합니다.

AWS CLI & AWS SDKs

정책을 업데이트하려면

정책을 업데이트하려면 다음 명령 중 한 가지를 사용합니다.

- AWS CLI: [update-policy](#)

다음 예제에서는 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "MyRenamedPolicy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "Blocks all IAM actions",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    }
  }
}
```

```

    },
    "Content": "{\"Version\":\"2012-10-17\",          \"Statement\": [{\"Sid\":
\\\"Statement1\\\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\"*\"]}]}\"
  }
}

```

다음 예제에서는 서비스 제어 정책에 대한 설명을 추가하거나 변경합니다.

```

$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new policy description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "My new policy description",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",          \"Statement\": [{\"Sid\":
\\\"Statement1\\\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\"*\"]}]}\"
  }
}

```

다음 예제에서는 새 JSON 정책 텍스트를 포함한 파일을 지정하여 SCP의 정책 문서를 변경합니다.

```

$ aws organizations update-policy \
  --policy-id p-zlfw1r64
  --content file://MyNewPolicyText.json
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "My new policy description",
      "Type": "SERVICE_CONTROL_POLICY",

```

```

        "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",          \"Statement\": [{\"Sid\": \"AModifiedPolicy\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\"*\"]}]}"
    }
}

```

- AWS SDKs: [UpdatePolicy](#)

리소스 제어 정책(RCP) 업데이트

조직의 관리 계정에 로그인하면, 정책의 이름을 변경하거나 내용을 변경할 수 있습니다. RCP 내용 변경은 연결된 모든 계정의 모든 리소스에 즉시 영향을 줍니다.

최소 권한

RCP를 업데이트하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 `organizations:UpdatePolicy`
- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 `organizations:DescribePolicy`

AWS Management Console

정책을 업데이트하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 리소스 제어 정책 페이지에서 업데이트할 정책의 이름을 선택합니다.
3. 정책의 세부 정보 페이지에서 정책 편집(Edit policy)을 선택합니다.
4. 다음 중 원하는 변경을 수행합니다.
 - 정책 이름(Policy name)에 새 이름을 입력하여 정책 이름을 변경할 수 있습니다.
 - 정책 설명(Policy description)에 새 텍스트를 입력하여 설명을 변경할 수 있습니다.

- 왼쪽 창에서 JSON 형식의 정책을 편집하여 정책 텍스트를 편집할 수 있습니다. 또는 오른쪽 편집기에서 문을 선택하고 컨트롤을 사용하여 해당 요소를 변경할 수도 있습니다. 각 컨트롤에 대한 자세한 내용은 이 주제 앞부분의 [RCP 프로시저 생성](#)을 참조하세요.

5. 작업을 마쳤으면 변경 내용 저장을 선택합니다.

AWS CLI & AWS SDKs

정책을 업데이트하려면

정책을 업데이트하려면 다음 명령 중 한 가지를 사용합니다.

- AWS CLI: [update-policy](#)

다음 예제에서는 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "MyRenamedPolicy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "Blocks all IAM actions",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\", \"Statement\": [{\"Sid\": \"Statement1\", \"Effect\": \"Deny\", \"Action\": [\"iam:*\"], \"Resource\": [\"*\"]}]}\""}
  }
}
```

다음 예제에서는 리소스 제어 정책에 대한 설명을 추가하거나 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new policy description"
{
  "Policy": {
```



```

    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "My new policy description",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",          \"Statement\": [{\"Sid\":
\\\"Statement1\\\", \\\"Effect\\\": \\\"Deny\\\", \\\"Action\\\": [\\\"iam:*\\\"], \\\"Resource\\\": [\\\"*\\\"]}]}"
  }
}

```

다음 예제에서는 새 JSON 정책 텍스트를 포함한 파일을 지정하여 RCP의 정책 문서를 변경합니다.

```

$ aws organizations update-policy \
  --policy-id p-zlfw1r64
  --content file://MyNewPolicyText.json
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
      "Name": "MyRenamedPolicy",
      "Description": "My new policy description",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"Version\":\"2012-10-17\",          \"Statement\": [{\"Sid\":
\\\"AModifiedPolicy\\\", \\\"Effect\\\": \\\"Deny\\\", \\\"Action\\\": [\\\"iam:*\\\"], \\\"Resource\\\": [\\\"*\\\"]}]}"
  }
}

```

- AWS SDKs: [UpdatePolicy](#)

선언적 정책 업데이트

최소 권한

선언적 정책을 업데이트하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.

- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 `organizations:UpdatePolicy`
- 동일한 정책 명령문에서 지정된 정책의 Amazon Resource Name(ARN)(또는 "*")을 포함하는 Resource 요소를 가진 `organizations:DescribePolicy`

AWS Management Console

선언적 정책을 업데이트하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [선언적 정책](#) 페이지에서 업데이트할 정책의 이름을 선택합니다.
3. 정책의 세부 정보 페이지에서 정책 편집(Edit policy)을 선택합니다.
4. 새 정책 이름, 정책 설명을 입력하거나, JSON 정책 텍스트를 편집할 수 있습니다. 선언적 정책 구문에 대한 자세한 내용은 [선언적 정책 구문 및 예시](#) 단원을 참조하세요.
5. 백업 정책 업데이트가 완료되면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

정책을 업데이트하려면

다음 중 하나를 사용하여 정책을 업데이트할 수 있습니다.

- AWS CLI: [update-policy](#)

다음 예제에서는 선언적 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "Renamed policy"
{
```

```

    "Policy": {
      "PolicySummary": {
        "Id": "p-i9j8k7l6m5",
        "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/declarative_policy_ec2/p-i9j8k7l6m5",
        "Name": "Renamed policy",
        "Type": "DECLARATIVE_POLICY_EC2",
        "AwsManaged": false
      },
      "Content": "{\"ec2-configuration\":{\"ec2_attributes\":{\"image_block_public_access\":{\"state\":{\"@@assign\":\"block_new_sharing\"}}}}\""}
    }
  }
}

```

다음 예제에서는 선언적 정책에 대한 설명을 추가하거나 변경합니다.

```

$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/declarative_policy_ec2/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Description": "My new description",
      "Type": "DECLARATIVE_POLICY_EC2",
      "AwsManaged": false
    },
    "Content": "{\"ec2_attributes\":{\"image_block_public_access\":{\"state\":{\"@@assign\":\"block_new_sharing\"}}}}\""}
  }
}

```

- AWS SDKs: [UpdatePolicy](#)

백업 정책 업데이트

조직의 관리 계정에 로그인하면 조직에서 변경이 필요한 정책을 편집할 수 있습니다.

i 최소 권한

백업 정책을 업데이트하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.

- 동일한 정책 명령문에서 업데이트할 정책의 ARN(또는 "**")을 포함하는 Resource 요소를 가진 `organizations:UpdatePolicy`
- 동일한 정책 명령문에서 업데이트할 정책의 ARN(또는 "**")을 포함하는 Resource 요소를 가진 `organizations:DescribePolicy`

AWS Management Console

백업 정책을 업데이트하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [백업 정책](#) 페이지에서 업데이트할 정책의 이름을 선택합니다.
3. 정책 편집을 선택합니다.
4. 새로운 정책 이름, 정책 설명을 입력할 수 있습니다. 정책 내용은 시각적 편집기를 사용하거나 JSON을 직접 편집해 변경할 수 있습니다.
5. 백업 정책 업데이트가 완료되면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

백업 정책을 업데이트하려면

다음 중 하나를 사용하여 백업 정책을 업데이트할 수 있습니다.

- AWS CLI: [update-policy](#)

다음 예제에서는 백업 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "Renamed policy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
```

```

        "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
        "Name": "Renamed policy",
        "Type": "BACKUP_POLICY",
        "AwsManaged": false
    },
    "Content": "{\\"plans\\":{\\"TestBackupPlan\\":{\\"regions\\":{\\"@@assign\\":
....TRUNCATED FOR BREVITY....  \\"@@assign\\":[\\"Yes\\"]}}}}}}}"
}
}

```

다음 예제에서는 백업 정책에 대한 설명을 추가하거나 변경합니다.

```

$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Description": "My new description",
      "Type": "BACKUP_POLICY",
      "AwsManaged": false
    },
    "Content": "{\\"plans\\":{\\"TestBackupPlan\\":{\\"regions\\":{\\"@@assign\\":
....TRUNCATED FOR BREVITY....  \\"@@assign\\":[\\"Yes\\"]}}}}}}}"
  }
}

```

다음 예제에서는 백업 정책에 연결된 JSON 정책 문서를 변경합니다. 이 예제에서 콘텐츠는 다음 텍스트를 포함한 policy.json이라는 파일에서 가져옵니다.

```

{
  "plans": {
    "PII_Backup_Plan": {
      "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
      "rules": {
        "Hourly": {

```

```

    "schedule_expression": { "@assign": "cron(0 5/1 ? * * *)" },
    "start_backup_window_minutes": { "@assign": "480" },
    "complete_backup_window_minutes": { "@assign": "10080" },
    "lifecycle": {
      "move_to_cold_storage_after_days": { "@assign": "180" },
      "delete_after_days": { "@assign": "270" },
      "opt_in_to_archive_for_supported_resources": {"@assign":
false}
    },
    "target_backup_vault_name": { "@assign": "FortKnox" },
    "copy_actions": {
      "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
        "lifecycle": {
          "move_to_cold_storage_after_days": { "@assign":
"10" },
          "delete_after_days": { "@assign": "100" },
          "opt_in_to_archive_for_supported_resources":
{"@assign": false}
        }
      }
    },
    "selections": {
      "tags": {
        "datatype": {
          "iam_role_arn": { "@assign": "arn:aws:iam::$account:role/
MyIamRole" },
          "tag_key": { "@assign": "dataType" },
          "tag_value": { "@assign": [ "PII" ] }
        }
      }
    }
  }
}

```

```

$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --content file://policy.json
{
  "Policy": {

```

```

    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Description": "My new description",
      "Type": "BACKUP_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n\"plans\":{\n\"TestBackupPlan\":{\n\"regions\":{\n\"@@assign\":
....TRUNCATED FOR BREVITY....    \"@@assign\":[\n\"Yes\"]}}}}}}}"
  }

```

- AWS SDKs: [UpdatePolicy](#)

태그 정책 업데이트

최소 권한

태그 정책을 업데이트하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.

- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "")을 포함하는 Resource 요소를 가진 `organizations:UpdatePolicy`
- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "")을 포함하는 Resource 요소를 가진 `organizations:DescribePolicy`

AWS Management Console

태그 정책을 업데이트하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [태그 정책\(Tag policies\)](#) 페이지에서 업데이트할 태그 정책을 선택합니다.
3. 정책 편집을 선택합니다.
4. 새로운 정책 이름, 정책 설명을 입력할 수 있습니다. 정책 내용은 시각적 편집기를 사용하거나 JSON을 편집해 변경할 수 있습니다.
5. 태그 정책 업데이트가 완료되면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

정책을 업데이트하려면

다음 중 하나를 사용하여 정책을 업데이트할 수 있습니다.

- AWS CLI: [update-policy](#)

다음 예제에서는 태그 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "Renamed tag policy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/tag_policy/p-i9j8k7l6m5",
      "Name": "Renamed tag policy",
      "Type": "TAG_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":\n\"CostCenter\"\n}\n}\n}\n}"
  }
}
```

다음 예제에서는 태그 정책에 대한 설명을 추가하거나 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new tag policy description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/tag_policy/p-i9j8k7l6m5",
      "Name": "Renamed tag policy",
      "Description": "My new tag policy description",
      "Type": "TAG_POLICY",
      "AwsManaged": false
    }
  }
}
```



```

    },
    "Content": "{\\n\\\"tags\\\":{\\n\\\"CostCenter\\\":{\\n\\\"tag_key\\\":{\\n\\\"@@assign\\\":\\n\\\"CostCenter\\\"\\n}\\n}\\n}\\n\\n}"
  }
}

```

다음 예제에서는 AI 서비스 옵트아웃 정책에 연결된 JSON 정책 문서를 변경합니다. 이 예제에서 콘텐츠는 다음 텍스트를 포함한 `policy.json`이라는 파일에서 가져옵니다.

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --content file://policy.json
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/tag_policy/p-i9j8k7l6m5",
      "Name": "Renamed tag policy",
      "Description": "My new tag policy description",
      "Type": "TAG_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":{\"Stage\\\"},\\\"tag_value\":{\"@@assign\":[\\\"Production\\\",\\\"Test\\\"]},\\\"enforced_for\":{\"@@assign\":[\\\"ec2:instance\\\"]}}}}}"
```

}

- AWS SDKs: [UpdatePolicy](#)

채팅 애플리케이션 정책 업데이트

최소 권한

채팅 애플리케이션 정책을 업데이트하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.

- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 `organizations:UpdatePolicy`
- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 `organizations:DescribePolicy`

AWS Management Console

채팅 애플리케이션 정책을 업데이트하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [채팅 정책](#) 페이지에서 업데이트할 채팅 애플리케이션 정책을 선택합니다.
3. 정책 편집을 선택합니다.
4. 새로운 정책 이름, 정책 설명을 입력할 수 있습니다. 정책 내용은 시각적 편집기를 사용하거나 JSON을 편집해 변경할 수 있습니다.
5. 태그 정책 업데이트가 완료되면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

정책을 업데이트하려면

다음 중 하나를 사용하여 정책을 업데이트할 수 있습니다.

- AWS CLI: [update-policy](#)

다음 예제에서는 채팅 애플리케이션 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "Renamed chat applications policy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-i9j8k7l6m5",
      "Name": "Renamed chat applications policy",
      "Type": "CHATBOT_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"chatbot\":{\"platforms\":{\"slack\":{\"client\":
{\"@@assign\":\"enabled\"},\"workspaces\":{\"@@assign\":[\"Slack-Workspace-Id\"],\"default\":
{\"supported_channel_types\":{\"@@assign\":[\"private\"]}}},\"microsoft_teams\":{\"client\":
{\"@@assign\":\"disabled\"}}}}}"
  }
}
```

- AWS SDKs: [UpdatePolicy](#)

AI 서비스 옵트아웃 정책 업데이트

최소 권한

AI 서비스 옵트아웃 정책을 업데이트하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.

- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "")을 포함하는 Resource 요소를 가진 `organizations:UpdatePolicy`
- 동일한 정책 명령문에서 지정된 정책의 Amazon Resource Name(ARN)(또는 "")을 포함하는 Resource 요소를 가진 `organizations:DescribePolicy`

AWS Management Console

AI 서비스 옵트아웃 정책을 업데이트하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AI 서비스 옵트아웃 정책\(AI services opt-out policies\)](#) 페이지에서 업데이트할 정책의 이름을 선택합니다.
3. 정책의 세부 정보 페이지에서 정책 편집(Edit policy)을 선택합니다.
4. 새 정책 이름, 정책 설명을 입력하거나, JSON 정책 텍스트를 편집할 수 있습니다. AI 서비스 옵트아웃 정책 구문에 대한 자세한 내용은 [AI 서비스 옵트아웃 정책 구문 및 예제](#) 단원을 참조하세요. 시작점으로 사용할 수 있는 정책 예제를 보려면 [AI 서비스 옵트아웃 정책 예제](#) 단원을 참조하세요.
5. 백업 정책 업데이트가 완료되면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

정책을 업데이트하려면

다음 중 하나를 사용하여 정책을 업데이트할 수 있습니다.

- AWS CLI: [update-policy](#)

다음 예제에서는 AI 서비스 옵트아웃 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --name "Renamed policy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/aiservices_opt_out_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Type": "AISERVICES_OPT_OUT_POLICY",
      "AwsManaged": false
    },
    "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
....TRUNCATED FOR BREVITY... :{\"@assign\":{\"optIn\"}}}}"
```

```
}
}
```

다음 예제에서는 AI 서비스 옵트아웃 정책에 대한 설명을 추가하거나 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --description "My new description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/aiservices_opt_out_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Description": "My new description",
      "Type": "AISERVICES_OPT_OUT_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n\"services\":{\n\"default\":{\n\"opt_out_policy\":\n....TRUNCATED FOR BREVITY...    :{\n\"@@assign\":{\n\"optIn\"}}}}}"
  }
}
```

다음 예제에서는 AI 서비스 옵트아웃 정책에 연결된 JSON 정책 문서를 변경합니다. 이 예제에서 콘텐츠는 다음 텍스트를 포함한 policy.json이라는 파일에서 가져옵니다.

```
{
  "services": {
    "default": {
      "opt_out_policy": {
        "@@assign": "optOut"
      }
    },
    "comprehend": {
      "opt_out_policy": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "@@assign": "optOut"
      }
    },
    "rekognition": {
      "opt_out_policy": {
```

```

        "@@assign": "optIn"
      }
    }
  }
}

```

```

$ aws organizations update-policy \
  --policy-id p-i9j8k7l6m5 \
  --content file://policy.json
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-i9j8k7l6m5",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/aiservices_opt_out_policy/p-i9j8k7l6m5",
      "Name": "Renamed policy",
      "Description": "My new description",
      "Type": "AISERVICES_OPT_OUT_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n\"services\": {\n\"default\": {\n\"    ....TRUNCATED FOR BREVITY....    \": \"optIn\"\n}\n}\n}"
  }
}

```

- AWS SDKs: [UpdatePolicy](#)

Security Hub 정책 업데이트

최소 권한

Security Hub 정책을 업데이트하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.

- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 `organizations:UpdatePolicy`
- 동일한 정책 명령문에서 지정된 정책의 Amazon Resource Name(ARN)(또는 "*")을 포함하는 Resource 요소를 가진 `organizations:DescribePolicy`

AWS Management Console

Security Hub 정책을 업데이트하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [Security Hub 정책](#) 페이지에서 업데이트할 정책의 이름을 선택합니다.
3. 정책의 세부 정보 페이지에서 정책 편집(Edit policy)을 선택합니다.
4. 새 정책 이름, 정책 설명을 입력하거나, JSON 정책 텍스트를 편집할 수 있습니다. Security Hub 정책 구문에 대한 자세한 내용은 [Security Hub 정책 구문 및 예제](#) 단원을 참조하세요. 시작점으로 사용할 수 있는 정책 예제를 보려면 [Security Hub 정책 예제](#) 단원을 참조하세요.
5. 백업 정책 업데이트가 완료되면 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

정책을 업데이트하려면

다음 중 하나를 사용하여 정책을 업데이트할 수 있습니다.

- AWS CLI: [update-policy](#)

다음 예제에서는 Security Hub 정책의 이름을 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-66ev7hgcvj \
  --name "Renamed policy"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-66ev7hgcvj",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/securityhub_policy/p-66ev7hgcvj",
      "Name": "Renamed policy",
      "Type": "SECURITYHUB_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":\n{\n      \"@assign\": [\n        \"ALL_SUPPORTED\"\n      ]\n    },\n    \"disable_in_regions\": {\n      \"@assign\": [\n      ]\n    }\n  }\n}"
  }
}
```

}

다음 예제에서는 Security Hub 정책에 대한 설명을 추가하거나 변경합니다.

```
$ aws organizations update-policy \
  --policy-id p-66ev7hgcvj \
  --name "My new description"
{
  "Policy": {
    "PolicySummary": {
      "Id": "p-66ev7hgcvj",
      "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/securityhub_policy/p-66ev7hgcvj",
      "Name": "My new description",
      "Type": "SECURITYHUB_POLICY",
      "AwsManaged": false
    },
    "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":\n  {\n    \"@assign\": [\n      \"ALL_SUPPORTED\"\n    ]\n  },\n  \"disable_in_regions\": {\n    \"@assign\": []\n  }\n}\n}"
  }
}
```

- AWS SDKs: [UpdatePolicy](#)

를 사용하여 조직 정책에 연결된 태그 편집 AWS Organizations

이 주제에서는를 사용하여 태그가 연결된 정책을 편집하는 방법을 설명합니다 AWS Organizations. 정책은 AWS 계정그룹에 적용할 컨트롤을 정의합니다.

주제

- [서비스 제어 정책\(SCP\)에 연결된 태그 편집](#)
- [리소스 제어 정책\(RCP\)에 연결된 태그 편집](#)
- [선언적 정책에 연결된 태그 편집](#)
- [백업 정책에 연결된 태그 편집](#)
- [태그 정책에 연결된 태그 편집](#)
- [채팅 애플리케이션 정책에 연결된 태그 편집](#)
- [AI 서비스 옵트아웃 정책에 연결된 태그 편집](#)

- [Security Hub 정책에 연결된 태그 편집](#)

서비스 제어 정책(SCP)에 연결된 태그 편집

조직의 관리 계정으로 로그인하여 SCP에 연결된 태그를 추가하거나 제거할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요 [AWS Organizations 리소스 태그 지정](#)

최소 권한

조직의 SCP에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:DescribePolicy` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

SCP에 연결된 태그를 편집하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [서비스 제어 정책\(Service control policies\)](#) 페이지에서 편집할 태그가 있는 정책의 이름을 선택합니다.
3. 정책 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 다음 중 원하는 변경을 수행합니다.
 - 이전 값 대신 새 값을 입력하여 태그 값을 변경합니다. 태그 키는 직접 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제한 다음 새 키를 가진 태그를 추가해야 합니다.
 - 제거(Remove)를 선택하여 기존 태그를 제거합니다.
 - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 null이 아닌 빈 문자열이 됩니다.

5. 작업을 마쳤으면 변경 내용 저장을 선택합니다.

AWS CLI & AWS SDKs

SCP에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 SCP에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: [tag-resource](#) 및 [untag-resource](#)
- AWS SDKs: [TagResource](#) 및 [UntagResource](#)

리소스 제어 정책(RCP)에 연결된 태그 편집

조직의 관리 계정으로 로그인하면 RCP에 연결된 태그를 추가하거나 제거할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요 [AWS Organizations 리소스 태그 지정](#)

최소 권한

AWS 조직의 RCP에 연결된 태그를 편집하려면 다음 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:DescribePolicy` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

RCP에 연결된 태그를 편집하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 리소스 제어 정책 페이지에서 편집할 태그가 있는 정책의 이름을 선택합니다.
3. 정책 세부 정보 페이지에서 태그 탭을 선택한 다음 태그 관리를 선택합니다.
4. 다음 중 원하는 변경을 수행합니다.

- 이전 값 대신 새 값을 입력하여 태그 값을 변경합니다. 태그 키는 직접 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제한 다음 새 키를 가진 태그를 추가해야 합니다.
- 제거(Remove)를 선택하여 기존 태그를 제거합니다.
- 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 null이 아닌 빈 문자열이 됩니다.

5. 작업을 마쳤으면 변경 내용 저장을 선택합니다.

AWS CLI & AWS SDKs

RCP에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 RCP에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: [tag-resource](#) 및 [untag-resource](#)
- AWS SDKs: [TagResource](#) 및 [UntagResource](#)

선언적 정책에 연결된 태그 편집

조직의 관리 계정으로 로그인하여 선언적 정책에 연결된 태그를 추가하거나 제거할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요 [AWS Organizations 리소스 태그 지정](#)

최소 권한

AWS 조직의 선언적 정책에 연결된 태그를 편집하려면 다음 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:DescribePolicy` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

선언적 정책에 연결된 태그를 편집하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [선언적 정책](#) 페이지에서 편집할 태그가 있는 정책의 이름을 선택합니다.
3. 선택한 정책의 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 이 페이지에서 다음과 같은 작업을 수행할 수 있습니다.
 - 이전 값 위에 새 값을 입력하여 태그의 값을 편집합니다. 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
 - 제거(Remove)를 선택하여 기존 태그를 제거합니다.
 - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 null이 아닌 빈 문자열이 됩니다.
5. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

선언적 정책에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 선언적 정책에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: [tag-resource](#) 및 [untag-resource](#)
- AWS SDKs: [TagResource](#) 및 [UntagResource](#)

백업 정책에 연결된 태그 편집

조직의 관리 계정으로 로그인하여 백업 정책에 연결된 태그를 추가하거나 제거할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요 [AWS Organizations 리소스 태그 지정](#)

최소 권한

조직의 백업 정책에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization`(콘솔만 해당 - 정책으로 이동하기 위해)

- `organizations:DescribePolicy`(콘솔만 해당 - 정책으로 이동하기 위해)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

백업 정책에 연결된 태그를 편집하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [백업 정책](#) 페이지
3. 편집할 태그가 있는 정책의 이름을 선택합니다.

정책 세부 정보 페이지가 나타납니다.

4. 태그 탭에서 태그 관리를 선택합니다.
5. 이 페이지에서 다음과 같은 작업을 수행할 수 있습니다.
 - 이전 값 위에 새 값을 입력하여 태그의 값을 편집합니다. 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
 - 제거(Remove)를 선택하여 기존 태그를 제거합니다.
 - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 null이 아닌 빈 문자열이 됩니다.
6. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

백업 정책에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 백업 정책에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: [tag-resource](#) 및 [untag-resource](#)
- AWS SDKs: [TagResource](#) 및 [UntagResource](#)

태그 정책에 연결된 태그 편집

조직의 관리 계정으로 로그인하여 태그 정책에 연결된 태그를 추가하거나 제거할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

최소 권한

조직의 태그 정책에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization`(콘솔만 해당 - 정책으로 이동하기 위해)
- `organizations:DescribePolicy`(콘솔만 해당 - 정책으로 이동하기 위해)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

태그 정책에 연결된 태그를 편집하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [태그 정책\(Tag policies\)](#) 페이지에서 편집할 태그가 있는 정책의 이름을 선택합니다.
3. 선택한 정책의 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 이 페이지에서 다음과 같은 작업을 수행할 수 있습니다.
 - 이전 값 위에 새 값을 입력하여 태그의 값을 편집합니다. 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
 - 제거(Remove)를 선택하여 기존 태그를 제거합니다.
 - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 null이 아닌 빈 문자열이 됩니다.
5. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

태그 정책에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 태그 정책에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: [tag-resource](#) 및 [untag-resource](#)
- AWS SDKs: [TagResource](#) 및 [UntagResource](#)

채팅 애플리케이션 정책에 연결된 태그 편집

조직의 관리 계정으로 로그인하면 채팅 애플리케이션 정책에 연결된 태그를 추가하거나 제거할 수 있습니다. 이렇게 하려면 다음 단계를 완료하세요.

최소 권한

조직의 채팅 애플리케이션 정책에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization`(콘솔만 해당 - 정책으로 이동하기 위해)
- `organizations:DescribePolicy`(콘솔만 해당 - 정책으로 이동하기 위해)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

채팅 애플리케이션 정책에 연결된 태그를 편집하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [채팅 정책](#) 페이지에서 편집하려는 태그가 있는 정책의 이름을 선택합니다.
3. 선택한 정책의 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 이 페이지에서 다음과 같은 작업을 수행할 수 있습니다.
 - 이전 값 위에 새 값을 입력하여 태그의 값을 편집합니다. 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
 - 제거(Remove)를 선택하여 기존 태그를 제거합니다.

- 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 null이 아닌 빈 문자열이 됩니다.
5. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

채팅 애플리케이션 정책에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 채팅 애플리케이션 정책에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: [tag-resource](#) 및 [untag-resource](#)
- AWS SDKs: [TagResource](#) 및 [UntagResource](#)

AI 서비스 옵트아웃 정책에 연결된 태그 편집

조직의 관리 계정으로 로그인하면 AI 서비스 옵트아웃 정책에 연결된 태그를 추가하거나 제거할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요 [AWS Organizations 리소스 태그 지정](#)

최소 권한

조직의 AI 서비스 옵트아웃 정책에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:DescribePolicy` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

AI 서비스 옵트아웃 정책에 연결된 태그를 편집하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

2. [AI 서비스 옵트아웃 정책\(AI services opt-out policies\)](#) 페이지에서 편집할 태그가 있는 정책의 이름을 선택합니다.
3. 선택한 정책의 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 이 페이지에서 다음과 같은 작업을 수행할 수 있습니다.
 - 이전 값 위에 새 값을 입력하여 태그의 값을 편집합니다. 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
 - 제거(Remove)를 선택하여 기존 태그를 제거합니다.
 - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 null이 아닌 빈 문자열이 됩니다.
5. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

AI 서비스 옵트아웃 정책에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 AI 서비스 옵트아웃 정책에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: [tag-resource](#) 및 [untag-resource](#)
- AWS SDKs: [TagResource](#) 및 [UntagResource](#)

Security Hub 정책에 연결된 태그 편집

조직의 관리 계정으로 로그인하여 Security Hub 정책에 연결된 태그를 추가하거나 제거할 수 있습니다. 태그 지정에 대한 자세한 내용은 단원을 참조하세요 [AWS Organizations 리소스 태그 지정](#)

최소 권한

조직의 Security Hub 정책에 연결된 태그를 편집하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:DescribeOrganization` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:DescribePolicy` – Organizations 콘솔을 사용하는 경우에만 필요합니다.
- `organizations:TagResource`

- `organizations:UntagResource`

AWS Management Console

Security Hub 정책에 연결된 태그를 편집하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [Security Hub 정책](#) 페이지에서 편집할 태그가 있는 정책의 이름을 선택합니다.
3. 선택한 정책의 세부 정보 페이지에서 태그(Tags) 탭을 선택한 다음 태그 관리(Manage tags)를 선택합니다.
4. 이 페이지에서 다음과 같은 작업을 수행할 수 있습니다.
 - 이전 값 위에 새 값을 입력하여 태그의 값을 편집합니다. 키는 수정할 수 없습니다. 키를 변경하려면 이전 키를 가진 태그를 삭제하고 새 키를 가진 태그를 추가해야 합니다.
 - 제거(Remove)를 선택하여 기존 태그를 제거합니다.
 - 새로운 태그 키 및 값 페어를 추가합니다. 태그 추가(Add tag)를 선택한 다음 제시되는 상자에 새로운 키 이름과 값을 입력합니다. 값은 선택 사항입니다. 값(Value) 상자를 비워두면 null이 아닌 빈 문자열이 됩니다.
5. 원하는 추가, 제거, 편집 작업을 모두 수행한 후 변경 사항 저장(Save changes)을 선택합니다.

AWS CLI & AWS SDKs

Security Hub 정책에 연결된 태그를 편집하려면

다음 명령 중 하나를 사용하여 Security Hub 정책에 연결된 태그를 편집할 수 있습니다.

- AWS CLI: [tag-resource](#) 및 [untag-resource](#)
- AWS SDKs: [TagResource](#) 및 [UntagResource](#)

를 사용하여 조직 정책 연결 AWS Organizations

이 주제에서는 AWS Organizations를 사용하여 정책을 연결하는 방법을 설명합니다. 정책은 그룹에 적용할 컨트롤을 정의합니다 AWS 계정.

주제

- [를 사용하여 정책 연결 AWS Organizations](#)

를 사용하여 정책 연결 AWS Organizations

최소 권한

정책을 연결하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.

- `organizations:AttachPolicy`

최소 권한

권한 부여 정책(SCP 또는 RCP)을 루트, OU 또는 계정에 연결하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- 동일한 정책 명령문에서 지정된 정책의 Amazon 리소스 이름(ARN)(또는 "*"), 루트의 ARN, 또는 정책을 연결할 루트, OU, 계정의 ARN을 포함하는 Resource 요소를 가진 `organizations:AttachPolicy`

AWS Management Console

Service control policies (SCPs)

정책으로 이동하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 SCP를 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 SCP를 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 SCP를 연결할 루트, OU, 계정을 찾아서 그 옆에 있는 확인란을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 ( 선택).
3. 정책 탭의 서비스 제어 정책에 대한 항목에서 연결을 선택합니다.
4. 원하는 정책을 찾아서 정책 연결(Attach policy)을 선택합니다.

정책 탭의 연결된 SCP 목록이 업데이트되어 새 추가 항목이 목록에 포함됩니다. 정책 변경은 즉시 적용되어 연결된 계정 또는 연결된 루트나 OU에 있는 모든 계정의 IAM 사용자와 역할이 가지는 권한에 영향을 줍니다.

정책으로 이동하여 SCP를 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [서비스 제어 정책](#) 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택).
5. 정책 연결을 선택합니다.

대상 탭의 연결된 SCP 목록이 업데이트되어 새 추가 항목이 목록에 포함됩니다. 정책 변경은 즉시 적용되어 연결된 계정 또는 연결된 루트나 OU에 있는 모든 계정의 IAM 사용자와 역할이 가지는 권한에 영향을 줍니다.

Resource control policies (RCPs)

정책으로 이동하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 RCP를 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 RCP를 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 RCP를 연결할 루트, OU, 계정을 찾아서 그 옆에 있는 확인란을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택).
3. 정책 탭의 리소스 제어 정책에 대한 항목에서 연결을 선택합니다.
4. 원하는 정책을 찾아서 정책 연결(Attach policy)을 선택합니다.

정책 탭의 연결된 RCP 목록이 업데이트되어 새 추가 항목이 목록에 포함됩니다. 정책 변경은 즉시 적용되어 연결된 계정 또는 연결된 루트나 OU에 있는 모든 계정의 리소스가 가지는 권한에 영향을 줍니다.

정책으로 이동하여 RCP를 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 리소스 제어 정책 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택).
5. 정책 연결을 선택합니다.

대상 탭의 연결된 RCP 목록이 업데이트되어 새 추가 항목이 목록에 포함됩니다. 정책 변경은 즉시 적용되어 연결된 계정 또는 연결된 루트나 OU에 있는 모든 계정의 리소스가 가지는 권한에 영향을 줍니다.

Declarative policies

정책을 탐색하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 선언적 정책을 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 선언적 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 연결할 루트, OU나 계정의 이름을 찾고 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택).
3. 정책 탭의 선언적 정책에 대한 항목에서 연결을 선택합니다.
4. 원하는 정책을 찾아서 정책 연결(Attach policy)을 선택합니다.

정책 탭의 연결된 선언적 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 선언적 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [선언적 정책](#) 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택).
5. 정책 연결을 선택합니다.

대상 탭의 연결된 선언적 정책 목록이 업데이트되어 새 추가 기능이 목록에 포함됩니다. 정책 변경은 즉시 적용됩니다.

Backup policies

정책을 탐색하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 백업 정책을 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 백업 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 연결할 루트, OU나 계정의 이름을 찾고 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택).
3. 정책 탭의 백업 정책에 대한 항목에서 연결을 선택합니다.
4. 원하는 정책을 찾아 정책 연결(Attach policy)을 선택합니다.

정책 탭의 연결된 백업 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 백업 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [백업 정책](#) 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택).
5. 정책 연결을 선택합니다.

대상 탭의 연결된 백업 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

Tag policies

정책을 탐색하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 태그 정책을 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 태그 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 연결할 루트, OU나 계정의 이름을 찾고 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택).
3. 정책 탭의 태그 정책에 대한 항목에서 연결을 선택합니다.
4. 원하는 정책을 찾아서 정책 연결(Attach policy)을 선택합니다.

정책 탭의 연결된 태그 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 태그 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [태그 정책](#) 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
5. 정책 연결을 선택합니다.

대상 탭의 연결된 태그 정책 목록이 업데이트되어 새 추가 기능이 목록에 포함됩니다. 정책 변경은 즉시 적용됩니다.

Chat applications policies

정책으로 이동하거나 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 채팅 애플리케이션 정책을 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 채팅 애플리케이션 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 연결할 루트, OU나 계정의 이름을 찾고 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 정책 탭의 채팅 애플리케이션 정책에 대한 항목에서 연결을 선택합니다.
4. 원하는 정책을 찾아서 정책 연결(Attach policy)을 선택합니다.

정책 탭의 연결된 채팅 애플리케이션 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 채팅 애플리케이션 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [채팅 정책](#) 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
5. 정책 연결을 선택합니다.

대상 탭의 연결된 채팅 애플리케이션 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

AI services opt-out policies

정책을 탐색하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 AI 서비스 옵트아웃 정책을 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 AI 서비스 옵트아웃 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 연결할 루트, OU나 계정의 이름을 찾고 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 정책 탭의 AI 서비스 옵트아웃 정책에 대한 항목에서 연결을 선택합니다.
4. 원하는 정책을 찾아 정책 연결(Attach policy)을 선택합니다.

정책 탭의 연결된 AI 서비스 옵트아웃 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 AI 서비스 옵트아웃 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AI 서비스 옵트아웃 정책](#) 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
5. 정책 연결을 선택합니다.

대상 탭의 연결된 AI 서비스 옵트아웃 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

Security Hub policies

정책을 탐색하거나, 정책을 연결하려는 루트, OU 또는 계정으로 이동하여 Security Hub 정책을 연결할 수 있습니다.

루트, OU 또는 계정으로 이동하여 Security Hub 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 연결할 루트, OU나 계정의 이름을 찾고 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 정책 탭의 Security Hub 정책에 대한 항목에서 연결을 선택합니다.
4. 원하는 정책을 찾아서 정책 연결(Attach policy)을 선택합니다.

정책 탭의 연결된 Security Hub 정책 목록이 업데이트되어 새로운 정책 추가를 반영합니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 Security Hub 정책을 연결하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [Security Hub 정책](#) 페이지에서 연결할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 연결(Attach)을 선택합니다.
4. 정책을 연결할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
5. 정책 연결을 선택합니다.

대상 탭의 연결된 Security Hub 정책 목록이 업데이트되어 새 추가 기능이 목록에 포함됩니다. 정책 변경은 즉시 적용됩니다.

AWS CLI & AWS SDKs

정책을 연결하려면

다음 코드 예시는 AttachPolicy의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
```

```

/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
    /// AttachPolicyAsync method to attach the policy to the root
    /// organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyId = "p-000000000";
        var targetId = "r-0000";

        var request = new AttachPolicyRequest
        {
            PolicyId = policyId,
            TargetId = targetId,
        };

        var response = await client.AttachPolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
        }
        else
        {
            Console.WriteLine("Was not successful in attaching the policy.");
        }
    }
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [AttachPolicy](#)를 참조하세요.

CLI

AWS CLI

정책을 루트, OU 또는 계정에 연결하는 방법

예시 1

다음 예시에서는 서비스 제어 정책(SCP)을 OU에 연결하는 방법을 보여줍니다.

```
aws organizations attach-policy
    --policy-id p-examplepolicyid111
    --target-id ou-examplerootid111-exampleouid111
```

예시 2

다음 예시에서는 계정에 서비스 제어 정책을 직접 연결하는 방법을 보여줍니다.

```
aws organizations attach-policy
    --policy-id p-examplepolicyid111
    --target-id 333333333333
```

- API 세부 정보는 AWS CLI 명령 참조의 [AttachPolicy](#)를 참조하세요.

Python

SDK for Python (Boto3)

 Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
    or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
```

```

        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise

```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [AttachPolicy](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```

TRY.
    lo_org->attachpolicy(
        iv_policyid = iv_policy_id
        iv_targetid = iv_target_id ).
    MESSAGE 'Policy attached to target.' TYPE 'I'.
CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to attach the policy.' TYPE 'E'.
CATCH /aws1/cx_orgpolicynotfoundex.
    MESSAGE 'The specified policy does not exist.' TYPE 'E'.
CATCH /aws1/cx_orgtargetnotfoundex.
    MESSAGE 'The specified target does not exist.' TYPE 'E'.
CATCH /aws1/cx_orgduplicateplyatta00.
    MESSAGE 'The policy is already attached to the target.' TYPE 'E'.
ENDTRY.

```

- API 세부 정보는 AWS SDK for SAP ABAP API 참조의 [AttachPolicy](#)를 참조하세요.

정책 변경은 즉시 적용되어 연결된 계정 또는 연결된 루트나 OU에 있는 모든 계정의 IAM 사용자와 역할이 가지는 권한에 영향을 줍니다.

를 사용하여 조직 정책 분리 AWS Organizations

이 주제에서는 AWS Organizations를 사용하여 정책을 분리하는 방법을 설명합니다. 정책은 그룹에 적용할 컨트롤을 정의합니다 AWS 계정.

주제

- [를 사용하여 정책 분리 AWS Organizations](#)

를 사용하여 정책 분리 AWS Organizations

최소 권한

조직 루트, OU 또는 계정에서 정책을 분리하려면 다음 작업을 실행할 수 있는 권한이 있어야 합니다.

- `organizations:DetachPolicy`

Note

마지막 권한 부여 정책(SCP 또는 RCP)은 루트, OU 또는 계정에서 분리할 수 없습니다. 모든 루트, OU, 계정에는 언제나 하나 이상의 SCP 및 RCP가 연결돼 있어야 합니다.

AWS Management Console

Service control policies (SCPs)

정책을 탐색하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 SCP를 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 SCP를 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

2. [AWS 계정](#) 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택). 루트, OU 또는 계정의 이름을 선택합니다.
3. 정책(Policies) 탭에서, 분리할 SCP 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

연결된 SCP의 목록이 업데이트됩니다. SCP 분리로 인해 발생하는 정책 변경은 즉시 적용됩니다. 예를 들어, SCP 분리는 이전에 연결된 계정이나 이전에 연결된 루트 또는 OU에 있는 계정의 IAM 사용자와 역할이 가지고 있는 권한에 즉시 영향을 미칩니다.

정책으로 이동하여 SCP를 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [서비스 제어 정책\(Service control policies\)](#) 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

연결된 SCP의 목록이 업데이트됩니다. SCP 분리로 인해 발생하는 정책 변경은 즉시 적용됩니다. 예를 들어, SCP 분리는 이전에 연결된 계정이나 이전에 연결된 루트 또는 OU에 있는 계정의 IAM 사용자와 역할이 가지고 있는 권한에 즉시 영향을 미칩니다.

Resource control policies (RCPs)

정책을 탐색하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 RCP를 분리할 수 있습니다. 엔터티에서 RCP를 분리한 후 해당 RCP는 현재 분리된 개체가 영향을 미쳤던 모든 리소스에 더 이상 적용되지 않습니다.

Note

RCPFullAWSAccess 정책을 분리할 수 없습니다.

RCPFullAWSAccess 정책은 루트, 모든 OU 및 조직의 모든 계정에 자동으로 연결됩니다.

이 정책은 분리할 수 없습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 RCP를 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택). 루트, OU 또는 계정의 이름을 선택합니다.
3. 정책 탭에서, 분리할 RCP 옆에 있는 라디오 버튼을 선택한 다음 분리를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

연결된 RCP의 목록이 업데이트됩니다. RCP 분리로 인해 발생하는 정책 변경은 즉시 적용됩니다. 예를 들어, RCP 분리는 이전에 연결된 계정이나 이전에 연결된 루트 또는 OU에 있는 계정의 IAM 사용자와 역할이 가지고 있는 권한에 즉시 영향을 미칩니다.

정책으로 이동하여 RCP를 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 리소스 제어 정책 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

연결된 RCP의 목록이 업데이트됩니다. RCP 분리로 인해 발생하는 정책 변경은 즉시 적용됩니다. 예를 들어, RCP 분리는 이전에 연결된 계정이나 이전에 연결된 루트 또는 OU에 있는 계정의 IAM 사용자와 역할이 가지고 있는 권한에 즉시 영향을 미칩니다.

Declarative policies

정책을 탐색하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 선언적 정책을 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 선언적 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택). 루트, OU 또는 계정의 이름을 선택합니다.
3. 정책 탭에서, 분리할 선언적 정책 옆에 있는 라디오 버튼을 선택한 다음 분리를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

연결된 선언적 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 선언적 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [선언적 정책](#) 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

연결된 선언적 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

Backup policies

정책을 탐색하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 백업 정책을 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 백업 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택). 루트, OU 또는 계정의 이름을 선택합니다.
3. 정책(Policies) 탭에서, 분리할 백업 정책 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

연결된 백업 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 백업 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [백업 정책\(Backup policies\)](#) 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

연결된 백업 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

Tag policies

정책을 탐색하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 태그 정책을 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 태그 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택). 루트, OU 또는 계정의 이름을 선택합니다.
3. 정책(Policies) 탭에서, 분리할 태그 정책 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

연결된 태그 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 태그 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [태그 정책\(Tag policies\)](#) 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

연결된 태그 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

Chat applications policies

정책으로 이동하거나 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 채팅 애플리케이션 정책을 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 채팅 애플리케이션 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택). 루트, OU 또는 계정의 이름을 선택합니다.
3. 정책 탭에서 분리하려는 채팅 애플리케이션 정책 옆에 있는 라디오 버튼을 선택한 다음 분리를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

연결된 채팅 애플리케이션 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 채팅 애플리케이션 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [채팅 정책](#) 페이지에서 루트, OU 또는 계정에서 분리하려는 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
(▶ 선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

연결된 채팅 애플리케이션 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

AI services opt-out policies

정책으로 이동하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 AI 서비스 옵트아웃 정책을 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 AI 서비스 옵트아웃 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

2. [AWS 계정](#) 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택). 루트, OU 또는 계정의 이름을 선택합니다.
3. 정책(Policies) 탭에서, 분리할 AI 서비스 옵트아웃 정책 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

연결된 AI 서비스 옵트아웃 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 AI 서비스 옵트아웃 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AI 서비스 옵트아웃 정책\(AI services opt-out policies\)](#) 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

연결된 AI 서비스 옵트아웃 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

Security Hub policies

정책을 탐색하거나, 정책을 분리하려는 루트, OU 또는 계정으로 이동하여 Security Hub 정책을 분리할 수 있습니다.

정책이 연결된 루트, OU 또는 계정으로 이동하여 Security Hub 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 분리할 루트, OU 또는 계정으로 이동합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다



선택). 루트, OU 또는 계정의 이름을 선택합니다.

3. 정책 탭에서 분리하려는 Security Hub 정책 옆에 있는 라디오 버튼을 선택한 다음 분리를 선택합니다.
4. 확인 대화 상자에서 정책 분리(Detach policy)를 선택합니다.

연결된 Security Hub 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

정책으로 이동하여 Security Hub 정책을 분리하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [Security Hub 정책](#) 페이지에서 루트, OU 또는 계정과 분리할 정책의 이름을 선택합니다.
3. 대상(Targets) 탭에서 정책을 분리할 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택합니다. 원하는 OU 또는 계정을 찾기 위해 OU를 확장해야 할 수도 있습니다
( 선택).
4. 분리를 선택합니다.
5. 확인 대화 상자에서 분리(Detach)를 선택합니다.

연결된 Security Hub 정책 목록이 업데이트됩니다. 정책 변경은 즉시 적용됩니다.

AWS CLI & AWS SDKs

정책을 연결하려면

다음 코드 예시는 DetachPolicy의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-000000000";
        var targetId = "r-0000";

        var request = new DetachPolicyRequest
        {
            PolicyId = policyId,
            TargetId = targetId,
        };

        var response = await client.DetachPolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
        }
        else
        {
            Console.WriteLine("Could not detach the policy.");
        }
    }
}
```


- API 세부 정보는 AWS SDK for .NET API 참조의 [DetachPolicy](#)를 참조하세요.

CLI

AWS CLI

정책을 루트, OU 또는 계정에서 분리하는 방법

다음 예시에서는 OU에서 정책을 분리하는 방법을 보여줍니다.

```
aws organizations detach-policy --target-id ou-examplerootid111-exampleouid111
--policy-id p-examplepolicyid111
```

- API 세부 정보는 AWS CLI 명령 참조의 [DetachPolicy](#)를 참조하세요.

Python

SDK for Python (Boto3)

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
    attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
```

```

logger.exception(
    "Couldn't detach policy %s from target %s.", policy_id, target_id
)
raise

```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [DetachPolicy](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```

TRY.
    lo_org->detachpolicy(
        iv_policyid = iv_policy_id
        iv_targetid = iv_target_id ).
    MESSAGE 'Policy detached from target.' TYPE 'I'.
CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to detach the policy.' TYPE 'E'.
CATCH /aws1/cx_orgpolicynotfoundex.
    MESSAGE 'The specified policy does not exist.' TYPE 'E'.
CATCH /aws1/cx_orgtargetnotfoundex.
    MESSAGE 'The specified target does not exist.' TYPE 'E'.
CATCH /aws1/cx_orgpolicynotattex.
    MESSAGE 'The policy is not attached to the target.' TYPE 'E'.
ENDTRY.

```

- API 세부 정보는 AWS SDK for SAP ABAP API 참조의 [DetachPolicy](#)를 참조하세요.

정책 변경은 즉시 적용되어 연결된 계정 또는 연결된 루트나 OU에 있는 모든 계정의 IAM 사용자와 역할 및 리소스가 가지는 권한에 영향을 줍니다.

조직의 정책에 대한 정보 가져오기

이 주제에서는 조직 내 정책에 대한 세부 정보를 확인하는 다양한 방법을 설명합니다. 이러한 절차는 모든 정책 유형에 적용됩니다. 해당 유형의 정책을 해당 조직 루트의 모든 엔터티에 연결하려면 먼저 조직 루트에서 정책 유형을 활성화해야 합니다.

주제

- [모든 정책 나열](#)
- [루트, OU, 계정에 연결된 정책 나열](#)
- [정책이 연결된 모든 루트, OU, 계정 나열](#)
- [정책 세부 정보 확인](#)

모든 정책 나열

최소 권한

조직 내 정책을 나열하려면 다음과 같은 권한이 있어야 합니다.

- `organizations:ListPolicies`

에서 또는 AWS Command Line Interface (AWS CLI) 명령 AWS Management Console 또는 AWS SDK 작업을 사용하여 조직의 정책을 볼 수 있습니다.

AWS Management Console

조직의 모든 정책을 나열하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [정책\(Policies\)](#) 페이지에서 나열할 정책을 선택합니다.

지정된 정책 유형이 활성화되어 있으면 조직에서 현재 사용 가능한 해당 유형의 모든 정책 목록이 콘솔에 표시됩니다.

3. [정책\(Policies\)](#) 페이지로 돌아가서 각 정책 유형에 대해 위의 과정을 반복합니다.

AWS CLI & AWS SDKs

다음 코드 예시는 ListPolicies의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
            Filter = "SERVICE_CONTROL_POLICY",
```

```

        MaxResults = 5,
    };

    var response = new ListPoliciesResponse();
    try
    {
        do
        {
            response = await client.ListPoliciesAsync(request);
            response.Policies.ForEach(p => DisplayPolicies(p));
            if (response.NextToken is not null)
            {
                request.NextToken = response.NextToken;
            }
        }
        while (response.NextToken is not null);
    }
    catch (AWSOrganizationsNotInUseException ex)
    {
        Console.WriteLine(ex.Message);
    }
}

/// <summary>
/// Displays information about the Organizations policies associated
/// with an organization.
/// </summary>
/// <param name="policy">An Organizations policy summary to display
/// information on the console.</param>
private static void DisplayPolicies(PolicySummary policy)
{
    string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

    Console.WriteLine(policyInfo);
}
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [ListPolicies](#)를 참조하십시오.

CLI

AWS CLI

특정 유형의 조직에 있는 모든 정책 목록을 검색하는 방법

다음 예시에서는 필터 파라미터로 지정된 SCP 목록을 가져오는 방법을 보여줍니다.

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

출력에는 요약 정보가 있는 정책 목록이 포함됩니다.

```
{
  "Policies": [
    {
      "Type": "SERVICE_CONTROL_POLICY",
      "Name": "AllowAllS3Actions",
      "AwsManaged": false,
      "Id": "p-examplepolicyid111",
      "Arn": "arn:aws:organizations::111111111111:policy/service_control_policy/p-examplepolicyid111",
      "Description": "Enables account admins to delegate permissions for any S3 actions to users and roles in their accounts."
    },
    {
      "Type": "SERVICE_CONTROL_POLICY",
      "Name": "AllowAllEC2Actions",
      "AwsManaged": false,
      "Id": "p-examplepolicyid222",
      "Arn": "arn:aws:organizations::111111111111:policy/service_control_policy/p-examplepolicyid222",
      "Description": "Enables account admins to delegate permissions for any EC2 actions to users and roles in their accounts."
    },
    {
      "AwsManaged": true,
      "Description": "Allows access to every operation",
      "Type": "SERVICE_CONTROL_POLICY",
      "Id": "p-FullAWSAccess",
      "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess",
      "Name": "FullAWSAccess"
    }
  ]
}
```

```
]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 [ListPolicies](#)를 참조하세요.

Python

SDK for Python (Boto3)

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [ListPolicies](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

 Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
TRY.
    oo_result = lo_org->listpolicies(          " oo_result is returned for
testing purposes. "
    iv_filter = iv_filter ).
    DATA(lt_policies) = oo_result->get_policies( ).
    MESSAGE 'Retrieved list of policies.' TYPE 'I'.
CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to list policies.' TYPE 'E'.
CATCH /aws1/cx_orgawsorgsnotinuseex.
    MESSAGE 'Your account is not a member of an organization.' TYPE 'E'.
ENDTRY.
```

- API 세부 정보는 AWS SDK for SAP ABAP API 참조의 [ListPolicies](#)를 참조하세요.

루트, OU, 계정에 연결된 정책 나열

 최소 권한

조직 내 루트, 조직 단위(OU) 또는 계정에 연결된 정책을 나열하려면 다음과 같은 권한이 있어야 합니다.

- 동일한 정책 명령문에서 지정된 대상의 Amazon 리소스 이름(ARN)(또는 "")을 포함하는 Resource 요소를 가진 `organizations:ListPoliciesForTarget`

AWS Management Console

지정된 루트, OU 또는 계정에 직접 연결된 모든 정책을 나열하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AWS 계정](#) 페이지에서 정책을 보려는 루트, OU 또는 계정의 이름을 선택합니다. 원하는 OU를 찾기 위해 OU를 확장해야 할 수도 있습니다 (▶ 선택).
3. 루트, OU 또는 계정 페이지에서 정책(Policies) 탭을 선택합니다.

정책 탭에는 해당 루트, OU 또는 계정에 연결된 모든 정책이 정책 유형별로 그룹화되어 표시됩니다.

AWS CLI & AWS SDKs

지정된 루트, OU 또는 계정에 직접 연결된 모든 정책 나열

다음 명령 중 하나를 사용하여 개체에 연결된 정책을 나열할 수 있습니다.

- AWS CLI: [list-policies-for-target](#)

다음 예제에서는 지정된 OU에 연결된 모든 서비스 제어 정책을 나열합니다. 루트, OU 또는 계정의 ID와 나열할 정책 유형을 모두 지정해야 합니다.

```
$ aws organizations list-policies-for-target \
  --target-id ou-a1b2-f6g7h222 \
  --filter SERVICE_CONTROL_POLICY
{
  "Policies": [
    {
      "Id": "p-FullAWSAccess",
      "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess",
      "Name": "FullAWSAccess",
      "Description": "Allows access to every operation",
      "Type": "SERVICE_CONTROL_POLICY",
      "AwsManaged": true
    }
  ]
}
```

}

- AWS SDKs: [ListPoliciesForTarget](#)

정책이 연결된 모든 루트, OU, 계정 나열

최소 권한

정책이 연결된 개체를 나열하려면 다음과 같은 권한이 있어야 합니다.

- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "**")을 포함하는 Resource 요소를 가진 `organizations:ListTargetsForPolicy`

AWS Management Console

지정된 정책이 연결된 모든 루트, OU, 계정을 나열하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [정책\(Policies\)](#) 페이지에서 정책 유형을 선택한 다음 연결을 검토하려는 정책의 이름을 선택합니다.
3. 대상(Targets) 탭을 선택하여 선택한 정책이 연결된 모든 루트, OU, 계정의 테이블을 표시합니다.

AWS CLI & AWS SDKs

지정된 정책이 연결된 모든 루트, OU, 계정을 나열하려면

다음 명령 중 하나를 사용하여 정책이 있는 개체를 나열할 수 있습니다.

- AWS CLI: [list-targets-for-policy](#)

다음 예제에서는 지정된 정책이 연결된 모든 루트, OU, 계정을 보여 줍니다.

```
$ aws organizations list-targets-for-policy \
  --policy-id p-FullAWSAccess
{
  "Targets": [
```

```

    {
      "TargetId": "ou-a1b2-f6g7h111",
      "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-f6g7h111",
      "Name": "testou2",
      "Type": "ORGANIZATIONAL_UNIT"
    },
    {
      "TargetId": "ou-a1b2-f6g7h222",
      "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-f6g7h222",
      "Name": "testou1",
      "Type": "ORGANIZATIONAL_UNIT"
    },
    {
      "TargetId": "123456789012",
      "Arn": "arn:aws:organizations::123456789012:account/o-aa111bb222/123456789012",
      "Name": "My Management Account (bisdavid)",
      "Type": "ACCOUNT"
    },
    {
      "TargetId": "r-a1b2",
      "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
      "Name": "Root",
      "Type": "ROOT"
    }
  ]
}

```

- AWS SDKs: [ListTargetsForPolicy](#)

정책 세부 정보 확인

최소 권한

정책 세부 정보를 표시하려면 다음과 같은 권한이 있어야 합니다.

- 동일한 정책 명령문에서 지정된 정책의 ARN(또는 "*")을 포함하는 Resource 요소를 가진 `organizations:DescribePolicy`

AWS Management Console

정책에 대한 세부 정보를 얻으려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [정책\(Policies\)](#) 페이지에서 검토하려는 정책의 정책 유형을 선택한 다음 정책의 이름을 선택합니다.

정책 페이지에는 ARN, 설명, 연결된 대상을 비롯해 정책에 대해 제공되는 정보가 표시됩니다.

- 내용(Content) 탭은 정책의 현재 내용을 JSON 형식으로 보여 줍니다.
- 대상(Targets) 탭에는 정책이 연결된 루트, OU, 계정의 목록이 표시됩니다.
- 태그(Tags) 탭에는 정책에 연결된 태그가 표시됩니다. 참고: AWS 관리형 정책은 태그(Tags) 탭을 이용할 수 없습니다.

정책을 편집하려면 정책 편집(Edit policy)을 선택합니다. 정책 유형마다 편집 요구 사항이 다르기 때문에 지정된 정책 유형의 정책 생성 및 업데이트에 대한 지침을 참조하세요.

AWS CLI & AWS SDKs

다음 코드 예시는 DescribePolicy의 사용 방법을 보여 줍니다.

CLI

AWS CLI

정책 정보 가져오기

다음 예시에서는 정책 정보를 요청하는 방법을 보여줍니다.

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

출력에는 정책의 세부 정보가 있는 정책 객체가 포함됩니다.

```
{
  "Policy": {
    "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*\"\n    }\n  ]\n}",
```

```

        "PolicySummary": {
            "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
            "Type": "SERVICE_CONTROL_POLICY",
            "Id": "p-examplepolicyid111",
            "AwsManaged": false,
            "Name": "AllowAllS3Actions",
            "Description": "Enables admins to delegate S3
permissions"
        }
    }
}

```

- API 세부 정보는 AWS CLI 명령 참조의 [DescribePolicy](#)를 참조하세요.

Python

SDK for Python (Boto3)

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```

def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy

```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [DescribePolicy](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
TRY.
    oo_result = lo_org->describepolicy(      " oo_result is returned for
testing purposes. "
    iv_policyid = iv_policy_id ).
    DATA(lo_policy) = oo_result->get_policy( ).
    MESSAGE 'Retrieved policy details.' TYPE 'I'.
CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to describe the policy.' TYPE 'E'.
CATCH /aws1/cx_orgpolicynotfoundex.
    MESSAGE 'The specified policy does not exist.' TYPE 'E'.
ENDTRY.
```

- API 세부 정보는 AWS SDK for SAP ABAP API 참조의 [DescribePolicy](#)를 참조하세요.

를 사용하여 조직 정책 삭제 AWS Organizations

정책이 더 이상 필요하지 않은 경우 모든 조직 단위(OU) 및 계정에서 정책을 분리한 후 삭제할 수 있습니다.

이 주제에서는를 사용하여 정책을 삭제하는 방법을 설명합니다 AWS Organizations. 정책은 그룹에 적용할 컨트롤을 정의합니다 AWS 계정.

주제

- [를 사용하여 정책 삭제 AWS Organizations](#)

를 사용하여 정책 삭제 AWS Organizations

조직의 관리 계정에 로그인하면 조직에서 더 이상 필요 없는 정책을 삭제할 수 있습니다.

정책을 삭제하기 전에 먼저 연결된 모든 개체에서 정책을 분리해야 합니다.

Note

- 라는 SCP와 같은 AWS 관리형 SCP는 삭제할 수 없습니다FullAWSAccess.
- 라는 RCP와 같은 AWS 관리형 RCP는 삭제할 수 없습니다RCPFullAWSAccess.

최소 권한

정책을 삭제하려면 다음 작업을 실행할 수 있는 권한이 필요합니다.

- organizations:DeletePolicy

AWS Management Console

Service control policies (SCPs)

SCP를 삭제하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [서비스 제어 정책\(Service control policies\)](#) 페이지에서 삭제할 SCP의 이름을 선택합니다.
3. 먼저 모든 루트, OU와 계정에서 삭제하려는 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제>Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제>Delete)를 선택합니다.

Resource control policies (RCPs)

RCP를 삭제하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [리소스 제어 정책](#) 페이지에서 삭제할 RCP의 이름을 선택합니다.
3. 먼저 모든 루트, OU, 계정에서 삭제하려는 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제>Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제>Delete)를 선택합니다.

Declarative policies

선언적 정책을 삭제하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [선언적 정책](#) 페이지에서 삭제할 정책의 이름을 선택합니다.
3. 먼저 모든 루트, OU, 계정에서 삭제하려는 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제>Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제>Delete)를 선택합니다.

Backup policies

백업 정책을 삭제하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [백업 정책](#) 페이지에서 삭제할 백업 정책의 이름을 선택합니다.

3. 먼저 모든 루트, OU와 계정에서 삭제하려는 백업 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제>Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제>Delete)를 선택합니다.

Tag policies

태그 정책을 삭제하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [태그 정책](#) 페이지에서 삭제할 정책을 선택합니다.
3. 먼저 모든 루트, OU와 계정에서 삭제하려는 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제>Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제>Delete)를 선택합니다.

Chat applications policies

채팅 애플리케이션 정책을 삭제하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [태그 정책](#) 페이지에서 삭제하려는 정책의 이름을 선택합니다.
3. 먼저 모든 루트, OU, 계정에서 삭제하려는 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제>Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제>Delete)를 선택합니다.

AI services opt-out policies

AI 서비스 옵트아웃 정책을 삭제하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [AI 서비스 옵트아웃 정책\(AI services opt-out policies\)](#) 페이지에서 삭제할 정책의 이름을 선택합니다.
3. 먼저 모든 루트, OU, 계정에서 삭제하려는 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제>Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제>Delete)를 선택합니다.

Security Hub policies

Security Hub 정책을 삭제하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [Security Hub 정책](#) 페이지에서 삭제하려는 정책의 이름을 선택합니다.
3. 먼저 모든 루트, OU, 계정에서 삭제하려는 정책을 분리해야 합니다. 대상(Targets) 탭을 선택하고 대상 목록에 표시된 각 루트, OU 또는 계정 옆에 있는 라디오 버튼을 선택한 다음 분리(Detach)를 선택합니다. 확인 대화 상자에서 분리(Detach)를 선택합니다. 모든 대상을 제거할 때까지 반복합니다.
4. 페이지 상단에서 삭제>Delete)를 선택합니다.
5. 확인 대화 상자에서 정책의 이름을 입력한 다음 삭제>Delete)를 선택합니다.

AWS CLI & AWS SDKs

정책을 삭제하려면

다음 코드 예시는 DeletePolicy의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-000000000";

        var request = new DeletePolicyRequest
        {
            PolicyId = policyId,
        };

        var response = await client.DeletePolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully deleted Policy: {policyId}.");
        }
    }
}
```

```

        else
        {
            Console.WriteLine($"Could not delete Policy: {policyId}.");
        }
    }
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [DeletePolicy](#)를 참조하십시오.

CLI

AWS CLI

정책을 삭제하는 방법

다음 예시에서는 조직에서 정책을 삭제하는 방법을 보여줍니다. 이 예시에서는 이전에 정책을 모든 엔터티에서 분리했다고 가정합니다.

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- API 세부 정보는 AWS CLI 명령 참조의 [DeletePolicy](#)를 참조하세요.

Python

SDK for Python (Boto3)

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```

def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.

```

```

"""
try:
    orgs_client.delete_policy(PolicyId=policy_id)
    logger.info("Deleted policy %s.", policy_id)
except ClientError:
    logger.exception("Couldn't delete policy %s.", policy_id)
    raise

```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [DeletePolicy](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```

TRY.
    lo_org->deletepolicy(
        iv_policyid = iv_policy_id ).
    MESSAGE 'Policy deleted.' TYPE 'I'.
CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to delete the policy.' TYPE 'E'.
CATCH /aws1/cx_orgpolicynotfoundex.
    MESSAGE 'The specified policy does not exist.' TYPE 'E'.
CATCH /aws1/cx_orgpolicyinuseex.
    MESSAGE 'The policy is still attached to one or more targets.' TYPE 'E'.
ENDTRY.

```

- API 세부 정보는 [AWS SDK for SAP ABAP API 참조](#)의 DeletePolicy를 참조하세요.

AWS Organizations 리소스 태그 지정

태그는 AWS 리소스를 쉽게 식별, 구성 및 검색할 수 있도록 리소스에 추가하는 사용자 지정 속성 레이블입니다. 각 태그는 두 부분으로 구성됩니다.

- 태그 키(예: CostCenter, Environment 또는 Project) 태그 키는 최대 128자이며 대/소문자를 구분합니다.
- 태그 값(예: 111122223333 또는 Production). 값은 최대 256자이며 태그 키와 같이 대/소문자를 구분합니다. 태그의 값을 빈 문자열로 설정할 수 있지만 태그의 값을 Null로 설정할 수는 없습니다. 태그 값을 생략하는 것은 빈 문자열을 사용하는 것과 같습니다.

태그 키 또는 값에 허용되는 문자에 대한 자세한 내용은 Resource Groups 태그 지정 API 참조에서 [태그 API의 태그 파라미터](#)를 참조하세요.

태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 자세한 내용은 [AWS 리소스 태그 지정 모범 사례를 참조하세요](#).

Tip

[태그 정책](#)을 사용하면 조직의 계정에 있는 리소스 전반에서 태그를 표준화할 수 있습니다.

주제

- [고려 사항](#)
- [태그 사용](#)
- [태그 추가, 업데이트 및 제거](#)

고려 사항

AWS Organizations 는 관리 계정에 로그인할 때 다음 태그 지정 작업을 지원합니다.

태그를 추가할 수 있는 조직 리소스

- AWS 계정
- 조직 단위
- 조직의 루트

- 정책

태그를 추가할 수 있는 시점

- [리소스를 생성할 때](#) — Organizations 콘솔에서 태그를 지정하거나 Create API 작업 중 하나에 Tags 파라미터를 사용합니다. 이는 조직의 루트에 적용되지 않습니다.
- [리소스를 생성한 후](#) — Organizations 콘솔을 사용하거나 [TagResource](#) 작업을 호출합니다.

기타 고려 사항

콘솔을 사용하거나 [ListTagsForResource](#) 작업을 호출 AWS Organizations 하역의 태그 지정 가능한 리소스에서 태그를 볼 수 있습니다.

콘솔을 사용하거나 [UntagResource](#) 작업을 호출하여 제거할 키를 지정하면 리소스에서 태그를 제거할 수 있습니다.

태그 사용

태그를 사용하면 유용한 범주별로 항목을 그룹화할 수 있어서 조직의 리소스를 구성하는 데 도움이 됩니다. 예를 들어 담당 부서를 추적하는 “부서(Department)” 태그를 할당할 수 있습니다. “환경(Environment)” 태그를 할당하면 주어진 리소스가 알파, 베타, 감마 또는 프로덕션 환경에 속하는지 추적할 수 있습니다.

태그를 사용하여 다음을 수행할 수도 있습니다.

- [리소스에 태깅 표준을 적용하세요.](#)
- [리소스에 액세스할 수 있는 제어.](#)

태그 추가, 업데이트 및 제거

조직의 관리 계정에 로그인하면 조직의 리소스에 태그를 추가할 수 있습니다.

리소스를 생성할 때 리소스에 태그 추가

최소 권한

리소스를 생성할 때 태그를 추가하려면 다음 권한이 필요합니다.

- 지정된 유형의 리소스를 생성할 수 있는 권한
- `organizations:TagResource`
- `organizations:ListTagsForResource` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

다음 리소스를 생성할 때 리소스에 연결되는 태그 키와 값을 포함할 수 있습니다.

- AWS 계정
 - [생성된 계정](#)
 - [초대된 계정](#)
- [조직 단위\(OU\)](#)
- 정책
 - [서비스 제어 정책](#)
 - [리소스 제어 정책](#)
 - [선언적 정책](#)
 - [백업 정책](#)
 - [태그 정책](#)
 - [채팅 애플리케이션 정책](#)
 - [AI 서비스 옵트아웃 정책](#)

조직 루트는 조직을 처음 만들 때 생성되므로 기존 리소스로만 태그를 추가할 수 있습니다.

기존 리소스에 대한 태그 추가 또는 업데이트

새 태그를 추가하거나 기존 리소스에 연결된 태그의 값을 업데이트할 수도 있습니다.

최소 권한

조직의 리소스에 태그를 추가하거나 업데이트하려면 다음 권한이 필요합니다.

- `organizations:TagResource`
- `organizations:ListTagsForResource` – Organizations 콘솔을 사용하는 경우에만 필요합니다.

조직의 리소스에서 태그를 제거하려면 다음 권한이 필요합니다.

- `organizations:UntagResource`

AWS Management Console

기존 리소스에 대한 태그를 추가, 업데이트 또는 제거하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 계정, 루트, OU 또는 정책을 탐색하여 선택하고 이름을 클릭해 세부 정보 페이지를 엽니다.
3. 태그 탭에서 태그 관리를 선택합니다.
4. 새 태그를 추가하거나, 기존 태그의 값을 수정하거나, 태그를 제거할 수 있습니다.

태그를 추가하려면 태그 추가(Add tag)를 선택한 다음 해당 태그에 대한 키와 값을 입력합니다. 값은 선택 사항입니다.

태그를 제거하려면 제거(Remove)를 선택합니다.

태그 키와 값은 대소문자를 구분합니다. 표준화하려는 대문자를 사용합니다. 또한 적용되는 태그 정책의 요구 사항을 준수해야 합니다.

5. 필요한 만큼 이전 단계를 반복합니다.
6. 변경 사항 저장을 선택합니다.

AWS CLI & AWS SDKs

태그를 업데이트하거나 기존 리소스에 추가하려면

다음 명령 중 하나를 사용하여 조직의 태그 지정 가능 리소스에 태그를 추가할 수 있습니다.

- AWS CLI: [tag-resource](#)
- AWS SDKs: [TagResource](#)

조직의 리소스에서 태그를 삭제하려면

다음 명령 중 하나를 사용하여 태그를 삭제할 수 있습니다.

- AWS CLI: [untag-resource](#)
- AWS SDKs: [UntagResource](#)

에 대한 다자간 승인 AWS Organizations

다자간 승인은 분산 승인 프로세스를 통해 사전 정의된 작업 목록을 보호할 수 있는 [AWS Organizations](#) 기능입니다. 다자간 승인을 사용하여 승인 워크플로를 설정하고 보안 프로세스를 팀 기반 의사 결정으로 변환합니다.

다자간 승인을 사용해야 하는 경우:

- '절대 신뢰하지 말고 항상 확인'이라는 제로 트러스트 원칙에 부합해야 하는 경우
- 적절한 사람이 올바른 방식으로 적절한 사물에 액세스할 수 있는지 확인해야 하는 경우
- 민감하거나 중요한 작업을 위해 분산된 의사 결정이 필요한 경우
- 민감하거나 중요한 리소스를 의도하지 않은 작업으로부터 보호해야 하는 경우
- 감사 또는 규정 준수를 위해 공식적인 검토 및 승인이 필요한 경우

자세한 내용은 다자간 승인 사용 설명서의 [다자간 승인이란 무엇입니까](#)를 참조하세요.

다른 AWS Organizations 와 함께 사용 AWS 서비스

신뢰할 수 있는 액세스를 사용하여 신뢰할 수 있는 AWS 서비스라고 하는 지정된 지원되는 서비스가 사용자를 대신하여 조직 및 해당 계정에서 작업을 수행할 수 있도록 할 수 있습니다. 이 과정에는 신뢰할 수 있는 서비스에 대한 권한 부여가 포함되지만 사용자 또는 역할에 대한 권한에는 달리 영향을 미치지 않습니다. 액세스를 활성화하면 신뢰할 수 있는 서비스는 필요할 때 언제든지 조직의 모든 계정에서 서비스 연결 역할(service-linked role)이라는 IAM 역할을 생성할 수 있습니다. 이 역할에는 신뢰할 수 있는 서비스가 해당 서비스의 설명서에 명시된 작업을 수행할 수 있도록 활성화하는 권한 정책이 있습니다. 따라서 신뢰할 수 있는 서비스가 사용자를 대신하여 사용자의 조직 계정으로 관리할 설정 및 구성 세부 정보를 지정할 수 있습니다. 신뢰할 수 있는 서비스는 조직의 모든 계정이 아니라 계정에 대한 관리 작업을 수행해야 하는 경우에만 서비스 연결 역할을 생성합니다.

Important

옵션을 사용할 수 있는 경우 신뢰할 수 있는 서비스의 콘솔 또는 AWS CLI 또는 API 작업과 동등한 것만 사용하여 신뢰할 수 있는 액세스를 활성화 및 비활성화하는 것이 좋습니다. 이렇게 하면 신뢰할 수 있는 액세스를 활성화할 때 신뢰할 수 있는 서비스가 모든 필수 리소스를 생성하는 등의 필요한 모든 초기화를 수행할 수 있으며, 신뢰할 수 있는 서비스를 비활성화할 때 필요한 모든 리소스 정리 작업을 수행할 수 있습니다.

신뢰할 수 있는 서비스를 사용해 조직에 대한 신뢰할 수 있는 서비스 액세스를 활성화하거나 비활성화하는 방법은 [AWS 서비스 와 함께 사용할 수 있는 AWS Organizations](#)의 신뢰할 수 있는 액세스 지원 열 아래에 있는 자세히 알아보기를 참조하세요.

Organizations 콘솔, CLI 명령 또는 API 작업을 사용하여 액세스를 비활성화하면 다음의 동작이 발생합니다.

- 조직 내 계정에서 더 이상 서비스 연결 역할을 만들 수 없습니다. 즉, 서비스가 사용자를 대신하여 조직의 새 계정에 대해 작업을 수행할 수 없습니다. 서비스는 서비스가 AWS Organizations의 정리를 완료할 때까지 이전 계정에서 작업을 계속 수행할 수 있습니다.
- 역할에 연결된 IAM 정책에서 작업을 명시적으로 허용하지 않는 한 서비스가 더 이상 조직의 멤버 계정에서 작업을 수행할 수 없습니다. 이러한 작업으로는 멤버 계정에서부터 관리 계정 또는 위임된 관리자 계정(해당하는 경우)에 이르는 모든 데이터의 집계도 있습니다.
- 일부 서비스는 이를 감지하고 통합과 관련된 나머지 데이터 또는 리소스를 정리하는 반면, 다른 서비스는 조직에 대한 액세스를 중지하되 통합의 재활성화를 지원하기 위해 기록 데이터 및 구성을 그대로 남겨둡니다.

그 대신 다른 서비스의 콘솔이나 명령을 사용하여 통합을 비활성화하면 다른 서비스가 통합에만 필요한 리소스를 정리할 수 있습니다. 서비스가 조직의 계정에서 리소스를 정리하는 방식은 해당 서비스에 따라 다릅니다. 자세한 내용은 다른 AWS 서비스의 설명서를 참조하세요.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한

신뢰할 수 있는 액세스에는 두 가지 서비스 AWS Organizations 및 신뢰할 수 있는 서비스에 대한 권한이 필요합니다. 신뢰할 수 있는 액세스를 활성화하려면 다음 시나리오 중 하나를 선택합니다.

- AWS Organizations 및 신뢰할 수 있는 서비스 모두에 권한이 있는 자격 증명이 있는 경우 신뢰할 수 있는 서비스에서 제공하는 도구(콘솔 또는 AWS CLI)를 사용하여 액세스를 활성화합니다. 이렇게 하면 서비스가 AWS Organizations 사용자를 대신하여에서 신뢰할 수 있는 액세스를 활성화하고 서비스가 조직에서 작동하는 데 필요한 리소스를 생성할 수 있습니다.

이러한 자격 증명에 필요한 최소 권한은 다음과 같습니다.

- `organizations:EnableAWSServiceAccess`. 이 작업에 `organizations:ServicePrincipal` 조건 키를 사용하여 승인된 서비스 보안 주체 이름의 목록에 대해 해당 작업이 수행하는 요청을 제한할 수 있습니다. 자세한 내용은 [조건 키](#) 단원을 참조하십시오.
- `organizations:ListAWSServiceAccessForOrganization` - AWS Organizations 콘솔을 사용하는 경우 필요합니다.
- 신뢰할 수 있는 서비스에서 필요한 최소 권한은 서비스에 따라 결정됩니다. 자세한 내용은 신뢰할 수 있는 서비스의 설명서를 참조하세요.
- 한 사람에게 권한이 있는 자격 증명을 가지고 AWS Organizations 있지만 다른 사람이 신뢰할 수 있는 서비스에서 권한이 있는 자격 증명을 가지고 있는 경우 다음 순서대로 다음 단계를 수행합니다.
 1. 에 권한이 있는 자격 증명이 있는 사람은 AWS Organizations 콘솔 AWS CLI, 또는 AWS SDK를 사용하여 신뢰할 수 있는 서비스에 대한 신뢰할 수 있는 액세스를 활성화 AWS Organizations 해야 합니다. 이렇게 하면 다음 단계(2단계)를 수행할 때 다른 서비스가 조직에서 필요한 권한을 수행할 수 있는 권한이 부여됩니다.

최소 AWS Organizations 권한은 다음과 같습니다.

- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization` - AWS Organizations 콘솔을 사용하는 경우에만 필요합니다.

에서 신뢰할 수 있는 액세스를 활성화하는 단계는 섹션을 AWS Organizations참조하세요 [신뢰할 수 있는 액세스를 활성화 또는 비활성화하는 방법](#).

2. 신뢰할 수 있는 서비스의 권한이 있는 자격 증명이 있는 사람이 해당 서비스를 AWS Organizations로 작업할 수 있도록 합니다. 이것은 해당 서비스에게 신뢰할 수 있는 서비스가 조직에서 작업하는 데 필요한 리소스 생성 같은 필요한 초기화를 수행하도록 지시하는 것입니다. 자세한 내용은 [AWS 서비스와 함께 사용할 수 있는 AWS Organizations](#)에서 서비스별 지침을 참조하세요.

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한

신뢰할 수 있는 서비스가 사용자의 조직이나 그 계정으로 작업하는 것을 중단하려면 다음 시나리오 중 하나를 선택하세요.

Important

신뢰할 수 있는 서비스 액세스를 비활성화한다고 해서 해당 권한이 있는 사용자와 역할이 해당 서비스를 사용하지 못하게 되는 것은 아닙니다. 사용자 및 역할이 AWS 서비스에 액세스하는 것을 완전히 차단하려면 해당 액세스 권한을 부여하는 IAM 권한을 제거하거나에서 [서비스 제어 정책\(SCPs\)](#) 사용할 수 있습니다 AWS Organizations.

SCP는 멤버 계정에만 적용할 수 있습니다. 관리 계정에는 SCP가 적용되지 않습니다. [관리 계정에서 서비스를 실행하지 않는 것이](#) 좋습니다. 그 대신 SCP를 사용하여 보안을 제어할 수 있는 멤버 계정에서 서비스를 실행합니다.

- AWS Organizations 및 신뢰할 수 있는 서비스 모두에 권한이 있는 자격 증명이 있는 경우 신뢰할 수 있는 서비스에 사용할 수 있는 도구(콘솔 또는 AWS CLI)를 사용하여 액세스를 비활성화합니다. 그러면 해당 서비스가 더 이상 필요하지 않는 리소스를 제거하고 사용자 대신 AWS Organizations에서 서비스에 대한 신뢰할 수 있는 액세스를 비활성화하여 정리됩니다.

이러한 자격 증명에 필요한 최소 권한은 다음과 같습니다.

- `organizations:DisableAWSServiceAccess`. 이 작업에 `organizations:ServicePrincipal` 조건 키를 사용하여 승인된 서비스 보안 주체 이름의 목록에 대해 해당 작업이 수행하는 요청을 제한할 수 있습니다. 자세한 내용은 [조건 키](#) 단원을 참조하십시오.
- `organizations:ListAWSServiceAccessForOrganization` - AWS Organizations 콘솔을 사용하는 경우 필요합니다.

- 신뢰할 수 있는 서비스에서 필요한 최소 권한은 서비스에 따라 결정됩니다. 자세한 내용은 신뢰할 수 있는 서비스의 설명서를 참조하세요.
- 의 권한이 있는 자격 증명 AWS Organizations 이 신뢰할 수 있는 서비스의 권한이 있는 자격 증명이 아닌 경우 다음 순서로 다음 단계를 수행합니다.
 1. 먼저 신뢰할 수 있는 서비스에 대한 권한이 있는 사람이 해당 서비스를 사용하여 액세스를 비활성화합니다. 이것은 신뢰할 수 있는 서비스에게 신뢰할 수 있는 액세스에 필요한 리소스를 삭제하여 정리하라고 지시하는 것입니다. 자세한 내용은 [AWS 서비스와 함께 사용할 수 있는 AWS Organizations](#)에서 서비스별 지침을 참조하세요.
 2. 그러면 권한이 있는 사용자가 콘솔 AWS CLI 또는 AWS SDK를 사용하여 AWS Organizations 신뢰할 수 있는 서비스에 대한 액세스를 비활성화할 수 있습니다. 이제 신뢰할 수 있는 서비스에 대한 권한이 조직과 그 계정에서 삭제됩니다.

최소 AWS Organizations 권한은 다음과 같습니다.

- `organizations:DisableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization` - AWS Organizations 콘솔을 사용하는 경우에만 필요합니다.

에서 신뢰할 수 있는 액세스를 비활성화하는 단계는 섹션을 AWS Organizations참조하세요 [신뢰할 수 있는 액세스를 활성화 또는 비활성화하는 방법](#).

신뢰할 수 있는 액세스를 활성화 또는 비활성화하는 방법

에 대한 권한만 AWS Organizations 있고 다른 AWS 서비스의 관리자를 대신하여 조직에 대한 신뢰할 수 있는 액세스를 활성화하거나 비활성화하려면 다음 절차를 사용합니다.

Important

옵션을 사용할 수 있는 경우 신뢰할 수 있는 서비스의 콘솔 또는 AWS CLI 또는 API 작업과 동등한 것만 사용하여 신뢰할 수 있는 액세스를 활성화 및 비활성화하는 것이 좋습니다. 이렇게 하면 신뢰할 수 있는 액세스를 활성화할 때 신뢰할 수 있는 서비스가 모든 필수 리소스를 생성하는 등의 필요한 모든 초기화를 수행할 수 있으며, 신뢰할 수 있는 서비스를 비활성화할 때 필요한 모든 리소스 정리 작업을 수행할 수 있습니다.

신뢰할 수 있는 서비스를 사용해 조직에 대한 신뢰할 수 있는 서비스 액세스를 활성화하거나 비활성화하는 방법은 [AWS 서비스와 함께 사용할 수 있는 AWS Organizations](#)의 신뢰할 수 있는 액세스 지원 열 아래에 있는 자세히 알아보기를 참조하세요.

Organizations 콘솔, CLI 명령 또는 API 작업을 사용하여 액세스를 비활성화하면 다음의 동작이 발생합니다.

- 조직 내 계정에서 더 이상 서비스 연결 역할을 만들 수 없습니다. 즉, 서비스가 사용자를 대신하여 조직의 새 계정에 대해 작업을 수행할 수 없습니다. 서비스는 서비스가 AWS Organizations의 정리를 완료할 때까지 이전 계정에서 작업을 계속 수행할 수 있습니다.
- 역할에 연결된 IAM 정책에서 작업을 명시적으로 허용하지 않는 한 서비스가 더 이상 조직의 멤버 계정에서 작업을 수행할 수 없습니다. 이러한 작업으로는 멤버 계정에서부터 관리 계정 또는 위임된 관리자 계정(해당하는 경우)에 이르는 모든 데이터의 집계가 있습니다.
- 일부 서비스는 이를 감지하고 통합과 관련된 나머지 데이터 또는 리소스를 정리하는 반면, 다른 서비스는 조직에 대한 액세스를 중지하되 통합의 재활성화를 지원하기 위해 기록 데이터 및 구성을 그대로 남겨둡니다.

그 대신 다른 서비스의 콘솔이나 명령을 사용하여 통합을 비활성화하면 다른 서비스가 통합에만 필요한 리소스를 정리할 수 있습니다. 서비스가 조직의 계정에서 리소스를 정리하는 방식은 해당 서비스에 따라 다릅니다. 자세한 내용은 다른 AWS 서비스에 대한 설명서를 참조하세요.

AWS Management Console

신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [서비스\(Services\)](#) 페이지에서 활성화하려는 서비스의 행을 찾고 그 이름을 선택합니다.
3. 신뢰할 수 있는 액세스 활성화를 선택합니다.
4. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화는 옵션 표시(Show the option to enable trusted access)를 선택하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
5. 액세스를 활성화하는 경우 다른 AWS 서비스의 관리자에게 이제 다른 서비스가 작동하도록 활성화할 수 있다고 알립니다 AWS Organizations.

신뢰할 수 있는 서비스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

2. [서비스\(Services\)](#) 페이지에서 비활성화하려는 서비스의 행을 찾고 그 이름을 선택합니다.
3. 다른 서비스의 관리자가, 서비스가 비활성화되어 해당 리소스가 정리되었다고 알려줄 때까지 기다립니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 신뢰할 수 있는 액세스 비활성화(Disable trusted access)를 선택합니다.

AWS CLI, AWS API

신뢰할 수 있는 서비스 액세스를 활성화 또는 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하거나 비활성화할 수 있습니다.

- AWS CLI: AWS organizations [enable-aws-service-access](#)
- AWS CLI: AWS organizations [disable-aws-service-access](#)
- AWS API: [EnableAWSServiceAccess](#)
- AWS API: [DisableAWSServiceAccess](#)

AWS Organizations 및 서비스 연결 역할

AWS Organizations 는 [IAM 서비스 연결 역할](#)을 사용하여 신뢰할 수 있는 서비스가 조직의 멤버 계정에서 사용자를 대신하여 작업을 수행할 수 있도록 합니다. 신뢰할 수 있는 서비스를 구성하고 이를 조직에 통합하도록 승인하면 이 서비스에서 AWS Organizations 가 해당 멤버 계정으로 서비스 연결 역할을 생성하도록 요청할 수 있습니다. 신뢰할 수 있는 서비스가 동시에 조직 내 모든 계정에 필수적으로 진행하지 않고 필요할 때 이를 비동기적으로 진행합니다. 서비스 연결 역할에는 신뢰할 수 있는 서비스가 해당 계정 내에서 특정 작업만을 수행하도록 허용하는 사전 정의된 IAM 권한이 있습니다. 일반적으로 AWS 에서 모든 서비스 연결 역할을 관리합니다. 따라서 사용자는 일반적으로 역할 또는 연결된 정책을 변경할 수 없습니다.

이 모든 것이 가능하도록 하려면 조직 내에 계정을 생성하거나 조직에 대한 기존 계정의 초대를 허용할 때 AWS Organizations 가 멤버 계정에 AWSServiceRoleForOrganizations라는 서비스 연결 역할을 프로비저닝합니다. AWS Organizations 서비스 자체만이 역할을 수임할 수 있습니다. 역할에는가 다른 AWS Organizations 에 대한 서비스 연결 역할을 생성할 수 있는 권한이 있습니다 AWS 서비스. 이 서비스 연결 역할은 모든 조직에 존재합니다.

권장하는 방법은 아니지만 조직에서 [통합 결제 기능](#)만 활성화된 경우, AWSServiceRoleForOrganizations라는 이름의 서비스 연결 역할이 절대 사용되지 않으며, 이를

삭제할 수 있습니다. 이후에 조직 내 [모든 기능](#)을 활성화하려면 이 역할이 필요하므로, 복원해야 합니다. 다음 상태 확인은 모든 기능을 활성화하는 절차를 시작할 때 발생합니다.

- 조직에 가입하도록 초대된 각 멤버 계정 – 계정 관리자가 모든 기능 활성화에 동의하는 요청을 수신합니다. 요청에 동의하려면 관리자가 `organizations:AcceptHandshake` 권한과 `iam:CreateServiceLinkedRole` 권한(서비스 연결 역할(AWSServiceRoleForOrganizations)이 아직 없는 경우)이 모두 있어야 합니다. `AWSServiceRoleForOrganizations` 역할이 이미 존재하는 경우 관리자는 요청 허용에 `organizations:AcceptHandshake` 권한만이 필요합니다. 관리자가 요청에 동의하면은 아직 존재하지 않는 경우 서비스 연결 역할을 AWS Organizations 생성합니다.
- 조직에 생성된 각 멤버 계정 – 계정 관리자가 서비스 연결 역할을 다시 생성하는 요청을 수신합니다. (멤버 계정의 관리자는 모든 기능을 활성화하는 요청을 수신하지 않습니다. 관리 계정(이전의 “마스터 계정”)의 관리자가 생성된 멤버 계정의 소유자로 간주되기 때문입니다.) 멤버 계정 관리자가 요청을 허용할 때 AWS Organizations 는 서비스 연결 역할을 생성합니다. 성공적으로 핸드셰이크를 수락하려면 관리자는 `organizations:AcceptHandshake` 및 `iam:CreateServiceLinkedRole` 권한을 보유해야 합니다.

조직에서 모든 기능을 활성화한 이후에는 더 이상 모든 계정에서 `AWSServiceRoleForOrganizations` 서비스 연결 역할을 삭제할 수 없습니다.

Important

AWS Organizations SCPs 서비스 연결 역할에 영향을 주지 않습니다. 이러한 역할은 모든 SCP 제한에서 제외됩니다.

AWSServiceRoleForDeclarativePoliciesEC2Report 서비스 연결 역할 사용

`AWSServiceRoleForDeclarativePoliciesEC2Report` 서비스 연결 역할은 Organizations에서 선언적 정책 보고서를 생성할 멤버 계정의 계정 속성 상태를 설명하는 데 사용됩니다. 역할의 권한은 [AWS 관리형 정책: DeclarativePoliciesEC2Report](#)에 정의되어 있습니다.

AWS 서비스와 함께 사용할 수 있는 AWS Organizations

를 AWS Organizations 사용하면 여러을 단일 조직 AWS 계정 으로 통합하여 대규모로 계정 관리 활동을 수행할 수 있습니다. 계정을 통합하면 다른를 사용하는 방법이 간소화됩니다 AWS 서비스. 에서 사용할 수 있는 다중 계정 관리 서비스를 선택 AWS 서비스 과 AWS Organizations 함께 활용하여 조직의 멤버인 모든 계정에서 작업을 수행할 수 있습니다.

다음 표에는에서 사용할 수 AWS 서비스 있는 목록 AWS Organizations과 조직 전체 수준에서 각 서비스를 사용할 때의 이점이 나와 있습니다.

신뢰할 수 있는 액세스 - 호환되는 AWS 서비스를 활성화하여 조직의 모든 AWS 계정 에서 작업을 수행할 수 있습니다. 자세한 내용은 [다른 AWS Organizations 와 함께 사용 AWS 서비스](#) 단원을 참조하십시오.

에 대한 위임된 관리자 AWS 서비스 - 호환되는 AWS 서비스는 조직의 AWS 멤버 계정을 해당 서비스의 조직 계정에 대한 관리자로 등록할 수 있습니다. 자세한 내용은 [Organizations에서 작업 AWS 서비스 하는의 위임된 관리자](#) 단원을 참조하십시오.

AWS 서비스	와 함께 사용할 때의 이점 AWS Organizations	신뢰할 수 있는 액세스 지원	위임된 관리자 지원	
AWS Account Management 조직의 모든에 대한 세부 정보 및 메타데이터 AWS 계정 를 관리합니다.	조직의 모든 AWS 계정에 대한 계정 세부 정보, 대체 연락처 및 리전을 관리합니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	
AWS Application Migration Service	여러 계정에 대해 대규모 마이	☑예	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Applicati on Migration Service 를 사 용하면 기업은 호환성 문제, 성 능 중단 또는 긴 전환 기간 없이 AWS 많은 수 의 물리적, 가상 또는 클라우드 서버로 lift-and- shift할 수 있습 니다.	그레이션 을 관리할 수 있습니 다.	자세히 알아보기		
AWS Artifact ISO 및 PCI 보 고서와 같은 AWS 보안 규정 준수 보고서를 다운로드합니 다.	조직 내 모 든 계정을 대신하여 계약을 수 락할 수 있 습니다.	☑예 자세히 알아보기	☒아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Audit Manager 지속적인 증거 수집을 자동화하여 클라우드 서비스 사용을 감사할 수 있습니다.	조직의 여러 계정에 서 AWS 사용을 지 속적으로 감사하여 위험 및 규 정 준수를 평가하는 방법을 간 소화합니 다.	☑예 자세히 알아보기	☑예 자세히 알아보기	
AWS Backup 조직의 모든 계 정에서 백업을 관리하고 모니 터링합니다.	전체 조 직 또는 OU(조직 단위)의 계정 그룹 에 대한 백 업 계획을 구성하고 관리할 수 있습니다. 모든 계정 의 백업을 중앙에서 모니터링 할 수 있습 니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS 결제 및 비용 관리 AWS 클라우드 재무 관리 데이 터에 대한 개요 를 제공하고 더 빠르고 정보에 입각한 결정을 내리는 데 도움 이 됩니다.	분할 비용 할당 데이 터가 해당 하는 경 우 AWS Organizat ions 정보 를 검색하 고 옵트인 한 분할 비 용 할당 데 이터 서비 스에 대한 원격 측정 데이터를 수집하도 록 허용합 니다. 자세한 내용은 Billing and Cost Managemen t 사용 설 명서의 What is AWS 결제 및 비용 관	☑예 자세히 알아보기	☒아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
	리? 를 참 조하세요.			
AWS CloudFormation StackSets 단일 작업으로 여러 계정 및 리 전에 대해 스택 을 생성, 업데이 트 또는 삭제합 니다.	관리 계정 또는 위임 된 관리자 계정의 사 용자는 서 비스 관리 형 권한을 사용하여 조직의 계 정에 스택 인스턴스 를 배포하 는 스택 세 트를 생성 할 수 있습 니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS CloudTrail 계정의 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화합니다.	관리 계정 또는 위임된 관리자 계정의 사용자는 조직의 모든 계정에 대한 모든 이벤트를 로깅하는 조직 추적 또는 이벤트 데이터 스토어를 생성할 수 있습니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
Amazon CloudWatch() AWS 에서 실행하는 AWS 리소스와 애플리케이션을 실시간으로 모니터링합니다. CloudWatch를 사용하여 리소스 및 애플리케이션에 대해 측정할 수 있는 변수인 지표를 수집하고 추적할 수 있습니다.	Organizat ions와 통 합하면 CloudWate h에서 두 가지 이점 이 있습니 다. 먼저 Organizat ions와 통 합하면 CloudWate h를 사 용하여 CloudWate h 콘솔의 중앙 보기 에서 AWS 리소스의 원격 측정 구성 상태 를 검색하 고 이해할 수 있습니 다. 둘째, CloudWate h의 Network	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
	Flow Monitor 를 사용하 여 네트워 크 성능 지 표에 대한 가시성을 확보할 수 있는 경우 Organizat ions와 통 합하여 하 나의 계정 대신 다중 계정의 리 소스에 대 한 네트워 크 성능 정 보를 볼 수 있습니다.			

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Compute Optimizer AWS 컴퓨팅 최적화 권장 사항을 가져옵니다.	조직의 계정에 있는 모든 리소스를 분석하여 최적화 권장 사항을 얻을 수 있습니다. 자세한 내용은 AWS Compute Optimizer 사용 설명서의 Compute Optimizer에서 지원되는 계정을 참조 하세요.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Config AWS 리소스의 구성을 액세스, 감사 및 평가합 니다.	규정 준 수 상태 를 조직 전 체 수준에 서 확인할 수 있습니 다. AWS Config API 작업 을 사용하 여 조직의 모든 AWS 계정 에 서 AWS Config 규 칙 및 적합 성 팩을 관 리할 수도 있습니다. 위임된 관 리자 계정 을 사용하 여 AWS Organizat ions에서 조직 내 모 든 멤버 계 정의 리소 스 구성 및	☑예 자세히 알아보기	☑예 자세히 알아보기: Config 규칙 적합성 팩 다중 계정 다중 리 전 데이터 집계	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
	규정 준수 데이터를 집계할 수 있습니다. 자세한 내 용은 AWS Config 개 발자 안내 서의 위임 된 관리자 등록을 참 조하세요.			

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Control Tower 안전하고 규정을 준수하는 다중 계정 AWS 환경을 설정하고 관리합니다.	모든 AWS 리소스에 대한 다중 계정 환경인 랜딩 존을 설정할 수 있습니다. 이 환경에는 조직과 조직 엔터티가 포함됩니다. 이 환경을 사용하여 모든에 규정 준수 규정을 적용할 수 있습니다 AWS 계정. 자세한 내용은 AWS Control Tower 사용 설명서의 AWS Control Tower의	☑예 자세히 알아보기	☒아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
	작동 방식 및 AWS Organizat ions 를 통 한 계정 관 리를 참조 하세요.			

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Cost Optimization Hub AWS 최적화 제 품 전반에서 비 용 권장 사항을 수집합니다.	AWS Organizat ions 멤버 계정 및 AWS 리전 에서 AWS 비용 최적 화 권장 사 항을 쉽게 식별, 필터 링 및 집계 할 수 있습 니다. 자세한 정 보는 Cost Optimizat ion Hub 사용 설명 서의 Cost Optimization Hub 를 참조하세 요.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
Amazon Detective 로그 데이터에 서 보안 결과 또 는 의심스러운 활동의 근본 원 인을 분석하고, 조사하고, 빠르 게 식별하기 위 한 시각화를 생 성합니다.	Amazon Detective AWS Organizat ions 를와 통합하여 Detective 동작 그래 프가 모든 조직 계정 의 활동에 대한 가시 성을 제공 하도록 할 수 있습니 다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
Amazon DevOps Guru 운영 데이터와 애플리케이션 지표 및 이벤트를 분석하여 정상적인 운영 패턴에서 벗어나는 동작을 식별합니다. DevOps Guru가 운영 문제 또는 위험을 감지하면 사용자에게 알림이 전송됩니다.	와 통합하여 조직 전체의 모든 계정에서 인사이트 AWS Organizations를 관리할 수 있습니다. 관리자가 모든 계정의 인사이트를 보고, 정렬하고, 필터링하여 조직 전체 수준에서 모니터링되는 모든 애플리케이션의 상태를 확인할 수 있도록 권한을 위임합니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Directory Service AWS 클라우 드에서 디렉터 리를 설정 및 실행하거나 리 소스를 AWS 기존 온프레미 스 Microsoft Active Directory에 연 결합니다.	여러 계정 과 리전의 모든 VPC 에서 원활 한 디렉터 리 공유 를 AWS Organizat ions 위해 Directory Service 와를 통합 할 수 있습 니다.	☑예 자세히 알아보기	☒아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
Amazon EventBridge AWS 리소스와 AWS에서 실시간으로 실행하는 애플리케이션을 모니터링합니다.	조직 내 모든 계정에서 모든 Amazon EventBridge events(이전 Amazon CloudWatch Events)를 공유하도록 설정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서의 AWS 계정 간 이벤트 전송 및 수신 을 참조하세요.	⊗아니요	⊗아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
- Amazon Elastic Compute Cloud Amazon VPC IP 주소 관리자 (IPAM)는 AWS 클라우드에서 확장 가능한 온디맨드 컴퓨팅 용량을 제공합니다.	선언적 정책 기능을 사용할 때 Organizations 관리자가 조직 전체의 계정에 대한 기존 구성이 무엇인지에 대한 보고서를 생성할 수 있습니다.	☑예 자세히 알아보기	☒아니요	
EC2 용량 관리자 EC2 용량 관리자는 EC2 온디맨드, 스팟, 용량 예약에서 용량 사용량을 확인, 분석, 관리하기 위해 집계되었습니다.	AWS Organization 통합과 함께 EC2 용량 관리자를 사용하면 조직 전체에서 용량 사용량을 확인, 분석 및 관리할 수 있습니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
Amazon Elastic Kubernetes Service: Amazon EKS 대시보드는 AWS 클라우드 전반의 Kubernetes 클러스터에 대한 집계된 가시성과 관리를 제공합니다.	Organizat ions 관리 자가 조직 전체의 버 전 배포, 상태, 업그 레이드 요 구 사항을 포함하여 클러스터 리소스에 대한 통합 대시보드 데이터를 볼 수 있습 니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	
AWS Firewall Manager 사용자의 계정과 애플리케이션 전체에서 웹 애플리케이션에 대한 방화벽 규칙을 중앙에서 구성하고 관리합니다.	조직의 계 정 전체에 서 AWS WAF 규칙 을 중앙에 서 구성하 고 관리할 수 있습니 다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
Amazon GuardDuty GuardDuty는 다양한 데이터 원본의 정보를 분석하고 처리하는 지속적 보안 모니터링 서비스입니다. 위협 인텔리전스 피드와 기계 학습을 바탕으로 Machine Learning을 적용하여 AWS 환경에서 예기치 않게 발생하는 잠재적 무단 활동과 악의적 활동을 찾아냅니다.	멤버 계정을 지정하여 조직의 모든 계정에 대해 GuardDuty를 확인하고 관리할 수 있습니다. 멤버 계정을 추가하면 선택한 해당 계정에 대해 GuardDuty가 자동으로 활성화됩니다 AWS 리전. 또한 조직에 추가된 새 계정에 GuardDuty를 자동으로 활성화할 수 있습니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
	자세한 내용은 Amazon GuardDuty 사용 설 명서의 GuardDuty 와 Organizat ions 를 참 조하세요.			
AWS Health AWS 서비스의 리소스 성능 또 는 가용성 문제 에 영향을 줄 수 있는 이벤트에 대한 가시성을 확보합니다.	조직의 계정 간 에 AWS Health 이 벤트를 집 계할 수 있 습니다.	 예 자세히 알아보기	 예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Identity and Access Management AWS 리소스에 대한 액세스를 안전하게 제어합니다.	IAM에서 서비스가 마지막으로 액세스한 데이터 를 사용하여 조직 전반의 AWS 활동을 더욱 잘 파악할 수 있습니다. 이 데이터를 사용하여 해당 조직의 계정이 사용하는 AWS 서비스로만 액세스를 제한하는 서비스 제어 정책(SCP) 을 생성하고 업데이트할 수 있습니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
	예시는 IAM 사용 설명서의 데이터를 사용하여 조직 단위 의 권한 구 체화를 참 조하세요. IAM 루트 액세스 관 리를 사용 하면 루트 사용자 자 격 증명을 중앙에서 관리하고 멤버 계정 에서 권한 있는 작업 을 수행할 수 있습니 다.			

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
IAM Access Analyzer AWS 환경의 리 소스 기반 정책 을 분석하여 신 뢰 영역 외부의 보안 주체에게 액세스 권한을 부여하는 모든 정책을 식별합 니다.	멤버 계정 을 IAM 액 세스 분석 기의 관리 자로 지정 할 수 있습 니다. 자세한 내 용은 IAM 사용 설 명서의 Access Analyzer 활성화 를 참조하세 요.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
Amazon Inspector – AWS 워크로드에서 취약성을 자동으로 검사하여 Amazon ECR에 상주하는 Amazon EC2 인스턴스 및 컨테이너 이미지에서 소프트웨어 취약성 및 의도하지 않은 네트워크 노출을 검색합니다.	관리자에게 멤버 계정의 스캔을 활성화하거나 비활성화하고, 전체 조직에서 집계된 결과 데이터를 보고, 억제 규칙을 생성하고 관리할 수 있는 권한을 위임합니다. 자세한 내용은 Amazon Inspector 사용 설명서의 AWS Organizations로 여러 계정 관리를 참조하세요.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS License Manager 소프트웨어 라이선스를 클라우드로 가져오는 프로세스를 간소화합니다.	조직 전체의 컴퓨팅 리소스에 대한 교차 계정 발견을 활성화할 수 있습니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
Amazon Macie 데이터 보안 및 개인 정보 보 호 요구 사항을 충족할 수 있도 록 기계 학습을 사용하여 비즈 니스 크리티컬 콘텐츠를 검색 및 분류합니다. Amazon S3에 저장된 콘텐츠 를 지속적으로 평가하고 잠재 적인 문제를 알 려줍니다.	조직의 모 든 계정 에 대해 Amazon Macie를 구성하여 지정된 Macie 관 리자 계정 의 모든 계정에 대 한 모든 데 이터의 통 합 보기를 Amazon S3로 가져 올 수 있습 니다. 조직 이 성장함 에 따라 새 계정의 리 소스를 자 동으로 보 호하도록 Macie를 구성할 수 있습니다. 조직 전체 의 S3 버	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
	킷에서 잘 못된 정책 구성을 수 정하면 경 고가 표시 됩니다.			
AWS Managed Services (AMS) 셀프 서비스 보고 (SSR) 다양한 네이티브 AWS 서비스에서 데이터를 수집하고 주요 AMS 제품에 대한 보고서에 대한 액세스를 제공합니다. SSR은 운영, 구성 관리, 자산 관리, 보안 관리, 규정 준수를 지원하는 데 사용할 수 있는 정보를 제공합니다.	고객은 관리 계정 또는 위임된 관리자 계정을 통해 조직 전체에서 통합 셀프 서비스 보고서를 볼 수 있는 기능인 집계 SSR을 활성화할 수 있습니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Marketplace 솔루션을 구축 하고 비즈니스 를 운영하는 데 필요한 타사 소 프트웨어, 데이 터, 서비스를 찾 아 구매, 배포 및 관리까지 할 수 있도록 큐레 이션 프로세스 를 거친 디지털 카탈로그입니 다.	조직의 계정 간 에 AWS Marketpla ce 구독 및 구매에 대한 라이 선스를 공 유할 수 있 습니다.	☑예 자세히 알아보기	☒아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Marketplace 프라이빗 마켓플레이스 에서 사용할 수 있는 광범위한 제품 카탈로그 AWS Marketplace와 해당 제품에 대한 세분화된 제어를 제공합니다.	전체 조직, 하나 이상의 OU 또는 조직 내 하나 이상의 계정에 연결된 여러 개의 프라이빗 마켓플레이스 경험을 만들 수 있으며, 각 경험에는 승인된 고유의 제품 세트가 있습니다. AWS 관리자는 회사 또는 팀의 로고, 메시징 및 색상 체계를 사용하여 각 프라이빗 마켓플레이스 환경에 회사 브	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
	랜딩을 적 용할 수도 있습니다.			
AWS Marketplace 조달 인사이트 대시보드 조직 내 AWS 계정 전체의 모든 AWS Marketplace 구매에 대한 계약 및 비용 분석 데이터를 볼 수 있습니다.	AWS Marketplace 조달 인사이트 대시보드는 조직에 가입한 계정과 같은 조직 변경 사항을 수신하고 해당 계약의 데이터를 집계하여 대시보드를 구축합니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Network Manager AWS 계정, 리 전 및 온프레 미스 위치에 서 AWS Cloud WAN 코어 네트워크와 AWS Transit Gateway 네트 워크를 중앙에 서 관리할 수 있 습니다.	조직 내 여 러 AWS 계정에서 전송 게이 트웨이 및 연결된 리 소스를 사 용하여 글 로벌 네트 워크를 중 앙에서 관 리하고 모 니터링할 수 있습니 다.	☑예 자세히 알아보기	☑예 자세히 알아보기	
Amazon Q Developer Amazon Q Developer는 AWS 애플리케 이션을 이해, 구 축, 확장 및 운 영하는 데 도움 이 되는 생성형 AI 기반 대화형 어시스턴트입 니다.	Amazon Q Developer 의 유료 구독 버 전에는 Organizat ions 통합 이 필요합 니다.	☑예 자세히 알아보기	☒아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Resource Access Manager 소유한 지정된 AWS 리소스를 다른 계정과 공유합니다.	추가 초대 를 교환하 지 않고도 조직 내에 서 리소스 를 공유할 수 있습니 다. 공유할 수 있는 리 소스에는 Route 53 Resolver 규칙 , 온디 맨드 용량 예약 등이 포함됩니 다. 용량 예 약 공유에 대한 자세 한 내용은 Amazon EC2 사 용 설명 서 또는 Amazon EC2 사용 설명서 를	☑예 자세히 알아보기	☒아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
	참조하세 요. 공유 가능 한 리소 스 목록 은 AWS RAM 사용 설명서의 공유 가 능한 리소 스 를 참조 하세요.			
AWS Resource Explorer 인터넷 검색 엔 진과 같은 경험 을 사용하여 리 소스를 탐색하 세요.	다중 계정 검색을 활 성화하십 시오.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Security Hub CSPM 에서 보안 상태 를 AWS 확인하 고 보안 업계 표 준 및 모범 사례 를 기준으로 환 경을 확인합니 다.	새 계정이 추가될 때 이를 포함 하여 조직 의 모든 계 정에 대해 Security Hub CSPM을 자동으로 활성화할 수 있습니 다. 이렇 게 하면 Security Hub CSPM 검 사 및 조사 결과에 대 한 적용 범 위가 늘어 나 전반적 인 보안 태 세를 보다 정확하게 파악할 수 있습니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
Amazon S3 Storage Lens Amazon S3 Storage 사용량과 활동 지표에 대한 가시성과, 스토리지 최적화를 위한 실효성 있는 권장 사항을 제공합니다.	Amazon S3 스토리지 사용량 및 활동 추세에 대한 가시성과, 조직의 모든 멤버 계정에 대한 권장 사항을 얻을 수 있도록 Amazon S3 Storage Lens를 구성합니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS 보안 인시 던트 대응 AWS 고객이 자 격 증명 도용 및 랜섬웨어 공격 과 같은 사이버 보안 인시던트 에 신속하게 대 응할 수 있도록 연중무휴 실시 간 인적 지원 보 안 인시던트 지 원을 제공하는 보안 서비스입 니다.	전체 조직 에 대한 보 안 범위입 니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	
Amazon Security Lake Amazon Security Lake 는 클라우드, 온 프레미스 및 사 용자 지정 소스 의 보안 데이터 를 계정에 저장 된 데이터 레이 크로 중앙 집중 화합니다.	계정 전체 에서 로그 와 이벤트를 수 집하는 데이터 레이크를 생성하 입니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Service Catalog AWS에서 사용하도록 승인된 IT 서비스의 카탈로그를 생성하고 관리합니다.	포트폴리오 ID를 공유하지 않고도 여러 계정에서 더 쉽게 포트폴리오를 공유하고 제품을 복사할 수 있습니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	
Service Quotas 중앙 위치에서 서비스 할당량(또는 한도)을 확인하고 관리합니다.	조직의 계정을 만들 때 할당량 요청 템플릿을 만들어 할당량 증가를 자동으로 요청할 수 있습니다.	☑예 자세히 알아보기	☒아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS IAM Identity Center 모든 계정 및 클라우드 애플리케이션에 대한 SSO(Single Sign-On) 액세스를 제공합니다.	사용자는 회사 자격 증명으로 AWS 액세스 포털에 로그인하고 할당된 관리 계정 또는 멤버 계정의 리소스에 액세스할 수 있습니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Systems Manager AWS 리소스의 가시성과 제어를 활성화합니다.	Systems Manager Explorer를 사용하여 조직의 모든 AWS 계정에서 작업 데이터를 동기화할 수 있습니다. Systems Manager Change Manager를 사용하여 위임된 관리자 계정에서 조직의 모든 멤버 계정에 대한 변경 템플릿, 승인, 보고를 관리할 수 있습니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS User Notifications AWS 알림의 중앙 위치입니다.	조직의 모든 계정에 서 알림을 중앙에서 구성하고 볼 수 있습 니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	
- 태그 정책 조직의 계정에 있는 리소스 전 체에서 태그를 표준화합니다.	태그 정책 을 생성하 여 특정 리 소스 및 리 소스 유형 에 대한 태 그 지정 규 칙을 정의 하고 이러 한 정책을 조직 단위 및 계정에 연결해 해 당 규칙을 적용할 수 있습니다.	☑예 자세히 알아보기	☒아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
AWS Trusted Advisor Trusted Advisor 는 AWS 환경을 검사하고 비용을 절감하거나, 시스템 가용성 및 성능을 개선하거나, 보안 격차를 좁힐 수 있는 기회가 있을 때 권장 사항을 제시합니다.	조직의 모든 AWS 계정에 대한 Trusted Advisor 검사를 실행합니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	
AWS Well-Architected Tool 는 워크로드의 상태를 문서화하고 이를 최신 AWS 아키텍처 모범 사례와 비교하는데 AWS Well-Architected Tool 도움이 됩니다.	AWS WA Tool 및 Organizations 고객 모두 조직의 다른 구성원과 AWS WA Tool 리소스를 공유하는 프로세스를 간소화할 수 있습니다.	☑예 자세히 알아보기	☒아니요	

AWS 서비스	와 함께 를 사용 할 때의 이 점 AWS Organizat ions	신뢰할 수 있는 액세 스 지원	위임된 관리자 지원	
Amazon VPC IP 주소 관리자 (IPAM) IPAM은 AWS 워크로드의 IP 주소를 더 쉽게 계획, 추적 및 모니터링할 수 있는 VPC 기능입니다.	조직 전체의 IP 주소 사용을 모니터링하고 멤버 계정 간에 IP 주소 풀을 공유합니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	
Amazon VPC Reachability Analyzer Reachability Analyzer는 Virtual Private Cloud(VPC)에서 소스 리소스와 대상 리소스 간의 연결을 테스트할 수 있는 구성 분석 도구입니다.	조직 내의 여러 계정에 걸쳐 경로를 추적합니다.	☑예 자세히 알아보기	☑예 자세히 알아보기	

AWS Account Management 및 AWS Organizations

AWS Account Management 를 사용하면 조직의 모든에 대한 계정 정보와 메타데이터 AWS 계정 를 관리할 수 있습니다. 조직의 각 멤버 계정에 대한 대체 연락처 정보를 설정, 수정 또는 삭제할 수 있습니다. 자세한 내용은 AWS Account Management 사용 설명서의 [조직에서 AWS Account Management 사용](#)을 참조하세요.

다음 정보를 사용하여 AWS Account Management 와 통합할 수 있습니다 AWS Organizations.

Account Management로 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Account Management는 멤버 계정을 조직의이 서비스에 대한 위임된 관리자로 지정하기 AWS Organizations 전에에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Account Management를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Account Management에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Account Management 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Account Management 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal account.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Account Management로 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다. AWS Account Management.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Account Management를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS Account Management에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.

6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 AWS Account Management 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Account Management를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal account.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Account Management에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 지정된 계정의 사용자 및 역할이 조직의 다른 멤버 계정의 AWS 계정 메타데이터를 관리할 수 있습니다. 위임된 관리자 계정을 활성화하지 않으면 조직의 관리 계정에서만 이러한 작업을 수행할 수 있습니다. 이렇게 하면 조직의 관리와 계정 세부 정보의 관리를 분리하는 데 도움이 됩니다.

최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Account Management에 대한 위임된 관리자로 구성할 수 있습니다

위임 정책을 구성하는 방법에 대한 일반적인 설명은 [틀 사용하여 리소스 기반 위임 정책 생성 AWS Organizations](#)을(를) 참조하세요.

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal account.amazonaws.com
```

- AWS SDK: Organizations RegisterDelegatedAdministrator 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체를 파라미터account.amazonaws.com로 식별합니다.

AWS Application Migration Service (애플리케이션 마이그레이션 서비스) 및 AWS Organizations

AWS Application Migration Service 는 애플리케이션을 로 마이그레이션하는 데 드는 비용을 간소화, 가속화 및 절감합니다 AWS. Organizations과 통합하면 글로벌 뷰 기능을 사용하여 여러 계정에 걸친 대규모 마이그레이션을 관리할 수 있습니다. 자세한 내용은 Application Migration Service 사용 설명서의 [AWS Organizations설정](#)을 참조하세요.

다음 정보를 사용하여 AWS Application Migration Service 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Application Migration Service는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Application Migration Service와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- AWSServiceRoleForApplicationMigrationService

Application Migration Service에서 사용하는 서비스 위탁자

앞 부분에서 다른 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Application Migration Service가 사용하는 서비스 연결 역할은 다음 서비스 위탁자에 대한 액세스 권한을 부여합니다.

- `mgn.amazonaws.com`

Application Migration Service를 사용하여 신뢰할 수 있는 액세스 활성화

Application Migration Service를 사용하여 신뢰할 수 있는 액세스를 활성화하면 글로벌 뷰 기능을 사용하여 여러 계정에 걸친 대규모 마이그레이션을 관리할 수 있습니다. 전역 보기는 다양한 AWS 계정의 소스 서버, 앱 및 웨이브에서 특정 작업을 수행할 수 있는 가시성과 기능을 제공합니다. 자세한 내용은 AWS Application Migration Service 사용 설명서의 [AWS 조직 설정을 참조하세요](#).

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS Application Migration Service 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Application Migration Service 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Application Migration Service 수행할 수 있습니다. AWS Application Migration Service에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Application Migration Service 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하는 경우 이 단계를 완료할 필요가 없습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Application Migration Service를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Application Migration Service에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Application Migration Service 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Application Migration Service 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal mgn.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Application Migration Service를 사용하여 신뢰할 수 있는 액세스 비활성화

Organizations 관리 계정의 관리자만 Application Migration Service를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Application Migration Service 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Important

가능하면 AWS Application Migration Service 콘솔 또는 도구를 사용하여 Organizations와의 통합을 비활성화하는 것이 좋습니다. 이렇게 하면 서비스에서 더 이상 필요하지 않은 리소스

또는 액세스 역할을 삭제하는 등 필요한 모든 정리를 AWS Application Migration Service 수행할 수 있습니다. AWS Application Migration Service에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.

AWS Application Migration Service 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화하면이 단계를 완료할 필요가 없습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Application Migration Service를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS Application Migration Service에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자인 경우에만 관리자에게 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 AWS Application Migration Service 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Application Migration Service 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
```

```
--service-principal mgn.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Application Migration Service에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Application Migration Service에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Application Migration Service 관리와 조직 관리를 분리하는 데 도움이 됩니다. 자세한 내용은 Application Migration Service 사용 설명서의 [AWS Organizations](#) 설정을 참조하세요.

최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Application Migration Service에 대해 위임된 관리자로 구성할 수 있습니다.

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal mgn.amazonaws.com
```

- AWS SDK: Organizations RegisterDelegatedAdministrator 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스를 파라미터 `mgn.amazonaws.com`로 식별합니다.

Application Migration Service에 대해 위임된 관리자 비활성화

Organizations 관리 계정의 관리자만 Application Migration Service의 위임된 관리자를 제거할 수 있습니다. Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다.

AWS Artifact 및 AWS Organizations

AWS Artifact 는 ISO 및 PCI 보고서와 같은 AWS 보안 규정 준수 보고서를 다운로드할 수 있는 서비스입니다. AWS Artifact를 사용하면 조직의 관리 계정 사용자가 새 보고서와 계정이 추가되더라도 조직의 모든 멤버 계정을 대신하여 계약을 자동으로 수락할 수 있습니다. 멤버 계정 사용자는 계약을 보고 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact 사용 설명서의 [AWS 아티팩트에서 여러 계정에 대한 계약 관리](#)를 참조하세요.

다음 정보를 사용하여 AWS Artifact 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 AWS Artifact 는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

AWS Artifact 와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

조직에서 멤버 계정을 제거하는 경우 이 역할을 삭제하거나 수정할 수 있지만 권장하지는 않습니다.

역할 수정은 교차 서비스의 혼동된 대리자와 같은 보안 문제를 발생시킬 수 있으므로 권장하지 않습니다. 혼동된 대리자 예방에 대해 자세히 알아보려면 AWS Artifact 사용 설명서의 [교차 서비스 대리자 예방](#)을 참조하세요.

- `AWSServiceRoleForArtifact`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. 다음 서비스 보안 주체에 대한 액세스 권한을 AWS Artifact 부여하는 데 사용되는 서비스 연결 역할:

- `artifact.amazonaws.com`

를 사용하여 신뢰할 수 있는 액세스 활성화 AWS Artifact

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Artifact를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Artifact에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Artifact 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Artifact 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal artifact.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

를 사용하여 신뢰할 수 있는 액세스 비활성화 AWS Artifact

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다 AWS Artifact.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Artifact 는 조직 계약을 사용하기 AWS Organizations 위해와 신뢰할 수 있는 액세스 권한이 필요합니다. 조직 계약에를 사용하는 AWS Organizations 동안 AWS Artifact 를 사용하여 신뢰할 수 있는 액세스를 비활성화하면 조직에 액세스할 수 없으므로 작동이 중지됩니다. 에서 수락하는 모든 조직 계약은 AWS Artifact 유지되지만에서 액세스할 수 없습니다 AWS Artifact. 에서 AWS Artifact 생성하는 AWS Artifact 역할은 그대로 유지됩니다. 신뢰할 수 있는 액세스를 다시 활성화하면 AWS Artifact 가 이전과 같이 계속 작동하므로 서비스를 다시 구성할 필요가 없습니다.

조직에서 제거된 독립 실행형 계정은 어떠한 조직 계약에도 더 이상 액세스할 수 없습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Artifact를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS Artifact에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 AWS Artifact 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Artifact 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal artifact.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

AWS Audit Manager 및 AWS Organizations

AWS Audit Manager 를 사용하면 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 평가하는 방법을 간소화할 수 있습니다. Audit Manager는 증거 수집을 자동화하여 정책, 절차 및 활동이 효과적으로 운영되는지 더욱 쉽게 평가할 수 있도록 합니다. 감사 시기에 Audit Manager는 수동 작업을 줄여주어 통제에 대한 이해 관계자 검토를 관리하고 감사 준비 보고서를 작성하는 데 도움을 줍니다.

Audit Manager를와 통합하면 평가 범위 내에 조직의 여려를 포함시켜 더 광범위한 소스 AWS 계정에서 증거를 수집할 AWS Organizations수 있습니다.

자세한 내용은 Audit Manager 사용 설명서의 [AWS 조직 활성화를 참조하세요](#).

다음 정보를 사용하여 AWS Audit Manager 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Audit Manager는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Audit Manager와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

Audit Manager가 이 역할을 사용하는 방식에 대한 자세한 내용은 AWS Audit Manager 사용 설명서의 [서비스 연결 역할 사용](#)을 참조하세요.

- AWSServiceRoleForAuditManager

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Audit Manager가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `auditmanager.amazonaws.com`

Audit Manager와 상호 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Audit Manager는 멤버 계정을 조직의 위임된 관리자로 지정하기 AWS Organizations 전역에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

콘솔 또는 AWS Audit Manager 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Audit Manager 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Audit Manager 수행할 수 있습니다. AWS Audit Manager에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Audit Manager 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하면이 단계를 완료할 필요가 없습니다.

Audit Manager 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 방법은 AWS Audit Manager 사용 설명서의 [설정](#)을 참조하세요.

Note

AWS Audit Manager 콘솔을 사용하여 위임된 관리자를 구성하면가 AWS Audit Manager 자동으로 신뢰할 수 있는 액세스를 활성화합니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Audit Manager 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal auditmanager.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Audit Manager와 상호 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 신뢰할 수 있는 액세스를 비활성화할 수 있습니다 AWS Audit Manager.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Audit Manager 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal auditmanager.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Audit Manager에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Audit Manager에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Audit Manager 관리와 조직 관리를 분리하는 데 도움을 줍니다.

최소 권한

다음 권한이 있는 Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Audit Manager에 대한 위임된 관리자로 구성할 수 있습니다.

`audit-manager:RegisterAccount`

Audit Manager에 대한 위임된 관리자 계정 활성화에 대한 설명은 AWS Audit Manager 사용 설명서의 [설정](#)을 참조하세요.

AWS Audit Manager 콘솔을 사용하여 위임된 관리자를 구성하면 Audit Manager가 자동으로 신뢰할 수 있는 액세스를 활성화합니다.

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws audit-manager register-account \
  --delegated-admin-account 123456789012
```

- AWS SDK: RegisterAccount 작업을 호출하고를 파라미터delegatedAdminAccount로 제공하여 관리자 계정을 위임합니다.

AWS Backup 및 AWS Organizations

AWS Backup 는 조직의 AWS Backup 작업을 관리하고 모니터링할 수 있는 서비스입니다. 를 사용하면 조직의 관리 계정에서 사용자로 로그인 AWS Backup하는 경우 조직 전체의 백업 보호 및 모니터링을 활성화할 수 있습니다. 백업 [정책을](#) 사용하여 조직의 모든 계정에 걸쳐 리소스에 AWS Backup 계획을 중앙에서 적용하여 규정 준수를 달성할 수 있습니다. AWS Backup 및 AWS Organizations 를 함께 사용하면 다음과 같은 이점을 얻을 수 있습니다.

보호

조직에서 [백업 정책 유형을 활성화](#)한 다음 조직의 루트, OU 또는 계정에 연결할 [백업 정책을 생성](#)할 수 있습니다. 백업 정책은 AWS Backup 계획을 계정에 자동으로 적용하는 데 필요한 다른 세부 정보와 결합합니다. 계정에 직접 연결된 정책은 조직의 루트 및 상위 OUs에서 [상속된](#) 정책과 병합되어 계정에 적용되는 [유효 정책을](#) 생성합니다. 정책에는 계정의 리소스 AWS Backup 에서 실행할 권한이 있는 IAM 역할의 ID가 포함됩니다.는 IAM 역할을 AWS Backup 사용하여 유효 정책의 백업 계획에 지정된 대로 사용자를 대신하여 백업을 수행합니다.

모니터링

조직에서 [AWS Backup에 대한 신뢰할 수 있는 액세스를 활성화](#)하면 AWS Backup 콘솔을 사용하여 조직의 모든 계정에서 백업, 복원 및 복사 작업의 세부 정보를 볼 수 있습니다. 자세한 내용은 AWS Backup 개발자 안내서의 [백업 작업 모니터링](#)을 참조하세요.

에 대한 자세한 내용은 [AWS Backup 개발자 안내서](#)를 AWS Backup참조하세요.

다음 정보를 사용하여 AWS Backup 와 통합할 수 있습니다 AWS Organizations.

를 사용하여 신뢰할 수 있는 액세스 활성화 AWS Backup

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS Backup 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Backup 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS

Backup 수행할 수 있습니다. AWS Backup에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.
AWS Backup 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하면이 단계를 완료할 필요가 없습니다.

를 사용하여 신뢰할 수 있는 액세스를 활성화하려면 AWS Backup 개발자 안내서의 [여러에서 백업 활성화 AWS 계정](#)를 AWS Backup참조하세요.

를 사용하여 신뢰할 수 있는 액세스 비활성화 AWS Backup

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Backup 는 조직 계정 전체에서 백업, 복원 및 복사 작업을 모니터링할 수 AWS Organizations 있도록 통한 신뢰할 수 있는 액세스 권한이 필요합니다. 신뢰할 수 있는 액세스를 비활성화하면 현재 계정 외부에서 작업을 볼 수 없게 AWS Backup됩니다. 에서 AWS Backup 생성하는 AWS Backup 역할은 그대로 유지됩니다. 나중에 신뢰할 수 있는 액세스를 다시 활성화하는 경우 서비스를 다시 구성할 필요 없이 AWS Backup 가 이전과 같이 계속 작동합니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Backup 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal backup.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

에 대한 위임된 관리자 계정 활성화 AWS Backup

AWS Backup 개발자 안내서의 [위임된 관리자](#)를 참조하세요.

AWS 결제 및 비용 관리 및 AWS Organizations

AWS 결제 및 비용 관리 는 결제를 설정하고, 인보이스를 검색 및 결제하고, 비용을 분석, 구성, 계획 및 최적화하는 데 도움이 되는 기능 모음을 제공합니다. 와 함께 Billing and Cost Management를 사용하면 해당하는 경우 AWS Organizations [분할 비용 할당 데이터가](#) AWS Organizations 정보를 검색하고 옵트인한 분할 비용 할당 데이터 서비스에 대한 원격 측정 데이터를 수집할 수 있습니다.

다음 정보를 사용하여 AWS 결제 및 비용 관리 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Billing and Cost Management는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Billing and Cost Management와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

자세한 내용은 Billing and Cost Management 사용 설명서의 [Billing and Cost Management에 대한 서비스 연결 역할 권한](#)을 참조하세요.

- AWSServiceRoleForSplitCostAllocationData

Billing and Cost Management에서 사용하는 서비스 위탁자

앞 부분에서 다른 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Billing and Cost Management가 사용하는 서비스 연결 역할은 다음 서비스 위탁자에 대한 액세스 권한을 부여합니다.

Billing and Cost Management는 `billing-cost-management.amazonaws.com` 서비스 위탁자를 사용합니다.

Billing and Cost Management를 사용하여 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

관리 계정을 통해 신뢰할 수 있는 액세스를 활성화하면 고객은 Billing and Cost Management의 분할 비용 할당 데이터 기능을 활용할 수 있습니다. 고객이 Amazon Managed Service for Prometheus를 사용하여 Amazon Elastic Kubernetes Service에 대한 분할 비용 할당 데이터를 활성화하면 신뢰할 수 있는 액세스가 호출되어 Organization 내의 모든 멤버 계정에 대한 서비스 연결 역할을 생성합니다. 이를 통해 분할 비용 할당 데이터는 고객의 Amazon Managed Service for Prometheus 작업 공간에서 원격 측정 데이터를 수집하고 이러한 지표를 기반으로 비용 할당을 수행할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS 결제 및 비용 관리 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal billing-cost-management.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

트러스트된 액세스 사용 중지

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS 결제 및 비용 관리 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal billing-cost-management.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

AWS CloudFormation StackSets 및 AWS Organizations

CloudFormation StackSets를 사용하면 단일 작업 AWS 리전 으로 여러 AWS 계정 및에서 스택을 생성, 업데이트 또는 삭제할 수 있습니다. StackSets와 AWS Organizations 의 통합으로 고객은 각 멤버 계정에서 관련 권한을 보유한 서비스 연결 역할을 사용하여 서비스 관리형 권한이 있는 스택 세트를 생성할 수 있습니다. 이를 통해 조직의 멤버 계정에 스택 인스턴스를 배포할 수 있습니다. 필요한 AWS Identity and Access Management 역할을 생성할 필요가 없습니다. StackSets는 사용자를 대신하여 각 멤버 계정에 IAM 역할을 생성합니다.

나중에 조직에 추가되는 계정에 자동 배포를 활성화하기로 선택할 수도 있습니다. 자동 배포가 활성화 되면 연결된 스택 세트 인스턴스의 역할 및 배포가 향후 해당 OU에 추가되는 모든 계정에 자동으로 추가됩니다.

StackSets와 Organizations 간의 신뢰할 수 있는 액세스가 활성화되면 관리 계정은 조직의 스택 세트를 생성하고 관리할 수 있는 권한을 보유하게 됩니다. 관리 계정은 최대 5개의 멤버 계정을 위임된 관리자로 등록할 수 있습니다. 신뢰할 수 있는 액세스를 활성화하면 위임된 관리자도 조직의 스택 세트를 생성하고 관리할 수 있는 권한을 갖습니다. 서비스 관리형 권한이 있는 스택 세트는 위임된 관리자가 생성한 스택 세트를 포함하여 관리 계정에 생성됩니다.

Important

위임된 관리자는 조직의 계정에 배포할 수 있는 모든 권한을 가집니다. 관리 계정은 위임된 관리자 권한을 특정 OU에 배포하는 권한 또는 특정 스택 세트 작업을 수행하는 권한으로 제한할 수 없습니다.

StackSets를 Organizations와 통합하는 방법에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 [AWS CloudFormation StackSets 작업을](#) 참조하세요.

다음 정보를 사용하여 AWS CloudFormation StackSets를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 CloudFormation Stacksets는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

CloudFormation Stacksets와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- 관리 계정: `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

서비스 연결 역할 `AWSServiceRoleForCloudFormationStackSetsOrgMember`를 생성하려면 조직 내 멤버 계정의 경우 먼저 관리 계정에 스택 세트를 생성해야 합니다. 이렇게 하면 스택 세트 인스턴스가 생성되고, 멤버 계정에 역할이 생성됩니다.

- 멤버 계정: `AWSServiceRoleForCloudFormationStackSetsOrgMember`

스택 세트 생성에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 [AWS CloudFormation StackSets 사용](#)을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. CloudFormation Stacksets에서 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- 관리 계정: `stacksets.cloudformation.amazonaws.com`

StackSets와 Organizations 간의 신뢰할 수 있는 액세스가 비활성화된 경우에만 이 역할을 수정하거나 삭제할 수 있습니다.

- 멤버 계정: `member.org.stacksets.cloudformation.amazonaws.com`

StackSets와 Organizations 간의 신뢰할 수 있는 액세스를 먼저 비활성화하거나, 계정을 대상 조직 또는 조직 단위(OU)에서 먼저 제거한 경우에만 이 역할을 수정하거나 삭제할 수 있습니다.

CloudFormation Stacksets를 사용하여 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Organizations 관리 계정의 관리자만 다른 AWS 서비스에서 신뢰할 수 있는 액세스를 활성화할 수 있는 권한이 있습니다. CloudFormation 콘솔 또는 Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

신뢰할 수 있는 액세스는 AWS CloudFormation StackSets로만 활성화할 수 있습니다.

Stacksets 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면 AWS CloudFormation 사용 설명서의 CloudFormation [를 사용하여 신뢰할 수 있는 액세스 활성화 AWS Organizations](#)를 참조하세요.

CloudFormation Stacksets에서 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Organizations 관리 계정의 관리자만 다른 AWS 서비스에서 신뢰할 수 있는 액세스를 비활성화할 수 있는 권한이 있습니다. 신뢰할 수 있는 액세스는 Organizations 콘솔로만 비활성화할 수 있습니다. StackSets를 사용하는 동안 Organizations와 상호 신뢰할 수 있는 액세스를 비활성화하면 이전에 생성된 모든 스택 인스턴스는 유지됩니다. 그러나 서비스 연결 역할의 권한을 사용하여 배포된 스택 세트는 더 이상 조직에서 관리하는 계정에 대한 배포를 수행할 수 없습니다.

CloudFormation 콘솔 또는 Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Important

프로그래밍 방식으로(예: AWS CLI API를 사용하거나 API를 사용하여) 신뢰할 수 있는 액세스를 비활성화하면 권한이 제거된다는 점에 유의하세요. CloudFormation 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하는 것이 좋습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS CloudFormation StackSets를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS CloudFormation StackSets 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자인 경우에만 이제 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 있음을 AWS CloudFormation StackSets 관리자에게 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 AWS CloudFormation StackSets를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal stacksets.cloudformation.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

CloudFormation Stacksets에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 CloudFormation Stacksets에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자

또는 역할만 관리 작업을 수행할 수 있습니다. 이렇게 하면 조직 관리와 CloudFormation Stacksets 관리를 분리할 수 있습니다.

조직에서 멤버 계정을 CloudFormation Stacksets의 위임된 관리자로 지정하는 방법에 관한 설명은 AWS CloudFormation 사용 설명서의 [위임된 관리자 등록](#)을 참조하세요.

AWS CloudTrail 및 AWS Organizations

AWS CloudTrail 는에 대한 거버넌스, 규정 준수, 운영 및 위험 감사를 활성화하는 데 도움이 되는 AWS 서비스입니다 AWS 계정. AWS CloudTrail를 사용하면 관리 계정의 사용자가 해당 조직의 모든에 대한 모든 이벤트를 로깅하는 조직 추적 AWS 계정 을 생성할 수 있습니다. 조직 추적 기록은 조직 내 모든 구성원 계정에 자동으로 적용됩니다. 구성원 계정은 조직 추적 기록을 볼 수 있지만 수정하거나 삭제할 수는 없습니다. 기본적으로 멤버 계정은 Amazon S3 버킷에 있는 조직 추적 기록에 대한 로그 파일에 액세스할 수 있는 권한이 없습니다. 이는 조직 내 계정에 걸쳐 이벤트 로깅 방식을 일관적으로 적용 및 시행하는 데 도움이 됩니다.

자세한 내용은 AWS CloudTrail 사용 설명서에서 [조직에 대한 추적 생성](#)을 참조하세요.

다음 정보를 사용하여 AWS CloudTrail 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 CloudTrail은 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

CloudTrail와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForCloudTrail`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. CloudTrail이 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `cloudtrail.amazonaws.com`

CloudTrail과 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS CloudTrail 콘솔에서 추적을 생성하여 신뢰할 수 있는 액세스를 활성화하면 신뢰할 수 있는 액세스가 자동으로 구성됩니다(권장). AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수도 있습니다. 조직 추적을 생성하려면 AWS Organizations 관리 계정으로 로그인해야 합니다.

AWS CLI 또는 AWS API를 사용하여 조직 추적을 생성하도록 선택한 경우 신뢰할 수 있는 액세스를 수동으로 구성해야 합니다. 자세한 내용은 AWS CloudTrail 사용 설명서의 [AWS Organizations에서 CloudTrail을 신뢰할 수 있는 서비스로 활성화](#)를 참조하세요.

Important

가능하면 AWS CloudTrail 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS CloudTrail 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal cloudtrail.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

CloudTrail과 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS CloudTrail 는 조직 추적 및 조직 이벤트 데이터 스토어를 사용하기 AWS Organizations 위해와 신뢰할 수 있는 액세스 권한이 필요합니다. 사용 중예를 사용하여 AWS Organizations 신뢰할 수 있는 액세스를 비활성화하면 CloudTrail이 조직에 액세스할 수 없으므로 멤버 계정에 대한 AWS CloudTrail 모든 조직 추적이 삭제됩니다. 모든 관리 계정 조직 추적 및 조직 이벤트 데이터 스토어는 계정 수준 추적 및 이벤트 데이터 스토어로 변환됩니다. CloudTrail과 AWS Organizations 간의 통합을 위해 생성된 `AWSServiceRoleForCloudTrail` 역할은 계정에 유지됩니다. 신뢰할 수 있는 액세스를 다시 활성화하면 CloudTrail은 기존 추적 및 이벤트 데이터 스토어에 대해 조치를 취하지 않습니다. 관리 계정은 모든 계정 수준 추적 및 이벤트 데이터 스토어를 업데이트하여 조직에 적용해야 합니다.

계정 수준 추적 또는 이벤트 데이터 스토어를 조직 추적 또는 조직 이벤트 데이터 스토어로 변환하려면 다음을 수행합니다.

- CloudTrail 콘솔에서 [추적](#) 또는 [이벤트 데이터 스토어](#)를 업데이트하고 조직의 모든 계정에 대해 활성화 옵션을 선택합니다.
- 에서 다음을 AWS CLI수행합니다.
 - 추적을 업데이트하려면 [update-trail](#) 명령을 실행하고 `--is-organization-trail` 파라미터를 포함합니다.
 - 이벤트 데이터 스토어를 업데이트하려면 [update-event-data-store](#) 명령을 실행하고 `--organization-enabled` 파라미터를 포함합니다.

AWS Organizations 관리 계정의 관리자만을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다 AWS CloudTrail. AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.

3. 서비스 목록에서 AWS CloudTrail를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS CloudTrail에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자만 있는 경우 이제 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 AWS CloudTrail 있음을 관리자에게 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS CloudTrail 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal cloudtrail.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

CloudTrail에 대해 위임된 관리자 계정 활성화

CloudTrail을 Organizations와 함께 사용하는 경우, 조직 내의 어떤 계정이든 CloudTrail 위임된 관리자 역할을 하도록 등록할 수 있습니다. 이 위임된 관리자는 조직을 대신하여 조직의 추적 및 이벤트 데이터 스토어를 관리합니다. 위임된 관리자는 CloudTrail에서 관리 계정과 동일한 관리 작업을 수행할 수 있는 조직의 멤버 계정입니다.

최소 권한

Organizations 관리 계정의 관리자만 CloudTrail의 위임된 관리자를 등록할 수 있습니다.

CloudTrail 콘솔을 사용하거나 Organizations RegisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자 계정을 등록할 수 있습니다. CloudTrail 콘솔을 사용하여 위임된 관리자를 등록하려면 [CloudTrail 위임된 관리자 추가](#)를 참조하세요.

CloudTrail에 대해 위임된 관리자 비활성화

Organizations 관리 계정의 관리자만 CloudTrail의 위임된 관리자를 제거할 수 있습니다. CloudTrail 콘솔을 사용하거나 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. CloudTrail 콘솔을 사용하여 위임된 관리자를 제거하는 방법은 [CloudTrail 위임된 관리자 제거](#)를 참조하세요.

Amazon CloudWatch 및 AWS Organizations

다음 사용 사례에 AWS Organizations 대해 Amazon CloudWatch에를 사용할 수 있습니다.

- CloudWatch 콘솔의 중앙 보기에서 AWS 리소스에 대한 원격 측정 구성 상태를 확인하고 파악합니다. 이렇게 하면 AWS 조직 또는 계정 전체에서 여러 리소스 유형에 대한 원격 측정 수집 구성을 감사하는 프로세스가 간소화됩니다. 조직 전체에서 원격 측정 구성을 사용하려면 신뢰할 수 있는 액세스를 켜야 합니다.

자세한 내용은 Amazon CloudWatch 사용 설명서의 [CloudWatch 원격 측정 구성 감사](#)를 참조하세요.

- Amazon CloudWatch Network Monitor의 기능인 Network Flow Monitor의 다중 계정으로 작업합니다. Network Flow Monitor는 Amazon EC2 인스턴스 간의 트래픽의 네트워크 성능에 실시간에 가까운 가시성을 제공합니다. 신뢰할 수 있는 액세스를 활성화하여 Organizations와 통합한 후 모니터를 생성하여 다중 계정의 네트워크 성능 세부 정보를 시각화할 수 있습니다.

자세한 내용은 Amazon CloudWatch 사용 설명서의 [다중 계정 모니터링을 위한 Network Flow Monitor 시작](#)을 참조하세요.

다음 정보는 Amazon CloudWatch와 AWS Organizations통합에 도움을 줍니다.

통합 활성화 시 서비스 연결 역할 생성

조직의 관리 계정에서 다음과 같은 [서비스 연결 역할](#)을 생성합니다. 신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 CloudWatch는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다. CloudWatch와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- AWSServiceRoleForObservabilityAdmin

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. CloudWatch가 사용하는 서비스 연결 역할은 다음 서비스 위탁자에 대한 액세스 권한을 부여합니다.

- observabilityadmin.amazonaws.com
- networkflowmonitor.amazonaws.com
- topology.networkflowmonitor.amazonaws.com

CloudWatch와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#)을 참조하세요.

Amazon CloudWatch 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

Important

가능하면 항상 Amazon CloudWatch 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 Amazon CloudWatch가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. Amazon CloudWatch에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오. Amazon CloudWatch 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

CloudWatch 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

자세한 내용은 [Amazon CloudWatch 사용 설명서](#)의 CloudWatch 원격 측정 감사 켜기를 참조하세요.

CloudWatch에서 신뢰할 수 있는 액세스를 켜면 원격 측정 감사를 활성화하고 Network Flow Monitor에서 다중 계정으로 작업할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 Amazon CloudWatch를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. Amazon CloudWatch에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자만 있는 경우 Amazon CloudWatch의 관리자에게 이제 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon CloudWatch를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal observabilityadmin.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

CloudWatch로 신뢰할 수 있는 액세스 끄기

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Amazon CloudWatch 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

⚠ Important

가능하다면 Amazon CloudWatch 콘솔이나 도구를 사용하여 Organizations와의 통합을 비활성화하는 것이 좋습니다. 이렇게 하면 Amazon CloudWatch가 서비스에 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등의 필요한 정리를 수행합니다. Amazon CloudWatch에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다. Amazon CloudWatch 콘솔이나 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화하는 경우 이러한 단계를 완료할 필요가 없습니다.

CloudWatch 콘솔을 사용하여 신뢰할 수 있는 액세스를 끄려면

자세한 내용은 Amazon CloudWatch 사용 설명서의 [CloudWatch 원격 측정 감사 끄기](#)를 참조하세요.

CloudWatch에서 신뢰할 수 있는 액세스를 끄면 원격 측정 감사가 더 이상 활성화되지 않으며 Network Flow Monitor에서 더 이상 다중 계정으로 작업할 수 없습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon CloudWatch를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal observabilityadmin.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

CloudWatch에 대한 위임된 관리자 계정 등록

조직의 위임된 관리자 계정으로 멤버 계정을 등록하면, 해당 계정의 사용자와 역할이 CloudWatch에 대한 관리 작업을 수행할 수 있습니다. 이 작업은 일반적으로 조직 관리 계정으로 로그인한 사용자나

역할만 수행할 수 있습니다. 위임된 관리자 계정을 사용하면 조직의 관리와 CloudWatch의 기능 관리를 분리할 수 있습니다.

최소 권한

Organizations 관리 계정의 관리자만이 조직의 CloudWatch에 대한 위임된 관리자 계정으로 멤버 계정을 등록할 수 있습니다.

CloudWatch 콘솔을 사용하거나 또는 SDK와 함께 Organizations RegisterDelegatedAdministrator API 작업을 사용하여 위임된 관리자 계정을 등록할 수 AWS Command Line Interface 있습니다.

CloudWatch 콘솔을 사용하여 위임된 관리자 계정을 등록하는 방법에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 [CloudWatch 원격 측정 감사 켜기](#)를 참조하세요.

CloudWatch에 위임된 관리자 계정을 등록할 때 원격 측정 감사 및 Network Flow Monitor를 사용하여 관리 작업에 계정을 사용할 수 있습니다.

CloudWatch의 위임된 관리자 등록 취소

최소 권한

Organizations 관리 계정으로 로그인한 관리자만이 조직에서 CloudWatch에 대한 위임된 관리자 계정을 등록 취소할 수 있습니다.

CloudWatch 콘솔을 사용하거나 AWS Command Line Interface 또는 SDK와 함께 Organizations DeregisterDelegatedAdministrator API 작업을 사용하여 위임된 관리자 계정의 등록을 취소할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 [위임된 관리자 계정 등록 취소](#)를 참조하세요.

CloudWatch에서 위임된 관리자 계정을 등록 취소할 때, 원격 측정 감사와 Network Flow Monitor를 사용한 관리 작업을 더 이상 사용할 수 없습니다.

AWS Compute Optimizer 및 AWS Organizations

AWS Compute Optimizer 는 AWS 리소스의 구성 및 사용을 지표 분석하는 서비스입니다. 리소스의 예로는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 Auto Scaling 그룹이 있습니다. Compute Optimizer는 리소스가 최적 상태인지 여부를 보고하고, 최적화 권장 사항을 생성하여 비용을

절감하고 워크로드의 성능을 개선합니다. Compute Optimizer에 대한 자세한 내용은 [AWS Compute Optimizer 사용 설명서](#)를 참조하세요.

다음 정보를 사용하여 AWS Compute Optimizer 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Compute Optimizer는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Compute Optimizer와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForComputeOptimizer`
- `AWSServiceRoleForComputeOptimizerAutomation`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Compute Optimizer가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `compute-optimizer.amazonaws.com`

Compute Optimizer와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS Compute Optimizer 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Compute Optimizer 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Compute Optimizer 수행할 수 있습니다. AWS Compute Optimizer에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Compute Optimizer 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하는 경우 이 단계를 완료할 필요가 없습니다.

Compute Optimizer 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

조직의 관리 계정을 사용하여 Compute Optimizer 콘솔에 로그인해야 합니다. AWS Compute Optimizer 사용 설명서에 있는 [계정 옵트인하기](#)의 설명에 따라 조직을 대신해 옵트인합니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Compute Optimizer를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Compute Optimizer에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Compute Optimizer 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Compute Optimizer 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
```



```
--service-principal compute-optimizer.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Compute Optimizer와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다. AWS Compute Optimizer.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Compute Optimizer를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal compute-optimizer.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Compute Optimizer에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 지정된 계정의 사용자 및 역할이 조직의 다른 멤버 계정의 AWS 계정 메타데이터를 관리할 수 있습니다. 위임된 관리자 계정을 활성화하지 않으면 조직의 관리 계정에서만 이러한 작업을 수행할 수 있습니다. 이렇게 하면 조직의 관리와 계정 세부 정보의 관리를 분리하는 데 도움이 됩니다.

최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Compute Optimizer에 대한 위임된 관리자로 구성할 수 있습니다

Compute Optimizer에 대한 위임된 관리자 계정 활성화에 대한 설명은 AWS Compute Optimizer 사용 설명서의 <https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html> 섹션을 참조하세요.

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal compute-optimizer.amazonaws.com
```

- AWS SDK: Organizations RegisterDelegatedAdministrator 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체를 파라미터 `account.amazonaws.com`로 식별합니다.

Compute Optimizer에 대한 위임된 관리자 비활성화

조직 관리 계정의 관리자만 Compute Optimizer에 대해 위임된 관리자를 구성할 수 있습니다.

Compute Optimizer 콘솔을 사용하여 위임된 관리자 Compute Optimizer 계정을 사용하지 않도록 설정하려면 AWS Compute Optimizer 사용 설명서의 <https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html> 섹션을 참조하세요.

를 사용하여 위임된 관리자를 제거하려면 AWS CLI 명령 `aws organizations deregister-delegated-administrator`를 참조하세요.

AWS Config 및 AWS Organizations

의 다중 계정, 다중 리전 데이터 집계 AWS Config 를 사용하면 여러 계정의 AWS Config 데이터를 단일 계정으로 집계 AWS 리전 할 수 있습니다. 다중 계정, 다중 리전 데이터 집계는 중앙 IT 관리자가 엔터프라이즈에서 여러 AWS 계정 의 규정 준수를 모니터링하는 데 유용합니다. 애그리게이터는 여러 소

스 계정 및 리전에서 AWS Config 데이터를 AWS Config 수집하는 리소스 유형입니다. 집계된 AWS Config 데이터를 보려는 리전에 집계자를 생성합니다. 집계를 생성할 때 개별 계정 ID 추가 또는 사용자 조직 추가 중에서 하나를 선택할 수 있습니다. 에 대한 자세한 내용은 [AWS Config 개발자 안내서](#)를 AWS Config참조하세요.

[AWS Config APIs](#) 사용하여 조직의 모든 AWS 계정 에서 규칙을 관리할 AWS Config 수도 있습니다. 자세한 내용은 AWS Config 개발자 안내서의 [조직 내 모든 계정에서 AWS Config 규칙 활성화](#)를 참조하세요.

다음 정보를 사용하여 AWS Config 와 통합할 수 있습니다 AWS Organizations.

서비스 연결 역할

다음 [서비스 연결 역할](#)을 통해서는 조직의 계정 내에서 지원되는 작업을 AWS Config 수행할 수 있습니다.

- AWSServiceRoleForConfig

AWS Config 개발자 안내서의 [AWS Config에 할당된 IAM 역할에 대한 권한](#)에서 이 역할을 생성하는 방법 자세히 알아보기

AWS Config 개발자 안내서의 서비스 연결 역할 AWS Config 사용에서 [서비스 연결 역할을 사용하는 방법에 대해 AWS Config](#) 자세히 알아보기

AWS Config 와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

를 사용하여 신뢰할 수 있는 액세스 활성화 AWS Config

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS Config 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Config 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Config

수행할 수 있습니다. AWS Config에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.
AWS Config 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하면이 단계를 완료할 필요가 없습니다.

AWS Config 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

를 AWS Organizations 사용하여에 대한 신뢰할 수 있는 액세스를 활성화하려면 다중 계정 애그리게이터를 AWS Config생성하고 조직을 추가합니다. 다중 계정 집계자를 구성하는 방법에 대한 자세한 내용은 AWS Config 개발자 안내서의 [집계자 생성](#)을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Config를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Config에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Config 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Config 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal config.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

를 사용하여 신뢰할 수 있는 액세스 비활성화 AWS Config

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Config 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal config.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

AWS Cost Optimization Hub 및 AWS Organizations

AWS Cost Optimization Hub 는 AWS 계정 및 AWS 리전에서 비용 최적화 권장 사항을 통합하고 우선 순위를 지정하여 AWS 지출을 최대한 활용할 수 있는 AWS Billing and Cost Management 기능입니다. Cost Optimization Hub를와 함께 사용하면 Organizations 멤버 계정 및 AWS 리전에서 AWS 비용 최적화 권장 사항을 쉽게 식별, 필터링 및 집계할 AWS Organizations 수 있습니다.

자세한 내용은 AWS Cost Management 사용 설명서의 [Cost Optimization Hub](#)를 참조하세요.

다음 정보를 사용하여 AWS Cost Optimization Hub 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Cost Optimization Hub는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Cost Optimization Hub와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

자세한 내용은 AWS Cost Management 사용 설명서의 [Cost Optimization Hub에 대한 서비스 연결 역할 권한](#)을 참조하세요.

- `AWSServiceRoleForCostOptimizationHub`

Cost Optimization Hub에서 사용하는 서비스 위탁자

Cost Optimization Hub는 `cost-optimization-hub.bcm.amazonaws.com` 서비스 위탁자를 사용합니다.

Cost Optimization Hub를 사용하여 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

조직의 관리 계정을 사용하여 옵트인하고 조직의 모든 멤버 계정을 포함하면 조직 계정에서 Cost Optimization Hub에 대한 신뢰할 수 있는 액세스가 자동으로 활성화됩니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Cost Optimization Hub를 선택합니다.

4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Cost Optimization Hub에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Cost Optimization Hub 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Cost Optimization Hub 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal cost-optimization-hub.bcm.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

트러스트된 액세스 사용 중지

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Important

옵트인 후에 Cost Optimization Hub 신뢰할 수 있는 액세스를 비활성화하면 Cost Optimization Hub는 조직의 멤버 계정에 대한 권장 사항에 대한 액세스를 거부합니다. 또한 조직 내 멤버 계정은 Cost Optimization Hub에 옵트인되지 않습니다. AWS Cost Management 사용 설명서의 [Cost Optimization Hub 및 Organizations 신뢰할 수 있는 액세스](#)에서 자세히 알아보세요.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Cost Optimization Hub를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal cost-optimization-hub.bcm.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Cost Optimization Hub에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 지정된 계정이 조직의 모든 계정에 대한 Cost Optimization Hub 권장 사항을 검색하고 Cost Optimization Hub 기본 설정을 관리하여 리소스 최적화 기회를 중앙에서 보다 유연하게 식별할 수 있습니다.

최소 권한

다음 권한이 있는 Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Cost Optimization Hub에 대해 위임된 관리자로 구성할 수 있습니다.

Cost Optimization Hub에 대한 위임된 관리자 계정 활성화에 대한 지침은 AWS Cost Management 사용 설명서의 [관리자 계정 위임](#)을 참조하세요.

Cost Optimization Hub에 대해 위임된 관리자 비활성화

Organizations 관리 계정의 관리자만 Cost Optimization Hub의 위임된 관리자를 제거할 수 있습니다.

Cost Optimization Hub 콘솔을 사용하여 위임된 관리자 Cost Optimization Hub 계정을 비활성화하려면 AWS Cost Management 사용 설명서의 [관리자 계정 위임](#)을 참조하세요.

AWS CLI를 사용하여 위임된 관리자를 제거하려면 AWS Config CLI 참조 [deregister-delegated-administrator](#)의 섹션을 참조하세요.

AWS Control Tower 및 AWS Organizations

AWS Control Tower 는 규범적 모범 사례를 따라 AWS 다중 계정 환경을 설정하고 관리하는 간단한 방법을 제공합니다. AWS Control Tower 오케스트레이션은의 기능을 확장합니다 AWS Organizations.는 예방 및 탐지 제어(가드레일)를 AWS Control Tower 적용하여 조직과 계정이 모범 사례(드리프트)에서 벗어나지 않도록 합니다.

AWS Control Tower 오케스트레이션은의 기능을 확장합니다 AWS Organizations.

자세한 내용은 [AWS Control Tower 사용 설명서를 참조하세요](#).

다음 정보를 사용하여 AWS Control Tower 와 통합할 수 있습니다 AWS Organizations.

통합에 필요한 역할

등록된 모든 계정에 `AWSControlTowerExecution` 역할이 있어야 합니다. 이를 통해 AWS Control Tower 는 개별 계정을 관리하고 이에 대한 정보를 감사 및 로그 아카이브 계정에 보고할 수 있습니다.

에서 사용하는 역할에 대한 자세한 내용은 [AWS Control Tower 가 역할과 함께 계정을 생성하고 관리하는 방법 및](#)에 대한 자격 증명 기반 정책(IAM 정책) 사용을 AWS Control Tower참조하세요. [AWS Control Tower](#)

에서 사용하는 서비스 보안 주체 AWS Control Tower

AWS Control Tower 는 `controltower.amazonaws.com` 서비스 보안 주체를 사용합니다.

를 사용하여 신뢰할 수 있는 액세스 활성화 AWS Control Tower

AWS Control Tower 는 신뢰할 수 있는 액세스를 사용하여 예방 제어를 위한 드리프트를 감지하고 드리프트를 유발하는 계정 및 OU 변경 사항을 추적합니다.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

Organizations 콘솔에서 신뢰할 수 있는 액세스를 활성화하려면 AWS Control Tower 옆의 **Enable access**를 선택합니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Control Tower 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal controltower.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

를 사용하여 신뢰할 수 있는 액세스 비활성화 AWS Control Tower

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Important

AWS Control Tower의 신뢰할 수 있는 액세스를 비활성화하면 AWS Control Tower 랜딩 존에 드리프트가 발생합니다. 드리프트를 해결할 수 있는 유일한 방법은 AWS Control Tower의 랜딩 존 수리를 사용하는 것입니다. 조직에서 신뢰할 수 있는 액세스를 다시 활성화해도 드리프트가 해결되지 않습니다. AWS Control Tower 사용 설명서에서 [드리프트에 대해 자세히 알아보세요](#).

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Control Tower 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal controltower.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Amazon Detective 및 AWS Organizations

Amazon Detective는 로그 데이터를 사용하여 시각화를 생성하며, 이 시각화를 사용하여 보안 결과 또는 의심스러운 활동의 근본 원인을 분석, 조사 및 식별할 수 있습니다.

를 AWS Organizations 사용하면 Detective 동작 그래프가 모든 조직 계정의 활동에 대한 가시성을 제공할 수 있습니다.

Detective 에 신뢰할 수 있는 액세스 권한을 부여하면 Detective 서비스가 조직 멤버십의 변화에 자동으로 대응할 수 있습니다. 위임된 관리자는 동작 그래프에서 모든 조직 계정을 멤버 계정으로 활성화할 수 있습니다. 또한 Detective는 자동으로 새 조직 계정을 멤버 계정으로 활성화할 수 있습니다. 조직 계정은 동작 그래프에서 자신을 연결 해제할 수 없습니다.

자세한 내용은 Amazon Detective 관리 안내서의 [조직에서 Amazon Detective 사용](#)을 참조하세요.

다음 정보를 사용하여 Amazon Detective를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Detective는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Detective와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- AWSServiceRoleForDetective

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Detective가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `detective.amazonaws.com`

Detective에서 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Note

Amazon Detective에 대해 위임된 관리자를 지정하면 조직의 Detective에 대해 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

Detective는 멤버 계정을 조직의이 서비스에 대한 위임된 관리자로 지정하기 AWS Organizations 전역에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 Amazon Detective를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. Amazon Detective에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만 Amazon Detective의 관리자에게 서비스 콘솔 AWS Organizations 에서 해당 서비스를 사용할 수 있도록 설정할 수 있다고 AWS Organizations알립니다.

Detective에서 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 Amazon Detective에서 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 Amazon Detective를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. Amazon Detective에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자만 있는 경우 Amazon Detective의 관리자에게 이제 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 있다고 AWS Organizations알립니다.

Detective에 대한 위임된 관리자 계정 활성화

Detective에 대한 위임된 관리자 계정은 Detective 동작 그래프의 관리자 계정입니다. 위임된 관리자는 동작 그래프에서 멤버 계정으로 활성화하거나 비활성화할 조직 계정을 결정합니다. 위임된 관리자는 새 조직 계정이 조직에 추가될 때 자동으로 새 조직 계정을 멤버 계정으로 활성화하도록 Detective를 구성할 수 있습니다. 위임된 관리자가 조직 계정을 관리하는 방법에 대한 자세한 내용은 Amazon Detective 관리 안내서의 [조직 계정을 멤버 계정으로 관리](#)를 참조하세요.

조직 관리 계정의 관리자만 Detective에 대해 위임된 관리자를 구성할 수 있습니다.

Detective 콘솔이나 API에서 또는 Organizations CLI 또는 SDK 작업을 사용하여 위임된 관리자 계정을 지정할 수 있습니다.

i 최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Detective에 대한 위임된 관리자로 구성할 수 있습니다

Detective 콘솔 또는 API를 사용하여 위임된 관리자를 구성하려면 Amazon Detective 관리 안내서의 [조직의 Detective 관리자 계정 지정](#)을 참조하세요.

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal detective.amazonaws.com
```

- AWS SDK: Organizations RegisterDelegatedAdministrator 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체를 파라미터account.amazonaws.com로 식별합니다.

Detective에 대해 위임된 관리자를 비활성화

Detective 콘솔이나 API에서 또는 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. Detective 콘솔 또는 API를 사용하거나 Organizations API를 사용하여 위임된 관리자를 제거하는 방법에 대한 자세한 내용은 Amazon Detective 관리 안내서의 [조직의 Detective 관리자 계정 지정](#)을 참조하세요.

Amazon DevOps Guru 및 AWS Organizations

Amazon DevOps Guru는 운영 데이터와 애플리케이션 지표 및 이벤트를 분석하여 정상적인 운영 패턴에서 벗어나는 동작을 식별합니다. DevOps Guru가 운영 문제 또는 위험을 감지하면 사용자에게 알림이 전송됩니다.

DevOps Guru를 사용하면에서 다중 계정 지원을 사용할 수 AWS Organizations있으므로 전체 조직에서 인사이트를 관리할 멤버 계정을 지정할 수 있습니다. 그러면 이 위임된 관리자는 조직 내의 모든 계정에서 인사이트를 보고 정렬하고 필터링할 수 있으므로 추가적으로 사용자 정의할 필요 없이 조직 내에서 모니터링되는 모든 애플리케이션의 상태를 전체적으로 파악할 수 있습니다.

자세한 내용은 Amazon DevOps Guru 사용 설명서에서 [조직 전체의 계정 모니터링](#)을 참조하세요.

다음 정보를 사용하여 Amazon DevOps Guru를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 DevOps Guru는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

DevOps Guru와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForDevOpsGuru`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. DevOps Guru가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `devops-guru.amazonaws.com`

자세한 내용은 Amazon DevOps Guru 사용 설명서에서 [DevOps Guru에 서비스 연결 역할 사용](#)을 참조하세요.

DevOps Guru에서 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Note

Amazon DevOps Guru에 대해 위임된 관리자를 지정하면 조직의 DevOps Guru에 대해 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

DevOps Guru는 멤버 계정을 조직의이 서비스에 대한 위임된 관리자로 지정하기 AWS Organizations 전에에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

⚠ Important

가능하면 항상 Amazon DevOps Guru 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 Amazon DevOps Guru가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. Amazon DevOps Guru에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Organizations 콘솔 또는 DevOps Guru 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [서비스\(Services\)](#) 페이지에서 Amazon DevOps Guru의 행을 찾고 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 의 관리자만 있는 경우 Amazon DevOps Guru의 관리자에게 콘솔을 사용하여 해당 서비스를 활성화할 수 있음을 AWS Organizations알립니다 AWS Organizations.

DevOps Guru console

DevOps Guru 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

1. 관리 계정에서 관리자로 로그인하고 [Amazon DevOps Guru 콘솔\(Amazon DevOps Guru console\)](#)을 선택하여 DevOps Guru 콘솔을 엽니다.
2. 신뢰할 수 있는 액세스 활성화를 선택합니다.

DevOps Guru에서 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 Amazon DevOps Guru에서 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 Amazon DevOps Guru를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. Amazon DevOps Guru에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자인 경우에만 Amazon DevOps Guru의 관리자에게 해당 서비스가 서비스 콘솔 또는 도구를 사용하여 작업 AWS Organizations 하지 못하도록 비활성화할 수 있다고 AWS Organizations알립니다.

DevOps Guru에 대한 위임된 관리자 계정 활성화

DevOps Guru의 위임된 관리자 계정은 조직에서 DevOps Guru에 온보딩된 모든 멤버 계정의 인사이드 데이터를 볼 수 있습니다. 위임된 관리자가 조직 계정을 관리하는 방법에 대한 자세한 내용은 Amazon DevOps Guru 사용 설명서의 [조직 전체의 계정 모니터링](#)을 참조하세요.

조직 관리 계정의 관리자만 DevOps Guru에 대해 위임된 관리자를 구성할 수 있습니다.

DevOps Guru 콘솔에서 또는 Organizations RegisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자 계정을 지정할 수 있습니다.

❗ 최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 DevOps Guru에 대한 위임된 관리자로 구성할 수 있습니다

DevOps Guru console

DevOps Guru 콘솔에서 위임된 관리자를 구성하려면

1. 관리 계정에서 관리자로 로그인하고 [Amazon DevOps Guru 콘솔\(Amazon DevOps Guru console\)](#)을 선택하여 DevOps Guru 콘솔을 엽니다.
2. 위임된 관리자 등록을 선택합니다. 관리 계정 또는 원하는 멤버 계정을 위임된 관리자로 선택할 수 있습니다.

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal devops-guru.amazonaws.com
```

- AWS SDK: Organizations RegisterDelegatedAdministrator 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체를 파라미터account.amazonaws.com로 식별합니다.

DevOps Guru에 대해 위임된 관리자를 비활성화

DevOps Guru 콘솔을 사용하거나 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. DevOps Guru 콘솔을 사용하여 위임된 관리자를 제거하는 방법에 대한 자세한 내용은 Amazon DevOps Guru 사용 설명서의 [조직 전체의 계정 모니터링](#)을 참조하세요.

AWS Directory Service 및 AWS Organizations

AWS Directory Service Microsoft Active Directory용 또는 AWS Managed Microsoft AD를 사용하면 Microsoft Active Directory(AD)를 관리형 서비스로 실행할 수 있습니다. AWS Directory Service 를 사용하면 AWS 클라우드에서 디렉터리를 쉽게 설정 및 실행하거나 AWS 리소스를 기존 온프레미스 Microsoft Active Directory와 연결할 수 있습니다. AWS Managed Microsoft AD 또한는와 긴밀하게 통합되어 리전의 여러 VPC AWS 계정 와 VPC 간에 디렉터리를 원활하게 공유할 수 AWS Organizations 있습니다. 자세한 정보는 [AWS Directory Service 관리 안내서](#)를 참조하세요.

조직 Directory Service 전체에서를 공유하려면 조직에 모든 기능이 활성화되어 있어야 하며 디렉터리가 조직 관리 계정에 있어야 합니다.

다음 정보를 사용하여 AWS Directory Service 와 통합할 수 있습니다 AWS Organizations.

를 사용하여 신뢰할 수 있는 액세스 활성화 Directory Service

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS Directory Service 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Directory Service 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Directory Service 수행할 수 있습니다. AWS Directory Service에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Directory Service 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하면이 단계를 완료할 필요가 없습니다.

Directory Service 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 자동으로 활성화하는 디렉터리를 공유하려면 AWS Directory Service 관리 안내서의 [내 디렉터리 공유](#)를 참조하세요. step-by-step[자습서: AWS 관리형 Microsoft AD 디렉터리 공유를 참조하세요.](#)

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Directory Service를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Directory Service에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔 AWS Organizations 에서 해당 서비스를 사용할 수 있도록 설정할 수 AWS Directory Service 있다고 AWS Organizations알립니다.

를 사용하여 신뢰할 수 있는 액세스 비활성화 Directory Service

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

사용 AWS Organizations 중어를 사용하여 신뢰할 수 있는 액세스를 비활성화하면 이전에 공유된 Directory Service모든 디렉터리가 정상적으로 계속 작동합니다. 하지만 신뢰할 수 있는 액세스를 다시 활성화할 때까지 조직 내에서 새 디렉터리를 더 이상 공유할 수 없습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Directory Service를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS Directory Service에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.

6. 의 관리자만 있는 경우 이제 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 AWS Directory Service 있다고 관리자에게 AWS Organizations 알립니다.

Amazon Elastic Compute Cloud 및 AWS Organizations

Amazon Elastic Compute Cloud는 AWS 클라우드에서 확장 가능한 온디맨드 컴퓨팅 용량을 제공합니다. Organizations로 Amazon EC2를 사용하는 경우 Organizations 관리자가 Amazon EC2의 [선언적 정책](#) 기능을 사용한 후 조직 전체의 계정에 대한 기존 구성에 대한 보고서를 생성할 수 있습니다.

다음 정보를 사용하여 Amazon Elastic Compute Cloud를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Amazon EC2는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Amazon EC2와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForDeclarativePoliciesEC2Report`

Amazon EC2가 사용하는 서비스 위탁자

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Amazon EC2가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `ec2.amazonaws.com`

Amazon EC2를 사용하여 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Organizations 관리자가 조직 전체의 계정에 대한 기존 구성에 대한 보고서를 생성하도록 하려면 신뢰할 수 있는 액세스를 활성화해야 합니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 EC2에 대한 선언적 정책을 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. EC2에 대한 선언적 정책에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만 Amazon Elastic Compute Cloud의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon Elastic Compute Cloud를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal ec2.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

트러스트된 액세스 사용 중지

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon Elastic Compute Cloud를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal ec2.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

EC2 용량 관리자 및 AWS Organizations

EC2 용량 관리자는 EC2 온디맨드, 스팟, 용량 예약 전반에서 용량 사용량을 집계, 확인, 분석, 관리할 수 있도록 API가 함께 제공되는 새로운 UI 환경입니다. AWS 조직에 EC2 용량 관리자에 대한 신뢰할 수 있는 액세스 권한을 부여하면 서비스는 모든 멤버 계정에서 조직 멤버십 정보를 읽을 수 있는 권한을 얻습니다. 특히 용량 관리자는 멤버 계정에서 모든 멤버 계정에서 EC2 사용 데이터(온디맨드 인스턴스, 스팟 인스턴스, 용량 예약 포함)를 수집하여 조직 전체 용량 보고서 및 대시보드로 집계하는 작업을 수행합니다. 서비스는 멤버 계정의 리소스 또는 구성을 수정하지 않고 AWS에서 이미 수집한 사용량 원격 측정 데이터만 읽습니다. 이를 통해 조직 관리자는 단일 대시보드에서 통합 용량 사용을 보고, 향후 요구 사항을 예측하고, 조직 전체의 리소스 할당을 최적화할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 [EC2 용량 관리자](#)를 참조하세요.

다음 정보를 사용하여 EC2 용량 관리자와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 EC2 용량 관리자는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

EC2 용량 관리자와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

신뢰할 수 있는 액세스를 활성화하면 관리 계정에 다음 서비스 연결 역할이 생성됩니다. 이 역할을 통해 EC2 용량 관리자는 사용자를 대신하여 조직과 계정에서 작업을 수행할 수 있습니다.

EC2 용량 관리자와 간에 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거하는 경우에만 이 역할을 삭제 AWS Organizations하거나 수정할 수 있습니다. 자세한 내용은 [EC2 용량 관리자에 대한 서비스 연결 역할 사용](#) 및 Amazon EC2 사용 설명서의 [AWS 관리형 정책: AWSEC2CapacityManagerServiceRolePolicy](#)를 참조하세요.

- AWSServiceRoleForEC2CapacityManager - EC2 용량 관리자가 사용자를 대신하여 EC2 용량 관리자가 사용하거나 관리하는 AWS 서비스 및 리소스에 액세스할 수 있도록 허용합니다.

EC2 용량 관리자가 사용하는 서비스 위탁자

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. EC2 용량 관리자가 사용하는 서비스 연결 역할은 다음 서비스 위탁자에 대한 액세스 권한을 부여합니다.

- `ec2.capacitymanager.amazonaws.com`

EC2 용량 관리자와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

EC2 용량 관리자에 대한 신뢰할 수 있는 액세스 권한을 AWS 조직에 부여하면 서비스는 모든 멤버 계정에서 조직 멤버십 정보를 읽을 수 있는 권한을 얻습니다. 이를 통해 조직 관리자는 단일 대시보드에서 통합 용량 사용을 보고, 향후 요구 사항을 예측하고, 조직 전체의 리소스 할당을 최적화할 수 있습니다.

EC2 용량 관리자 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

Important

가능하면 항상 EC2 용량 관리자 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 EC2 용량 관리자가 서비스에 필요한 리소스 생성 등 모든 필

수 구성을 수행합니다. EC2 용량 관리자에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오. EC2 용량 관리자 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

EC2 용량 관리자 콘솔에서 신뢰할 수 있는 액세스를 활성화하려면 관리 계정에서 관리자로 로그인하고 Amazon EC2 콘솔을 엽니다. 용량 관리자로 이동하여 설정 탭으로 이동합니다. 신뢰할 수 있는 액세스 섹션에서 신뢰할 수 있는 액세스 관리를 선택하여 활성화합니다.

AWS Organizations 콘솔을 사용하거나, 명령을 실행 AWS CLI 하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 EC2 용량 관리자를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. EC2 용량 관리자에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만 EC2 용량 관리자의 관리자에게 서비스 콘솔 AWS Organizations 에서 해당 서비스를 사용할 수 있도록 설정할 수 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 EC2 용량 관리자를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
```

```
--service-principal ec2.capacitymanager.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

트러스트된 액세스 사용 중지

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

EC2 용량 관리자 콘솔에서 신뢰할 수 있는 액세스를 비활성화하려면 Amazon EC2 용량 관리자 설정 탭으로 이동합니다. 신뢰할 수 있는 액세스 섹션에서 신뢰할 수 있는 액세스 관리를 선택하여 비활성화합니다. 참고: 신뢰할 수 있는 액세스를 비활성화하기 전에 위임된 모든 관리자를 제거해야 합니다.

EC2 용량 관리자 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Important

가능하면 항상 EC2 용량 관리자 콘솔 또는 도구를 사용하여 Organizations 통합을 비활성화할 것을 적극 권장합니다. 이렇게 하면 EC2 용량 관리자가 서비스에 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등의 필요한 정리를 수행합니다. EC2 용량 관리자에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다. EC2 용량 관리자 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 EC2 용량 관리자를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal ec2.capacitymanager.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

EC2 용량 관리자에 대한 위임된 관리자 계정 활성화

EC2 용량 관리자의 위임된 관리자는 관리 계정을 사용하지 않고도 조직의 용량 관리자를 관리할 수 있습니다. 위임된 관리자는 조직 수준의 용량 관리를 활성화하고, 모든 멤버 계정의 용량 데이터를 보고, 계정 수준과 조직 수준 범위 간의 설정을 수정하고, 전체 조직의 용량 예측을 관리할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 [EC2 용량 관리자의 위임된 관리자](#)를 참조하세요.

최소 권한

Organizations 관리 계정의 관리자만 EC2 용량 관리자에 대해 위임된 관리자를 구성할 수 있습니다.

설정으로 이동하여 위임된 관리자를 관리하거나 Organizations RegisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 EC2 용량 관리자 콘솔을 사용하여 위임된 관리자 계정을 지정할 수 있습니다. EC2 용량 관리자 콘솔을 사용하여 위임된 관리자를 구성하려면 Amazon EC2 사용 설명서의 [위임된 관리자 추가](#)를 참조하세요.

AWS CLI, AWS API

AWS CLI 또는 AWS SDKs.

- AWS CLI: [register-delegated-administrator](#)

```
$ aws organizations register-delegated-administrator \
  --account-id ACCOUNT_ID \
  --service-principal ec2.capacitymanager.amazonaws.com
```

- AWS API: [RegisterDelegatedAdministrator](#)

EC2 용량 관리자에 위임된 관리자 계정 비활성화

Organizations 관리 계정 또는 EC2 용량 관리자의 위임된 관리자 계정의 관리자만 조직에서 위임된 관리자 계정을 제거할 수 있습니다. 설정 탭에서 위임된 관리자 제거를 선택하거나 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여, EC2 용량 관리자 콘솔을 사용하여 위임된 관리자를 제거할 수 있습니다. EC2 용량 관리자 콘솔을 사용하여 위임된 관리자를 제거하려면 Amazon EC2 사용 설명서의 [위임된 관리자 제거](#)를 참조하세요.

AWS CLI, AWS API

AWS CLI 또는 AWS SDKs.

- AWS CLI: [deregister-delegated-administrator](#)

```
$ aws organizations deregister-delegated-administrator \
  --account-id ACCOUNT_ID \
  --service-principal ec2.capacitymanager.amazonaws.com
```

- AWS API: [DeregisterDelegatedAdministrator](#)

Amazon Elastic Kubernetes Service 및 AWS Organizations

Amazon Elastic Kubernetes 서비스 대시보드는 여러 AWS 리전 및 AWS 계정의 Kubernetes 클러스터를 모니터링, 관리 및 파악하는 데 사용할 수 있는 통합 대시보드입니다. EKS 대시보드는 중앙 집중식 인터페이스를 통해 Amazon EKS 인프라에 대한 포괄적인 제어 및 인사이트를 제공합니다.

Amazon Elastic Kubernetes 서비스 대시보드를 사용하면 업그레이드 예약된 클러스터를 추적하고, 프로젝트별 컨트롤 플레인 비용을 관리하고, 클러스터 인사이트를 검토하고, 조직 전체의 노드 그룹 분포를 모니터링할 수 있습니다. AWS 관리자는 그래프, 리소스 목록, 지리적 맵 등 다양한 시각화 옵션을 통해 상태, 버전 배포, 추가 기능 구성을 포함한 클러스터 리소스에 대한 집계된 데이터를 볼 수 있습니다. 대시보드는 AWS Organizations와 통합되어 EKS 리소스에 대한 안전한 교차 계정 및 교차 리전 가시성을 제공합니다.

다음 정보를 사용하여 Amazon Elastic Kubernetes Service를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

Amazon Elastic Kubernetes 서비스 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Amazon EKS는 조직의 계정

내에서 지원되는 작업을 수행할 수 있습니다. Amazon Elastic Kubernetes 서비스와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

Organizations 콘솔, CLI 또는 SDK에서 직접 신뢰할 수 있는 액세스를 활성화하면 서비스 연결 역할이 자동으로 생성되지 않습니다.

- `AWSServiceRoleForAmazonEKSDashboard`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Amazon EKS가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `dashboard.eks.amazonaws.com`

Amazon EKS를 사용하여 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Amazon EKS 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

Amazon EKS 사용 설명서의 [신뢰할 수 있는 액세스 활성화](#)를 참조하세요.

Amazon EKS를 사용하여 신뢰할 수 있는 액세스 비활성화

Amazon EKS 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

Amazon EKS 사용 설명서의 [신뢰할 수 있는 액세스 비활성화](#)를 참조하세요.

Amazon EKS에 대한 위임된 관리자 계정 활성화

관리 계정 관리자는 Amazon EKS 관리 권한을 위임된 관리자라고 하는 지정된 멤버 계정에 위임할 수 있습니다.

관리 계정과 위임된 관리자 계정만 Amazon EKS 대시보드를 볼 수 있습니다.

위임된 관리자 계정 활성화

Amazon EKS 사용 설명서의 [위임된 관리자 계정 활성화](#)를 참조하세요.

Amazon EKS에 대해 위임된 관리자를 비활성화

조직 관리 계정의 관리자만 Amazon EKS에 대해 위임된 관리자를 구성할 수 있습니다.

위임된 관리자 계정 비활성화

Amazon EKS 사용 설명서의 [위임된 관리자 계정 비활성화](#)를 참조하세요.

AWS Firewall Manager 및 AWS Organizations

AWS Firewall Manager 는 조직의 및 애플리케이션에서 방화벽 규칙 및 기타 보호를 중앙에서 구성 AWS 계정 하고 관리하는 데 사용하는 보안 관리 서비스입니다. Firewall Manager를 사용하면 AWS WAF 규칙을 롤아웃하고, 보호를 생성하고 AWS Shield Advanced , Amazon Virtual Private Cloud(Amazon VPC) 보안 그룹을 구성 및 감사하고, AWS Network Firewall를 배포할 수 있습니다. Firewall Manager를 사용하여 보호 기능을 한 번만 설정하고, 조직 내 모든 계정과 리소스에 자동으로 적용합니다. 새로운 리소스와 계정이 추가될 때도 같습니다. 에 대한 자세한 내용은 [AWS Firewall Manager 개발자 안내서](#)를 AWS Firewall Manager참조하세요.

다음 정보를 사용하여 AWS Firewall Manager 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Firewall Manager는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Firewall Manager와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForFMS`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다른 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Firewall Manager가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `fms.amazonaws.com`

Firewall Manager와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS Firewall Manager 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Firewall Manager 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Firewall Manager 수행할 수 있습니다. AWS Firewall Manager에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Firewall Manager 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하면이 단계를 완료할 필요가 없습니다.

AWS Organizations 관리 계정으로 로그인하고 조직 내 계정을 AWS Firewall Manager 관리자 계정으로 구성해야 합니다. 자세한 내용은 AWS Firewall Manager 개발자 안내서의 [AWS Firewall Manager 관리자 계정 설정](#)을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Firewall Manager를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Firewall Manager에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.

6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Firewall Manager 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Firewall Manager 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal fms.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Firewall Manager와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Firewall Manager 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Important

가능하면 AWS Firewall Manager 콘솔 또는 도구를 사용하여 Organizations와의 통합을 비활성화하는 것이 좋습니다. 이렇게 하면 서비스에서 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등 필요한 모든 정리를 AWS Firewall Manager 수행할 수 있습니다. AWS Firewall Manager에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.

AWS Firewall Manager 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화하면이 단계를 완료할 필요가 없습니다.

Firewall Manager 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

AWS Firewall Manager 개발자 안내서의 다른 계정을 AWS Firewall Manager 관리자 [계정으로 지칭의 지침에 따라 AWS Firewall Manager 관리자 계정을](#) 변경하거나 취소할 수 있습니다.

관리자 계정을 취소하는 경우 AWS Organizations 관리 계정에 로그인하고 새 관리자 계정을 설정해야 합니다 AWS Firewall Manager.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Firewall Manager를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS Firewall Manager에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 AWS Firewall Manager 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Firewall Manager 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal fms.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Firewall Manager에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Firewall Manager에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Firewall Manager 관리와 조직 관리를 분리하는 데 도움을 줍니다.

최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Firewall Manager에 대한 위임된 관리자로 구성할 수 있습니다.

멤버 계정을 조직의 Firewall Manager 관리자로 지정하는 방법에 대한 지침은 AWS Firewall Manager 개발자 안내서 [의 AWS Firewall Manager 관리자 계정 설정을](#) 참조하세요.

Amazon GuardDuty 및 AWS Organizations

Amazon GuardDuty는 AWS 환경 내에서 예상치 못한 잠재적으로 악의적인 무단 활동을 식별하기 위해 위협 인텔리전스 피드와 기계 학습을 사용하여 다양한 데이터 원본을 분석 및 처리하는 지속적 보안 모니터링 서비스입니다. 여기에는 권한 에스컬레이션, 노출된 자격 증명 사용, 악의적인 IP 주소, URL 또는 도메인과의 통신, Amazon Elastic Compute Cloud 인스턴스 및 컨테이너 워크로드에 존재하는 맬웨어 같은 문제가 포함될 수 있습니다.

Organizations를 사용하여 조직의 모든 계정에서 GuardDuty를 관리하면 GuardDuty 관리를 단순화할 수 있습니다.

자세한 내용은 Amazon GuardDuty 사용 설명서의 [AWS Organizations로 GuardDuty 계정 관리](#)를 참조하세요.

다음 정보를 사용하여 Amazon GuardDuty를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다. 이러한 역할을 통해 GuardDuty는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

GuardDuty와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 역할을 삭제할 수 있습니다.

- AWSServiceRoleForAmazonGuardDuty 서비스 연결 역할은 GuardDuty가 Organizations와 통합된 계정에 자동으로 생성됩니다. 자세한 내용은 Amazon GuardDuty 사용 설명서의 [Organizations로 GuardDuty 계정 관리](#)를 참조하세요.
- AmazonGuardDutyMalwareProtectionServiceRolePolicy 서비스 연결 역할은 GuardDuty Malware Protection이 활성화된 계정에 자동으로 생성됩니다. 자세한 내용은 Amazon GuardDuty 사용 설명서의 [GuardDuty Malware Protection을 위한 서비스 연결 역할 권한](#)을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

- AWSServiceRoleForAmazonGuardDuty 서비스 연결 역할에서 사용하는 `guardduty.amazonaws.com`.
- `malware-protection.guardduty.amazonaws.com` 서비스 연결 역할에서 사용하는 `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

GuardDuty와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Amazon GuardDuty로만 활성화할 수 있습니다.

멤버 계정을 조직의 GuardDuty 관리자로 지정하려면 Amazon GuardDuty에서에 대한 신뢰할 AWS Organizations 수 있는 액세스 권한이 필요합니다. GuardDuty 콘솔을 사용해 위임된 관리자를 구성하는 경우 GuardDuty가 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

그러나 AWS CLI 또는 AWS SDKs 중 하나를 사용하여 위임된 관리자 계정을 구성하려면 [EnableAWSServiceAccess](#) 작업을 명시적으로 호출하고 서비스 보안 주체를 파라미터로 제공해야 합니다. 그러면 [EnableOrganizationAdminAccount](#)를 호출해 GuardDuty 관리자 계정을 위임할 수 있습니다.

GuardDuty와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon GuardDuty를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal guardduty.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

GuardDuty에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 GuardDuty에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 GuardDuty 관리와 조직 관리를 분리하는 데 도움을 줍니다.

최소 권한

멤버 계정을 위임된 관리자로 지정하는 데 필요한 권한에 관한 내용은 Amazon GuardDuty 사용 설명서의 [위임된 관리자를 지정하는 데 필요한 권한](#)을 참조하세요.

멤버 계정을 GuardDuty에 대한 위임된 관리자로 지정하려면

[위임된 관리자 지정 및 멤버 계정 추가\(콘솔\)](#) 및 [위임된 관리자 지정 및 멤버 계정 추가\(API\)](#)를 참조하세요.

AWS Health 및 AWS Organizations

AWS Health는 리소스 성능과 AWS 서비스 및 계정의 가용성에 대한 지속적인 가시성을 제공합니다. 이는 AWS 리소스 및 서비스가 문제의 영향을 받거나 향후 변경 사항의 영향을 받을 때 이벤트를 AWS

Health 전달합니다. 조직 보기를 활성화하면 조직의 관리 계정 사용자가 조직의 모든 계정에서 AWS Health 이벤트를 집계할 수 있습니다. 조직 보기는 기능이 활성화된 후에 전달된 AWS Health 이벤트만 표시하고 90일 동안 유지합니다.

AWS Health 콘솔, (AWS CLI) 또는 AWS Health API를 AWS Command Line Interface 사용하여 조직 보기를 활성화할 수 있습니다.

자세한 내용은 AWS Health 사용 설명서의 [AWS Health 이벤트 집계](#)를 참조하세요.

다음 정보를 사용하여 AWS Health 와 통합할 수 있습니다 AWS Organizations.

통합을 위한 서비스 연결 역할

AWSServiceRoleForHealth_Organizations 서비스 연결 역할을 사용하면 조직의 계정 내에서 지원되는 작업을 AWS Health 수행할 수 있습니다.

이 역할은 [EnableHealthServiceAccessForOrganization](#) API 작업을 호출하여 신뢰할 수 있는 액세스를 활성화하면 조직의 관리 계정에 자동으로 생성됩니다. 그렇지 않으면 [IAM 사용 설명서](#)의 서비스 연결 역할 생성에 설명된 대로 AWS Health 콘솔, API 또는 CLI를 사용하여 역할을 생성합니다. <https://docs.aws.amazon.com/IAM/latest/UserGuide/using-service-linked-roles.html#create-service-linked-role>

AWS Health 및 Organizations 간에 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거하는 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. 다음 서비스 보안 주체에 대한 액세스 권한을 AWS Health 부여하는 데 사용되는 서비스 연결 역할:

- `health.amazonaws.com`

를 사용하여 신뢰할 수 있는 액세스 활성화 AWS Health

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

에 대한 조직 보기 활성화 기능을 사용하면 신뢰할 수 있는 AWS Health 액세스도 자동으로 활성화됩니다.

콘솔 또는 AWS Health 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

⚠ Important

가능하면 AWS Health 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Health 수행할 수 있습니다. AWS Health에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Health 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하면이 단계를 완료할 필요가 없습니다.

AWS Health 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Health 및 다음 옵션 중 하나를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

- AWS Health 콘솔을 사용합니다. 자세한 내용은 AWS Health 사용 설명서의 [조직 보기\(콘솔\)](#)을 참조하세요.
- AWS CLI를 사용합니다. 자세한 내용은 AWS Health 사용 설명서의 [조직 보기\(CLI\)](#)를 참조하세요.
- [EnableHealthServiceAccessForOrganization](#) API 작업을 호출합니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Health 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal health.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

를 사용하여 신뢰할 수 있는 액세스 비활성화 AWS Health

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

조직 보기 기능을 비활성화하면가 조직의 다른 모든 계정에 대한 이벤트 집계를 AWS Health 중지합니다. 또한 신뢰할 수 있는 액세스도 자동으로 비활성화됩니다.

AWS Health 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Important

가능하면 AWS Health 콘솔 또는 도구를 사용하여 Organizations와의 통합을 비활성화하는 것이 좋습니다. 이렇게 하면 서비스에서 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등 필요한 모든 정리를 AWS Health 수행할 수 있습니다. AWS Health에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.

AWS Health 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화하면이 단계를 완료할 필요가 없습니다.

AWS Health 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

다음 옵션 중 하나를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

- AWS Health 콘솔을 사용합니다. 자세한 내용은 AWS Health 사용 설명서의 [조직 보기 비활성화\(콘솔\)](#)를 참조하세요.
- AWS CLI를 사용합니다. 자세한 내용은 AWS Health 사용 설명서의 [조직 보기 비활성화\(CLI\)](#)를 참조하세요.
- [DisableHealthServiceAccessForOrganization](#) API 작업을 호출합니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Health 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal health.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

에 대한 위임된 관리자 계정 활성화 AWS Health

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 AWS Health 에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 AWS Health관리와 조직 관리를 분리하는 데 도움이 됩니다.

멤버 계정을의 위임된 관리자로 지정하려면 AWS Health

[조직 보기에 대한 위임된 관리자 등록](#) 참조

에 대한 위임된 관리자를 제거하려면 AWS Health

[조직 보기에서 위임된 관리자 제거](#) 참조

AWS Identity and Access Management 및 AWS Organizations

AWS Identity and Access Management 는 서비스에 대한 액세스를 안전하게 제어하기 위한 웹 AWS 서비스입니다.

IAM에서 [서비스가 마지막으로 액세스한 데이터](#)를 사용하여 조직 전반의 AWS 활동을 더욱 잘 파악할 수 있습니다. 이 데이터를 사용하여 해당 조직의 계정이 사용하는 AWS 서비스로만 액세스를 제한하는 [서비스 제어 정책\(SCP\)](#)을 생성하고 업데이트할 수 있습니다.

예시는 IAM 사용 설명서의 [데이터를 사용하여 조직 단위의 권한 구체화](#)를 참조하세요.

IAM을 사용하면 루트 사용자 자격 증명을 중앙에서 관리하고 멤버 계정에서 권한 있는 작업을 수행할 수 있습니다. 에서 IAM에 대한 신뢰할 수 있는 액세스를 활성화하는 루트 액세스 관리를 활성화 AWS

Organizations하면 멤버 계정의 루트 사용자 자격 증명을 중앙에서 보호할 수 있습니다. 멤버 계정은 루트 사용자로 로그인하거나 루트 사용자의 암호 복구를 수행할 수 없습니다. IAM의 관리 계정 또는 위임된 관리자 계정은 단기 루트 액세스를 사용하여 멤버 계정에서 권한 있는 작업을 수행할 수 있습니다. 단기 권한 있는 세션은 조직의 멤버 계정에서 권한 있는 작업을 수행하도록 범위를 지정할 수 있는 임시 자격 증명을 제공합니다.

자세한 내용은 IAM 사용 설명서의 [멤버 계정에 대한 루트 액세스 중앙 관리](#)를 참조하세요.

다음 정보를 사용하여 AWS Identity and Access Management 와 통합할 수 있습니다 AWS Organizations.

IAM에서 신뢰할 수 있는 액세스 활성화

루트 액세스 관리가 비활성화되어 있는 경우 AWS Organizations에서 IAM에 대해 신뢰할 수 있는 액세스를 활성화하세요.

IAM에서 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다 AWS Identity and Access Management.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Identity and Access Management를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS Identity and Access Management에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.

6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 AWS Identity and Access Management 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Identity and Access Management 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal iam.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

IAM에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 멤버 계정에 대한 권한 있는 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [Organizations 멤버 계정에서 권한 있는 작업 수행](#)을 참조하세요.

조직 관리 계정의 관리자만 IAM에 대해 위임된 관리자를 구성할 수 있습니다.

IAM 콘솔이나 API에서 또는 Organizations CLI 또는 SDK 작업을 사용하여 위임된 관리자 계정을 지정할 수 있습니다.

IAM에 대해 위임된 관리자를 비활성화

Organizations 관리 계정 또는 IAM의 위임된 관리자 계정의 관리자만 조직에서 위임된 관리자 계정을 제거할 수 있습니다. Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 비활성화할 수 있습니다.

Amazon Inspector 및 AWS Organizations

Amazon Inspector는 Amazon EC2 및 컨테이너 워크로드에서 소프트웨어 취약성 및 의도하지 않은 네트워크 노출을 지속적으로 스캔하는 자동화된 취약성 관리 서비스입니다.

Amazon Inspector를 사용하면 Amazon Inspector의 관리자 계정을 위임 AWS Organizations 하기만 하면 통해 연결된 여러 계정을 관리할 수 있습니다. 위임된 관리자는 조직의 Amazon Inspector를 관리하며 조직을 대신하여 다음과 같은 작업을 수행할 수 있는 특별 권한을 부여받습니다.

- 멤버 계정에 대한 스캔 활성화 또는 비활성화
- 전체 조직의 집계된 결과 데이터 보기
- 억제 규칙 생성 및 관리

자세한 내용은 Amazon Inspector 사용 설명서의 [AWS Organizations로 여러 계정 관리](#)를 참조하세요.

다음 정보를 사용하여 Amazon Inspector를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Amazon Inspector는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Amazon Inspector와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForAmazonInspector2`

자세한 내용은 Amazon Inspector 사용 설명서의 [Amazon Inspector에 대한 서비스 연결 역할 사용](#)을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Amazon Inspector가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `inspector2.amazonaws.com`

Amazon Inspector에서 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Amazon Inspector는 멤버 계정을 조직의이 서비스에 대한 위임된 관리자로 지정하기 AWS Organizations 전이에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

Amazon Inspector에 대해 위임된 관리자를 지정하면 조직의 Amazon Inspector에 대해 신뢰할 수 있는 액세스가 자동으로 활성화됩니다.

그러나 CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 `EnableAWSServiceAccess` 작업을 명시적으로 호출하고 서비스 보안 주체를 파라미터로 제공해야 합니다. 그런 다음 `EnableDelegatedAdminAccount`를 호출하여 Inspector 관리자 계정을 위임할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon Inspector를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal inspector2.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Note

`EnableAWSServiceAccess` API를 사용 중인 경우 [EnableDelegatedAdminAccount](#)를 호출하여 Inspector 관리자 계정도 위임해야 합니다.

Amazon Inspector에서 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 Amazon Inspector에서 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon Inspector를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal inspector2.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Amazon Inspector에 대한 위임된 관리자 계정 활성화

Amazon Inspector를 사용하면 AWS Organizations 서비스와 함께 위임된 관리자를 사용하여 조직의 여러 계정을 관리할 수 있습니다.

AWS Organizations 관리 계정은 조직 내 계정을 Amazon Inspector의 위임된 관리자 계정으로 지정합니다. 위임된 관리자는 조직의 Amazon Inspector를 관리하며 조직을 대신하여 멤버 계정에 대한 스캔 활성화 또는 비활성화, 전체 조직의 집계된 결과 데이터 보기, 억제 규칙 생성 및 관리와 같은 작업을 수행할 수 있는 특별 권한을 부여받습니다.

위임된 관리자가 조직 계정을 관리하는 방법에 대한 자세한 내용은 Amazon Inspector 사용 설명서에서 [관리자 계정과 멤버 계정 간의 관계 이해](#)를 참조하세요.

조직 관리 계정의 관리자만 Amazon Inspector에 대해 위임된 관리자를 구성할 수 있습니다.

Amazon Inspector 콘솔이나 API에서 또는 Organizations CLI 또는 SDK 작업을 사용하여 위임된 관리자 계정을 지정할 수 있습니다.

최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Amazon Inspector에 대한 위임된 관리자로 구성할 수 있습니다

Amazon Inspector 콘솔을 사용하여 위임된 관리자를 구성하려면 Amazon Inspector 사용 설명서에서 [1단계: Amazon Inspector - 다중 계정 환경 활성화](#)를 참조하세요.

Note

Amazon Inspector를 사용하는 각 리전의 `inspector2:enableDelegatedAdminAccount`에 연락해야 합니다.

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal inspector2.amazonaws.com
```

- AWS SDK: Organizations RegisterDelegatedAdministrator 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체를 파라미터 `account.amazonaws.com`로 식별합니다.

Amazon Inspector에 대해 위임된 관리자를 비활성화

AWS Organizations 관리 계정의 관리자만 조직에서 위임된 관리자 계정을 제거할 수 있습니다.

Amazon Inspector 콘솔이나 API에서 또는 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. Amazon Inspector 콘솔을 사용

하여 위임된 관리자를 제거하려면 Amazon Inspector 사용 설명서에서 [위임된 관리자 제거](#)를 참조하세요.

AWS License Manager 및 AWS Organizations

AWS License Manager는 소프트웨어 공급업체 라이선스를 클라우드로 가져오는 프로세스를 간소화합니다. 클라우드 인프라를 구축할 AWS때 기존 라이선스 인벤토리를 클라우드 리소스와 함께 사용하도록 용도를 변경하여 bring-your-own-license(BYOL) 기회를 사용하여 비용을 절감할 수 있습니다. 라이선스 소비에 대한 역할 기반 제어를 이용하면, 관리자는 신규 및 기존 클라우드 배포에 하드 또는 소프트웨어 제한을 설정해 비호환 서버 사용을 사전에 차단할 수 있습니다.

License Manager에 관한 자세한 내용은 [License Manager 사용 설명서](#)를 참조하세요.

License Manager를에 연결 AWS Organizations하면 다음을 수행할 수 있습니다.

- 조직 전체의 컴퓨팅 리소스에 대한 교차 계정 발견을 활성화할 수 있습니다.
- AWS에 보유해 실행하는 상용 Linux 구독을 확인하고 관리할 수 있습니다. 자세한 내용은 [AWS License Manager의 Linux 구독](#)을 참조하세요.

다음 정보를 사용하여 AWS License Manager와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 License Manager는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

License Manager와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 역할을 삭제하거나 수정할 수 있습니다.

- AWSLicenseManagerMasterAccountRole
- AWSLicenseManagerMemberAccountRole
- AWSServiceRoleForAWSLicenseManagerRole
- AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService

자세한 내용은 [License Manager—관리 계정 역할](#), [License Manager—멤버 계정 역할](#), [License Manager—Linux 구독 역할](#)을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다른 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. License Manager가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

License Manager와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스는 AWS License Manager로만 활성화할 수 있습니다.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

License Manager와 상호 신뢰할 수 있는 액세스를 활성화하려면

AWS Organizations 관리 계정을 사용하여 License Manager 콘솔에 로그인하고 License Manager 계정과 연결해야 합니다. 자세한 내용은 [의 설정을 AWS License Manager](#) 참조하세요.

License Manager와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS License Manager 를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal license-manager.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

신뢰할 수 있는 액세스 비활성화:

```
$ aws organizations disable-aws-service-access \
  --service-principal license-manager-linux-subscriptions.amazonaws.com
```

- AWS API: [DisableAWSServiceAccess](#)

License Manager에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 License Manager에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 License Manager 관리와 조직 관리를 분리하는 데 도움을 줍니다.

멤버 계정을 License Manager에 대한 관리자로 지정하려면 License Manager 사용 설명서의 [위임된 관리자 등록](#)에 설명된 단계를 따릅니다.

AWS Managed Services (AMS) 셀프 서비스 보고(SSR) 및 AWS Organizations

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

와 통합한 후 집계 셀프 서비스 보고(SSR)를 활성화 AWS Organizations할 수 있습니다. 이는 Advanced 및 Accelerate 고객이 조직 수준, 교차 계정에서 집계된 기존 셀프 서비스 보고서를 보도록 AMS 기능입니다. 이를 통해 내의 모든 AMS 관리 계정에서 패치 규정 준수, 백업 적용 범위 및 인시던트와 같은 주요 운영 지표를 파악할 수 있습니다 AWS Organizations.

다음 정보를 사용하여 AWS Managed Services (AMS) 자체 서비스 보고(SSR)를와 통합합니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 AMS는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

AMS와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForManagedServices_SelfServiceReporting`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. AMS에서 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `selfservicereporting.managedservices.amazonaws.com`

AMS에서 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 AWS Managed Services (AMS) 자체 서비스 보고(SSR)를 Organizations의 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal selfservicereporting.managedservices.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

AMS에서 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Managed Services (AMS) 자체 서비스 보고(SSR)를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal selfservicereporting.managedservices.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

AMS에 대한 위임된 관리자 계정 활성화

위임된 관리자 계정은 AMS 콘솔의 단일 집계 보기에서 모든 계정의 AMS 보고서(패치 및 백업 등)를 볼 수 있습니다.

AMS 콘솔이나 API에서 또는 Organizations RegisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 추가할 수 있습니다.

AMS에 대해 위임된 관리자를 비활성화

조직 관리 계정의 관리자만 AMS에 대해 위임된 관리자를 구성할 수 있습니다.

AMS 콘솔이나 API에서 또는 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다.

Amazon Macie 및 AWS Organizations

Amazon Macie는 기계 학습과 패턴 일치를 사용하여 Amazon Simple Storage Service(Amazon S3)에서 민감한 데이터를 검색, 모니터링, 보호하는 완전관리형 데이터 보안 및 데이터 개인 정보 보호 서비스입니다. Macie는 개인 식별 정보(PII) 및 지적 재산권과 같은 민감한 데이터의 검색을 자동화하여 조직이 Amazon S3에 저장하는 데이터를 더 잘 이해할 수 있도록 합니다.

자세한 내용은 [Amazon Macie 사용 설명서](#)의 [AWS Organizations로 Amazon Macie 계정들 관리](#)를 참조하세요.

다음 정보를 사용하여 Amazon Macie를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 위임된 Macie 관리자 계정에 자동으로 생성됩니다. 이 역할을 통해 Macie는 조직의 계정에 대해 지원되는 작업을 수행할 수 있습니다.

Macie와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제할 수 있습니다.

- `AWSServiceRoleForAmazonMacie`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Macie가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `macie.amazonaws.com`

Macie와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Amazon Macie 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

⚠ Important

가능하면 항상 Amazon Macie 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 Amazon Macie가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. Amazon Macie에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

Amazon Macie 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Macie 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

Amazon Macie는 멤버 계정을 조직의 Macie 관리자로 지정 AWS Organizations 하려면에 대한 신뢰할 수 있는 액세스 권한이 필요합니다. Macie 관리 콘솔을 사용해 위임된 관리자를 구성하는 경우 Macie가 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

자세한 내용은 Amazon Macie 사용 설명서의 [Amazon Macie에서 조직 통합 및 구성](#)을 참조하십시오.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon Macie를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal macie.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Macie에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Macie에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Macie 관리와 조직 관리를 분리하는 데 도움을 줍니다.

최소 권한

다음 권한이 있는 Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Macie에 대한 위임된 관리자로 구성할 수 있습니다.

- `organizations:EnableAWSServiceAccess`
- `macie:EnableOrganizationAdminAccount`

멤버 계정을 Macie에 대한 위임된 관리자로 지정하려면

Amazon Macie는 멤버 계정을 조직의 Macie 관리자로 지정 AWS Organizations 하려면에 대한 신뢰할 수 있는 액세스 권한이 필요합니다. Macie 관리 콘솔을 사용해 위임된 관리자를 구성하는 경우 Macie가 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

자세한 내용은 <https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin> 섹션을 참조하세요.

AWS Marketplace 및 AWS Organizations

AWS Marketplace는 솔루션을 구축하고 비즈니스를 운영하는 데 필요한 타사 소프트웨어, 데이터 및 서비스를 찾고, 구매하고, 배포하고, 관리하는 데 사용할 수 있는 엄선된 디지털 카탈로그입니다.

AWS Marketplace에서 구매 AWS License Manager 에를 사용하여 라이선스를 생성하고 관리합니다 AWS Marketplace. 조직의 다른 계정과 라이선스를 공유(액세스 권한을 부여)하면 AWS Marketplace가 해당 계정에 대해 새 라이선스를 생성하고 관리합니다.

자세한 내용은 AWS Marketplace 구매자 설명서의 [AWS Marketplace에 대한 서비스 연결 역할](#)을 참조하세요.

다음 정보를 사용하여 AWS Marketplace와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 AWS Marketplace 는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

AWS Marketplace 와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForMarketplaceLicenseManagement`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. 다음 서비스 보안 주체에 대한 액세스 권한을 AWS Marketplace 부여하는 데 사용되는 서비스 연결 역할:

- `license-management.marketplace.amazonaws.com`

를 사용하여 신뢰할 수 있는 액세스 활성화 AWS Marketplace

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS Marketplace 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Marketplace 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Marketplace 수행할 수 있습니다. AWS Marketplace에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오. AWS Marketplace 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하는 경우이 단계를 완료할 필요가 없습니다.

AWS Marketplace 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Marketplace 구매자 가이드에서 [AWS Marketplace에 대한 서비스 연결 역할 생성](#)을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Marketplace를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Marketplace에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Marketplace 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Marketplace 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal license-management.marketplace.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

를 사용하여 신뢰할 수 있는 액세스 비활성화 AWS Marketplace

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Marketplace 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal license-management.marketplace.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

AWS Marketplace Private Marketplace 및 AWS Organizations

AWS Marketplace 는 솔루션을 구축하고 비즈니스를 운영하는 데 필요한 타사 소프트웨어, 데이터 및 서비스를 찾고, 구매하고, 배포하고, 관리하는 데 사용할 수 있는 엄선된 디지털 카탈로그입니다. 프라이빗 마켓플레이스에서는 사용할 수 있는 광범위한 제품 카탈로그 AWS Marketplace와 해당 제품에 대한 세분화된 제어를 제공합니다.

AWS Marketplace 프라이빗 마켓플레이스를 사용하면 조직 전체, 하나 이상의 OUs 또는 조직의 하나 이상의 계정과 연결된 여러 프라이빗 마켓플레이스 경험을 생성할 수 있으며, 각각 고유한 승인된 제품 세트가 있습니다. AWS 또한 관리자는 회사 또는 팀의 로고, 메시징 및 색상 체계를 사용하여 각 프라이빗 마켓플레이스 환경에 회사 브랜딩을 적용할 수 있습니다.

자세한 내용은 AWS Marketplace 구매자 안내서의 [역할을 사용하여 AWS Marketplace에서 Private Marketplace 구성](#)을 참조하세요.

다음 정보를 사용하여 AWS Marketplace Private Marketplace를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

AWS Marketplace Private Marketplace 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하면 조직의 관리 계정에 다음 서비스 연결 역할이 자동으로 생성됩니다. 이 역할을 통해 Private Marketplace는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다. AWS Marketplace Private Marketplace와 Organizations 간에 신뢰할 수 있는 액세스를 비활성화하고 조직의 모든 프라이빗 마켓플레이스 경험을 연결 해제하는 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

Organizations 콘솔, CLI 또는 SDK에서 직접 신뢰할 수 있는 액세스를 활성화하면 서비스 연결 역할이 자동으로 생성되지 않습니다.

- `AWSServiceRoleForPrivateMarketplaceAdmin`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. Private Marketplace가 사용하는 서비스 연결 역할은 다음 서비스 위탁자에 대한 액세스 권한을 부여합니다.

- `private-marketplace.marketplace.amazonaws.com`

Private Marketplace를 사용하여 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Marketplace Private Marketplace 콘솔 또는 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 AWS Organizations 있습니다.

Important

가능하면 AWS Marketplace Private Marketplace 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이를 통해 AWS Marketplace Private Marketplace는 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 수행할 수 있습니다. AWS Marketplace Private Marketplace에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 이 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Marketplace Private Marketplace 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하는 경우 이 단계를 완료할 필요가 없습니다.

Private Marketplace 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Marketplace 구매자 안내서의 [Private Marketplace 시작하기](#)를 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Marketplace Private Marketplace를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Marketplace Private Marketplace에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만 AWS Marketplace Private Marketplace의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 AWS Marketplace Private Marketplace를 Organizations의 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal private-marketplace.marketplace.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Private Marketplace를 사용하여 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Marketplace Private Marketplace를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal private-marketplace.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Private Marketplace에 대한 위임된 관리자 계정 활성화

관리 계정 관리자는 Private Marketplace 관리 권한을 위임된 관리자라고 하는 지정된 멤버 계정에 위임할 수 있습니다. 프라이빗 마켓플레이스의 위임된 관리자로 계정을 등록하려면 관리 계정 관리자가 신뢰할 수 있는 액세스 및 서비스 연결 역할이 활성화되었는지 확인하고 새 관리자 등록을 선택하고 12자리 AWS 계정 번호를 입력한 다음 제출을 선택해야 합니다.

관리 계정과 위임된 관리자 계정은 경험 생성, 브랜딩 설정 업데이트, 대상 연결 또는 연결 해제, 제품 추가 또는 제거, 보류 중인 요청 승인 또는 거부와 같은 Private Marketplace 관리 작업을 수행할 수 있습니다.

Private Marketplace 콘솔을 사용하여 위임된 관리자를 구성하려면 AWS Marketplace 구매자 안내서의 [프라이빗 마켓플레이스 생성 및 관리](#)를 참조하세요.

Organizations RegisterDelegatedAdministrator API를 사용하여 위임된 관리자를 구성할 수도 있습니다. 자세한 내용은 Organizations 명령 참조에서 [RegisterDelegatedAdministrator](#)를 참조하세요.

Private Marketplace에 대해 위임된 관리자 비활성화

조직 관리 계정의 관리자만 Private Marketplace에 대해 위임된 관리자를 구성할 수 있습니다.

Private Marketplace 콘솔이나 API에서 또는 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다.

Private Marketplace 콘솔을 사용하여 위임된 관리자 Private Marketplace 계정을 비활성화하려면 AWS Marketplace 구매자 안내서의 [프라이빗 마켓플레이스 생성 및 관리](#)를 참조하세요.

AWS Marketplace 조달 인사이트 대시보드 및 AWS Organizations

AWS Marketplace 조달 인사이트 대시보드를 사용하여 조직의 모든 AWS 계정에 대한 계약 및 비용 분석 데이터를 볼 수 있습니다. Organizations와 통합되면 AWS Marketplace 조달 인사이트 대시보드는 조직에 가입하는 계정과 같은 조직 변경 사항을 수신하고 해당 계약의 데이터를 집계하여 대시보드를 구축합니다.

자세한 내용은 AWS Marketplace 구매자 안내서의 [조달 인사이트](#)를 참조하세요.

다음 정보를 사용하여 AWS Marketplace 조달 인사이트 대시보드와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 및 관리형 정책 생성

AWS Marketplace 조달 인사이트 대시보드 대시보드를 활성화하면 [AWSServiceRoleForProcurementInsightsPolicy](#) 서비스 연결 역할과 [AWSServiceRoleForProcurementInsightsPolicy](#) AWS 관리형 정책이 생성됩니다.

AWS Marketplace 조달 인사이트를 통해 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하면 AWS Marketplace 조달 인사이트 대시보드에 고객의 Organizations 서비스와 통합할 수 있는 기능이 부여됩니다. AWS Marketplace 조달 인사이트 대시보드는 조직에 가입한 계정과 같은 조직 변경 사항을 수신하고 해당 계약의 데이터를 집계하여 대시보드를 빌드합니다.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Marketplace 조달 인사이트 대시보드 콘솔 또는 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Marketplace 조달 인사이트 대시보드 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이를 통해 AWS Marketplace 조달 인사이트 대시보드는 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 수행할 수 있습니다. AWS Marketplace 조달 인사이트 대시보드에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만이 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오. AWS Marketplace 조달 인사이트 대시보드 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하는 경우이 단계를 완료할 필요가 없습니다.

AWS Marketplace 조달 인사이트 대시보드를 활성화하여 신뢰할 수 있는 액세스를 활성화하려면 AWS Marketplace 구매자 안내서 [의 AWS Marketplace 조달 인사이트 대시보드 활성화](#)를 참조하세요.

Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Marketplace 조달 인사이트 대시보드를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Marketplace 조달 인사이트 대시보드에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만 AWS Marketplace 조달 인사이트 대시보드의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 있다고 AWS Organizations 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Marketplace 조달 인사이트 대시보드를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal procurement-insights.marketplace.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

AWS Marketplace 조달 인사이트를 사용하여 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Marketplace 조달 인사이트 대시보드를 신뢰할 수 있는 서비스로 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal procurement-insights.marketplace.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

AWS Marketplace 조달 인사이트를 위해 위임된 관리자 계정 활성화

AWS Marketplace 조달 인사이트 콘솔에서 위임된 관리자를 구성하려면 AWS Marketplace 구매자 안내서의 [위임된 관리자 등록](#)을 참조하세요.

Organizations RegisterDelegatedAdministrator API를 사용하여 위임된 관리자를 구성할 수도 있습니다. 자세한 내용은 Organizations 명령 참조에서 [RegisterDelegatedAdministrator](#)를 참조하세요.

AWS Marketplace 조달 인사이트를 위해 위임된 관리자 비활성화

조직 관리 계정의 관리자만 AWS Marketplace 조달 인사이트를 위해 위임된 관리자를 구성할 수 있습니다.

AWS Marketplace 조달 인사이트 콘솔을 통해 위임된 관리자를 제거하려면 AWS Marketplace 구매자 안내서의 [위임된 관리자 등록 취소](#)를 참조하세요.

Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수도 있습니다.

AWS Network Manager 및 AWS Organizations

Network Manager를 사용하면 AWS 계정, 리전 및 온프레미스 위치에서 AWS Cloud WAN 코어 네트워크와 Transit Gateway 네트워크를 중앙에서 관리할 수 있습니다 AWS . 다중 계정 지원을 사용하면 모든 AWS 계정에 대해 단일 글로벌 네트워크를 생성하고 Network Manager 콘솔을 사용하여 여러 계정에서 글로벌 네트워크로 전송 게이트웨이를 등록할 수 있습니다.

Network Manager와 Organizations 사이의 신뢰할 수 있는 액세스가 활성화되면 멤버 계정에 배포된 서비스 연결 역할을 등록된 위임된 관리자와 관리 계정에서 활용하여 글로벌 네트워크에 연결된 리소스를 설명할 수 있습니다. 등록된 위임된 관리자와 관리 계정에서는 Network Manager 콘솔에서 멤버 계정에 배포된 사용자 정의 IAM 역할을 말할 수 있습니다(다중 계정 모니터링 및 이벤트 처리의 경우 CloudWatch-CrossAccountSharingRole, 다중 계정 리소스를 보고 관리하는 콘솔 전환 역할 액세스의 경우 IAMRoleForAWSNetworkManagerCrossAccountResourceAccess).

Important

- 다중 계정 설정(신뢰할 수 있는 액세스 활성화/비활성화 및 위임된 관리자 등록/등록 취소)을 관리하려면 Network Manager 콘솔을 사용하는 것이 좋습니다. 콘솔에서 이러한 설정을 관

리하면 필요한 모든 서비스 연결 역할과 사용자 정의 IAM 역할이 다중 계정 액세스에 필요한 멤버 계정에 자동으로 배포되고 관리됩니다.

- Network Manager 콘솔에서 Network Manager에 대한 신뢰할 수 있는 액세스를 활성화하면 콘솔도 CloudFormation StackSets 서비스를 활성화합니다. Network Manager에서는 StackSets를 사용하여 다중 계정 관리에 필요한 사용자 정의 IAM 역할을 배포합니다.

Organizations와 Network Manager 통합에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [AWS Organizations로 Network Manager에서 여러 계정 관리](#)를 참조하세요.

다음 정보를 사용하여 AWS Network Manager를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 나열된 조직 계정에 자동으로 생성됩니다. 조직의 계정 내에서 지원되는 작업을 Network Manager에서 이러한 역할을 통해 수행할 수 있습니다. 신뢰할 수 있는 액세스를 비활성화하는 경우 Network Manager에서는 조직의 계정에서 이러한 역할을 삭제하지 않습니다. IAM 콘솔을 사용하여 해당 역할을 수동으로 삭제할 수 있습니다.

관리 계정

- AWSServiceRoleForNetworkManager
- AWSServiceRoleForCloudFormationStackSetsOrgAdmin
- AWSServiceRoleForCloudWatchCrossAccount

멤버 계정

- AWSServiceRoleForNetworkManager
- AWSServiceRoleForCloudFormationStackSetsOrgMember

멤버 계정을 위임된 관리자로 등록하면 위임된 관리자 계정에 다음과 같은 추가 역할이 자동으로 생성됩니다.

- AWSServiceRoleForCloudWatchCrossAccount

서비스 연결 역할이 사용하는 서비스 보안 주체

서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말을 수 있습니다.

- `AWSServiceRoleForNetworkManager` service-linked 역할의 경우, `networkmanager.amazonaws.com`이 액세스 권한이 있는 유일한 서비스 보안 주체입니다.
- `AWSServiceRoleForCloudFormationStackSetsOrgMember` 서비스 연결 역할의 경우, `member.org.stacksets.cloudformation.amazonaws.com`이 액세스 권한이 있는 유일한 서비스 보안 주체입니다.
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin` 서비스 연결 역할의 경우, `stacksets.cloudformation.amazonaws.com`이 액세스 권한이 있는 유일한 서비스 보안 주체입니다.
- `AWSServiceRoleForCloudWatchCrossAccount` 서비스 연결 역할의 경우, `cloudwatch-crossaccount.amazonaws.com`이 액세스 권한이 있는 유일한 서비스 보안 주체입니다.

이러한 역할을 삭제하면 Network Manager의 다중 계정 기능이 손상됩니다.

Network Manager와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Organizations 관리 계정의 관리자만 다른 AWS 서비스에서 신뢰할 수 있는 액세스를 활성화할 수 있는 권한이 있습니다. 권한 문제를 방지하려면 Network Manager 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화해야 합니다. 자세한 내용은 Amazon VPC 사용 설명서의 [AWS Organizations로 Network Manager에서 여러 계정 관리](#)를 참조하세요.

Network Manager와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Organizations 관리 계정의 관리자만 다른 AWS 서비스에서 신뢰할 수 있는 액세스를 비활성화할 수 있는 권한이 있습니다.

⚠ Important

신뢰할 수 있는 액세스를 비활성화하려면 Network Manager 콘솔을 사용하는 것이 좋습니다. AWS CLI API 또는 CloudFormation 콘솔에서 사용하는 등 다른 방식으로 신뢰할 수 있는 액세스를 비활성화하면 배포된 CloudFormation StackSets 및 사용자 지정 IAM 역할이 제대로 정리되지 않을 수 있습니다. 신뢰할 수 있는 서비스 액세스를 비활성화하려면 [Network Manager 콘솔](#)에 로그인하세요.

Network Manager에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Network Manager에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Network Manager 관리와 조직 관리를 분리하는 데 도움이 됩니다.

조직에서 멤버 계정을 Network Manager의 위임된 관리자로 지정하는 방법에 관한 지침은 Amazon VPC 사용 설명서의 [위임된 관리자 등록](#)을 참조하세요.

Amazon Q Developer 및 AWS Organizations

Amazon Q Developer는 AWS 애플리케이션을 이해, 구축, 확장 및 운영하는 데 도움이 되는 생성형 AI 기반 대화형 어시스턴트입니다. 또한 실시간으로 코드를 제안하는 범용 기계 학습 기반 코드 생성기이기도 합니다. Amazon Q Developer의 유료 구독 버전에는 Organizations 통합이 필요합니다. 자세한 내용은 Amazon Q 사용 설명서의 [계정, IAM Identity Center 및 조직 설정](#)을 참조하세요.

다음 정보를 사용하여 Amazon Q Developer를와 통합할 수 있습니다 AWS Organizations.

서비스 연결 역할

AWSServiceRoleForAmazonQDeveloper 서비스 연결 역할을 통해 Amazon Q Developer는 조직 내에서 지원되는 작업을 수행할 수 있습니다. [IAM 사용 설명서](#)의 [서비스 연결 역할 생성](#)에 설명된 대로 Amazon Q Developer 콘솔, API 또는 CLI를 사용하여 역할을 생성합니다.

멤버 계정을 사용하는 경우 Amazon Q Developer와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

Amazon Q Developer에서 사용하는 서비스 위탁자

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Amazon Q Developer가 사용하는 서비스 연결 역할은 다음 서비스 위탁자에 대한 액세스 권한을 부여합니다.

- `q.amazonaws.com`

Amazon Q Developer를 사용하여 신뢰할 수 있는 액세스 활성화

Amazon Q Developer Pro는 신뢰할 수 있는 액세스를 사용하여 Organizations 관리 계정의 설정을 동일한 조직의 멤버 계정과 공유합니다.

예를 들어 Organizations 관리 계정에서 작업하는 Amazon Q Developer Pro 관리자는 코드 참조가 있는 제안을 활성화할 수 있습니다. 신뢰할 수 있는 액세스가 활성화된 경우 코드 참조가 있는 제안도 해당 조직의 모든 멤버 계정에 대해 활성화됩니다.

신뢰할 수 있는 액세스는 Amazon Q Developer로만 활성화할 수 있습니다.

Amazon Q Developer에 대해 신뢰할 수 있는 액세스를 활성화하려면 다음 절차를 따르세요.

1. Amazon Q Developer 설정 페이지의 멤버 계정 설정에서 편집을 선택합니다.
2. 팝업 창에서 커짐을 선택합니다.
3. 저장을 선택합니다.

자세한 내용은 Amazon Q Developer 사용 설명서의 [신뢰할 수 있는 액세스 활성화](#)를 참조하세요.

Amazon Q Developer를 사용하여 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스는 Amazon Q Developer 도구로만 비활성화할 수 있습니다.

Amazon Q Developer에 대해 신뢰할 수 있는 액세스를 비활성화하려면 다음 절차를 따르세요.

1. Amazon Q Developer 설정 페이지의 멤버 계정 설정에서 편집을 선택합니다.
2. 팝업 창에서 꺼짐을 선택합니다.
3. 저장을 선택합니다.

자세한 내용은 Amazon Q Developer 사용 설명서의 [신뢰할 수 있는 액세스 활성화](#)를 참조하세요.

AWS Resource Access Manager 및 AWS Organizations

AWS Resource Access Manager (AWS RAM)를 사용하면 소유한 지정된 AWS 리소스를 다른와 공유할 수 있습니다 AWS 계정. 여러 계정에서 다양한 유형의 AWS 리소스를 공유할 수 있는 일관된 경험을 제공하는 중앙 집중식 서비스입니다.

에 대한 자세한 내용은 [AWS RAM 사용 설명서](#)를 AWS RAM참조하세요.

다음 정보를 사용하여 AWS Resource Access Manager 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 사용하면 AWS RAM 가 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

AWS RAM 와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForResourceAccessManager`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다른 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. 다음 서비스 보안 주체에 대한 액세스 권한을 AWS RAM 부여하는 데 사용되는 서비스 연결 역할:

- `ram.amazonaws.com`

를 사용하여 신뢰할 수 있는 액세스 활성화 AWS RAM

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS Resource Access Manager 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Resource Access Manager 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한

모든 구성을 AWS Resource Access Manager 수행할 수 있습니다. AWS Resource Access Manager에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Resource Access Manager 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하는 경우 이 단계를 완료할 필요가 없습니다.

AWS RAM 콘솔 또는 CLI를 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS RAM 사용 설명서의 [AWS Organizations를 사용하여 공유 사용](#)을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Resource Access Manager를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Resource Access Manager에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Resource Access Manager 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Resource Access Manager 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal ram.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

를 사용하여 신뢰할 수 있는 액세스 비활성화 AWS RAM

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Resource Access Manager 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Important

가능하면 AWS Resource Access Manager 콘솔 또는 도구를 사용하여 Organizations와의 통합을 비활성화하는 것이 좋습니다. 이렇게 하면 서비스에서 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등 필요한 모든 정리를 AWS Resource Access Manager 수행할 수 있습니다. AWS Resource Access Manager에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.

AWS Resource Access Manager 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화하면 이 단계를 완료할 필요가 없습니다.

AWS Resource Access Manager 콘솔 또는 CLI를 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

AWS RAM 사용 설명서의 [AWS Organizations를 사용하여 공유 사용](#)을 참조하세요.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.

3. 서비스 목록에서 AWS Resource Access Manager를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS Resource Access Manager에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔 또는 도구를 사용하여 해당 서비스의 작업을 AWS Organizations 비활성화할 수 AWS Resource Access Manager 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Resource Access Manager 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal ram.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

AWS Resource Explorer 및 AWS Organizations

AWS Resource Explorer 는 리소스 검색 및 검색 서비스입니다. 리소스 탐색기를 사용하면 인터넷 검색 엔진과 유사한 환경을 사용하여 Amazon Elastic Compute Cloud 인스턴스, Amazon Kinesis Data Streams 또는 Amazon DynamoDB 테이블과 같은 리소스를 탐색할 수 있습니다. 이름, 태그, ID와 같은 리소스 메타데이터를 사용하여 리소스를 검색할 수 있습니다. Resource Explorer는 계정의 AWS 여러 리전에서 작동하여 리전 간 워크로드를 간소화합니다.

Resource Explorer를와 통합하면 평가 범위 내에 조직의 여려를 포함시켜 더 광범위한 소스 AWS 계정에서 증거를 수집할 AWS Organizations수 있습니다.

다음 정보를 사용하여 AWS Resource Explorer 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Resource Explorer(는) 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Resource Explorer와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

Resource Explorer가 이 역할을 사용하는 방식에 대한 자세한 내용은 AWS Resource Explorer 사용 설명서의 [서비스 연결 역할 사용](#)을 참조하세요.

- `AWSServiceRoleForResourceExplorer`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Resource Explorer이 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `resource-explorer-2.amazonaws.com`

를 사용하여 신뢰할 수 있는 액세스를 활성화하려면 AWS Resource Explorer

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Resource Explorer는 멤버 계정을 조직의 위임된 관리자로 지정하기 AWS Organizations 전이에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

Resource Explorer 콘솔 또는 Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다. 가능하면 항상 Resource Explorer 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Resource Explorer 수행할 수 있습니다.

Resource Explorer 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하는 방법

신뢰할 수 있는 액세스를 활성화하는 방법은 AWS Resource Explorer 사용 설명서의 [Resource Explorer를 사용하기 위한 사전 요구 사항](#)을 참조하세요.

Note

AWS Resource Explorer 콘솔을 사용하여 위임된 관리자를 구성하면 AWS Resource Explorer 자동으로 신뢰할 수 있는 액세스를 활성화합니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Resource Explorer 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal resource-explorer-2.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Resource Explorer에서 신뢰할 수 있는 액세스를 비활성화하는 방법

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다 AWS Resource Explorer.

AWS Resource Explorer 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Important

가능하면 AWS Resource Explorer 콘솔 또는 도구를 사용하여 Organizations와의 통합을 비활성화하는 것이 좋습니다. 이렇게 하면 서비스에서 더 이상 필요하지 않은 리소스 또는 액세스

스 역할을 삭제하는 등 필요한 모든 정리를 AWS Resource Explorer 수행할 수 있습니다. AWS Resource Explorer에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.

AWS Resource Explorer 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화하면 이 단계를 완료할 필요가 없습니다.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Resource Explorer 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal resource-explorer-2.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Resource Explorer에 대한 위임된 관리자 계정 활성화

위임된 관리자 계정을 사용하여 다중 계정 리소스 보기를 만들고 조직 단위 또는 전체 조직으로 범위를 지정할 수 있습니다. 리소스 공유를 생성 AWS Resource Access Manager 하역을 통해 조직의 모든 계정과 다중 계정 보기를 공유할 수 있습니다.

최소 권한

다음 권한이 있는 Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Resource Explorer에 대한 위임된 관리자로 구성할 수 있습니다.

`resource-explorer:RegisterAccount`

Resource Explorer에 대한 위임된 관리자 계정 활성화에 대한 설명은 AWS Resource Explorer 사용 설명서의 [설정](#)을 참조하세요.

AWS Resource Explorer 콘솔을 사용하여 위임된 관리자를 구성하면 Resource Explorer가 자동으로 신뢰할 수 있는 액세스를 활성화합니다.

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK: Organizations RegisterDelegatedAdministrator 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스를 파라미터resource-explorer-2.amazonaws.com로 식별합니다.

Resource Explorer에 대해 위임된 관리자를 비활성화

Organizations 관리 계정 또는 Resource Explorer의 위임된 관리자 계정의 관리자만 Resource Explorer의 위임된 관리자를 제거할 수 있습니다. 신뢰할 수 있는 액세스는 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용해 비활성화할 수 있습니다.

AWS Security Hub CSPM 및 AWS Organizations

AWS Security Hub CSPM 는의 보안 상태에 대한 포괄적인 보기를 AWS 제공하며 보안 업계 표준 및 모범 사례를 기준으로 환경을 확인하는 데 도움이 됩니다.

Security Hub CSPM은 AWS 서비스 사용자 AWS 계정, 사용자가 사용하는 및 지원되는 타사 파트너 제품에서 보안 데이터를 수집합니다. 이 서비스는 보안 추세를 분석하고 우선 순위가 가장 높은 보안 문제를 식별하는 데 도움을 줍니다.

Security Hub CSPM과 AWS Organizations 를 함께 사용하면 새 계정이 추가될 때 이를 포함하여 모든 계정에 대해 Security Hub CSPM을 자동으로 활성화할 수 있습니다. 이렇게 하면 Security Hub CSPM 검사 및 조사 결과에 대한 적용 범위가 늘어나 전반적인 보안 태세를 보다 포괄적이고 정확하게 파악할 수 있습니다.

Security Hub CSPM에 대한 자세한 내용은 [AWS Security Hub 사용 설명서](#)를 참조하세요.

다음 정보를 사용하여 AWS Security Hub CSPM 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Security Hub CSPM은 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Security Hub CSPM과 Organizations 간에 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거하는 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForSecurityHub`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Security Hub CSPM에서 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `securityhub.amazonaws.com`

Security Hub CSPM을 사용하여 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Security Hub CSPM에 대해 위임된 관리자를 지정하면 Security Hub CSPM은 조직의 Security Hub에 대해 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

Security Hub CSPM을 사용하여 신뢰할 수 있는 액세스 비활성화

필요한 권한에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#)을 참조하세요.

신뢰할 수 있는 액세스를 비활성화하기 전에 조직의 위임된 관리자와 협력하여 멤버 계정에서 Security Hub CSPM을 비활성화하고 해당 계정에서 Security Hub CSPM 리소스를 정리하는 것이 좋습니다.

AWS Organizations 콘솔, Organizations API 또는를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다 AWS CLI. Organizations 관리 계정의 관리자만 Security Hub CSPM을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Security Hub CSPM으로 신뢰할 수 있는 액세스를 비활성화하는 방법에 대한 지침은 [와 Security Hub CSPM 통합 비활성화 AWS Organizations](#)를 참조하세요.

Security Hub CSPM에 대해 위임된 관리자 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할은 Security Hub CSPM에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않으면 조직의 관리 계정의 사용자 또는 역할만 수행할 수 있습니다. 이렇게 하면 조직 관리와 Security Hub CSPM 관리를 분리할 수 있습니다.

자세한 내용은 AWS Security Hub 사용 설명서의 [Security Hub CSPM 관리자 계정 지정](#)을 참조하세요.

멤버 계정을 Security Hub CSPM의 위임된 관리자로 지정하려면

1. Organizations의 관리 계정을 사용하여 로그인합니다.
2. 다음 중 하나를 수행합니다.
 - 관리 계정에 Security Hub CSPM이 활성화되어 있지 않은 경우 Security Hub CSPM 콘솔에서 Security Hub CSPM으로 이동을 선택합니다.
 - 관리 계정에 Security Hub CSPM이 활성화된 경우 Security Hub CSPM 콘솔의 일반에서 설정을 선택합니다.
3. 위임된 관리자(Delegated Administrator)에 계정 ID를 입력합니다.

Security Hub CSPM에 대해 위임된 관리자 비활성화

조직 관리 계정만 위임된 Security Hub CSPM 관리자 계정을 제거할 수 있습니다.

위임된 Security Hub CSPM 관리자 계정을 변경하려면 먼저 현재 위임된 관리자 계정을 제거하고 새로운 관리자 계정을 지정해야 합니다.

Security Hub CSPM 콘솔을 사용하여 한 리전에서 위임된 관리자를 제거하면 모든 리전에서 자동으로 제거됩니다.

Security Hub CSPM API는 API 직접 호출 또는 명령이 실행된 리전에서만 위임된 Security Hub CSPM 관리자 계정을 제거합니다. 다른 리전에서도 이 작업을 반복해야 합니다.

Organizations API를 사용하여 위임된 Security Hub CSPM 관리자 계정을 제거하는 경우 모든 리전에서 자동으로 제거됩니다.

위임된 Security Hub CSPM 관리자를 비활성화하는 방법에 대한 지침은 [위임된 관리자 제거 또는 변경을 참조하세요](#).

Amazon S3 Storage Lens 및 AWS Organizations

Amazon S3 Storage Lens에 조직에 대한 신뢰할 수 있는 액세스 권한을 부여하면 조직의 모든 AWS 계정에서 지표를 수집하고 집계할 수 있습니다. 이를 위해 S3 Storage Lens는 조직에 속한 계정 목록에 액세스하여 모든 계정의 스토리지, 사용량 및 활동 지표를 수집하고 분석합니다.

자세한 내용은 Amazon S3 Storage Lens 사용 설명서의 [Amazon S3 Storage Lens에 대한 서비스 연결 역할 사용](#)을 참조하세요.

다음 정보를 사용하여 Amazon S3 Storage Lens를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하고 Storage Lens 구성이 조직에 적용되면 다음 [서비스 연결 역할](#)이 조직의 위임된 관리자 계정에 자동으로 생성됩니다. 이 역할을 통해 Amazon S3 Storage Lens는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Amazon S3 Storage Lens와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForS3StorageLens`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Amazon S3 Storage Lens가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `storage-lens.s3.amazonaws.com`

Amazon S3 Storage Lens와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Amazon S3 Storage Lens 콘솔 또는 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

⚠ Important

가능하면 항상 Amazon S3 Storage Lens 콘솔 또는 도구를 사용하여 Organizations 통합을 활성화할 것을 적극 권장합니다. 이렇게 하면 Amazon S3 Storage Lens가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다. Amazon S3 Storage Lens에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 이 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

Amazon S3 Storage Lens 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있다면 이 단계를 완료할 필요가 없습니다.

Amazon S3 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

Amazon Simple Storage Service 사용 설명서의 [S3 Storage Lens에 대한 신뢰할 수 있는 액세스 활성화](#)를 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 Amazon S3 Storage Lens를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. Amazon S3 Storage Lens에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자만 있는 경우 Amazon S3 Storage Lens의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon S3 Storage Lens를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal storage-lens.s3.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Amazon S3 Storage Lens와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Amazon S3 Storage Lens 도구로만 비활성화할 수 있습니다.

Amazon S3 콘솔, AWS CLI 또는 AWS SDKs.

Amazon S3 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

Amazon Simple Storage Service 사용 설명서의 [S3 Storage Lens에 대한 신뢰할 수 있는 액세스 비활성화](#)를 참조하세요.

Amazon S3 Storage Lens에 대한 위임된 관리자 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Amazon S3 Storage Lens에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Amazon S3 Storage Lens 관리와 조직 관리를 분리하는데 도움을 줍니다.

최소 권한

다음 권한이 있는 Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Amazon S3 Storage Lens에 대한 위임된 관리자로 구성할 수 있습니다.

```
organizations:RegisterDelegatedAdministrator
organizations:DeregisterDelegatedAdministrator
```

Amazon S3 Storage Lens는 조직 내에서 위임된 관리자 계정을 최대 5개까지 지원합니다.

멤버 계정을 Amazon S3 Storage Lens에 대한 위임된 관리자로 지정하려면

Amazon S3 콘솔, AWS CLI 또는 AWS SDKs. Amazon S3 콘솔을 사용하여 멤버 계정을 조직의 위임된 관리자 계정으로 등록하려면 Amazon Simple Storage Service 사용 설명서의 [S3 Storage Lens에 대해 위임된 관리자 등록](#)을 참조하세요.

Amazon S3 Storage Lens에 대한 위임된 관리자의 등록을 취소하려면

Amazon S3 콘솔, AWS CLI 또는 AWS SDKs. Amazon S3 콘솔을 사용하여 관리자 계정의 등록을 취소하려면 Amazon Simple Storage Service 사용 설명서의 [S3 Storage Lens에 대해 위임된 관리자 등록 취소](#)를 참조하세요.

AWS 보안 인시던트 대응 및 AWS Organizations

AWS 보안 인시던트 대응은 고객이 자격 증명 도용 및 랜섬웨어 공격과 같은 사이버 보안 인시던트에 신속하게 대응할 수 있도록 연중무휴 실시간 인적 지원 보안 인시던트 지원을 제공하는 보안 서비스입니다. Organizations와 통합하면 전체 조직에 대한 보안 적용 범위를 활성화할 수 있습니다. 자세한 내용은 [AWS 보안 인시던트 대응 사용 설명서의를 사용하여 보안 인시던트 대응 계정 관리를 AWS Organizations](#) 참조하세요.

다음 정보를 사용하여 AWS 보안 인시던트 대응을와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 서비스 연결 역할이 조직의 관리 계정에 자동으로 생성됩니다.

- `AWSServiceRoleForSecurityIncidentResponse` - 보안 인시던트 대응 멤버십 생성에 사용됨 -를 통한 서비스 구독 AWS Organizations.
- `AWSServiceRoleForSecurityIncidentResponse_Triage` - 가입 중 분류 기능을 활성화한 경우에만 사용.

Security Incident Response에서 사용하는 서비스 위탁자

앞 부분에서 다른 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 위탁자만 맡을 수 있습니다. Security Incident Response가 사용하는 서비스 연결 역할은 다음 서비스 위탁자에 대한 액세스 권한을 부여합니다.

- security-ir.amazonaws.com

Security Incident Response에 대한 신뢰할 수 있는 액세스 활성화

Security Incident Response에 대한 신뢰할 수 있는 액세스를 활성화하면 서비스가 조직의 구조를 추적하고 조직의 모든 계정에 활성 보안 인시던트 적용 범위가 있는지 확인할 수 있습니다. 또한 분류 기능을 활성화하면 서비스가 멤버 계정에서 서비스 연결 역할을 사용하여 기능을 분류할 수 있습니다.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS 보안 인시던트 대응 콘솔 또는 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다
AWS Organizations .

Important

가능하면 AWS 보안 인시던트 대응 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이를 통해 AWS Security Incident Response는 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 수행할 수 있습니다. AWS 보안 인시던트 대응에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS 보안 인시던트 대응 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하는 경우 이 단계를 완료할 필요가 없습니다.

Organizations는 설정 및 관리를 위해 Security Incident Response 콘솔을 사용할 때 Organizations의 신뢰할 수 있는 액세스를 자동으로 활성화합니다. Security Incident Response CLI/SDK를 사용하는 경우 [EnableAWSServiceAccess API](#)를 사용하여 신뢰할 수 있는 액세스를 수동으로 활성화해야 합니다. 보안 인시던트 대응 콘솔을 통해 신뢰할 수 있는 액세스를 활성화하는 방법을 알아보려면 보안 인시던트 대응 사용 설명서의 [AWS 계정 관리에 대한 신뢰할 수 있는 액세스 활성화](#)를 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.

2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Security Incident Response를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS 보안 인시던트 대응에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자만 있는 경우 AWS 보안 인시던트 대응 관리자에게 해당 서비스가 서비스 콘솔에서 작동 AWS Organizations 하도록 활성화할 수 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS 보안 인시던트 대응을 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal security-ir.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Security Incident Response에 대한 신뢰할 수 있는 액세스 비활성화

Organizations 관리 계정의 관리자만 Security Incident Response를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Security Incident Response를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS 보안 인시던트 대응에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자인 경우에만 AWS 보안 인시던트 대응 관리자에게 해당 서비스가 서비스 콘솔 또는 도구를 사용하여 작업 AWS Organizations 하지 못하도록 비활성화할 수 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS 보안 인시던트 대응을 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal security-ir.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Security Incident Response에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Security Incident Response에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자

또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Security Incident Response 관리와 조직 관리를 분리하는 데 도움이 됩니다. 자세한 내용은 [AWS 보안 인시던트 대응 사용 설명서의](#) [사용하여 보안 인시던트 대응 계정 관리를 AWS Organizations](#) 참조하세요.

최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Security Incident Response에 대해 위임된 관리자로 구성할 수 있습니다.

Security Incident Response 콘솔을 통해 위임된 관리자를 구성하는 방법을 알아보려면 [Security Incident Response 사용 설명서](#)의 위임된 Security Incident Response 관리자 계정 지정을 참조하세요.

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal security-ir.amazonaws.com
```

- AWS SDK: Organizations RegisterDelegatedAdministrator 작업 및 멤버 계정의 ID 번호를 호출하고 계정 서비스를 파라미터security-ir.amazonaws.com로 식별합니다.

Security Incident Response에 대한 위임된 관리자 비활성화

Important

위임된 관리자 계정에서 멤버십이 생성된 경우 위임된 관리자의 등록 취소는 파괴적인 작업이며 서비스 중단이 발생합니다. 위임된 관리자 다시 등록:

1. <https://console.aws.amazon.com/security-ir/home#/membership/settings> 웹페이지에서 Security Incident Response에 로그인합니다.
2. 서비스 콘솔에서 멤버십을 취소합니다. 멤버십은 결제 주기가 끝날 때까지 활성 상태로 유지됩니다.

3. 멤버십이 취소되면 Organizations 콘솔, CLI 또는 SDK를 통해 서비스 액세스를 비활성화합니다.

Organizations 관리 계정의 관리자만 Security Incident Response의 위임된 관리자를 제거할 수 있습니다. Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다.

Amazon Security Lake 및 AWS Organizations

Amazon Security Lake는 클라우드, 온프레미스 및 사용자 지정 소스의 보안 데이터를 계정에 저장된 데이터 레이크로 중앙 집중화합니다. Organizations와 통합하면 계정 전체에서 로그와 이벤트를 수집하는 데이터 레이크를 생성할 수 있습니다. 자세한 내용은 Amazon Security Lake User Guide의 [Managing multiple accounts with AWS Organizations](#)를 참조하세요.

다음 정보를 사용하여 Amazon Security Lake를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

[RegisterDataLakeDelegatedAdministrator](#) API를 호출하면 조직의 관리 계정에 다음 [서비스 연결 역할](#)이 자동으로 생성됩니다. 이 역할을 통해 Amazon Security Lake는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Amazon Security Lake와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForSecurityLake`

⚠️ 권장 사항: Security Lake의 RegisterDataLakeDelegatedAdministrator API를 사용하여 Security Lake가 조직에 액세스하도록 허용하고 조직의 위임된 관리자 등록 Organizations의 API를 사용하여 위임된 관리자를 등록하는 경우 Organizations에 대한 서비스 연결 역할이 성공적으로 생성되지 않을 수 있습니다. 전체 기능을 보장하려면 Security Lake API를 사용합니다.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Amazon Security Lake가 사용하는 서비스 연결 역할은 다음 서비스 위탁자에 대한 액세스 권한을 부여합니다.

- `securitylake.amazonaws.com`

Amazon Security Lake를 사용하여 신뢰할 수 있는 액세스 활성화

Security Lake와 상호 신뢰할 수 있는 액세스를 활성화하면 Security Lake가 조직 멤버십의 변경 사항에 자동으로 대응할 수 있습니다. 위임된 관리자는 모든 조직 계정의 지원되는 서비스에서 AWS 로그 수집을 활성화할 수 있습니다. 자세한 내용은 Amazon Security Lake User Guide의 [Service-linked role for Amazon Security Lake](#)를 참조하세요.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 Amazon Security Lake를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. Amazon Security Lake에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만 Amazon Security Lake의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon Security Lake를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal securitylake.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Amazon Security Lake를 사용하여 신뢰할 수 있는 액세스 비활성화

Organizations 관리 계정의 관리자만 Amazon Security Lake를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 Amazon Security Lake를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. Amazon Security Lake에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자인 경우에만 Amazon Security Lake의 관리자에게 서비스 콘솔 또는 도구를 AWS Organizations 사용하여 해당 서비스를 비활성화할 수 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon Security Lake를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal securitylake.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Amazon Security Lake에 대한 위임된 관리자 계정 활성화

Amazon Security Lake의 위임된 관리자는 조직의 다른 계정을 멤버 계정으로 추가합니다. 위임된 관리자는 Amazon Security Lake를 활성화하고 멤버 계정에 대한 Amazon Security Lake 설정을 구성할 수 있습니다. 위임된 관리자는 Amazon Security Lake가 활성화된 모든 AWS 리전(현재 사용 중인 리전 엔드포인트에 관계없이)의 조직 전체에서 로그를 수집할 수 있습니다.

위임된 관리자가 조직의 새 계정을 멤버로 자동 추가하도록 설정할 수도 있습니다. Amazon Security Lake의 위임된 관리자는 연결된 멤버 계정의 로그 및 이벤트에 액세스할 수 있습니다. 따라서 연결된 멤버 계정이 소유한 데이터를 수집하도록 Amazon Security Lake를 설정할 수 있습니다. 연결된 멤버 계정이 소유한 데이터를 사용할 수 있는 권한을 구독자에게 부여할 수도 있습니다.

자세한 내용은 Amazon Security Lake User Guide의 [Managing multiple accounts with AWS Organizations](#)를 참조하세요.

최소 권한

Organizations 관리 계정의 관리자만 멤버 계정을 조직의 Amazon Security Lake에 대해 위임된 관리자로 구성할 수 있습니다.

Amazon Security Lake 콘솔, Amazon Security Lake CreateDataLakeDelegatedAdmin API 작업 또는 create-datalake-delegated-admin CLI 명령을 사용하여 위임된 관리자 계정을 지정할 수 있습니다. Organizations RegisterDelegatedAdministrator CLI 또는 SDK 작업을 사용할 수도 있습니다. Amazon Security Lake에 대해 위임된 관리자 계정을 활성화하는 방법은 Amazon Security Lake 사용 설명서의 [위임된 Security Lake 관리자 지정 및 멤버 계정 추가](#)를 참조하세요.

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \ --service-principal securitylake.amazonaws.com
```

- AWS SDK: Organizations RegisterDelegatedAdministrator 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체를 파라미터account.amazonaws.com로 식별합니다.

Amazon Security Lake에 대해 위임된 관리자 비활성화

Organizations 관리 계정 또는 Amazon Security Lake 위임된 관리자 계정의 관리자만 조직에서 위임된 관리자 계정을 제거할 수 있습니다.

Amazon Security Lake DeregisterDataLakeDelegatedAdministrator API 작업, deregister-data-lake-delegated-administrator CLI 명령, Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. Amazon Security Lake를 사용하여 위임된 관리자를 제거하려면 Amazon Security Lake 사용 설명서의 [Security Lake 위임된 관리자 제거](#)를 참조하세요.

AWS Service Catalog 및 AWS Organizations

Service Catalog를 사용하면 AWS에서 사용이 승인된 IT 서비스 카탈로그를 생성하고 관리할 수 있습니다.

Service Catalog를와 통합하면 조직 전체의 포트폴리오 공유 및 제품 복사가 AWS Organizations 간소화됩니다. Service Catalog 관리자는 포트폴리오를 공유할 AWS Organizations 때의 기존 조직을 참조할 수 있으며, 조직의 트리 구조에서 신뢰할 수 있는 조직 단위(OU)와 포트폴리오를 공유할 수 있습니다. 따라서 포트폴리오 ID를 공유할 필요가 없고, 수신하는 계정은 포트폴리오를 가져올 때 포트폴리오

ID를 수동으로 참조하지 않아도 됩니다. 이 메커니즘을 통해 공유된 포트폴리오는 Service Catalog에서 관리자의 가져온 포트폴리오(Imported Portfolio) 보기에 공유 대상 계정으로 나열됩니다.

Service Catalog에 대한 자세한 내용은 [Service Catalog 관리자 안내서](#)를 참조하세요.

다음 정보를 사용하여 AWS Service Catalog 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

AWS Service Catalog 는 신뢰할 수 있는 액세스를 활성화하는 과정에서 서비스 연결 역할을 생성하지 않습니다.

권한을 부여하는 데 사용되는 서비스 보안 주체

신뢰할 수 있는 액세스를 활성화하려면 다음 서비스 보안 주체를 지정해야 합니다.

- `servicecatalog.amazonaws.com`

Service Catalog와 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS Service Catalog 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS Service Catalog 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Service Catalog 수행할 수 있습니다. AWS Service Catalog에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Service Catalog 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하면이 단계를 완료할 필요가 없습니다.

Service Catalog CLI 또는 AWS SDK를 사용하여 신뢰할 수 있는 액세스를 활성화하려면

다음 명령 또는 작업 중 하나를 호출합니다.

- AWS CLI: [aws servicecatalog enable-aws-organizations-access](#)
- AWS SDKs: [AWSServiceCatalog::EnableAWSOrganizationsAccess](#)

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Service Catalog를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Service Catalog에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Service Catalog 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Service Catalog 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal servicecatalog.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Service Catalog과 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Service Catalog를 사용하는 AWS Organizations 동안 사용되어 신뢰할 수 있는 액세스를 비활성화 하면 현재 공유가 삭제되지 않지만 조직 전체에서 새 공유를 생성할 수 없습니다. 이 작업을 호출한 후 조직 구조가 변경되면, 현재 공유는 조직 구조와 동기화되지 않습니다.

Service Catalog CLI 또는 AWS SDK를 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

다음 명령 또는 작업 중 하나를 호출합니다.

- AWS CLI: [aws servicecatalog disable-aws-organizations-access](#)
- AWS SDKs: [DisableAWSOrganizationsAccess](#)

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Service Catalog를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS Service Catalog에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 AWS Service Catalog 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Service Catalog 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal servicecatalog.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Service Quotas 및 AWS Organizations

Service Quotas는 중앙 위치에서 할당량을 보고 관리할 수 있는 AWS 서비스입니다. 제한이라고도 하는 할당량은 AWS 계정의 리소스, 작업, 항목의 최대값입니다.

Service Quotas가와 연결되면 할당량 요청 템플릿을 생성하여 계정이 생성될 때 할당량 증가를 자동으로 요청할 AWS Organizations수 있습니다.

서비스 할당량에 대한 자세한 내용은 [Service Quotas 사용 설명서](#)를 참조하세요.

다음 정보를 사용하여 Service Quotas를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Service Quotas는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Service Quotas와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- AWSServiceRoleForServiceQuotas

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Service Quotas가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `servicequotas.amazonaws.com`

Service Quotas와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Service Quotas로만 활성화할 수 있습니다.

Service Quotas 콘솔 AWS CLI 또는 SDK를 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

- Service Quotas 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Organizations 관리 계정으로 로그인한 다음 Service Quotas 콘솔에서 템플릿을 구성합니다. 자세한 내용은 Service Quotas 사용 설명서의 [Service Quotas 템플릿 사용](#)을 참조하세요.

- Service Quotas AWS CLI 또는 SDK를 사용하여 신뢰할 수 있는 액세스를 활성화하려면

다음 명령 또는 작업을 호출합니다.

- AWS CLI: [aws service-quotas associate-service-quota-template](#)
- AWS SDKs: [AssociateServiceQuotaTemplate](#)

AWS IAM Identity Center 및 AWS Organizations

AWS IAM Identity Center 는 모든 AWS 계정 및 클라우드 애플리케이션에 대한 Single Sign-On 액세스를 제공합니다. AWS Directory Service 를 통해 Microsoft Active Directory와 연결하여 해당 디렉터리의 사용자가 기존 Active Directory 사용자 이름과 암호를 사용하여 개인화된 AWS 액세스 포털에 로그인할 수 있도록 합니다. AWS 액세스 포털에서 사용자는 권한이 있는 모든 AWS 계정 및 클라우드 애플리케이션에 액세스할 수 있습니다.

IAM Identity Center에 대한 자세한 내용은 [AWS IAM Identity Center 사용 설명서](#)를 참조하세요.

다음 정보를 사용하여 AWS IAM Identity Center 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 IAM Identity Center는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

IAM Identity Center와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForSSO`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. IAM Identity Center가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `sso.amazonaws.com`

IAM Identity Center와의 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS IAM Identity Center 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

Important

가능하면 AWS IAM Identity Center 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS IAM Identity Center 수행할 수 있습니다. AWS IAM Identity Center에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS IAM Identity Center 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하면 이 단계를 완료할 필요가 없습니다.

IAM Identity Center가 작동 AWS Organizations 하려면를 통한 신뢰할 수 있는 액세스가 필요합니다. 신뢰할 수 있는 액세스는 IAM Identity Center를 설정할 때 활성화합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [시작하기 - 1단계: AWS IAM Identity Center활성화](#)를 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS IAM Identity Center를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS IAM Identity Center에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS IAM Identity Center 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS IAM Identity Center 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal sso.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

IAM Identity Center와의 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

IAM Identity Center를 작동 AWS Organizations 하려면를 통한 신뢰할 수 있는 액세스가 필요합니다. IAM Identity Center를 사용하는 AWS Organizations 동안를 사용하여 신뢰할 수 있는 액세스를 비활성화하면 조직에 액세스할 수 없으므로 작동이 중지됩니다. 사용자는 IAM Identity Center를 사용하여 계정에 액세스할 수 없게 됩니다. IAM Identity Center가 생성한 역할은 그대로 남아 있지만 IAM Identity Center 서비스가 해당 역할에 액세스할 수 없습니다. IAM Identity Center 서비스 연결 역할은 그대로 유지됩니다. 신뢰할 수 있는 액세스를 다시 활성화하면 IAM Identity Center가 이전과 같이 계속 작동하므로 서비스를 다시 구성할 필요가 없습니다.

조직에서 계정을 제거한 경우 IAM Identity Center는 서비스 연결 역할과 같은 모든 메타데이터 및 리소스를 자동으로 정리합니다. 조직에서 제거된 독립 실행형 계정은 더 이상 IAM Identity Center에서 사용할 수 없습니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS IAM Identity Center를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS IAM Identity Center에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자만 있는 경우 이제 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 AWS IAM Identity Center 있음을 관리자에게 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS IAM Identity Center 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal sso.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

IAM Identity Center에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 IAM Identity Center에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 IAM Identity Center 관리와 조직 관리를 분리하는 데 도움이 됩니다.

최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 IAM Identity Center에 대한 위임된 관리자로 구성할 수 있습니다.

IAM Identity Center에 대한 위임된 관리자 계정을 활성화하는 방법에 대한 지침은 AWS IAM Identity Center 사용 설명서의 [위임된 관리](#)를 참조하세요.

AWS Systems Manager 및 AWS Organizations

AWS Systems Manager 는 리소스의 가시성과 제어를 지원하는 기능 모음입니다 AWS . 다음 Systems Manager 기능은 조직의 모든 AWS 계정 에 걸쳐 Organizations과 함께 사용할 수 있습니다.

- Systems Manager Explorer는 AWS 리소스에 대한 정보를 보고하는 사용자 지정 가능한 작업 대시보드입니다. Organizations 및 Systems Manager Explorer를 사용하여 조직의 모든 AWS 계정 에서 작업 데이터를 동기화할 수 있습니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 [Systems Manager Explorer](#)를 참조하세요.
- Systems Manager Change Manager는 애플리케이션 구성 및 인프라에 대한 운영 변경을 요청, 승인, 구현 및 보고하기 위한 엔터프라이즈 변경 관리 프레임워크입니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 [AWS Systems Manager Change Manager](#)를 참조하세요.

- Systems Manager OpsCenter는 운영 엔지니어와 IT 전문가가 AWS 리소스와 관련된 운영 작업 항목(OpsItems)을 보고, 조사하고, 해결할 수 있는 중앙 위치를 제공합니다. Organizations와 함께 OpsCenter를 사용하면 단일 세션 동안 관리 계정(Organizations 관리 계정 또는 Systems Manager 위임 관리자 계정) 및 다른 계정 하나의 OpsItem에 대한 작업을 수행할 수 있습니다. 구성되면 사용자는 다음 유형의 작업을 수행할 수 있습니다.
- 다른 계정의 OpsItem을 만들고 보고 업데이트합니다.
- 다른 계정의 OpsItems에 지정된 AWS 리소스에 대한 자세한 정보를 봅니다.
- Systems Manager Automation 런북을 시작하여 다른 계정의 AWS 리소스 문제를 해결합니다.

자세한 내용은 AWS Systems Manager 사용 설명서의 [AWS Systems Manager OpsCenter](#)을 참조하세요.

- 빠른 설정을 사용하면 권장 모범 사례에 따라 자주 사용되는 AWS 서비스 및 기능을 빠르게 구성할 수 있습니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 [AWS Systems Manager 빠른 설정](#)을 참조하세요.

Systems Manager에 AWS Organizations 위임된 관리자 계정을 등록하면 조직의 조직 단위를 대상으로 하는 빠른 설정 구성 관리자를 생성, 업데이트, 확인 및 삭제할 수 있습니다. AWS Systems Manager 사용 설명서의 [빠른 설정을 위해 위임된 관리자 사용](#)에서 자세히 알아봅니다.

- Systems Manager용 통합 콘솔을 설정할 때 위임된 관리자 계정을 입력합니다. 이 계정은 빠른 설정, 탐색기, CloudFormation StackSets 및 Resource Explorer에 AWS Organizations 위임된 관리자 계정을 등록하는 데 사용됩니다. 자세한 내용은 [조직용 Systems Manager 통합 콘솔 설정 AWS Systems Manager 사용 설명서](#)를 참조하세요.

다음 정보를 사용하여 AWS Systems Manager와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Systems Manager는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Systems Manager와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- AWSServiceRoleForAmazonSSM_AccountDiscovery

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다른 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Systems Manager가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `ssm.amazonaws.com`

Systems Manager와 상호 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 Organizations 도구로만 활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Systems Manager를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Systems Manager에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Systems Manager 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Systems Manager 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal ssm.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Systems Manager와 상호 신뢰할 수 있는 액세스 비활성화

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Systems Manager는 조직의에서 작업 데이터를 동기화 AWS Organizations 하기 위해와 신뢰할 수 있는 액세스 AWS 계정 가 필요합니다. 신뢰할 수 있는 액세스를 비활성화하면 Systems Manager에서 작업 데이터가 동기화되지 않고 오류가 보고됩니다.

신뢰할 수 있는 액세스는 Organizations 도구로만 비활성화할 수 있습니다.

AWS Organizations 콘솔을 사용하거나, Organizations AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Systems Manager를 선택합니다.
4. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
5. AWS Systems Manager에 대한 신뢰할 수 있는 액세스 비활성화 대화 상자에서 비활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 의 관리자만 있는 경우 이제 서비스 콘솔 또는 도구를 사용하여 해당 서비스 작업을 AWS Organizations 비활성화할 수 AWS Systems Manager 있음을 관리자에게 AWS Organizations 알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화할 수 있습니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Systems Manager 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
  --service-principal ssm.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Systems Manager에 대한 위임된 관리자 계정 활성화

멤버 계정을 조직의 위임된 관리자로 지정하면 해당 계정의 사용자 및 역할이 Systems Manager에 대한 관리 작업을 수행할 수 있습니다. 그렇지 않은 경우 조직의 관리 계정에 속한 사용자 또는 역할만 관리 작업을 수행할 수 있습니다. 이는 Systems Manager 관리와 조직 관리를 분리하는 데 도움을 줍니다.

조직 전체에서 Systems Manager를 사용하는 경우 위임된 관리자 계정을 사용합니다. Change Manager에서 변경 템플릿, 변경 요청, 변경 실행서 및 승인 워크플로를 관리하기 위한 계정으로 AWS 계정 지정된 입니다. 위임된 계정은 조직 전체의 변경 활동을 관리합니다. Change Manager에서 사용할 조직을 설정할 때 이 역할을 수행하는 계정을 지정합니다. 조직의 관리 계정일 필요는 없습니다. 계정 하나만으로 Change Manager를 사용하는 경우 위임된 관리자 계정이 필요하지 않습니다.

멤버 계정을 위임된 관리자로 지정하려면 AWS Systems Manager 사용 설명서에서 다음 주제를 참조하세요.

- Explorer 및 OpsCenter의 경우 [위임된 관리자 구성](#)을 참조하세요.
- Change Manager의 경우, [Change Manager에 대해 조직 및 위임된 계정 설정](#)을 참조하세요.
- 빠른 설정은 [빠른 설정을 위해 위임된 관리자 등록](#)을 참조하세요.

Systems Manager에 대한 위임된 관리자 계정 비활성화

위임된 관리자 등록을 취소하려면 AWS Systems Manager 사용 설명서에서 다음 주제를 참조하세요.

- Explorer 및 OpsCenter는 [Explorer 위임된 관리자 등록 취소](#)를 참조하세요.
- Change Manager의 경우, [Change Manager에 대해 조직 및 위임된 계정 설정](#)을 참조하세요.
- 빠른 설정은 [빠른 설정을 위해 위임된 관리자 등록 취소](#)를 참조하세요.

AWS User Notifications 및 AWS Organizations

[AWS User Notifications](#)는 AWS 알림의 중앙 위치입니다.

와 통합한 후 조직의 여러 계정에서 알림을 중앙에서 구성하고 볼 AWS Organizations수 있습니다.

다음 정보를 사용하여 AWS User Notifications 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 사용하면 사용자 알림 가 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

사용자 알림 와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForAWSUserNotifications`

자세한 내용은 AWS User Notifications 사용 설명서의 [서비스 연결 역할 사용](#)을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. 다음 서비스 보안 주체에 대한 액세스 권한을 사용자 알림 부여하는 데 사용되는 서비스 연결 역할:

- `notifications.amazon.com`

를 사용하여 신뢰할 수 있는 액세스 활성화 사용자 알림

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 AWS User Notifications로만 활성화할 수 있습니다.

사용자 알림 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면 사용자 알림 사용 설명서의 [AWS Organizations에서 활성화 AWS User Notifications](#)를 참조하세요.

를 사용하여 신뢰할 수 있는 액세스 비활성화 사용자 알림

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 AWS User Notifications로만 활성화할 수 있습니다.

사용자 알림 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면 사용자 알림 사용 설명서의 [AWS Organizations에서 활성화 AWS User Notifications](#)를 참조하세요.

에 대한 위임된 관리자 계정 활성화 사용자 알림

관리 계정 관리자는 위임된 관리자라고 하는 지정된 멤버 계정에 사용자 알림 관리 권한을 위임할 수 있습니다. 프라이빗 마켓플레이스의 위임된 관리자로 계정을 등록하려면 관리 계정 관리자가 신뢰할 수 있는 액세스 및 서비스 연결 역할이 활성화되었는지 확인하고 새 관리자 등록을 선택하고 12자리 AWS 계정 번호를 입력한 다음 제출을 선택해야 합니다.

관리 계정과 위임된 관리자 계정은 경험 생성, 브랜딩 설정 업데이트, 대상 연결 또는 연결 해제, 제품 추가 또는 제거, 보류 중인 요청 승인 또는 거부와 같은 사용자 알림 관리 작업을 수행할 수 있습니다.

사용자 알림 콘솔을 사용하여 위임된 관리자를 구성하려면 사용자 알림 사용 설명서의 [에서 위임된 관리자 등록 AWS User Notifications](#)을 참조하세요.

Organizations RegisterDelegatedAdministrator API를 사용하여 위임된 관리자를 구성할 수도 있습니다. 자세한 내용은 Organizations 명령 참조에서 [RegisterDelegatedAdministrator](#)를 참조하세요.

에 대해 위임된 관리자 비활성화 사용자 알림

조직 관리 계정의 관리자만 사용자 알림에 대해 위임된 관리자를 구성할 수 있습니다.

사용자 알림 콘솔 또는 API를 사용하거나 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다.

사용자 알림 콘솔을 사용하여 위임된 관리자 사용자 알림 계정을 비활성화하려면 사용자 알림 사용 설명서의 [에서 위임된 관리자 제거 AWS User Notifications](#)를 참조하세요.

태그 정책 및 AWS Organizations

태그 정책은 조직 계정의 리소스 간에 태그를 표준화 AWS Organizations 하는 데 도움이 되는의 정책 유형입니다. 태그 정책에 대한 자세한 내용은 [- 태그 정책](#) 단원을 참조하세요.

다음 정보를 사용하여 태그 정책들과 통합할 수 있습니다 AWS Organizations.

서비스 연결 역할이 사용하는 서비스 보안 주체

Organizations는 다음 서비스 보안 주체를 사용하여 리소스에 연결된 태그와 상호 작용합니다.

- `tagpolicies.tag.amazonaws.com`

태그 정책에 대해 신뢰할 수 있는 액세스 활성화

조직에서 태그 정책을 활성화하거나 AWS Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

Important

태그 정책을 활성화하여 신뢰할 수 있는 액세스를 활성화하는 것이 좋습니다. 이렇게 하면 Organizations가 필요한 설정 작업을 수행합니다.

AWS Organizations 콘솔에서 태그 정책 유형을 활성화하여 태그 정책에 대한 신뢰할 수 있는 액세스를 활성화할 수 있습니다. 자세한 내용은 [정책 유형 활성화](#) 단원을 참조하십시오.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 태그 정책을 선택합니다.

4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. 태그 정책에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만 태그 정책 관리자에게 해당 서비스가 서비스 콘솔에서 작동 AWS Organizations 하도록 활성화할 수 있음을 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 태그 정책을 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
  --service-principal tagpolicies.tag.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

태그 정책과 상호 신뢰할 수 있는 액세스 비활성화

AWS Organizations 콘솔에서 태그 정책 유형을 비활성화하여 태그 정책에 대한 신뢰할 수 있는 액세스를 비활성화할 수 있습니다. 자세한 내용은 [정책 유형 비활성화](#) 단원을 참조하십시오.

AWS Trusted Advisor 및 AWS Organizations

AWS Trusted Advisor 는 AWS 환경을 검사하고 비용을 절감하거나, 시스템 가용성 및 성능을 개선하거나, 보안 격차를 좁힐 수 있는 기회가 있을 때 권장 사항을 제시합니다. Organizations와 통합하면 조직의 모든 계정에 대한 Trusted Advisor 검사 결과를 수신하고 보고서를 다운로드하여 검사 요약 및 영향을 받는 리소스를 볼 수 있습니다.

자세한 내용은 AWS Support 사용 설명서의 [AWS Trusted Advisor에 대한 조직 보기](#)를 참조하세요.

다음 정보를 사용하여 AWS Trusted Advisor 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Trusted Advisor 는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Trusted Advisor 와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForTrustedAdvisorReporting`

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 맡을 수 있습니다. 다음 서비스 보안 주체에 대한 액세스 권한을 Trusted Advisor 부여하는데 사용되는 서비스 연결 역할:

- `reporting.trustedadvisor.amazonaws.com`

를 사용하여 신뢰할 수 있는 액세스 활성화 Trusted Advisor

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

신뢰할 수 있는 액세스는 AWS Trusted Advisor로만 활성화할 수 있습니다.

Trusted Advisor 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Support 사용 설명서의 [조직 보기 사용](#)을 참조하세요.

를 사용하여 신뢰할 수 있는 액세스 비활성화 Trusted Advisor

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

이 기능을 비활성화하면는 조직의 다른 모든 계정에 대한 검사 정보 기록을 Trusted Advisor 중지합니다. 기존 보고서를 보거나 다운로드하거나 새 보고서를 만들 수 없습니다.

AWS Trusted Advisor 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

⚠ Important

가능하면 AWS Trusted Advisor 콘솔 또는 도구를 사용하여 Organizations와의 통합을 비활성화하는 것이 좋습니다. 이렇게 하면 서비스에서 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등 필요한 모든 정리를 AWS Trusted Advisor 수행할 수 있습니다. AWS Trusted Advisor에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.

AWS Trusted Advisor 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화하면이 단계를 완료할 필요가 없습니다.

Trusted Advisor 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

AWS Support 사용 설명서의 [조직 보기 사용 안 함](#)을 참조하세요.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 신뢰할 수 있는 서비스로 AWS Trusted Advisor 를 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

에 대한 위임된 관리자 계정 활성화 Trusted Advisor

멤버 계정을 조직의 위임된 관리자로 지정하면 지정된 계정의 사용자 및 역할이 조직의 다른 멤버 계정의 AWS 계정 메타데이터를 관리할 수 있습니다. 위임된 관리자 계정을 활성화하지 않으면 조직의 관

리 계정에서만 이러한 작업을 수행할 수 있습니다. 이렇게 하면 조직의 관리와 계정 세부 정보의 관리를 분리하는 데 도움이 됩니다.

최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의에 대한 위임된 관리자로 구성할 수 Trusted Advisor 있습니다.

에 대한 위임된 관리자 계정 활성화에 대한 지침은 지원 사용 설명서의 위임된 관리자 등록을 Trusted Advisor참조하세요. <https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor-priority.html#register-delegated-administrators>

AWS CLI, AWS API

CLI 또는 AWS SDKs 중 하나를 사용하여 AWS 위임된 관리자 계정을 구성하려면 다음 명령을 사용할 수 있습니다.

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
  --account-id 123456789012 \
  --service-principal reporting.trustedadvisor.amazonaws.com
```

- AWS SDK: Organizations RegisterDelegatedAdministrator 작업과 멤버 계정의 ID 번호를 호출하고 계정 서비스 보안 주체를 파라미터account.amazonaws.com로 식별합니다.

에 대해 위임된 관리자 비활성화 Trusted Advisor

Trusted Advisor 콘솔을 사용하거나 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다. Trusted Advisor 콘솔을 사용하여 위임된 관리자 Trusted Advisor 계정을 비활성화하는 방법에 대한 자세한 내용은 지원 사용 설명서의 [위임된 관리자 등록 취소를 참조하세요](#).

AWS Well-Architected Tool 및 AWS Organizations

는 워크로드의 상태를 문서화하고 이를 최신 AWS 아키텍처 모범 사례와 비교하는 데 AWS Well-Architected Tool 도움이 됩니다.

Organizations와 AWS Well-Architected Tool 함께를 사용하면 AWS Well-Architected Tool 및 Organizations 고객 모두 조직의 다른 구성원과 AWS Well-Architected Tool 리소스를 공유하는 프로세스를 간소화할 수 있습니다.

자세한 내용은 AWS Well-Architected Tool 사용 설명서의 [AWS Well-Architected Tool 리소스 공유](#)를 참조하세요.

다음 정보를 사용하여 AWS Well-Architected Tool 와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 AWS WA Tool 는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

AWS WA Tool 와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForWellArchitected`

서비스 역할 정책은 `AWSCloudFormationServiceRolePolicy`입니다.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다른 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. 다음 서비스 보안 주체에 대한 액세스 권한을 AWS WA Tool 부여하는 데 사용되는 서비스 연결 역할:

- `wellarchitected.amazonaws.com`

를 사용하여 신뢰할 수 있는 액세스 활성화 AWS WA Tool

를 업데이트 AWS WA Tool 하여 조직의 계층적 변경 사항을 반영할 수 있습니다.

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

콘솔 또는 AWS Well-Architected Tool 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다 AWS Organizations .

⚠ Important

가능하면 AWS Well-Architected Tool 콘솔 또는 도구를 사용하여 Organizations와의 통합을 활성화하는 것이 좋습니다. 이렇게 하면 서비스에 필요한 리소스 생성과 같이 필요한 모든 구성을 AWS Well-Architected Tool 수행할 수 있습니다. AWS Well-Architected Tool에서 제공하는 도구를 사용하여 통합을 활성화할 수 없는 경우에만 다음 단계를 진행합니다. 자세한 내용은 [이 메모](#)를 참조하십시오.

AWS Well-Architected Tool 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 활성화하는 경우가 단계를 완료할 필요가 없습니다.

AWS WA Tool 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화하려면

AWS Well-Architected Tool 사용 설명서의 [AWS Well-Architected Tool 리소스 공유를 참조하세요](#).

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. 탐색 창에서 서비스를 선택합니다.
3. 서비스 목록에서 AWS Well-Architected Tool를 선택합니다.
4. 신뢰할 수 있는 액세스 활성화를 선택합니다.
5. AWS Well-Architected Tool에 대한 신뢰할 수 있는 액세스 활성화 대화 상자에서 활성화를 입력하여 확인한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
6. 의 관리자인 경우에만의 관리자에게 서비스 콘솔에서 해당 서비스를 사용할 AWS Organizations 수 있도록 설정할 수 AWS Well-Architected Tool 있다고 AWS Organizations알립니다.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화합니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Well-Architected Tool 를 신뢰할 수 있는 서비스로 활성화합니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal wellarchitected.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

를 사용하여 신뢰할 수 있는 액세스 비활성화 AWS WA Tool

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Well-Architected Tool 또는 AWS Organizations 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다.

Important

가능하면 AWS Well-Architected Tool 콘솔 또는 도구를 사용하여 Organizations와의 통합을 비활성화하는 것이 좋습니다. 이렇게 하면 서비스에서 더 이상 필요하지 않은 리소스 또는 액세스 역할을 삭제하는 등 필요한 모든 정리를 AWS Well-Architected Tool 수행할 수 있습니다. AWS Well-Architected Tool에서 제공하는 도구를 사용하여 통합을 비활성화할 수 없는 경우에만 다음 단계를 진행합니다.

AWS Well-Architected Tool 콘솔 또는 도구를 사용하여 신뢰할 수 있는 액세스를 비활성화하면 이 단계를 완료할 필요가 없습니다.

AWS WA Tool 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면

AWS Well-Architected Tool 사용 설명서의 [AWS Well-Architected Tool 리소스 공유를 참조하세요](#).

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하여 Organizations에서 AWS Well-Architected Tool 를 신뢰할 수 있는 서비스로 비활성화합니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal wellarchitected.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

Amazon VPC IP 주소 관리자(IPAM) 및 AWS Organizations

Amazon VPC IP 주소 관리자(IPAM)는 AWS 워크로드의 IP 주소를 더 쉽게 계획, 추적 및 모니터링할 수 있는 VPC 기능입니다.

AWS Organizations 를 사용하면 조직 전체의 IP 주소 사용량을 모니터링하고 멤버 계정 간에 IP 주소 풀을 공유할 수 있습니다.

자세한 내용은 Amazon VPC IPAM 사용 설명서의 [AWS Organizations와 IPAM 통합](#)을 참조하십시오.

다음 정보를 사용하여 Amazon VPC IP 주소 관리자(IPAM)를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

다음 서비스 연결 역할은 IPAM 콘솔을 사용하거나 IPAM의 EnableIpamOrganizationAdminAccount API를 사용하여 IPAM을 AWS Organizations 와 통합할 때 조직의 관리 계정 및 각 멤버 계정에 자동으로 생성됩니다.

- AWSServiceRoleForIPAM

자세한 내용은 Amazon VPC IPAM 사용 설명서의 [IPAM에 대한 서비스 연결 역할](#)을 참조하십시오.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다른 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. IPAM에서 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `ipam.amazonaws.com`

IPAM에서 신뢰할 수 있는 액세스 활성화

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Note

IPAM에 대해 위임된 관리자를 지정하면 조직의 IPAM에 대해 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

멤버 계정을 조직의이 서비스에 대한 위임된 관리자로 지정하려면 IPAM에에 대한 신뢰할 AWS Organizations 수 있는 액세스 권한이 필요합니다.

Amazon VPC IP 주소 관리자(IPAM) 도구만 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다.

IPAM 콘솔 또는 IPAM `EnableIpamOrganizationAdminAccount` API AWS Organizations 를 사용하여 IPAM을와 통합하는 경우 IPAM에 대한 신뢰할 수 있는 액세스 권한을 자동으로 부여합니다. 신뢰할 수 있는 액세스 권한을 부여하면 관리 계정과 조직의 모든 멤버 계정에 서비스 연결 역할 `AWS ServiceRoleForIPAM`가 생성됩니다. IPAM은 서비스 연결 역할을 사용하여 조직의 EC2 네트워킹 리소스와 연결된 CIDR을 모니터링하고 Amazon CloudWatch에 IPAM과 관련된 지표를 저장합니다. 자세한 내용은 Amazon VPC IPAM 사용 설명서의 [IPAM에 대한 서비스 연결 역할](#)을 참조하십시오.

신뢰할 수 있는 액세스 활성화에 대한 지침은 Amazon VPC IPAM 사용 설명서의 [AWS Organizations 와 IPAM 통합](#)을 참조하십시오

Note

AWS Organizations 콘솔 또는 [EnableAWSServiceAccess](#) API를 사용하여 IPAM으로 신뢰할 수 있는 액세스를 활성화할 수 없습니다.

IPAM에서 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

AWS Organizations 관리 계정의 관리자만 API를 사용하여 IPAM으로 신뢰할 수 있는 액세스를 비활성화할 수 있습니다. `disable-aws-service-access` 있습니다.

IPAM 계정 권한 비활성화 및 서비스 연결 역할 삭제에 대한 자세한 내용은 Amazon VPC IPAM 사용 설명서의 [IPAM에 대한 서비스 연결 역할](#)을 참조하십시오.

Organizations AWS CLI 명령을 실행하거나 AWS SDKs.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 비활성화합니다.

- AWS CLI: [disable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Amazon VPC IP Address Manager(IPAM)를 비활성화할 수 있습니다.

```
$ aws organizations disable-aws-service-access \
    --service-principal ipam.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [DisableAWSServiceAccess](#)

IPAM에 대한 위임된 관리자 계정 활성화

IPAM에 대해 위임된 관리자 계정은 IPAM 및 IP 주소 풀 생성, 조직의 IP 주소 사용 관리 및 모니터링, 멤버 계정 간에 IP 주소 풀 공유를 담당합니다. 자세한 내용은 Amazon VPC IPAM 사용 설명서의 [AWS Organizations와 IPAM 통합](#)을 참조하십시오.

조직 관리 계정의 관리자만 IPAM에 대해 위임된 관리자를 구성할 수 있습니다.

IPAM 콘솔에서 또는 `enable-ipam-organization-admin-account` API를 사용하여 위임된 관리자 계정을 지정할 수 있습니다. 자세한 내용은 명령 참조의 [enable-ipam-organization-admin-account](#)를 참조하세요. AWS CLI

i 최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 IPAM에 대한 위임된 관리자 구성할 수 있습니다

IPAM 콘솔을 사용하여 위임된 관리자를 구성하려면 [Amazon VPC IPAM 사용 설명서](#)에서 AWS Organizations와 IPAM 통합을 참조하세요.

IPAM에 대해 위임된 관리자를 비활성화

조직 관리 계정의 관리자만 IPAM에 대해 위임된 관리자를 구성할 수 있습니다.

를 사용하여 위임된 관리자를 제거하려면 AWS CLI 명령 `aws cli` 참조의 [disable-ipam-organization-admin-account](#)를 참조하세요.

IPAM 콘솔을 사용하여 위임된 관리자 IPAM 계정을 비활성화하려면 Amazon VPC IPAM 사용 설명서에서 [AWS Organizations와 IPAM 통합](#)을 참조하세요.

Amazon VPC Reachability Analyzer 및 AWS Organizations

Reachability Analyzer는 Virtual Private Cloud(VPC)에서 소스 리소스와 대상 리소스 간의 연결을 테스트할 수 있는 구성 분석 도구입니다.

Reachability Analyzer와 AWS Organizations 함께 사용하면 조직의 계정 간에 경로를 추적할 수 있습니다.

자세한 내용은 [Reachability Analyzer 사용 설명서](#)의 Reachability Analyzer에서 위임된 관리자 계정 관리를 참조하세요.

다음 정보를 사용하여 Reachability Analyzer를와 통합할 수 있습니다 AWS Organizations.

통합 활성화 시 서비스 연결 역할 생성

신뢰할 수 있는 액세스를 활성화하면 다음 [서비스 연결 역할](#)이 조직의 관리 계정에 자동으로 생성됩니다. 이 역할을 통해 Reachability Analyzer는 조직의 계정 내에서 지원되는 작업을 수행할 수 있습니다.

Reachability Analyzer와 Organizations 간의 신뢰할 수 있는 액세스를 비활성화하거나 조직에서 멤버 계정을 제거한 경우에만 이 역할을 삭제하거나 수정할 수 있습니다.

- `AWSServiceRoleForReachabilityAnalyzer`

자세한 내용은 [Reachability Analyzer 사용 설명서](#)에서 Reachability Analyzer의 계정 간 분석을 참조하세요.

서비스 연결 역할이 사용하는 서비스 보안 주체

앞 부분에서 다룬 서비스 연결 역할은 역할에 대해 정의된 신뢰 관계에 의해 권한이 부여되는 서비스 보안 주체만 말할 수 있습니다. Reachability Analyzer가 사용하는 서비스 연결 역할은 다음 서비스 보안 주체에 대한 액세스 권한을 부여합니다.

- `reachabilityanalyzer.networkinsights.amazonaws.com`

Reachability Analyzer를 통한 신뢰할 수 있는 액세스를 활성화하려면

신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Reachability Analyzer에 대해 위임된 관리자를 지정하면 조직의 Reachability Analyzer에 대해 신뢰할 수 있는 액세스를 자동으로 활성화합니다.

Reachability Analyzer는 멤버 계정을 조직의이 서비스에 대한 위임된 관리자로 지정하기 AWS Organizations 전에에 대한 신뢰할 수 있는 액세스 권한이 필요합니다.

Important

- Reachability Analyzer 콘솔 또는 Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 활성화할 수 있습니다. 하지만 Organizations와의 통합을 설정하는 데에는 Reachability Analyzer 콘솔이나 `EnableMultiAccountAnalysisForAwsOrganization` API를 사용하는 것이 좋습니다. 이렇게 하면 Reachability Analyzer가 서비스에 필요한 리소스 생성 등 모든 필수 구성을 수행합니다.
- 신뢰할 수 있는 액세스 권한을 부여하면 관리 계정과 조직의 모든 멤버 계정에 서비스 연결 역할 `AWSServiceRoleForReachabilityAnalyzer`가 생성됩니다. Reachability Analyzer는 서비스 연결 역할을 사용하여 관리자와 위임된 관리자가 조직 내 모든 리소스 간의 연결에 대한 분석을 실행할 수 있도록 합니다. Reachability Analyzer는 조직 내 계정의 네트워킹 요소에 대한 스냅샷을 생성하여 연결 쿼리에 응답할 수 있습니다.
- 자세한 내용과 Reachability Analyzer를 통한 신뢰할 수 있는 액세스를 활성화하는 방법에 대한 지침은 Reachability Analyzer 사용 설명서에서 [Reachability Analyzer의 계정 간 분석](#)을 참조하세요.

AWS Organizations 콘솔을 사용하거나, AWS CLI 명령을 실행하거나, AWS SDKs.

AWS Management Console

Organizations 콘솔을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

1. [AWS Organizations 콘솔](#)에 로그인합니다. 조직의 관리 계정에서 IAM 사용자로 로그인하거나 IAM 역할을 맡거나 루트 사용자로 로그인([권장되지 않음](#))해야 합니다.
2. [서비스](#) 페이지에서 VPC Reachability Analyzer에 대한 행을 찾아 서비스의 이름을 선택한 다음 신뢰할 수 있는 액세스 활성화를 선택합니다.
3. 확인 대화 상자에서 신뢰할 수 있는 액세스를 활성화하는 옵션 표시(Show the option to enable trusted access)를 사용하도록 설정하고, 상자에 **enable**을 입력한 다음 신뢰할 수 있는 액세스 활성화(Enable trusted access)를 선택합니다.
4. 의 관리자인 경우에만 Reachability Analyzer 관리자에게 콘솔을 사용하여 해당 서비스를 활성화할 수 있음을 AWS Organizations알립니다 AWS Organizations.

AWS CLI, AWS API

Organizations CLI/SDK를 사용하여 신뢰할 수 있는 서비스 액세스를 활성화하려면

다음 AWS CLI 명령 또는 API 작업을 사용하여 신뢰할 수 있는 서비스 액세스를 활성화할 수 있습니다.

- AWS CLI: [enable-aws-service-access](#)

다음 명령을 실행하면 Organizations와 상호 신뢰할 수 있는 서비스로 Reachability Analyzer를 활성화할 수 있습니다.

```
$ aws organizations enable-aws-service-access \
    --service-principal reachabilityanalyzer.networkinsights.amazonaws.com
```

이 명령은 성공 시 출력을 생성하지 않습니다.

- AWS API: [EnableAWSServiceAccess](#)

Reachability Analyzer를 통한 신뢰할 수 있는 액세스를 비활성화하려면

신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한에 관한 내용은 [신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한](#) 단원을 참조하세요.

Reachability Analyzer 콘솔(권장) 또는 Organizations 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화할 수 있습니다. Reachability Analyzer 콘솔을 사용하여 신뢰할 수 있는 액세스를 비활성화하려면 Reachability Analyzer 사용 설명서에서 [Reachability Analyzer의 계정 간 분석](#)을 참조하세요.

Reachability Analyzer에 대해 위임된 관리자 계정 활성화

위임된 관리자 계정은 조직 내의 모든 리소스에 대해 연결 분석을 실행할 수 있습니다. 자세한 내용은 Reachability Analyzer 사용 설명서에서 [Reachability Analyzer와 AWS Organizations통합](#)을 참조하세요.

조직 관리 계정의 관리자만 Reachability Analyzer에 대해 위임된 관리자를 구성할 수 있습니다.

Reachability Analyzer 콘솔에서 또는 RegisterDelegatedAdministrator API를 사용하여 위임된 관리자 계정을 지정할 수 있습니다. 자세한 내용은 Organizations 명령 참조에서 [RegisterDelegatedAdministrator](#)를 참조하세요.

최소 권한

Organizations 관리 계정의 사용자 또는 역할만 멤버 계정을 조직의 Reachability Analyzer에 대한 위임된 관리자로 구성할 수 있습니다

Reachability Analyzer 콘솔을 사용하여 위임된 관리자를 구성하려면 Reachability Analyzer 사용 설명서에서 [Reachability Analyzer와 AWS Organizations통합](#)을 참조하세요.

Reachability Analyzer에 대해 위임된 관리자 비활성화

조직 관리 계정의 관리자만 Reachability Analyzer에 대해 위임된 관리자를 구성할 수 있습니다.

Reachability Analyzer 콘솔이나 API에서 또는 Organizations DeregisterDelegatedAdministrator CLI 또는 SDK 작업을 사용하여 위임된 관리자를 제거할 수 있습니다.

Reachability Analyzer 콘솔을 사용하여 Reachability Analyzer의 위임된 관리자 계정을 비활성화하려면 Reachability Analyzer 사용 설명서에서 [Reachability Analyzer의 계정 간 분석](#)을 참조하세요.

Organizations에서 작업 AWS 서비스 하는의 위임된 관리자

AWS Organizations 관리 계정과 해당 사용자 및 역할은 해당 계정에서 수행해야 하는 작업에만 사용하는 것이 좋습니다. 또한 리소스는 조직의 AWS 다른 멤버 계정에 저장하고 관리 계정에서 제외하는

것이 좋습니다. 이는 Organizations 서비스 제어 정책(SCP)과 같은 보안 기능이 관리 계정의 사용자나 역할을 제한하지 않기 때문입니다. 관리 계정에서 리소스를 분리하면 인보이스의 요금을 파악하는 데도 도움이 될 수 있습니다.

Organizations와 통합 AWS 서비스 되는 많은를 사용하면 관리 계정의 사용량을 줄일 수 있습니다. 이러한 서비스를 통해 하나 이상의 멤버 계정을 관리자로 등록하여 서비스에 사용되는 모든 조직 계정을 관리하도록 할 수 있습니다. 이러한 계정을 해당 특정 서비스의 위임된 관리자라고 합니다. 멤버 계정을 AWS 서비스의 위임된 관리자로 등록하면 해당 계정은 해당 서비스에 대한 일부 관리 권한과 Organizations 읽기 전용 작업에 대한 권한을 가질 수 있습니다.

계정을 서비스의 위임된 관리자로 등록하기 전 다음 사항을 수행합니다.

- 서비스가 위임된 관리자를 지원하는지 확인합니다. 어떤 서비스가 위임된 관리자를 지원하지 않아 보려면 [AWS 서비스와 함께 사용할 수 있는 AWS Organizations](#)의 표를 참조하십시오.
- 해당 서비스에 대해 신뢰할 수 있는 액세스를 활성화합니다.

Note

서비스의 위임된 관리자를 활성화하는 방법을 알아보려면, [AWS 서비스와 함께 사용할 수 있는 AWS Organizations](#)의 표를 참조하여 해당 서비스에 대한 위임된 관리자 지원 열에서 자세히 알아보기 링크를 선택하십시오.

위임된 관리자 계정에 부여된 권한

각 서비스별 위임 관리자 계정에는 해당 서비스에서 부여하는 권한이 있습니다. 자세한 내용은 [AWS 서비스와 함께 사용할 수 있는 AWS Organizations](#)의 표를 참조하여 해당 서비스에 대한 위임된 관리자 지원 열에서 자세히 알아보기 링크를 선택하십시오.

위임된 관리자 계정에는 다음과 같은 읽기 전용 권한도 있습니다.

- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit

- DescribePolicy
- DescribeResourcePolicy
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy

이러한 권한을 사용하여 다음 콘솔 항목을 볼 수 있으며 변경할 수는 없습니다.

- Organizations 구조, 모든 계정 및 OU, 조직 정책
- 멤버십
- 모든 계정 및 OU.
- Organizations 정책

의 보안 AWS Organizations

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

보안은 AWS 와 사용자 간의 공동 책임입니다. [공동 책임 모델](#)은 이를 클라우드의 보안과 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 클라우드 AWS 서비스 에서 AWS 실행되는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 [AWS 규정 준수 프로그램](#)의 일환으로 보안 효과를 테스트하고 검증합니다. 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 [AWS 서비스 규정 준수 프로그램 제공 범위 섹션](#)을 AWS Organizations참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Organizations 사용 시 책임 분담 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Organizations를 구성하는 방법을 보여줍니다. 또한 Organizations 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스 또는 다른 방법을 사용합니다.

주제

- [AWS PrivateLink 용 AWS Organizations](#)
- [에 대한 자격 증명 및 액세스 관리 AWS Organizations](#)
- [에서 로깅 및 모니터링 AWS Organizations](#)
- [에 대한 규정 준수 검증 AWS Organizations](#)
- [의 복원력 AWS Organizations](#)
- [의 인프라 보안 AWS Organizations](#)

AWS PrivateLink 용 AWS Organizations

AWS PrivateLink 용 AWS Organizations를 사용하면 퍼블릭 인터넷을 통과하지 않고도 Virtual Private Cloud(VPC) 내에서 AWS Organizations 서비스에 액세스할 수 있습니다.

Amazon VPC를 사용하면 사용자 지정 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. VPC를 사용하여 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등의 네트워크 설정을 제어할 수 있습니다. VPC에 대한 자세한 내용은 [Amazon VPC 사용 설명서](#)를 참조하세요.

Amazon VPC를에 연결하려면 먼저 인터페이스 VPC 엔드포인트(인터페이스 엔드포인트)를 정의 AWS Organizations해야 합니다. 인터페이스 엔드포인트는 VPC의 서브넷에서 프라이빗 IP 주소가 할당된 하나 이상의 탄력적 네트워크 인터페이스(ENI)로 표시됩니다. VPC에서 AWS Organizations 경유 인터페이스 엔드포인트로의 요청은 Amazon 네트워크에 남아 있습니다.

인터페이스 엔드포인트에 대한 일반적인 내용은 Amazon [VPC 사용 설명서의 인터페이스 VPC 엔드포인트를 사용하여 AWS 서비스 액세스](#)를 참조하세요.

주제

- [에 AWS PrivateLink 대한의 제한 및 제약 AWS Organizations](#)
- [에 대한 VPC 엔드포인트 생성 AWS Organizations](#)
- [에 대한 VPC 엔드포인트 정책 생성 AWS Organizations](#)

에 AWS PrivateLink 대한의 제한 및 제약 AWS Organizations

에 AWS PrivateLink 대한 VPC 제한 사항이 적용됩니다 AWS Organizations. 자세한 내용은 Amazon [VPC 사용 설명서의 인터페이스 VPC 엔드포인트 및 할당량을 사용하여 AWS 서비스 액세스](#)를 참조하세요. [AWS PrivateLink](#) 또한 다음과 같은 제한 사항이 적용됩니다.

- us-east-1 리전에서만 사용 가능
- Transport Layer Security(TLS) 1.1을 지원하지 않음

에 대한 VPC 엔드포인트 생성 AWS Organizations

Amazon VPC 콘솔, AWS Command Line Interface (AWS CLI) 또는를 사용하여 VPC에서 AWS Organizations 엔드포인트를 생성할 수 있습니다 CloudFormation.

Amazon VPC 콘솔 또는를 사용하여 엔드포인트를 생성하고 구성하는 방법에 대한 자세한 내용은 Amazon [VPC 사용 설명서의 VPC 엔드포인트 생성](#)을 AWS CLI참조하세요. 를 사용하여 엔드포인트를 생성하고 구성하는 방법에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 [AWS::EC2::VPCEndpoint](#) 리소스를 CloudFormation참조하세요.

AWS Organizations 엔드포인트를 생성할 때 다음을 서비스 이름으로 사용합니다.

```
com.amazonaws.us-east-1.organizations
```

에 액세스할 때 FIPS 140-2 검증 암호화 모듈이 필요한 경우 다음 AWS Organizations FIPS 서비스 이름을 AWS사용합니다.

```
com.amazonaws.us-east-1.organizations-fips
```

에 대한 VPC 엔드포인트 정책 생성 AWS Organizations

Organizations에 대한 액세스를 제어하는 VPC 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 위탁자.
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스

자세한 내용은 Amazon VPC 사용자 가이드의 [엔드포인트 정책을 사용하여 VPC 엔드포인트로 액세스 제어](#)를 참조하세요.

예: AWS Organizations 작업에 대한 VPC 엔드포인트 정책

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "Organizations:DescribeAccount"
      ],
      "Resource": "*"
    }
  ]
}
```

에 대한 자격 증명 및 액세스 관리 AWS Organizations

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 AWS 서비스입니다. IAM 관리자는 어떤 사용자가 Organizations 리소스를 사용할 수 있도록 인증(로그인)되고 권한이 부여(권한 있음)될 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

- [대상](#)
- [ID를 통한 인증](#)
- [정책을 사용하여 액세스 관리](#)
- [AWS Organizations에서 IAM을 사용하는 방법](#)
- [를 사용하여 조직의 액세스 권한 관리 AWS Organizations](#)
- [에 대한 자격 증명 기반 정책 예제 AWS Organizations](#)
- [에 대한 리소스 기반 정책 예제 AWS Organizations](#)
- [AWS에 대한 관리형 정책 AWS Organizations](#)
- [에 대한 태그를 사용한 속성 기반 액세스 제어 AWS Organizations](#)
- [AWS Organizations 자격 증명 및 액세스 문제 해결](#)

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청([참조 AWS Organizations 자격 증명 및 액세스 문제 해결](#))
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출([AWS Organizations에서 IAM을 사용하는 방법 참조](#))
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성([에 대한 자격 증명 기반 정책 예제 AWS Organizations 참조](#))

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다.

로그인하는 방법에 대한 자세한 내용은 AWS Sign-In 사용 설명서의 [AWS 계정에 로그인하는 방법](#) 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해서는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 [API 요청용 AWS Signature Version 4](#) 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 [루트 사용자 자격 증명이 필요한 작업](#) 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 [What is IAM Identity Center?](#)를 참조하세요.

IAM 사용자 및 그룹

[IAM 사용자](#)는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명에 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여 액세스하도록 인간 사용자에게 요구](#)하기를 참조하세요.

[IAM 그룹](#)은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 [IAM 사용자 사용 사례](#) 섹션을 참조하세요.

IAM 역할

[IAM 역할](#)은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. [사용자에서 IAM 역할\(콘솔\)로 전환하거나 또는 API 작업을 호출하여 역할을](#) 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 [역할 수임 방법](#)을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 [교차 계정 리소스 액세스](#)를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다. 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 [JSON 정책 개요](#) 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 [고객 관리형 정책으로 사용자 지정 IAM 권한 정의](#)를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 [관리형 정책 및 인라인 정책 중에서 선택](#) 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다.

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

기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 [IAM 엔터티의 권한 범위](#)를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 [서비스 제어 정책](#)을 참조하세요.
- 리소스 제어 정책(RCP) - 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 [리소스 제어 정책\(RCP\)](#)을 참조하세요.
- 세션 정책 - 역할 또는 페더레이션 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 [세션 정책](#)을 참조하세요.

여러 정책 유형

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

AWS Organizations 에서 IAM을 사용하는 방법

IAM을 사용하여 Organizations에 대한 액세스를 관리하기 전에 Organizations와 함께 사용할 수 있는 IAM 기능을 알아보세요.

IAM 특성	Organizations 지원
자격 증명 기반 정책	예
리소스 기반 정책	예
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예

IAM 특성	Organizations 지원
ACL	아니요
ABAC(정책의 태그)	예
임시 보안 인증	아니요
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	예

Organizations 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 [AWS IAM으로 작업하는 서비스를](#) 참조하세요.

Organizations의 자격 증명 기반 정책

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. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 [IAM JSON 정책 요소 참조](#)를 참조하세요.

Organizations의 자격 증명 기반 정책 예

Organizations 자격 증명 기반 정책의 예를 보려면 [예 대한 자격 증명 기반 정책 예제 AWS Organizations](#)를 참조하세요.

Organizations 내 리소스 기반 정책

리소스 기반 정책 지원: 예

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 관리자

는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [IAM에서 교차 계정 리소스 액세스](#)를 참조하세요.

Organizations 서비스는 정책에 대한 작업을 수행할 수 있는 멤버 계정을 지정하는 리소스 기반 위임 정책이라고 하는 리소스 기반 정책 유형 하나만 지원합니다. 정책에 여러 명령문을 추가하여 멤버 계정마다 다양하게 구성된 권한을 부여할 수 있습니다.

자세한 내용은 [에 대한 위임된 관리자 AWS Organizations](#) 단원을 참조하십시오.

Organizations 내 리소스 기반 정책 예

Organizations 리소스 기반 정책의 예를 보려면 [에 대한 리소스 기반 정책 예제 AWS Organizations](#)를 참조하세요.

Organizations의 정책 작업

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

Organizations 작업 목록을 보려면 서비스 권한 부여 참조의 [AWS Organizations에서 정의한 작업](#)을 참조하세요.

Organizations의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
organizations
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

```
"Action": [
```

```
"organizations:action1",
"organizations:action2"
]
```

Organizations 자격 증명 기반 정책의 예를 보려면 [에 대한 자격 증명 기반 정책 예제 AWS Organizations](#)를 참조하세요.

Organizations의 정책 리소스

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 객체를 지정합니다. 모범 사례에 따라 [Amazon 리소스 이름\(ARN\)](#)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"

```

Organizations 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 권한 부여 참조의 [AWS Organizations에서 정의한 리소스](#)를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 [AWS Organizations에서 정의한 작업](#)을 참조하세요.

Organizations 자격 증명 기반 정책의 예를 보려면 [에 대한 자격 증명 기반 정책 예제 AWS Organizations](#)를 참조하세요.

Organizations의 정책 조건 키

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 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 [조건 연산자](#)를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 [AWS 전역 조건 컨텍스트 키](#)를 참조하세요.

Organizations 조건 키 목록을 보려면 서비스 권한 부여 참조의 [AWS Organizations의 조건 키](#)를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 [에서 정의한 작업을 AWS Organizations](#) 참조하세요.

Organizations 자격 증명 기반 정책의 예를 보려면 [에 대한 자격 증명 기반 정책 예제 AWS Organizations](#)를 참조하세요.

Organizations의 ACL

ACL 지원: 아니요

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.

Organizations를 사용한 ABAC

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 [조건 요소](#)에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 [ABAC 권한 부여를 통한 권한 정의](#)를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 [속성 기반 액세스 제어\(ABAC\) 사용](#)을 참조하세요.

Organizations에서 임시 자격 증명 사용

임시 자격 증명 지원: 아니요

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션을 사용하거나 역할을 전환할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이 AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 [IAM의 임시 보안 자격 증명](#) 및 [IAM으로 작업하는 AWS 서비스](#) 섹션을 참조하세요.

Organizations의 전달 액세스 세션

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은 호출하는 보안 주체의 권한을 다운스트림 서비스에 대한 요청 AWS 서비스 과 AWS 서비스 함께 사용합니다. FAS 요청 시 정책 세부 정보는 [전달 액세스 세션](#)을 참조하세요.

Organizations의 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 내용은 IAM 사용 설명서의 [AWS 서비스 AWS에 권한을 위임할 역할 생성](#)을 참조하세요.

Warning

서비스 역할에 대한 권한을 변경하면 Organizations 기능이 중단될 수 있습니다. Organizations 에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

Organizations의 서비스 연결 역할

서비스 연결 역할 지원: 예

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 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

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

를 사용하여 조직의 액세스 권한 관리 AWS Organizations

조직의 루트, OUs, 계정 및 정책을 포함한 모든 AWS 리소스는 소유 AWS 계정하며 리소스를 생성하거나 액세스할 수 있는 권한은 권한 정책에 의해 관리됩니다. 조직의 경우, 조직의 관리 계정이 모든 리소스를 소유합니다. 계정 관리자는 IAM 자격 증명(사용자, 그룹 및 역할)에 권한 정책을 연결하여 AWS 리소스에 대한 액세스를 제어할 수 있습니다.

Note

계정 관리자(또는 관리자 사용자)는 관리자 권한이 있는 사용자입니다. 자세한 내용은 AWS Account Management IAM 사용 설명서의 [IAM의 보안 모범 사례](#)를 참조하세요.

권한을 부여하려면 권한을 부여 받을 사용자, 권한 대상이 되는 리소스, 해당 리소스에 허용되는 특정 작업을 결정합니다.

기본적으로 IAM 사용자, 그룹 및 역할에는 어떠한 권한도 없습니다. 조직의 관리 계정에 속한 관리자는 관리 업무를 수행하거나 관리 계정의 다른 IAM 사용자나 역할에 관리 권한을 위임할 수 있습니다. 이렇게 하려면 IAM 권한 정책을 IAM 사용자, 그룹 또는 역할에 연결해야 합니다. 기본적으로 사용자는 어떤 권한도 가지지 않습니다. 이를 묵시적 거부라고 합니다. 이 정책은 사용자가 수행할 수 있는 작업과 사용자가 작업을 수행할 수 있는 리소스를 지정하는 명시적 허용으로 묵시적 거부를 무시합니다. 권한을 역할에 부여하면, 해당 역할은 조직 내 다른 계정 사용자가 맡을 수 있습니다.

AWS Organizations 리소스 및 작업

이 섹션에서는 AWS Organizations 개념이 IAM에 상응하는 개념에 매핑되는 방법을 설명합니다.

리소스

에서 다음 리소스에 대한 액세스를 제어할 AWS Organizations 수 있습니다.

- 조직의 계층적 구조를 구성하는 루트 및 OU
- 조직의 멤버가 되는 계정
- 조직 내 다음 개체에 연결하는 정책
- 조직 상태를 변경할 때 사용하는 핸드셰이크

각 리소스에는 관련된 고유 Amazon 리소스 이름(ARN)이 있습니다. IAM 권한 정책의 Resource 요소에 ARN을 지정하면 리소스에 대한 액세스를 제어할 수 있습니다. 에서 사용되는 리소스에 대한 ARN 형식의 전체 목록은 서비스 승인 AWS Organizations 참조의에서 [정의한 리소스 유형을 AWS Organizations](#) 참조하세요.

운영

AWS 는 조직의 리소스로 작업할 수 있는 일련의 작업을 제공합니다. 이를 통해 리소스 콘텐츠 생성, 나열, 수정, 액세스 및 리소스 삭제 같은 일을 할 수 있습니다. 대부분의 작업을 IAM 정책의 Action 요소에 참조해 해당 작업을 사용하는 사람을 제어할 수 있습니다. IAM 정책에서 권한으로 사용할 수 있는

AWS Organizations 작업 목록은 서비스 권한 부여 참조의 [Organizations에서 정의한 작업을](#) 참조하세요.

Action과 Resource를 단일 권한 정책 Statement로 결합하면, 특정 작업 모음을 사용할 수 있는 리소스를 정확하게 제어할 수 있습니다.

조건 키

AWS 는 특정 작업에 대한 보다 세분화된 제어를 제공하기 위해 쿼리할 수 있는 조건 키를 제공합니다. IAM 정책의 Condition 요소에서 이러한 조건 키를 참조하여 문을 일치로 간주하기 위해 충족해야 하는 추가적인 상황을 지정할 수 있습니다.

다음 조건 키는 특히 유용합니다 AWS Organizations.

- `aws:PrincipalOrgID` - 리소스 기반 정책의 Principal 요소 지정을 간소화합니다. 이 전역 키는 조직 내 모든 AWS 계정 의 계정 ID를 전부 나열하는 대안을 제공합니다. 조직의 멤버인 모든 계정을 나열하는 대신 Condition 요소에 [조직 ID](#)를 지정할 수 있습니다.

Note

이 전역 조건은 조직의 관리 계정에도 적용됩니다.

자세한 내용은 IAM 사용 설명서의 [AWS 전역 조건 컨텍스트 키](#)에서 `PrincipalOrgID`에 대한 설명을 참조하세요.

- `aws:PrincipalOrgPaths` - 이 조건 키를 사용하여 특정 조직 루트, OU 또는 해당 하위 항목의 멤버를 일치시킵니다. 요청을 수행하는 보안 주체(루트, IAM 사용자 또는 역할)가 지정된 조직 경로에 있는 경우 `aws:PrincipalOrgPaths` 조건 키는 `true`를 반환합니다. 경로는 AWS Organizations 개체 구조의 텍스트 표현입니다. 경로에 대한 자세한 내용은 IAM 사용 설명서의 [AWS Organizations 개체 경로 이해](#)를 참조하세요. 이 조건 키 사용에 대한 자세한 내용은 IAM 사용 설명서의 [aws:PrincipalOrgPaths](#)를 참조하세요.

예를 들어, 다음 조건 요소는 동일한 조직에 있는 두 OU 중 하나의 멤버에 대해 일치합니다.

```
"Condition": {
  "ForAnyValue:StringLike": {
    "aws:PrincipalOrgPaths": [
      "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbbb/",
      "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsdddddd/"
    ]
  }
}
```

```
}
}
```

- **organizations:PolicyType** – 이 조건 키를 사용하여 Organizations 정책 관련 API 작업이 특정 유형의 Organizations 정책에서만 동작하도록 제한할 수 있습니다. 이 조건 키는 Organizations 정책과 상호 작용하는 작업이 포함된 모든 정책 문에 적용할 수 있습니다.

이 조건 키에는 다음 값을 사용할 수 있습니다.

- SERVICE_CONTROL_POLICY
- RESOURCE_CONTROL_POLICY
- DECLARATIVE_POLICY_EC2
- BACKUP_POLICY
- TAG_POLICY
- CHATBOT_POLICY
- AISERVICES_OPT_OUT_POLICY

예를 들어 다음 예제 정책은 사용자가 모든 Organizations 작업을 수행할 수 있도록 허용합니다. 그러나 사용자가 정책을 인수하는 작업을 수행하는 경우 지정된 정책이 태그 지정 정책인 경우에만 작업이 허용됩니다. 사용자가 다른 유형의 정책을 지정하면 작업이 실패합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": [ "TAG_POLICY" ]
        }
      }
    }
  ]
}
```

- `organizations:ServicePrincipal` – [EnableAWSServiceAccess](#) 또는 [DisableAWSServiceAccess](#) 작업을 사용하여 다른 AWS 서비스와의 [신뢰할 수 있는 액세스](#)를 활성화하거나 비활성화하는 경우 조건으로 사용할 수 있습니다. `organizations:ServicePrincipal`을 사용하여 승인된 서비스 보안 주체 이름의 목록에 대하여 이런 작업 요청을 제한할 수 있습니다.

예를 들어 다음 정책은 신뢰할 수 있는 액세스를 활성화 및 비활성화할 AWS Firewall Manager 때만 사용자가를 지정하도록 허용합니다 AWS Organizations.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOnlyAWSFirewallIntegration",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
        }
      }
    }
  ]
}
```

IAM 정책에서 권한으로 사용할 수 있는 모든 AWS Organizations 특정 조건 키 목록은 서비스 권한 부여 참조의 [대한 조건 키를 AWS Organizations](#) 참조하세요.

리소스 소유권 이해

는 리소스를 생성한 사용자에게 관계없이 계정에서 생성된 리소스를 AWS 계정 소유합니다. 특히 리소스 소유자는 리소스 생성 요청을 인증하는 AWS 계정 [보안 주체 엔터티](#)(즉, 루트 사용자, IAM 사용자 또는 IAM 역할)의 입입니다. 조직의 경우 이는 언제나 관리 계정입니다. 멤버 계정에서 조직 리소스를 생성 또는 액세스하는 작업은 대부분 호출할 수 없습니다. 다음 예제에서는 이러한 작동 방법을 설명합니다.

- 관리 계정의 루트 계정 자격 증명을 사용하여 OU를 생성하는 경우, 관리 계정이 리소스 소유자가 됩니다. (에서 AWS Organizations 리소스는 OU입니다).
- 관리 계정에서 IAM 사용자를 만들고 사용자에 OU 생성 권한을 부여하면, 해당 사용자는 OU를 만들 수 있습니다. 하지만 사용자가 속한 관리 계정이 OU 리소스를 소유합니다.
- 관리 계정에서 OU를 생성할 권한이 있는 IAM 역할을 만드는 경우, 해당 역할을 담당할 수 있는 사람은 누구나 OU를 만들 수 있습니다. 역할(역할을 담당하는 사용자가 아님)이 속하게 될 관리 계정이 OU 리소스를 소유합니다.

리소스 액세스 관리

권한 정책은 누가 무엇에 액세스 할 수 있는지를 나타냅니다. 다음 섹션에서는 권한 정책을 만드는 데 사용 가능한 옵션에 대해 설명합니다.

Note

이 섹션에서는 컨텍스트에서 IAM을 사용하는 방법에 대해 설명합니다 AWS Organizations. IAM 서비스에 대한 자세한 내용은 다루지 않습니다. IAM 설명서 전체 내용은 [IAM 사용 설명서](#)를 참조하세요. IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 참조](#)를 참조하세요.

IAM ID에 연결된 정책을 ID 기반 정책(IAM 정책)이라고 합니다. 리소스에 연결된 정책을 리소스 기반 정책이라고 합니다.

주제

- [자격 증명 기반 권한 정책\(IAM 정책\)](#)

자격 증명 기반 권한 정책(IAM 정책)

IAM 자격 증명에 정책을 연결하여 해당 자격 증명이 AWS 리소스에 대한 작업을 수행하도록 허용할 수 있습니다. 예를 들면, 다음을 수행할 수 있습니다.

- 계정의 사용자 또는 그룹에 권한 정책 연결 - 사용자에게 [서비스 제어 정책\(SCP\)](#) 또는 OU와 같은 AWS Organizations 리소스를 생성할 수 있는 권한을 부여하려면 사용자 또는 사용자가 속한 그룹에 권한 정책을 연결할 수 있습니다. 사용자나 그룹은 조직의 관리 계정에 있어야 합니다.

- 역할에 권한 정책 연결(교차 계정 권한 부여) – 자격 증명 기반 권한 정책을 IAM 역할에 연결하여 조직에 대한 교차 계정 액세스를 부여할 수 있습니다. 예를 들어 관리 계정 관리자는 다음과 같이 멤버 계정 사용자에게 교차 계정 권한을 부여하는 역할을 만들 수 있습니다.
 1. 관리 계정 관리자는 IAM 역할을 생성하고 조직의 리소스에 권한을 부여하는 역할에 권한 정책을 연결합니다.
 2. 관리 계정 관리자는 멤버 계정 ID를 역할 수임 가능 Principal로 식별하는 역할에 신뢰 정책을 연결합니다.
 3. 이후 멤버 계정 관리자는 멤버 계정의 모든 사용자에게 역할을 맡는 권한을 위임할 수 있습니다. 이렇게 하면 멤버 계정 사용자는 관리 계정과 조직의 리소스를 생성하거나 리소스에 액세스할 수 있습니다. 역할을 수임할 권한을 AWS 서비스에 부여하려는 경우 신뢰 정책의 보안 주체가 AWS 서비스 보안 주체가 될 수도 있습니다.

IAM을 사용하여 권한을 위임하는 방법에 대한 자세한 내용은 IAM 사용자 안내서의 [액세스 관리](#)를 참조하세요.

다음은 사용자가 조직에서 CreateAccount 작업을 수행하도록 허용하는 정책의 예입니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt10rgPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:CreateAccount"
      ],
      "Resource": "*"
    }
  ]
}
```

정책의 Resource 요소에 리소스 유형을 가리키는 부분 ARN을 제공할 수도 있습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCreatingAccountsOnResource",
      "Effect": "Allow",
      "Action": "organizations:CreateAccount",
      "Resource": "arn:aws:organizations::*:account/*"
    }
  ]
}
```

또한 생성 중인 계정에 특정 태그를 포함하지 않는 계정의 생성을 거부할 수도 있습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreatingAccountsOnResourceBasedOnTag",
      "Effect": "Deny",
      "Action": "organizations:CreateAccount",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/key": "value"
        }
      }
    }
  ]
}
```

사용자, 그룹, 역할 및 권한에 대한 자세한 내용은 IAM 사용 설명서의 [자격 증명\(사용자, 그룹 및 역할\)](#)을 참조하세요.

정책 요소 지정: 작업, 조건, 효과, 리소스

각 AWS Organizations 리소스에 대해 서비스는 어떤 식으로든 해당 리소스와 상호 작용하거나 해당 리소스를 조작할 수 있는 일련의 API 작업 또는 작업을 정의합니다. 이러한 작업에 대한 권한을 부여하기 위해서는 정책에서 지정할 수 있는 일련의 작업을 AWS Organizations 정의합니다. 예를 들어 OU 리소스의 경우는 다음과 같은 작업을 AWS Organizations 정의합니다.

- AttachPolicy 및 DetachPolicy
- CreateOrganizationalUnit 및 DeleteOrganizationalUnit
- ListOrganizationalUnits 및 DescribeOrganizationalUnit

단 일부 인스턴스에서는 API 작업을 수행하려면 하나 이상의 작업에 대한 권한과, 하나 이상의 리소스에 대한 권한이 필요할 수도 있다는 점을 기억하세요.

다음은 IAM 권한 정책에서 사용할 수 있는 가장 기본적인 요소입니다.

- 작업(Action) – 이 키워드를 사용하여 허용 또는 거부할 작업을 식별합니다. 예를 들어 지정된에 따라 CreateAccount 작업을 수행할 수 있는 사용자 권한을 Effect organizations:CreateAccount 허용하거나 거부합니다 AWS Organizations . 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 작업](#)을 참조하세요.
- 리소스(Resource) – 이 키워드를 사용하여 정책 문을 적용할 리소스의 ARN을 지정합니다. 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 리소스](#)를 참조하세요.
- 조건(Condition) – 이 키워드를 사용하여 정책 문이 적용되기 위해 충족해야 하는 조건을 지정합니다. Condition은 일반적으로 정책이 일치하려면 충족해야 하는 추가 상황을 지정합니다. 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.
- 효과(Effect) – 이 키워드를 사용하여 정책 문이 리소스에 대한 작업을 허용 또는 거부할지를 지정합니다. 명시적으로 리소스에 대한 액세스 권한을 부여(또는 허용)하지 않는다면, 액세스는 암시적으로 거부됩니다. 사용자가 특정 리소스에 대한 특정 작업을 수행하지 못하게 하도록, 다른 정책이 부여한 액세스를 포함한 리소스에 대한 액세스를 명시적으로 거부할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 효과](#)를 참조하세요.
- 보안 주체(Principal) – 자격 증명 기반 정책(IAM 정책)에서, 해당 정책이 연결된 사용자는 자동으로 묵시적으로 보안 주체가 됩니다. 리소스 기반 정책의 경우, 사용자, 계정, 서비스 또는 권한의 수신자인 기타 엔터티를 지정합니다(리소스 기반 정책에만 해당).

IAM 정책 구문과 설명에 대해 자세히 알아보려면 IAM 사용 설명서의 [IAM JSON 정책 참조](#)를 참조하세요.

에 대한 자격 증명 기반 정책 예제 AWS Organizations

기본적으로 사용자 및 역할에는 Organizations 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성\(콘솔\)](#)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 Organizations에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 [AWS Organizations의 작업, 리소스 및 조건 키](#)를 참조하세요.

주제

- [정책 모범 사례](#)
- [Organizations 콘솔 사용](#)
- [사용자가 자신의 고유한 권한을 볼 수 있도록 허용](#)
- [사용자에게 전체 관리자 권한 부여](#)
- [작업에 따른 제한적 액세스 부여](#)
- [특정 리소스에 대한 액세스 권한 부여](#)
- [제한된 서비스 보안 주체에게 신뢰할 수 있는 액세스를 활성화할 수 있는 권한 부여](#)

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 Organizations 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 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 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 내용은 IAM 사용 설명서의 [AWS 관리형 정책](#) 또는 [AWS 직무에 대한 관리형 정책](#)을 참조하세요.
- 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. AWS 서비스와 같은 특징을 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 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 계정칩니다. API 작업을 직접적으로 호출할 때 MFA가 필요하다면 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.

Organizations 콘솔 사용

AWS Organizations 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 Organizations 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 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 API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 Organizations 콘솔을 계속 사용할 수 있도록 하려면 Organizations [AWSOrganizationsFullAccess](#) 또는 [AWSOrganizationsReadOnlyAccess](#) AWS 관리형 정책도 엔티티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 [사용자에게 권한 추가](#)를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

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

```

    "Statement": [
      {
        "Sid": "ViewOwnUserInfo",
        "Effect": "Allow",
        "Action": [
          "iam:GetUserPolicy",
          "iam:ListGroupsForUser",
          "iam:ListAttachedUserPolicies",
          "iam:ListUserPolicies",
          "iam:GetUser"
        ],
        "Resource": ["arn:aws:iam::*:user/${aws:username}"]
      },
      {
        "Sid": "NavigateInConsole",
        "Effect": "Allow",
        "Action": [
          "iam:GetGroupPolicy",
          "iam:GetPolicyVersion",
          "iam:GetPolicy",
          "iam:ListAttachedGroupPolicies",
          "iam:ListGroupPolicies",
          "iam:ListPolicyVersions",
          "iam:ListPolicies",
          "iam:ListUsers"
        ],
        "Resource": "*"
      }
    ]
  }
}

```

사용자에게 전체 관리자 권한 부여

조직의 IAM 사용자에게 전체 AWS Organizations 관리자 권한을 부여하는 IAM 정책을 생성할 수 있습니다. IAM 콘솔에서 JSON 정책 편집기를 사용하여 이 작업을 수행할 수 있습니다.

JSON 정책 편집기를 사용하여 정책을 생성하는 방법

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/iam/> IAM 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 정책을 선택합니다.

정책을 처음으로 선택하는 경우 관리형 정책 소개 페이지가 나타납니다. 시작을 선택합니다.

3. 페이지 상단에서 정책 생성을 선택합니다.
4. 정책 편집기 섹션에서 JSON 옵션을 선택합니다.
5. 다음 JSON 정책 문서를 입력합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "organizations:*",
    "Resource": "*"
  }
}
```

6. 다음을 선택합니다.

Note

언제든지 시각적 편집기 옵션과 JSON 편집기 옵션 간에 전환할 수 있습니다. 그러나 변경을 적용하거나 시각적 편집기에서 다음을 선택한 경우 IAM은 시각적 편집기에 최적화되도록 정책을 재구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [정책 재구성](#)을 참조하세요.

7. 검토 및 생성 페이지에서 생성하는 정책에 대한 정책 이름과 설명(선택 사항)을 입력합니다. 이 정책에 정의된 권한을 검토하여 정책이 부여한 권한을 확인합니다.
8. 정책 생성을 선택하고 새로운 정책을 저장합니다.

IAM 정책 생성에 대해 자세히 알아보려면 IAM 사용 설명서의 [IAM 정책 생성](#)을 참조하세요.

작업에 따른 제한적 액세스 부여

전체 권한이 아닌 제한적 권한을 부여하려면, IAM 권한 정책의 Action 요소에서 허용할 개별 권한을 나열하는 정책을 만들어야 합니다. 다음 예제와 같이 와일드카드(*) 문자를 사용해 Describe*와 List* 권한만 부여함으로써 조직에 읽기 전용 액세스를 제공할 수 있습니다.

Note

서비스 제어 정책(SCP)에서 Action 요소에 와일드카드(*) 문자를 단독으로 또는 문자열 끝에 사용할 수 있습니다. 문자열 처음이나 중간에는 표시할 수 없습니다.

따라서 "servicename:action*"은 유효하지만 "servicename:*action"과 "servicename:some*action"은 SCP에서 유효하지 않습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "organizations:Describe*",
      "organizations:List*"
    ],
    "Resource": "*"
  }
}
```

IAM 정책에서 할당할 수 있는 모든 권한 목록은 서비스 권한 부여 참조의 [AWS Organizations에서 정의한 작업을](#) 참조하세요.

특정 리소스에 대한 액세스 권한 부여

특정 작업에 대한 액세스를 제한하는 것 외에도 조직의 특정 엔터티에 대한 액세스를 제한할 수 있습니다. 이전 섹션 예제에 등장하는 Resource 요소는 모두 와일드카드 문자("*")를 지정하는데, 이는 "작업이 액세스할 수 있는 모든 리소스"라는 뜻입니다. "*"를 액세스를 허용할 특정 엔터티의 Amazon 리소스 이름(ARN)으로 바꿔도 됩니다.

예: 단일 OU에 권한 부여

다음 정책의 첫 번째 문은 IAM 사용자에게 전체 조직에 대한 읽기 전용 액세스 권한을 부여하지만, 두 번째 문은 사용자가 지정된 단일 조직 단위(OU) 내의 AWS Organizations 관리 작업만 수행할 수 있게 합니다. 이는 하위 OU로 확장되지 않습니다. 결제 액세스는 부여되지 않습니다. 이렇게 해도 OU의 AWS 계정에 대한 관리 액세스 권한이 부여되지는 않습니다. 지정된 OU 내의 계정에서 AWS Organizations 작업을 수행할 수 있는 권한만 부여합니다.

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "organizations:Describe*",
          "organizations:List*"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "arn:aws:organizations::123456789012:ou/o-
        <organizationId>/ou-<organizationalUnitId>"
      }
    ]
  }
}

```

AWS Organizations 콘솔에서 또는 List* APIs를 호출하여 OU 및 조직의 IDs를 가져옵니다. 이 정책을 적용하는 사용자나 그룹은 특정 OU에 직접적으로 포함된 모든 엔터티에서 모든 작업 ("organizations:*")을 수행할 수 있습니다. OU는 Amazon 리소스 이름(ARN)으로 식별합니다.

다양한 리소스의 ARN에 대한 자세한 내용은 서비스 권한 부여 참조의 [AWS Organizations에서 정의한 리소스 유형](#)을 참조하세요.

제한된 서비스 보안 주체에게 신뢰할 수 있는 액세스를 활성화할 수 있는 권한 부여 정책 문의 Condition 요소를 사용하여 정책 문이 일치하는 상황을 추가로 제한할 수 있습니다.

예: 지정된 하나의 서비스에 신뢰할 수 있는 액세스를 활성화하는 권한 부여

다음 문은 사용자가 지정한 서비스에 대해서만 신뢰할 수 있는 액세스를 활성화하도록 권한을 제한하는 방법을 보여 줍니다. 사용자가와 다른 서비스 보안 주체를 사용하여 API를 호출하려고 하면 AWS IAM Identity Center이 정책이 일치하지 않고 요청이 거부됩니다.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```

    {
      "Effect": "Allow",
      "Action": "organizations:EnableAWSServiceAccess",
      "Resource": "*",
      "Condition": {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    }
  ]
}

```

다양한 리소스의 ARN에 대한 자세한 내용은 서비스 권한 부여 참조의 [AWS Organizations에서 정의한 리소스 유형](#)을 참조하세요.

에 대한 리소스 기반 정책 예제 AWS Organizations

다음 코드 예제는 리소스 기반 위임 정책을 사용하는 방법을 보여줍니다. 자세한 내용은 [에 대한 위임된 관리자 AWS Organizations](#) 단원을 참조하십시오.

주제

- [예: 조직, OU, 계정 및 정책 보기](#)
- [예: 정책 생성, 읽기, 업데이트, 삭제](#)
- [예: 태그 지정 및 태그 해제 정책](#)
- [예: 단일 OU 또는 계정에 정책 연결](#)
- [예: 조직의 백업 정책을 관리하기 위한 통합 권한](#)

예: 조직, OU, 계정 및 정책 보기

정책 관리 작업을 위임하기 전에 먼저 조직 구조를 탐색하고, 조직 단위(OU)와 계정, 그리고 거기에 연결된 정책을 확인할 수 있는 권한을 위임해야 합니다.

이 예에서는 *AccountId*라는 멤버 계정에 대한 리소스 기반 위임 정책에 이 권한을 포함하는 방법을 보여줍니다.

⚠ Important

이 정책을 사용하면 어떠한 Organizations 읽기 전용 작업이든 위임할 수 있지만, 이 예에서 보듯이 최소한의 필수 작업에 대한 권한만 포함하는 것이 좋습니다.

이 위임 정책 예제는 AWS API 또는에서 프로그래밍 방식으로 작업을 완료하는 데 필요한 권한을 부여합니다 AWS CLI. 이 위임 정책을 사용하려면 *AccountId*의 AWS [자리 표시자 텍스트를](#) 자신의 정보로 바꿉니다. 그런 다음 [에 대한 위임된 관리자 AWS Organizations](#)의 지침을 따릅니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

}

예: 정책 생성, 읽기, 업데이트, 삭제

관리 계정이 모든 정책 유형에 대한 create, read, update, delete 작업을 위임할 수 있도록 허용하는 리소스 기반 위임 정책을 생성할 수 있습니다. 이 예에서는 서비스 제어 정책에 대한 이러한 작업을 멤버 계정인 *MemberAccountId*에 위임하는 방법을 보여줍니다. 예제에 표시된 두 리소스는 각각 고객 관리형 및 AWS 관리형 서비스 제어 정책에 대한 액세스 권한을 부여합니다.

Important

위임된 관리자는 이 정책을 통해 관리 계정을 비롯하여 조직의 모든 계정에서 생성한 정책에 대해 지정된 작업을 수행할 수 있습니다.

이 정책에는 organizations:AttachPolicy 및 organizations:DetachPolicy 작업을 수행하는 데 필요한 권한이 포함되어 있지 않으므로 위임된 관리자는 정책을 연결하거나 분리할 수 없습니다.

이 위임 정책 예제는 AWS API 또는에서 프로그래밍 방식으로 작업을 완료하는 데 필요한 권한을 부여합니다 AWS CLI. *MemberAccountId*, *ManagementAccountId* 및 *OrganizationId*의 AWS 자리 표시자 텍스트를 자신의 정보로 바꿉니다. 그런 다음 [에 대한 위임된 관리자 AWS Organizations](#)의 지침을 따릅니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingDescribeListActionsWithoutCondition",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",

```



```

        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListTagsForResource"
    ],
    "Resource": "*"
},
{
    "Sid": "DelegatingPolicyActionsWithCondition",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy"
    ],
    "Resource": "*",
    "Condition": {
        "StringLikeIfExists": {
            "organizations:PolicyType": "SERVICE_CONTROL_POLICY"
        }
    }
},
{
    "Sid": "DelegatingMinimalActionsForSCPs",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "organizations:CreatePolicy",
        "organizations:DescribePolicy",
        "organizations:UpdatePolicy",
        "organizations>DeletePolicy"
    ],
    "Resource": [
        "arn:aws:organizations::111122223333:policy/o-OrganizationId/service_control_policy/*",

```

```

        "arn:aws:organizations::aws:policy/service_control_policy/*"
    ]
}
]
}

```

예: 태그 지정 및 태그 해제 정책

이 예에서는 위임된 관리자가 백업 정책에 태그를 지정하거나 태그를 해제할 수 있도록 허용하는 리소스 기반 위임 정책을 생성하는 방법을 보여줍니다. API AWS 또는에서 프로그래밍 방식으로 작업을 완료하는 데 필요한 권한을 부여합니다 AWS CLI.

이 위임 정책을 사용하려면 *MemberAccountId*, *ManagementAccountId*, *OrganizationId*의 AWS 자리 표시자 텍스트를 사용자의 실제 정보로 바꿉니다. 그런 다음 [예 대한 위임된 관리자 AWS Organizations](#)의 지침을 따릅니다.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActionsWithoutCondition",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    },
  ],
}

```

```

{
  "Sid": "DelegatingNecessaryDescribeListActionsWithCondition",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": [
    "organizations:DescribePolicy",
    "organizations:DescribeEffectivePolicy",
    "organizations:ListPolicies",
    "organizations:ListPoliciesForTarget",
    "organizations:ListTargetsForPolicy"
  ],
  "Resource": "*",
  "Condition": {
    "StringLikeIfExists": {
      "organizations:PolicyType": "BACKUP_POLICY"
    }
  }
},
{
  "Sid": "DelegatingTaggingBackupPolicies",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": [
    "organizations:TagResource",
    "organizations:UntagResource"
  ],
  "Resource": "arn:aws:organizations::111122223333:policy/
o-OrganizationId/backup_policy/*"
}
]
}

```

예: 단일 OU 또는 계정에 정책 연결

이 예에서는 위임된 관리자가 지정된 조직 단위(OU) 또는 지정된 계정에서 Organizations 정책을 attach 또는 detach할 수 있도록 허용하는 리소스 기반 위임 정책을 생성하는 방법을 보여줍니다. 이러한 작업을 위임하기 전에 조직의 구조를 탐색하고 조직에 있는 계정을 볼 수 있는 권한을 위임해야 합니다. 자세한 내용은 [예: 조직, OU, 계정 및 정책 보기](#) 섹션을 참조하세요.

⚠ Important

- 이 정책은 지정된 OU 또는 계정에서 정책을 연결하거나 분리하도록 허용하지만 하위 OU 및 하위 OU에 있는 계정은 제외됩니다.
- 위임된 관리자는 이 정책을 통해, 관리 계정을 비롯하여 조직의 모든 계정에서 생성한 정책에 대해 지정된 작업을 수행할 수 있습니다.

이 위임 정책 예제는 AWS API 또는에서 프로그래밍 방식으로 작업을 완료하는 데 필요한 권한을 부여합니다 AWS CLI. 이 위임 정책을 사용하려면 *MemberAccountId*, *ManagementAccountId*, *OrganizationId* 및 *TargetAccountId*의 AWS 자리 표시자 텍스트를 사용자의 실제 정보로 바꿉니다. 그런 다음 [예 대한 위임된 관리자 AWS Organizations](#)의 지침을 따릅니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "AttachDetachPoliciesSpecifiedAccountOU",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
      "organizations:AttachPolicy",
      "organizations:DetachPolicy"
    ],
    "Resource": [
      "arn:aws:organizations::111122223333:ou/o-OrganizationId/ou-OUId",
      "arn:aws:organizations::111122223333:account/o-OrganizationId/TargetAccountId",
      "arn:aws:organizations::111122223333:policy/o-OrganizationId/backup_policy/*"
    ]
  }
]
}

```

OU 또는 조직의 계정에 정책 연결 및 분리를 위임하려면 이전 예의 리소스를 다음 리소스로 바꿉니다.

```

"Resource": [
  "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
  "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
  "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/backup_policy/*"
]

```

예: 조직의 백업 정책을 관리하기 위한 통합 권한

이 예에서는 create, read, update, delete 작업 권한 등 조직 내에서 백업 정책을 관리하는 데 필요한 모든 권한과 attach 및 detach 정책 작업 권한을 관리 계정에서 위임할 수 있도록 하는 리소스 기반 위임 정책을 생성하는 방법을 보여줍니다.

⚠ Important

위임된 관리자는 이 정책을 통해, 관리 계정을 비롯하여 조직의 모든 계정에서 생성한 정책에 대해 지정된 작업을 수행할 수 있습니다.

이 위임 정책 예제는 AWS API 또는에서 프로그래밍 방식으로 작업을 완료하는 데 필요한 권한을 부여합니다 AWS CLI. 이 위임 정책을 사용하려면 *MemberAccountId*, *ManagementAccountId*, *OrganizationId* 및 *RootId*의 AWS [자리 표시자 텍스트](#)를 사용자의 실제 정보로 바꿉니다. 그런 다음 [에 대한 위임된 관리자 AWS Organizations](#)의 지침을 따릅니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<111122223333:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DelegatingNecessaryDescribeListActionsForSpecificPolicyType",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<111122223333:root"
      },
      "Action": [
        "organizations:DescribePolicy",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForParent",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    },
    "Action": [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy"
    ],
    "Resource": "*",
    "Condition": {
        "StringLikeIfExists": {
            "organizations:PolicyType": "BACKUP_POLICY"
        }
    }
},
{
    "Sid": "DelegatingAllActionsForBackupPolicies",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations>DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
    ],
    "Resource": [
        "arn:aws:organizations::111122223333:root/o-OrganizationId/
r-RootId",
        "arn:aws:organizations::111122223333:ou/o-OrganizationId/*",
        "arn:aws:organizations::111122223333:account/o-OrganizationId/*",
        "arn:aws:organizations::111122223333:policy/o-OrganizationId/
backup_policy/*"
    ],
    "Condition": {
        "StringLikeIfExists": {
            "organizations:PolicyType": "BACKUP_POLICY"
        }
    }
}
}

```

```

    ]
  }

```

AWS 에 대한 관리형 정책 AWS Organizations

이 섹션에서는 조직을 관리하는 데 사용할 수 있도록 제공되는 AWS관리형 정책을 설명합니다. AWS 관리형 정책은 수정하거나 삭제할 수 없지만 필요에 따라 조직의 엔터티에 연결하거나 분리할 수 있습니다.

AWS Organizations 와 함께 사용할 관리형 정책 AWS Identity and Access Management (IAM)

IAM 관리형 정책은 AWS에서 제공하고 관리합니다. 관리형 정책은 관리형 정책을 적절한 IAM 사용자 또는 역할 객체에 연결하여 사용자에게 할당할 수 있는 일반 작업에 대한 권한을 제공합니다. 정책을 직접 작성할 필요가 없으며,가 새 서비스를 지원하기 위해 정책을 적절하게 AWS 업데이트하면 자동으로 즉시 업데이트의 이점을 얻을 수 있습니다.

AWS 관리형 정책 목록은 IAM 콘솔의 [정책\(Policies\)](#) 페이지에서 볼 수 있습니다. 정책 필터 드롭다운을 사용해 AWS 관리형을 선택합니다.

다음의 관리형 정책을 사용하여 조직의 사용자에게 권한을 부여할 수 있습니다.

AWS 관리형 정책: `AWSOrganizationsFullAccess`

조직을 생성하고 완전히 관리하는 데 필요한 모든 권한을 제공합니다.

정책 보기: [AWSOrganizationsFullAccess](#).

AWS 관리형 정책: `AWSOrganizationsReadOnlyAccess`

조직 관련 정보에 대한 읽기 전용 액세스를 제공합니다. 사용자가 변경할 수 없습니다.

정책 보기: [AWSOrganizationsReadOnlyAccess](#).

AWS 관리형 정책: `DeclarativePoliciesEC2Report`

이 정책은 [AWSServiceRoleForDeclarativePoliciesEC2Report](#) 서비스 연결 역할에서 멤버 계정의 계정 속성 상태를 설명할 수 있도록 하는 데 사용됩니다.

정책 보기: [DeclarativePoliciesEC2Report](#).

Organizations AWS 관리형 정책 업데이트

다음 표에는이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 AWS 관리형 정책에 대한 업데이트가 자세히 나와 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 [문서 기록](#) 페이지에서 RSS 피드를 구독하세요.

변경	설명	Date
AWSOrganizationsFullAccess – Organizations 콘솔을 통해 계정 이름을 조회하거나 수정하는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	조직 내 계정의 계정 이름을 볼 수 있는 액세스 권한을 활성화하는 <code>account:GetAccountInformation</code> 작업과 조직의 계정 이름을 수정할 수 있는 액세스 권한을 활성화하는 <code>account:PutAccountName</code> 작업이 추가되었습니다.	2025년 4월 22일
DeclarativePoliciesEC2Report – 새로운 관리형 정책	<code>AWSServiceRoleForDeclarativePoliciesEC2Report</code> 서비스 연결 역할의 기능을 활성화하는 <code>DeclarativePoliciesEC2Report</code> 정책을 추가했습니다.	2024년 11월 22일
AWSOrganizationsReadOnlyAccess – 루트 사용자 이메일 주소를 보는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	조직 내 모든 멤버 계정의 루트 사용자 이메일 주소를 조회할 수 있는 권한을 부여하는 <code>account:GetPrimaryEmail</code> 작업을 추가했습니다. 또한 조직 내 모든 멤버 계정의 활성화된 리전을 조회할 수 있는 권한을 부여하는 <code>account:GetRegionOptStatus</code> 작업을 추가했습니다.	2024년 6월 6일
AWSOrganizationsFullAccess -정책 문을 설명하는 Sid 요소를 포함하도록 업데이트되었습니다.	<code>AWSOrganizationsFullAccess</code> 관리형 정책에 대한 Sid 요소가 추가되었습니다.	2024년 2월 6일

변경	설명	Date
AWSOrganizationsReadOnlyAccess - 정책 문을 설명하는 Sid 요소를 포함하도록 업데이트되었습니다.	AWSOrganizationsReadOnlyAccess 관리형 정책에 대한 Sid 요소가 추가되었습니다.	2024년 2월 6일
AWSOrganizationsFullAccess - Organizations 콘솔을 통해 AWS 리전을 활성화하거나 비활성화하는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정에 대해 리전을 활성화하거나 비활성화하기 위한 쓰기 액세스를 활성화할 수 있도록 해당 정책에 account:ListRegions , account:EnableRegion 및 account:DisableRegion 작업이 추가되었습니다.	2022년 12월 22일
AWSOrganizationsReadOnlyAccess - Organizations 콘솔을 AWS 리전 통해 나열하는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정의 리전을 보기 위한 액세스를 활성화할 수 있도록 해당 정책에 account:ListRegions 작업이 추가되었습니다.	2022년 12월 22일
AWSOrganizationsFullAccess - Organizations 콘솔을 통해 계정 연락처를 추가 또는 편집하는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정의 연락처를 수정하기 위한 쓰기 액세스를 활성화할 수 있도록 해당 정책에 account:GetContactInformation 및 account:PutContactInformation 작업이 추가되었습니다.	2022년 10월 21일
AWSOrganizationsReadOnlyAccess - Organizations 콘솔을 통해 대체 연락처를 보는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정의 연락처를 보기 위한 액세스를 활성화할 수 있도록 해당 정책에 account:GetContactInformation 작업이 추가되었습니다.	2022년 10월 21일

변경	설명	Date
AWSOrganizationsFullAccess – 조직을 생성할 수 있도록 업데이트되었습니다.	조직을 생성하는 데 필요한 서비스 연결 역할 생성을 지원하기 위해 CreateServiceLinkedRole 권한을 해당 정책에 추가했습니다. 이 권한은 organizations.amazonaws.com 서비스에서만 사용할 수 있는 역할을 생성하는 것으로 제한됩니다.	2022년 8월 24일
AWSOrganizationsFullAccess – Organizations 콘솔을 통해 계정 대체 연락처를 추가, 편집 또는 삭제하는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정의 대체 연락처를 수정하기 위한 쓰기 액세스를 활성화할 수 있도록 해당 정책에 account:GetAlternateContact , account:DeleteAlternateContact , account:PutAlternateContact 작업이 추가되었습니다.	2022년 2월 7일
AWSOrganizationsReadOnlyAccess – Organizations 콘솔을 통해 계정 대체 연락처를 보는 데 필요한 계정 API 권한을 허용하도록 업데이트되었습니다.	계정의 대체 연락처를 보기 위한 액세스를 활성화할 수 있도록 해당 정책에 account:GetAlternateContact 작업이 추가되었습니다.	2022년 2월 7일

AWS 관리형 권한 부여 정책

[권한 부여 정책](#)은 IAM 권한 정책과 유사하지만 IAM AWS Organizations 이 아닌의 기능입니다. 권한 부여 정책을 사용하여 멤버 계정의 위탁자 및 리소스에 대한 액세스를 중앙에서 구성하고 관리합니다.

Organizations 콘솔의 [정책\(Policies\)](#) 페이지에서 조직의 정책 목록을 확인할 수 있습니다.

정책 이름	설명	ARN
FullAWSAccess	모든 작업에 대한 액세스를 허용합니다.	arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess
RCPPFullAWSAccess	모든 리소스에 대한 액세스를 허용합니다.	arn:aws:organizations::aws:policy/resource_control_policy/p-RCPFullAWSAccess

에 대한 태그를 사용한 속성 기반 액세스 제어 AWS Organizations

[속성 기반 액세스 제어](#)를 사용하면 AWS 리소스 및 AWS 자격 증명 모두에 연결된 [태그](#)와 같은 관리자 관리형 속성을 사용하여 해당 리소스에 대한 액세스를 제어할 수 있습니다. 예를 들어 사용자와 리소스 모두 특정 태그에 대해 동일한 값을 가질 때 사용자가 리소스에 액세스할 수 있도록 지정할 수 있습니다.

AWS Organizations 태그 지정 가능한 리소스에는 조직의 루트 AWS 계정, 조직 단위(OUs, Organizations 리소스에 태그를 연결하면 해당 태그를 사용하여 해당 리소스에 액세스할 수 있는 사용자를 제어할 수 있습니다. 작업을 허용하기 전에 특정 태그 키와 값이 있는지 확인하는 Condition 요소를 AWS Identity and Access Management (IAM) 권한 정책 문에 추가하면 됩니다. 이렇게 하면 "키 X와 값 Y를 가진 태그가 있는 OU만 사용자가 관리하도록 허용" 또는 "키 Z로 태그 지정되고 사용자의 연결된 태그 키 Z와 동일한 값을 갖는 OU만 사용자가 관리하도록 허용"이라고 효과적으로 언급하는 IAM 정책을 생성할 수 있습니다.

관리자는 IAM 정책의 다양한 태그 참조 유형을 Condition 테스트할 수 있습니다.

- [요청에 지정된 리소스에 연결된 태그 확인](#)
- [요청을 수행하는 IAM 사용자 또는 역할에 연결된 태그 확인](#)
- [요청에 파라미터로 포함된 태그 확인](#)

정책에서 액세스 제어를 위해 태그를 사용하는 방법에 대한 자세한 내용은 [리소스 태그를 사용하여 IAM 사용자 및 역할에 대한 액세스 제어](#)를 참조하세요. IAM 권한 정책의 전체 구문은 [IAM JSON 정책 참조](#)를 참조하세요.

요청에 지정된 리소스에 연결된 태그 확인

AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS SDKs 중 하나를 사용하여 요청할 때 해당 요청으로 액세스할 리소스를 지정합니다. 사용 가능한 특정 유형의 리소스를 나열하거나, 리소스를 읽거나, 쓰거나, 수정하거나, 업데이트할 때 액세스할 리소스를 요청에 파라미터로 지정합니다. 이러한 요청은 사용자 및 역할에 연결한 IAM 권한 정책에 의해 제어됩니다. 이러한 정책에서, 요청된 리소스에 연결된 태그를 비교하고 해당 태그의 키와 값에 따라 액세스를 허용하거나 거부하도록 선택할 수 있습니다.

리소스에 연결된 태그를 확인하려면 태그 키 이름 앞에 `aws:ResourceTag/` 문자열을 추가하여 Condition 요소의 태그를 참조합니다.

예를 들어 다음 정책 샘플은 해당 리소스에 키 `department`와 값 `security`를 가진 태그가 없는 한 사용자 또는 역할이 모든 AWS Organizations 작업을 수행하도록 허용합니다. 해당 키와 값이 있는 경우 정책은 `UntagResource` 작업을 명시적으로 거부합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "organizations:UntagResource",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "security"
        }
      }
    }
  ]
}
```

이 요소를 사용하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [리소스에 대한 액세스 제어](#) 및 [aws:ResourceTag](#)를 참조하세요.

요청을 수행하는 IAM 사용자 또는 역할에 연결된 태그 확인

요청을 하는 사람(보안 주체)이 자신의 IAM 사용자 또는 역할에 연결된 태그를 기반으로 수행할 수 있는 대상을 제어할 수 있습니다. 이렇게 하려면 `aws:PrincipalTag/key-name` 조건 키를 사용하여 호출하는 사용자 또는 역할에 연결해야 할 태그와 값을 지정합니다.

다음 예제는 작업을 호출하는 보안 주체와 작업이 액세스하는 리소스 모두에 대해 지정된 태그(cost-center)가 동일한 값을 갖는 경우에만 작업을 허용하는 방법을 보여줍니다. 이 예제에서 호출하는 사용자는 인스턴스에 사용자와 동일한 cost-center 값으로 태그가 지정된 경우에만 Amazon EC2 인스턴스를 시작하고 중지할 수 있습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "ec2:startInstances",
      "ec2:stopInstances"
    ],
    "Resource": "*",
    "Condition": { "StringEquals": {
      "ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"
    } }
  }
}
```

이 요소를 사용하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [IAM 보안 주체에 대한 액세스 제어](#) 및 [aws:PrincipalTag](#)를 참조하세요.

요청에 파라미터로 포함된 태그 확인

몇 가지 작업을 통해 태그를 요청의 일부로 지정할 수 있습니다. 예를 들어 리소스를 만들 때 새 리소스에 연결되는 태그를 지정할 수 있습니다. `aws:TagKeys`를 사용하여 특정 태그 키 또는 키 집합이 요청에 포함되는지 여부에 따라 작업을 허용하거나 거부하는 Condition 요소를 지정할 수 있습니다. 이 비교 연산자는 태그에 포함된 값을 고려하지 않습니다. 지정된 키를 가진 태그가 있는지 여부만 확인합니다.

태그 키 또는 키 목록을 확인하려면 Condition 요소를 다음과 같은 구문으로 지정합니다.

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

[ForAllValues](#):를 사용하면 비교 연산자를 앞에 삽입하여 요청의 모든 키가 정책에 지정된 키 중 하나와 일치하도록 할 수 있습니다. 예를 들어 다음 샘플 정책은 요청에 있는 모든 태그가 이 정책의 태그 세 개의 하위 집합인 경우에만 Organizations 작업을 허용합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "organizations:*",
    "Resource": "*",
    "Condition": {
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "department",
          "costcenter",
          "manager"
        ]
      }
    }
  }
}
```

또는 [ForAnyValue](#):를 사용해 비교 연산자를 앞에 삽입하여 요청의 하나 이상의 키가 정책에 지정된 키 중 하나와 일치하도록 할 수 있습니다. 예를 들어, 다음 정책은 지정된 태그 키 중 하나 이상이 요청에 존재하는 경우에만 Organizations 작업을 허용합니다.

JSON

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

```

    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "stage",
                "us-east-1",
                "domain"
            ]
        }
    }
}

```

몇 가지 작업을 통해 요청에 태그를 지정할 수 있습니다. 예를 들어 리소스를 만들 때 새 리소스에 연결되는 태그를 지정할 수 있습니다. 정책의 태그 키-값 페어를 요청에 함께 포함된 키-값 페어와 비교할 수 있습니다. 이렇게 하려면 태그 키 이름 앞에 문자열(`aws:RequestTag/key-name`)을 삽입하고 존재해야 하는 태그 값을 지정하여 Condition 요소의 태그를 참조합니다.

예를 들어 다음 샘플 정책은 사용자 또는 역할이 태그가 누락된 AWS 계정 요청을 생성하거나 해당 태그에 1, costcenter 또는 이외의 값을 제공하는 요청을 거부합니다²³.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "organizations:CreateAccount",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/costcenter": "true"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "organizations:CreateAccount",
      "Resource": "*",
      "Condition": {

```



```

    "ForAnyValue:StringNotEquals": {
      "aws:RequestTag/costcenter": [
        "1",
        "2",
        "3"
      ]
    }
  }
}

```

이러한 요소를 사용하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [aws:TagKeys](#) 및 [aws:RequestTag](#)를 참조하세요.

AWS Organizations 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Organizations 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

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

Organizations에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

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

```

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

```

이 경우, organizations:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Organizations에 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 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예시 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 Organizations에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

이 경우, Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 Organizations 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 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- Organizations가 이러한 기능을 지원하는지 여부를 알아보려면 [AWS Organizations에서 IAM을 사용하는 방법](#)을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 [IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요](#).
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [타사가 AWS 계정 소유한에 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.

에서 로깅 및 모니터링 AWS Organizations

조직에서 변경 사항이 기록되고 있는지 모니터링하는 것이 좋습니다. 이를 통해 예기치 않은 변경 사항을 조사하고 원치 않는 변경 사항을 롤백할 수 있습니다. AWS Organizations 현재 조직과 조직 내에서 발생하는 활동을 모니터링할 수 AWS 서비스 있는 두 가지를 지원합니다.

주제

- [AWS CloudTrail 용를 사용하여 API 호출 로깅 AWS Organizations](#)
- [Amazon EventBridge 및 AWS Organizations](#)

AWS CloudTrail 용를 사용하여 API 호출 로깅 AWS Organizations

AWS Organizations 는 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다 AWS Organizations. CloudTrail은 AWS Organizations 콘솔의 호출 및 API에 대한 코드 호출을 포함하여에 대한 모든 API 호출을 이벤트 AWS Organizations 로 캡처합니다. AWS Organizations APIs 추적을 생성하면 이벤트를 포함하여 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다 AWS Organizations. 추적을 구성하지 않은 경우에도 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 수행된 요청, 수행된 AWS Organizations IP 주소, 수행된 사람, 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

Important

미국 동부(버지니아 북부) 리전 AWS Organizations 에서만에 대한 모든 CloudTrail 정보를 볼 수 있습니다. CloudTrail 콘솔에 AWS Organizations 활동이 표시되지 않으면 오른쪽 상단의 메뉴를 사용하여 콘솔을 미국 동부(버지니아 북부)로 설정합니다. AWS CLI 또는 SDK 도구를 사용하여 CloudTrail을 쿼리하는 경우 쿼리를 미국 동부(버지니아 북부) 엔드포인트로 전달합니다.

AWS Organizations CloudTrail의 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. 활동이 발생하면 AWS Organizations 해당 활동은 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 설명은 [CloudTrail 이벤트 기록으로 이벤트 보기](#)를 참조하세요.

AWS Organizations에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 에서 CloudTrail 로깅이 활성화되면 AWS Organizations 작업에 대한 AWS 계정 API 호출이 CloudTrail 로그 파일에서 추적되며, 여기에서 다른 AWS 서비스 레코드와 함께 기록됩니다. CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취 AWS 서비스 하도록 다른를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- [추적 생성 개요](#)
- [CloudTrail 지원 서비스 및 통합](#)
- [CloudTrail에서 Amazon SNS 알림 구성](#)

모든 AWS Organizations 작업은 CloudTrail에서 로깅되며 [AWS Organizations API 참조](#)에 문서화됩니다. 예를 들어 CreateAccount(CreateAccountResult 이벤트 포함), ListHandshakesForAccount, CreatePolicy, InviteAccountToOrganization을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 로그 항목은 누가 요청을 생성했는가에 대한 정보가 들어 있습니다. 로그 항목의 사용자 신원 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트 사용자로 했는지 IAM 사용자 자격 증명으로 했는지 여부
- [IAM 역할](#) 또는 [연합된 사용자](#)용 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 요청이 다른 AWS 서비스에서 이루어졌는지 여부

자세한 설명은 [CloudTrail userIdentity 요소](#)를 참조하세요.

Note

CloudTrail은 지정된 작업을 수행하는 계정(즉, 멤버 계정이 작업을 수행한 경우 관리 계정이 아닌 멤버 계정)의 이벤트를 로깅합니다. 예를 들어 조직을 떠나는 멤버 계정은 멤버 계정 추적에 로그인되고 멤버 계정을 제거하는 관리 계정은 관리 계정 추적에 로그인됩니다.

AWS Organizations 로그 파일 항목 이해

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

로그 항목 예: CloseAccount

다음 예제는 API가 호출되고 계정을 생성하기 위한 워크플로가 백그라운드에서 처리를 시작할 때 해지되는 CloseAccount 호출 샘플에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
    "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/my-admin-role",
        "accountId": "111122223333",
        "userName": "my-session-id"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2022-03-18T18:17:06Z"
      }
    }
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccount",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
  "requestParameters": {
    "accountId": "555555555555"
  }
}
```

```

    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  }
}

```

다음 예제는 계정 해지를 위한 백그라운드 워크플로가 성공적으로 완료된 후 `CloseAccountResult` 호출에 대한 CloudTrail 로그 항목을 보여줍니다.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
  }
},

```

```

    "eventCategory": "Management"
  }

```

로그 항목 예: CreateAccount

다음 예제는 API가 호출되고 계정을 생성하기 위한 워크플로가 백그라운드에서 처리를 시작할 때 생성되는 CreateAccount 호출 샘플의 CloudTrail 로그 항목을 보여 줍니다.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
    "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/my-admin-role",
        "accountId": "111122223333",
        "userName": "my-session-id"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-09-16T21:16:45Z"
      }
    }
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccount",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
  "requestParameters": {
    "tags": [],
    "email": "*****",
    "accountName": "*****"
  },
  "responseElements": {

```

```

    "createAccountStatus": {
      "accountName": "*****",
      "state": "IN_PROGRESS",
      "id": "car-examplecreateaccountrequestid111",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
    }
  },
  "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}

```

다음 예제는 계정 생성을 위한 백그라운드 워크플로가 성공적으로 완료된 후 CreateAccount 호출의 CloudTrail 로그 항목을 보여줍니다.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "*****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}

```



```
}
}
```

다음 예제는 계정 생성을 위한 백그라운드 워크플로가 성공적으로 완료된 후 CreateAccount 호출의 CloudTrail 로그 항목을 보여 줍니다.

```
{
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "*****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": "Jun 21, 2018 10:06:27 PM",
      "completedTimestamp": "Jun 21, 2018 10:07:15 PM"
    }
  }
}
```

로그 항목의 예: CreateOrganizationalUnit

다음 예제에서는 샘플 CreateOrganizationalUnit 호출의 CloudTrail 로그 항목을 보여 줍니다.

```
{
  "eventVersion": "1.05",
```

```

    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAMVNPBQA3EXAMPLE",
      "arn": "arn:aws:iam::111111111111:user/diego",
      "accountId": "111111111111",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
      "name": "OU-Developers-1",
      "parentId": "r-a1b2"
    },
    "responseElements": {
      "organizationalUnit": {
        "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-examplerootid111-exampleouid111",
        "id": "ou-examplerootid111-exampleouid111",
        "name": "test-cloud-trail",
        "path": "o-aa111bb222/r-a1b2/ou-examplerootid111-exampleouid111/"
      }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
  }
}

```

로그 항목의 예: InviteAccountToOrganization

다음 예제에서는 샘플 InviteAccountToOrganization 호출의 CloudTrail 로그 항목을 보여 줍니다.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",

```

```

    "principalId": "AIDAMVNPBQA3EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/diego",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "diego"
  },
  "eventTime": "2017-01-18T21:41:17Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "InviteAccountToOrganization",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
  "requestParameters": {
    "notes": "This is a request for Mary's account to join Diego's organization.",
    "target": {
      "type": "ACCOUNT",
      "id": "111111111111"
    }
  },
  "responseElements": {
    "handshake": {
      "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
      "state": "OPEN",
      "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
      "id": "h-examplehandshakeid111",
      "parties": [
        {
          "type": "ORGANIZATION",
          "id": "o-aa111bb222"
        },
        {
          "type": "ACCOUNT",
          "id": "222222222222"
        }
      ],
      "action": "invite",
      "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
      "resources": [
        {
          "resources": [
            {
              "type": "MASTER_EMAIL",

```

```

        "value": "diego@example.com"
      },
      {
        "type": "MASTER_NAME",
        "value": "Management account for organization"
      },
      {
        "type": "ORGANIZATION_FEATURE_SET",
        "value": "ALL"
      }
    ],
    "type": "ORGANIZATION",
    "value": "o-aa111bb222"
  },
  {
    "type": "ACCOUNT",
    "value": "222222222222"
  },
  {
    "type": "NOTES",
    "value": "This is a request for Mary's account to join Diego's
organization."
  }
]
}
},
"requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
"eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
"eventType": "AwsApiCall",
"recipientAccountId": "111111111111"
}

```

로그 항목의 예: AttachPolicy

다음 예제에서는 샘플 AttachPolicy 호출의 CloudTrail 로그 항목을 보여 줍니다. 요청한 정책 유형이 연결 요청을 시도한 루트에서 활성화되지 않았기 때문에 응답에서 호출이 실패했다고 표시됩니다.

```

{
  "eventVersion": "1.06",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAMVNPBQA3EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/diego",

```

```

    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "diego"
  },
  "eventTime": "2017-01-18T21:42:44Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "AttachPolicy",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
  "errorCode": "PolicyTypeNotEnabledException",
  "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the current view",
  "requestParameters": {
    "policyId": "p-examplepolicyid111",
    "targetId": "ou-examplerootid111-exampleouid111"
  },
  "responseElements": null,
  "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}

```

로그 항목 예: 잘못된 유효 정책

다음 예제에서는 샘플 EffectivePolicyValidation 이벤트의 CloudTrail 로그 항목을 보여 줍니다. 이 이벤트는 조직의 업데이트로 인해 모든 계정에 잘못된 유효 정책이 생성될 때마다 조직의 관리 계정으로 내보내집니다.

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2025-07-17T14:53:40Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "EffectivePolicyValidation",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",

```

```

    "requestParameters": null,
    "responseElements": null,
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "readOnly": true,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "serviceEventDetails": {
      "accountId": "111111111111",
      "policyType": "BACKUP_POLICY",
      "state": "INVALID",
      "requestTimestamp": "Jul 17, 2025, 2:53:40 PM",
      "info": "All validation errors listed",
      "validationErrors": [
        {
          "accountPath": "o-aa111bb222/r-a1b2/111111111111/",
          "evaluationTimestamp": "Jul 17, 2025, 2:53:40 PM",
          "errorCode": "ELEMENTS_TOO_MANY",
          "errorMessage": "'hourly_rule' exceeds the allowed maximum limit 10",
          "pathToError": "plans/hourly-backup/rules/hourly_rule",
          "contributingPolicies": [
            "p-examplepolicyid111"
          ]
        }
      ]
    },
    "eventCategory": "Management"
  }
}

```

로그 항목 예: 유효한 유효 정책

다음 예제에서는 샘플 EffectivePolicyValidation 이벤트의 CloudTrail 로그 항목을 보여 줍니다. 이 이벤트는 조직의 업데이트로 인해 이전에 유효하지 않았던 정책이 계정에 대해 유효하게 수정될 때마다 조직의 관리 계정으로 내보내집니다.

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "accountId": "111111111111",
    "invokedBy": "AWS Internal"
  },

```

```

    "eventTime": "2025-07-17T14:54:40Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "EffectivePolicyValidation",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "readOnly": true,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "serviceEventDetails": {
      "accountId": "111111111111",
      "policyType": "BACKUP_POLICY",
      "state": "VALID",
      "requestTimestamp": "Jul 17, 2025, 2:54:40 PM",
      "info": "Previous effective policy validation error(s) resolved for this
account/policyType"
    },
    "eventCategory": "Management"
  }
}

```

Amazon EventBridge 및 AWS Organizations

AWS Organizations 는 이전 Amazon CloudWatch Events인 Amazon EventBridge와 함께 작동하여 조직에서 관리자가 지정한 작업이 발생할 때 이벤트를 발생시킬 수 있습니다. 예를 들어 작업의 중요성 때문에 대부분의 관리자는 사용자가 조직에 새 계정을 만들 때마다 또는 멤버 계정의 관리자가 조직을 탈퇴하려고 할 때 경고를 표시하려고 합니다. 이 작업을 찾는 EventBridge 규칙을 구성한 후 관리자가 정의한 대상으로 생성된 이벤트를 보낼 수 있습니다. 대상은 해당 구독자에게 이메일 또는 문자 메시지를 보내는 Amazon SNS 주제가 될 수 있습니다. 나중에 검토할 수 있도록 작업의 세부 정보를 로깅하는 AWS Lambda 함수를 만들 수도 있습니다.

EventBridge에서 조직의 주요 활동을 모니터링하도록 설정하는 방법을 보여 주는 자습서는 [자습서: Amazon EventBridge를 사용하여 조직에 대한 중요 변경 사항 모니터링](#)(을) 참조하세요.

⚠ Important

현재 AWS Organizations 는 미국 동부(버지니아 북부) 리전에서만 호스팅됩니다(전 세계적으로 사용 가능하더라도). 이 자습서의 단계를 수행하려면 해당 리전을 사용하도록 AWS Management Console 를 구성해야 합니다.

구성 및 활성화 방법 등 EventBridge에 대해 자세히 알아보려면 [Amazon EventBridge 사용 설명서](#)를 참조하세요.

에 대한 규정 준수 검증 AWS Organizations

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 [AWS 서비스 규정 준수 프로그램 제공 범위 내](#)를 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 [AWS 규정 준수 프로그램](#).

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

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다. 사용 시 규정 준수 책임에 대한 자세한 내용은 [AWS 보안 설명서를](#) AWS 서비스 참조하세요.

의 복원력 AWS Organizations

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 지연 시간이 짧고 처리량이 많으며 중복성이 높은 네트워킹과 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공합니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

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

의 인프라 보안 AWS Organizations

관리형 서비스인 AWS 글로벌 네트워크 보안으로 보호 AWS Organizations 됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 [AWS 클라우드 보안을](#) 참조하세요. 인프

라 보안 모범 사례를 사용하여 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 [인프라 보호](#)를 참조하세요 AWS .

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Organizations에 액세스합니다. 클라이언트는 다음을 지원해야 합니다.

- Transport Layer Security(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [Federal Information Processing Standard\(FIPS\) 140-2](#)를 참조하세요.

문제 해결 AWS Organizations

작업 시 문제가 발생하면이 섹션의 주제를 AWS Organizations참조하세요.

일반적인 문제 해결

여기의 정보를 사용하여 작업 시 발생할 수 있는 액세스 거부 또는 기타 일반적인 문제를 진단하고 수정할 수 있습니다 AWS Organizations.

주제

- [에 요청할 때 "액세스 거부" 메시지가 표시됨 AWS Organizations](#)
- [임시 보안 자격 증명으로 요청하면 "액세스 거부" 메시지가 표시됩니다](#)
- [멤버 계정으로 조직을 나가거나 관리 계정으로 멤버 계정을 제거하려고 하면 "액세스 거부" 메시지가 표시됩니다](#)
- [조직에 계정을 추가하려고 하면 "할당량 초과" 메시지가 표시됩니다.](#)
- [계정을 추가 또는 제거할 때 "이 작업에는 대기 시간이 필요합니다."라는 메시지가 표시됩니다.](#)
- [조직에 계정을 추가하려고 하면 "조직이 아직 초기화 중임"이라는 메시지가 표시됩니다.](#)
- [내 조직에 계정을 초대하려고 할 때 "초대장이 비활성화되었습니다."라는 메시지가 표시됩니다.](#)
- [변경 사항이 매번 즉시 표시되는 것은 아닙니다.](#)
- [이미 조직의 일부인 계정에 액세스하려고 하면 '등록 완료' 메시지가 표시됩니다.](#)

에 요청할 때 "액세스 거부" 메시지가 표시됨 AWS Organizations

- 요청한 작업 및 리소스를 호출할 권한이 있는지 확인하세요. 관리자가 IAM 정책을 자신의 사용자, 그룹 또는 역할에 연결해 권한을 부여해야 합니다. 이러한 권한을 부여하는 정책 명령문에 시간이나 IP 주소 제한 정책이 포함된다면, 요청을 전송할 때 이러한 요구사항을 충족해야 합니다. 사용자, 그룹 또는 역할에 대한 정책을 확인 또는 수정하는 방법은 IAM 사용 설명서에 있는 [정책 작업](#) 섹션을 참조하세요.
- ([AWS SDK](#)를 사용하지 않고) API 요청에 수동으로 서명할 경우, [요청에 올바르게 서명했는지](#) 확인합니다.

임시 보안 자격 증명으로 요청하면 "액세스 거부" 메시지가 표시됩니다

- 요청을 위해 사용 중인 사용자나 역할에 올바른 권한이 있는지 확인합니다. 임시 보안 자격 증명의 권한은 사용자 또는 역할에서 파생되므로 사용자 또는 역할에 부여된 권한으로 제한됩니다. 임시 보안 자격 증명의 권한이 결정되는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [임시 보안 자격 증명을 위한 권한 제어](#) 섹션을 참조하세요.
- 요청에 올바르게 서명했고 요청이 잘 구성되었는지 확인합니다. 자세한 내용은 IAM 사용 설명서의 선택한 SDK에 대한 [도구 키트](#) 설명서 또는 [임시 보안 자격 증명을 사용하여 AWS 리소스에 대한 액세스 요청을 참조하세요](#).
- 임시 보안 자격 증명이 만료되지 않았는지 확인합니다. 자세한 내용은 IAM 사용 설명서의 [임시 보안 자격 증명 요청](#) 섹션을 참조하세요.

멤버 계정으로 조직을 나가거나 관리 계정으로 멤버 계정을 제거하려고 하면 "액세스 거부" 메시지가 표시됩니다

- 멤버 계정에서 결제에 대한 IAM 사용자 액세스를 활성화한 후에만 멤버 계정을 제거할 수 있습니다. 자세한 내용은 AWS Billing 사용 설명서의 [Billing and Cost Management 콘솔에 대한 액세스 활성화](#)를 참조하세요.
- 계정에 독립형 계정으로 실행하는 데 필요한 정보가 있는 경우에만 조직에서 계정을 제거할 수 있습니다. AWS Organizations 콘솔, API 또는 AWS CLI 명령을 사용하여 조직에서 계정을 생성하면 해당 정보가 자동으로 수집되지 않습니다. 독립 실행형으로 만들려는 계정의 경우 AWS 고객 계약을 수락하고, 지원 플랜을 선택하고, 필요한 연락처 정보를 제공 및 확인하고, 현재 결제 방법을 제공해야 합니다.는 결제 방법을 AWS 사용하여 계정이 조직에 연결되어 있지 않은 동안 발생하는 청구 가능한(AWS 프리 티어가 아닌) AWS 활동에 대해 요금을 청구합니다. 자세한 내용은 [를 사용하여 멤버 계정에서 조직 탈퇴 AWS Organizations](#) 단원을 참조하십시오.

조직에 계정을 추가하려고 하면 "할당량 초과" 메시지가 표시됩니다.

조직에서 최대 보유할 수 있는 계정 수는 제한되어 있습니다. 삭제 또는 종료된 계정은 이 할당량을 기준으로 계속 계산됩니다.

가입 초대는 조직의 최대 계정 수를 기준으로 계산됩니다. 초대된 계정에서 초대를 거부하면 해당 카운트가 반환되고 관리 계정이 초대를 취소하거나 초대가 만료됩니다.

- 를 달거나 삭제하기 전에 할당량에 계속 포함되지 않도록 조직에서 AWS 계정제거합니다. [???](#)
- 할당량 증가를 요청하는 방법에 대한 자세한 내용은 [최대값 및 최소값](#) 단원을 참조하세요.

계정을 추가 또는 제거할 때 "이 작업에는 대기 시간이 필요합니다."라는 메시지가 표시됩니다.

계정 할당량으로 인해 대기 기간이 필요한 작업도 있습니다. 예를 들어 새로 생성한 계정을 즉시 제거할 수는 없습니다. 며칠 후에 다시 작업을 시도하세요.

계정 추가와 관련된 문제는 할당량 [기본 최대 계정 수](#)를 참조하세요. 계정 제거와 관련된 문제는 할당량 [30일 이내에 해지할 수 있는 계정 수](#)를 참조하세요.

조직에 계정을 추가하려고 하면 "조직이 아직 초기화 중임"이라는 메시지가 표시됩니다.

조직을 생성한 지 1시간 이상 지난 상태에서 이 오류를 수신한 경우 [AWS Support](#)에 문의하세요.

내 조직에 계정을 초대하려고 할 때 "초대장이 비활성화되었습니다."라는 메시지가 표시됩니다.

이 문제는 [조직에서 모든 기능을 활성화](#)하는 경우에 발생합니다. 이 작업은 시간이 걸릴 수 있으며 모든 멤버 계정이 응답해야 합니다. 작업이 완료될 때까지 새 계정을 조직에 가입하도록 초대할 수 없습니다.

변경 사항이 매번 즉시 표시되는 것은 아닙니다.

사용자들이 전세계 데이터 센터의 컴퓨터들을 통해 액세스하는 서비스인 AWS Organizations 은 [최종 일관성](#)이라고 하는 분산 컴퓨팅 모델을 사용합니다. 에서 변경한 내용은 가능한 모든 엔드포인트에서 표시되는 데 시간이 AWS Organizations 걸립니다. 일부 지연은 서버에서 서버로 또는 복제 영역에서 복제 영역으로 데이터를 전송하는 데 걸리는 시간으로 인해 발생합니다. AWS Organizations 또한 캐싱을 사용하여 성능을 개선하지만 경우에 따라 시간이 더 걸릴 수 있습니다. 이러한 변화는 이전에 캐싱된 데이터가 끝날 때까지 가시화되지 않을 수 있습니다.

한 위치에서 변경한 내용이 다른 위치에서 즉시 보이지 않을 때조차도 전역 애플리케이션이 이러한 잠재적 지연을 설명하고 예상대로 작동하도록 설계하세요.

이로 인해 다른 일부 AWS 서비스 가 어떤 영향을 받는지에 대한 자세한 내용은 다음 리소스를 참조하세요.

- Amazon Redshift 데이터베이스 개발자 안내서의 [데이터 일관성 관리](#)
- Amazon Simple Storage Service 사용 설명서의 [Amazon S3 데이터 일관성 모델](#)

- AWS 빅 데이터 블로그의 [ETL 워크플로에 Amazon S3 및 Amazon Elastic MapReduce를 사용할 때 일관성 보장](#)
- Amazon EC2 API 참조의 [EC2 최종 일관성](#)

이미 조직의 일부인 계정에 액세스하려고 하면 ‘등록 완료’ 메시지가 표시됩니다.

- 멤버 계정이 관리 계정의 결제 세부 정보를 상속하는 데 최대 48시간이 걸릴 수 있습니다.
- 48시간 후에도 문제가 지속되면 계정 및 결제 지원 팀에 지원 케이스를 개설할 수 있습니다. 자세한 내용은 [지원 케이스 생성](#)을 참조하세요.

HTTP 쿼리 요청을 통한 API 호출

이 섹션에는 쿼리 API 사용에 대한 일반적인 정보가 포함되어 있습니다 AWS Organizations. API 작업 및 오류에 대한 자세한 정보는 [AWS Organizations API 참조](#)를 참조하세요.

Note

AWS Organizations 쿼리 API를 직접 호출하는 AWS 대신 SDKs. AWS SDKs는 다양한 프로그래밍 언어 및 플랫폼(Java, Ruby, .NET, iOS, Android 등)을 위한 라이브러리와 샘플 코드로 구성됩니다. SDKs는 AWS Organizations 및에 프로그래밍 방식으로 액세스할 수 있는 편리한 방법을 제공합니다 AWS. 예를 들어 SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 처리합니다. 다운로드 및 설치 방법을 포함하여 AWS SDKs에 대한 자세한 내용은 [Amazon Web Services용 도구](#)를 참조하세요.

용 쿼리 API AWS Organizations 를 사용하면 서비스 작업을 호출할 수 있습니다. 쿼리 API 요청은 수행할 작업을 나타내는 Action 파라미터를 포함해야 하는 HTTPS 요청입니다. 모든 작업에 대해 GET 및 POST 요청을 AWS Organizations 지원합니다. 즉, API 사용 시 어떤 작업에는 GET을 사용하고 또 어떤 작업에는 POST를 사용할 필요가 없습니다. 하지만 GET 요청에는 URL 크기 제한이 적용됩니다. 제한은 브라우저에 따라 다르지만, 일반적으로 2,048바이트입니다. 따라서 더 큰 크기가 필요한 쿼리 API 요청의 경우 POST 요청을 사용해야 합니다.

응답은 XML 문서입니다. 응답에 대한 자세한 정보는 [AWS Organizations API 참조](#)의 개별 작업 페이지를 참조하세요.

주제

- [엔드포인트](#)
- [HTTPS 필요](#)
- [AWS Organizations API 요청 서명](#)

엔드포인트

AWS Organizations 에는 미국 동부(버지니아 북부) 리전에서 호스팅되는 단일 글로벌 API 엔드포인트가 있습니다.

모든 서비스의 AWS 엔드포인트 및 리전에 대한 자세한 내용은 [리전 엔드포인트](#)를 참조하세요 AWS 일반 참조.

HTTPS 필요

쿼리 API는 보안 자격 증명과 같이 민감한 정보를 반환하므로 HTTPS를 이용해 모든 API 요청을 암호화해야 합니다.

AWS Organizations API 요청 서명

액세스 키 ID와 보안 액세스 키를 사용하여 요청에 서명해야 합니다. 일상적인 작업에 자격 AWS 계정 루트 사용자 증명을 사용하지 않는 것이 좋습니다 AWS Organizations. 그 대신 사용자나 역할의 보안 인증 정보를 사용하면 됩니다.

API 요청에 서명하려면 AWS 서명 버전 4를 사용해야 합니다. 서명 버전 4 사용에 대한 자세한 내용은 IAM 사용 설명서의 [AWS API 요청 서명](#)을 참조하세요.

AWS Organizations 는 서명 버전 2와 같은 이전 버전을 지원하지 않습니다.

자세한 내용은 다음을 참조하세요.

- [AWS 보안 자격 증명](#) - 액세스에 사용할 수 있는 자격 증명 유형에 대한 일반 정보를 제공합니다 AWS.
- [IAM의 보안 모범 사례](#) - IAM 서비스를 사용하여의 리소스를 포함한 AWS 리소스를 보호하는 데 도움이 되는 제안을 제공합니다 AWS Organizations.
- [IAM의 임시 자격 증명](#) - 임시 보안 자격 증명을 생성하고 사용하는 방법에 대해 설명합니다.

AWS SDKs를 사용하는 조직에 대한 코드 예제

다음 코드 예제에서는 AWS 소프트웨어 개발 키트(SDK)와 함께 Organizations를 사용하는 방법을 보여줍니다.

작업은 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 작업은 개별 서비스 함수를 직접 호출하는 방법을 보여주며, 관련 시나리오의 컨텍스트에 맞는 작업을 볼 수 있습니다.

시나리오는 동일한 서비스 내에서 또는 다른 AWS 서비스와 결합된 상태에서 여러 함수를 직접적으로 호출하여 특정 태스크를 수행하는 방법을 보여주는 코드 예제입니다.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

코드 예시

- [AWS SDKs를 사용하는 조직에 대한 기본 예제](#)
 - [AWS SDKs를 사용하는 조직에 대한 작업](#)
 - [AWS SDK 또는 CLI와 AttachPolicy 함께 사용](#)
 - [AWS SDK 또는 CLI와 CreateAccount 함께 사용](#)
 - [AWS SDK 또는 CLI와 CreateOrganization 함께 사용](#)
 - [AWS SDK 또는 CLI와 CreateOrganizationalUnit 함께 사용](#)
 - [AWS SDK 또는 CLI와 CreatePolicy 함께 사용](#)
 - [AWS SDK 또는 CLI와 DeleteOrganization 함께 사용](#)
 - [AWS SDK 또는 CLI와 DeleteOrganizationalUnit 함께 사용](#)
 - [AWS SDK 또는 CLI와 DeletePolicy 함께 사용](#)
 - [AWS SDK 또는 CLI와 DescribePolicy 함께 사용](#)
 - [AWS SDK 또는 CLI와 DetachPolicy 함께 사용](#)
 - [AWS SDK 또는 CLI와 ListAccounts 함께 사용](#)
 - [AWS SDK 또는 CLI와 ListOrganizationalUnitsForParent 함께 사용](#)
 - [AWS SDK 또는 CLI와 ListPolicies 함께 사용](#)
- [AWS SDKs를 사용하는 조직에 대한 시나리오](#)
 - [AWS Compute Optimizer 자동화 기능이 권장 작업을 적용하도록 허용](#)
 - [조직 전반의 자동화를 활성화하는 정책](#)

- [계정의 자동화를 활성화하는 정책](#)
- [조직의 관리 계정에 Compute Optimizer 자동화에 대한 전체 액세스 권한을 부여하기 위한 정책](#)
- [독립 실행형 AWS 계정에 대해 Compute Optimizer Automation에 대한 전체 액세스 권한을 부여하는 정책](#)
- [조직의 관리 계정에 Compute Optimizer 자동화에 대한 읽기 전용 액세스 권한을 부여하기 위한 정책](#)
- [독립 실행형 AWS 계정에 대해 Compute Optimizer Automation에 대한 읽기 전용 액세스 권한을 부여하는 정책](#)
- [컴퓨팅 최적화 자동화에 대한 서비스 연결 역할 권한을 부여하는 정책](#)

AWS SDKs를 사용하는 조직에 대한 기본 예제

다음 코드 예제에서는 AWS Organizations SDKs에서의 기본 사항을 AWS 사용하는 방법을 보여줍니다.

예제

- [AWS SDKs를 사용하는 조직에 대한 작업](#)
 - [AWS SDK 또는 CLI와 AttachPolicy 함께 사용](#)
 - [AWS SDK 또는 CLI와 CreateAccount 함께 사용](#)
 - [AWS SDK 또는 CLI와 CreateOrganization 함께 사용](#)
 - [AWS SDK 또는 CLI와 CreateOrganizationalUnit 함께 사용](#)
 - [AWS SDK 또는 CLI와 CreatePolicy 함께 사용](#)
 - [AWS SDK 또는 CLI와 DeleteOrganization 함께 사용](#)
 - [AWS SDK 또는 CLI와 DeleteOrganizationalUnit 함께 사용](#)
 - [AWS SDK 또는 CLI와 DeletePolicy 함께 사용](#)
 - [AWS SDK 또는 CLI와 DescribePolicy 함께 사용](#)
 - [AWS SDK 또는 CLI와 DetachPolicy 함께 사용](#)
 - [AWS SDK 또는 CLI와 ListAccounts 함께 사용](#)
 - [AWS SDK 또는 CLI와 ListOrganizationalUnitsForParent 함께 사용](#)
 - [AWS SDK 또는 CLI와 ListPolicies 함께 사용](#)

AWS SDKs를 사용하는 조직에 대한 작업

다음 코드 예제에서는 AWS SDKs를 사용하여 개별 Organizations 작업을 수행하는 방법을 보여줍니다. 각 예제에는 GitHub에 대한 링크가 포함되어 있습니다. 여기에서 코드 설정 및 실행에 대한 지침을 찾을 수 있습니다.

이들 발췌문은 Organizations API를 호출하며, 컨텍스트에서 실행되어야 하는 더 큰 프로그램에서 발췌한 코드입니다. [AWS SDKs를 사용하는 조직에 대한 시나리오](#)에서 컨텍스트에 맞는 작업을 볼 수 있습니다.

다음 예제에는 가장 일반적으로 사용되는 작업만 포함되어 있습니다. 전체 목록은 [AWS Organizations API 참조](#)를 참조하세요.

예제

- [AWS SDK 또는 CLI와 AttachPolicy 함께 사용](#)
- [AWS SDK 또는 CLI와 CreateAccount 함께 사용](#)
- [AWS SDK 또는 CLI와 CreateOrganization 함께 사용](#)
- [AWS SDK 또는 CLI와 CreateOrganizationalUnit 함께 사용](#)
- [AWS SDK 또는 CLI와 CreatePolicy 함께 사용](#)
- [AWS SDK 또는 CLI와 DeleteOrganization 함께 사용](#)
- [AWS SDK 또는 CLI와 DeleteOrganizationalUnit 함께 사용](#)
- [AWS SDK 또는 CLI와 DeletePolicy 함께 사용](#)
- [AWS SDK 또는 CLI와 DescribePolicy 함께 사용](#)
- [AWS SDK 또는 CLI와 DetachPolicy 함께 사용](#)
- [AWS SDK 또는 CLI와 ListAccounts 함께 사용](#)
- [AWS SDK 또는 CLI와 ListOrganizationalUnitsForParent 함께 사용](#)
- [AWS SDK 또는 CLI와 ListPolicies 함께 사용](#)

AWS SDK 또는 CLI와 **AttachPolicy** 함께 사용

다음 코드 예시는 AttachPolicy의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
    /// AttachPolicyAsync method to attach the policy to the root
    /// organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyId = "p-000000000";
        var targetId = "r-0000";

        var request = new AttachPolicyRequest
        {
            PolicyId = policyId,
            TargetId = targetId,
        };

        var response = await client.AttachPolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {

```

```

        Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
    }
    else
    {
        Console.WriteLine("Was not successful in attaching the policy.");
    }
}
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [AttachPolicy](#)를 참조하세요.

CLI

AWS CLI

정책을 루트, OU 또는 계정에 연결하는 방법

예시 1

다음 예시에서는 서비스 제어 정책(SCP)을 OU에 연결하는 방법을 보여줍니다.

```

aws organizations attach-policy
    --policy-id p-examplepolicyid111
    --target-id ou-examplerootid111-exampleouid111

```

예시 2

다음 예시에서는 계정에 서비스 제어 정책을 직접 연결하는 방법을 보여줍니다.

```

aws organizations attach-policy
    --policy-id p-examplepolicyid111
    --target-id 333333333333

```

- API 세부 정보는 AWS CLI 명령 참조의 [AttachPolicy](#)를 참조하세요.

Python

SDK for Python (Boto3)

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
    or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [AttachPolicy](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
TRY.  
    lo_org->attachpolicy(  
        iv_policyid = iv_policy_id  
        iv_targetid = iv_target_id ).  
    MESSAGE 'Policy attached to target.' TYPE 'I'.  
CATCH /aws1/cx_orgaccessdeniedex.  
    MESSAGE 'You do not have permission to attach the policy.' TYPE 'E'.  
CATCH /aws1/cx_orgpolicynotfoundex.  
    MESSAGE 'The specified policy does not exist.' TYPE 'E'.  
CATCH /aws1/cx_orgtargetnotfoundex.  
    MESSAGE 'The specified target does not exist.' TYPE 'E'.  
CATCH /aws1/cx_orgduplicateplyatta00.  
    MESSAGE 'The policy is already attached to the target.' TYPE 'E'.  
ENDTRY.
```

- API 세부 정보는 AWS SDK for SAP ABAP API 참조의 [AttachPolicy](#)를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations 에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **CreateAccount** 함께 사용

다음 코드 예시는 CreateAccount의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var accountName = "ExampleAccount";
        var email = "someone@example.com";

        var request = new CreateAccountRequest
        {
            AccountName = accountName,
            Email = email,
        };

        var response = await client.CreateAccountAsync(request);
        var status = response.CreateAccountStatus;

        Console.WriteLine($"The status of {status.AccountName} is
{status.State}.");
    }
}
```

```
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 [CreateAccount](#)를 참조하세요.

CLI

AWS CLI

자동으로 조직의 일부가 되는 멤버 계정을 생성하는 방법

다음 예시에서는 조직 내에 멤버 계정을 생성하는 방법을 보여줍니다. 멤버 계정은 Production Account라는 이름과 susan@example.com이라는 이메일 주소로 구성됩니다. roleName 파라미터가 지정되지 않았으므로 Organizations는 OrganizationAccountAccessRole의 기본 이름을 사용하여 IAM 역할을 자동으로 생성합니다. 또한 iamUserAccessToBilling 파라미터가 지정되지 않았으므로 IAM 사용자 또는 역할에 계정 결제 데이터에 액세스할 수 있는 충분한 권한을 허용하는 설정은 기본값인 ALLOW로 설정됩니다. Organizations는 Susan에게 "Welcome to AWS" 이메일을 자동으로 보냅니다.

```
aws organizations create-account --email susan@example.com --account-name "Production Account"
```

출력에는 현재 IN_PROGRESS 상태임을 보여주는 요청 객체가 포함됩니다.

```
{
  "CreateAccountStatus": {
    "State": "IN_PROGRESS",
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

나중에 describe-create-account-status 명령에 대한 Id 응답 값을 create-account-request-id 파라미터의 값으로 제공하여 요청의 현재 상태를 쿼리할 수 있습니다.

자세한 내용은 AWS Organizations 사용 설명서의 조직에서 AWS 계정 생성을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 [CreateAccount](#)를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations](#) 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **CreateOrganization** 함께 사용

다음 코드 예시는 CreateOrganization의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
public class CreateOrganization
{
    /// <summary>
    /// Creates an Organizations client object and then uses it to create
    /// a new organization with the default user as the administrator, and
    /// then displays information about the new organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var response = await client.CreateOrganizationAsync(new
        CreateOrganizationRequest
        {
            FeatureSet = "ALL",
        });
    }
}
```

```

        Organization newOrg = response.Organization;

        Console.WriteLine($"Organization: {newOrg.Id} Main Account:
{newOrg.MasterAccountId}");
    }
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [CreateOrganization](#)을 참조하세요.

CLI

AWS CLI

예 1: 새 조직을 생성하는 방법

Bill은 111111111111 계정의 자격 증명을 사용하여 조직을 만들려고 합니다. 다음 예시에서는 해당 계정이 새 조직의 마스터 계정이 되는 것을 보여줍니다. Bill이 기능 세트를 지정하지 않기 때문에 새 조직에서는 기본적으로 모든 기능이 활성화되고 서비스 제어 정책은 루트에서 활성화 됩니다.

```
aws organizations create-organization
```

출력에는 새 조직의 세부 정보가 있는 조직 객체가 포함됩니다.

```

{
    "Organization": {
        "AvailablePolicyTypes": [
            {
                "Status": "ENABLED",
                "Type": "SERVICE_CONTROL_POLICY"
            }
        ],
        "MasterAccountId": "111111111111",
        "MasterAccountArn": "arn:aws:organizations::111111111111:account/o-exampleorgid/111111111111",
        "MasterAccountEmail": "bill@example.com",
        "FeatureSet": "ALL",
        "Id": "o-exampleorgid",
    }
}

```

```

        "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
    }
}

```

예 2: 통합 결제 기능만 활성화된 새 조직 생성

다음 예시에서는 통합 결제 기능만 지원하는 조직을 만듭니다.

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

출력에는 새 조직의 세부 정보가 있는 조직 객체가 포함됩니다.

```

{
    "Organization": {
        "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
        "AvailablePolicyTypes": [],
        "Id": "o-exampleorgid",
        "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
        "MasterAccountEmail": "bill@example.com",
        "MasterAccountId": "111111111111",
        "FeatureSet": "CONSOLIDATED_BILLING"
    }
}

```

자세한 내용은 AWS Organizations 사용자 안내서의 조직 생성을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 [CreateOrganization](#)을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations 에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **CreateOrganizationalUnit** 함께 사용

다음 코드 예시는 CreateOrganizationalUnit의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitName = "ProductDevelopmentUnit";

        var request = new CreateOrganizationalUnitRequest
        {
            Name = orgUnitName,
            ParentId = "r-0000",
        };

        var response = await client.CreateOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {

```

```

        Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
        Console.WriteLine($"Organizational unit {orgUnitName} Details");
        Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
    }
    else
    {
        Console.WriteLine("Could not create new organizational unit.");
    }
}
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [CreateOrganizationalUnit](#)을 참조하세요.

CLI

AWS CLI

루트 또는 상위 OU에 OU를 생성하는 방법

다음 예시에서는 AccountingOU라는 OU를 생성하는 방법을 보여줍니다.

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

출력에는 새 OU의 세부 정보가 있는 organizationalUnit 객체가 포함됩니다.

```

{
    "OrganizationalUnit": {
        "Id": "ou-examplerootid111-exampleouid111",
        "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
        "Name": "AccountingOU"
    }
}

```

- API 세부 정보는 AWS CLI 명령 참조의 [CreateOrganizationalUnit](#)을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations](#) 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **CreatePolicy** 함께 사용

다음 코드 예시는 CreatePolicy의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations Policy.
/// </summary>
public class CreatePolicy
{
    /// <summary>
    /// Initializes the AWS Organizations client object, uses it to
    /// create a new Organizations Policy, and then displays information
    /// about the newly created Policy.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyContent = "{" +
            "  \"Version\": \"2012-10-17\", " +
            "  \"Statement\" : [{" +
            "    \"Action\" : [\"s3:*\"], " +
            "    \"Effect\" : \"Allow\", " +
            "    \"Resource\" : \"*\" " +
```

```

        "}]" +
        "}}";

        try
        {
            var response = await client.CreatePolicyAsync(new
CreatePolicyRequest
            {
                Content = policyContent,
                Description = "Enables admins of attached accounts to
delegate all Amazon S3 permissions",
                Name = "AllowAllS3Actions",
                Type = "SERVICE_CONTROL_POLICY",
            });

            Policy policy = response.Policy;
            Console.WriteLine($"{policy.PolicySummary.Name} has the following
content: {policy.Content}");
        }
        catch (Exception ex)
        {
            Console.WriteLine(ex.Message);
        }
    }
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [CreatePolicy](#)를 참조하십시오.

CLI

AWS CLI

예 1: JSON 정책의 텍스트 소스 파일을 사용하여 정책을 생성하는 방법

다음 예시에서는 이름이 AllowAllS3Actions인 서비스 제어 정책(SCP)을 생성하는 방법을 보여줍니다. 정책 콘텐츠는 policy.json이라는 로컬 컴퓨터에 있는 파일에서 가져온 것입니다.

```
aws organizations create-policy --content file://policy.json --
name AllowAllS3Actions, --type SERVICE_CONTROL_POLICY --description "Allows
delegation of all S3 actions"
```

출력에는 새 정책의 세부 정보가 있는 정책 객체가 포함됩니다.

```
{
  "Policy": {
    "Content": "{\n\"Version\":\n\"2012-10-17\", \"Statement\": [{\n\"Effect\
\n\":\n\"Allow\", \"Action\": [\n\"s3:*\"], \"Resource\": [\n\"*\"]}]}",
    "PolicySummary": {
      "Arn": "arn:aws:organizations::o-exampleorgid:policy/
service_control_policy/p-examplepolicyid111",
      "Description": "Allows delegation of all S3 actions",
      "Name": "AllowAllS3Actions",
      "Type": "SERVICE_CONTROL_POLICY"
    }
  }
}
```

예시 2: JSON 정책을 파라미터로 사용하여 정책 생성

다음 예시에서는 동일한 SCP를 생성하는 방법을 보여줍니다. 이번에는 정책 콘텐츠를 파라미터에 JSON 문자열로 임베딩합니다. 파라미터에서 문자열을 큰따옴표로 묶은 리터럴로 취급하려면 큰따옴표 앞에 백슬래시를 추가하여 문자열을 이스케이프 처리해야 합니다.

```
aws organizations create-policy --content "{\n\"Version\":\n\"2012-10-17\",
\n\"Statement\": [{\n\"Effect\":\n\"Allow\", \"Action\": [\n\"s3:*\"], \"Resource
\n\": [\n\"*\"]}]}" --name AllowAllS3Actions --type SERVICE_CONTROL_POLICY --
description "Allows delegation of all S3 actions"
```

조직에서 정책을 만들고 사용하는 방법에 대한 자세한 내용은 AWS Organizations 사용자 안내서의 조직 정책 관리를 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 [CreatePolicy](#)를 참조하세요.

Python

SDK for Python (Boto3)

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
def create_policy(name, description, content, policy_type, orgs_client):
    """
    Creates a policy.

    :param name: The name of the policy.
    :param description: The description of the policy.
    :param content: The policy content as a dict. This is converted to JSON
    before
                    it is sent to AWS. The specific format depends on the policy
    type.
    :param policy_type: The type of the policy.
    :param orgs_client: The Boto3 Organizations client.
    :return: The newly created policy.
    """
    try:
        response = orgs_client.create_policy(
            Name=name,
            Description=description,
            Content=json.dumps(content),
            Type=policy_type,
        )
        policy = response["Policy"]
        logger.info("Created policy %s.", name)
    except ClientError:
        logger.exception("Couldn't create policy %s.", name)
        raise
    else:
        return policy
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [CreatePolicy](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
TRY.
    oo_result = lo_org->createpolicy(          " oo_result is returned for
testing purposes. "
        iv_name      = iv_policy_name
        iv_description = iv_policy_description
        iv_content    = iv_policy_content
        iv_type       = iv_policy_type ).
    MESSAGE 'Policy created.' TYPE 'I'.
CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to create a policy.' TYPE 'E'.
CATCH /aws1/cx_orgduplicatepolicyex.
    MESSAGE 'A policy with this name already exists.' TYPE 'E'.
CATCH /aws1/cx_orgmalformedplydocex.
    MESSAGE 'The policy content is malformed.' TYPE 'E'.
ENDTRY.
```

- API 세부 정보는 AWS SDK for SAP ABAP API의 [CreatePolicy](#)를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations 에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **DeleteOrganization** 함께 사용

다음 코드 예시는 DeleteOrganization의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
{
    /// <summary>
    /// Initializes the Organizations client and then calls
    /// DeleteOrganizationAsync to delete the organization.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine("Successfully deleted organization.");
        }
        else
        {
            Console.WriteLine("Could not delete organization.");
        }
    }
}
```

```
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 [DeleteOrganization](#)을 참조하세요.

CLI

AWS CLI

조직을 삭제하는 방법

다음 예시에서는 조직을 삭제하는 방법을 보여줍니다. 이 작업을 수행하려면 조직의 마스터 계정 관리자여야 합니다. 이 예시에서는 이전에 조직에서 모든 멤버 계정, OU 및 정책을 제거했다고 가정합니다.

```
aws organizations delete-organization
```

- API 세부 정보는 AWS CLI 명령 참조의 [DeleteOrganization](#)을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **DeleteOrganizationalUnit** 함께 사용

다음 코드 예시는 DeleteOrganizationalUnit의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
```

```
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
    /// with the selected ID.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitId = "ou-0000-000000000";

        var request = new DeleteOrganizationalUnitRequest
        {
            OrganizationalUnitId = orgUnitId,
        };

        var response = await client.DeleteOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
        }
        else
        {
            Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
        }
    }
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 [DeleteOrganizationalUnit](#)을 참조하세요.

CLI

AWS CLI

OU를 삭제하는 방법

다음 예시에서는 OU를 삭제하는 방법을 보여줍니다. 이 예시에서는 이전에 OU에서 모든 계정과 다른 OU를 제거했다고 가정합니다.

```
aws organizations delete-organizational-unit --organizational-unit-id ou-examplerootid111-exampleouid111
```

- API 세부 정보는 AWS CLI 명령 참조의 [DeleteOrganizationalUnit](#)을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **DeletePolicy** 함께 사용

다음 코드 예시는 DeletePolicy의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

 Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
```

```
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-000000000";

        var request = new DeletePolicyRequest
        {
            PolicyId = policyId,
        };

        var response = await client.DeletePolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully deleted Policy: {policyId}.");
        }
        else
        {
            Console.WriteLine($"Could not delete Policy: {policyId}.");
        }
    }
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 [DeletePolicy](#)를 참조하십시오.

CLI

AWS CLI

정책을 삭제하는 방법

다음 예시에서는 조직에서 정책을 삭제하는 방법을 보여줍니다. 이 예시에서는 이전에 정책을 모든 엔터티에서 분리했다고 가정합니다.

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- API 세부 정보는 AWS CLI 명령 참조의 [DeletePolicy](#)를 참조하세요.

Python

SDK for Python (Boto3)

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
def delete_policy(policy_id, orgs_client):  
    """  
    Deletes a policy.  
  
    :param policy_id: The ID of the policy to delete.  
    :param orgs_client: The Boto3 Organizations client.  
    """  
    try:  
        orgs_client.delete_policy(PolicyId=policy_id)  
        logger.info("Deleted policy %s.", policy_id)  
    except ClientError:  
        logger.exception("Couldn't delete policy %s.", policy_id)  
        raise
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [DeletePolicy](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

 Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
TRY.
    lo_org->deletepolicy(
        iv_policyid = iv_policy_id ).
    MESSAGE 'Policy deleted.' TYPE 'I'.
CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to delete the policy.' TYPE 'E'.
CATCH /aws1/cx_orgpolicynotfoundex.
    MESSAGE 'The specified policy does not exist.' TYPE 'E'.
CATCH /aws1/cx_orgpolicyinuseex.
    MESSAGE 'The policy is still attached to one or more targets.' TYPE 'E'.
ENDTRY.
```

- API 세부 정보는 [AWS SDK for SAP ABAP API 참조](#)의 DeletePolicy를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations 에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **DescribePolicy** 함께 사용

다음 코드 예시는 DescribePolicy의 사용 방법을 보여 줍니다.

CLI

AWS CLI

정책 정보 가져오기

다음 예시에서는 정책 정보를 요청하는 방법을 보여줍니다.

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

출력에는 정책의 세부 정보가 있는 정책 객체가 포함됩니다.

```
{
  "Policy": {
    "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*\"\n    }\n  ]\n}",
    "PolicySummary": {
      "Arn": "arn:aws:organizations::111111111111:policy/o-exampleorgid/service_control_policy/p-examplepolicyid111",
      "Type": "SERVICE_CONTROL_POLICY",
      "Id": "p-examplepolicyid111",
      "AwsManaged": false,
      "Name": "AllowAllS3Actions",
      "Description": "Enables admins to delegate S3 permissions"
    }
  }
}
```

- API 세부 정보는 AWS CLI 명령 참조의 [DescribePolicy](#)를 참조하세요.

Python

SDK for Python (Boto3)

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
```

```

: return: The description of the policy.
"""
try:
    response = orgs_client.describe_policy(PolicyId=policy_id)
    policy = response["Policy"]
    logger.info("Got policy %s.", policy_id)
except ClientError:
    logger.exception("Couldn't get policy %s.", policy_id)
    raise
else:
    return policy

```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [DescribePolicy](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```

TRY.
    oo_result = lo_org->describepolicy(      " oo_result is returned for
testing purposes. "
    iv_policyid = iv_policy_id ).
    DATA(lo_policy) = oo_result->get_policy( ).
    MESSAGE 'Retrieved policy details.' TYPE 'I'.
CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to describe the policy.' TYPE 'E'.
CATCH /aws1/cx_organypolicynotfoundex.
    MESSAGE 'The specified policy does not exist.' TYPE 'E'.
ENDTRY.

```

- API 세부 정보는 AWS SDK for SAP ABAP API 참조의 [DescribePolicy](#)를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations](#) 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **DetachPolicy** 함께 사용

다음 코드 예시는 DetachPolicy의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-000000000";
        var targetId = "r-0000";

        var request = new DetachPolicyRequest
```

```
{
    PolicyId = policyId,
    TargetId = targetId,
};

var response = await client.DetachPolicyAsync(request);

if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
{
    Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
}
else
{
    Console.WriteLine("Could not detach the policy.");
}
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 [DetachPolicy](#)를 참조하세요.

CLI

AWS CLI

정책을 루트, OU 또는 계정에서 분리하는 방법

다음 예시에서는 OU에서 정책을 분리하는 방법을 보여줍니다.

```
aws organizations detach-policy --target-id ou-examplerootid111-exampleouid111
--policy-id p-examplepolicyid111
```

- API 세부 정보는 AWS CLI 명령 참조의 [DetachPolicy](#)를 참조하세요.

Python

SDK for Python (Boto3)

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
    attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [DetachPolicy](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
TRY.  
    lo_org->detachpolicy(  
        iv_policyid = iv_policy_id  
        iv_targetid = iv_target_id ).  
    MESSAGE 'Policy detached from target.' TYPE 'I'.  
CATCH /aws1/cx_orgaccessdeniedex.  
    MESSAGE 'You do not have permission to detach the policy.' TYPE 'E'.  
CATCH /aws1/cx_orgpolicynotfoundex.  
    MESSAGE 'The specified policy does not exist.' TYPE 'E'.  
CATCH /aws1/cx_orgtargetnotfoundex.  
    MESSAGE 'The specified target does not exist.' TYPE 'E'.  
CATCH /aws1/cx_orgpolicynotattex.  
    MESSAGE 'The policy is not attached to the target.' TYPE 'E'.  
ENDTRY.
```

- API 세부 정보는 AWS SDK for SAP ABAP API 참조의 [DetachPolicy](#)를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations 에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **ListAccounts** 함께 사용

다음 코드 예시는 ListAccounts의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Uses the AWS Organizations service to list the accounts associated
/// with the default account.
/// </summary>
public class ListAccounts
{
    /// <summary>
    /// Creates the Organizations client and then calls its
    /// ListAccountsAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var request = new ListAccountsRequest
        {
            MaxResults = 5,
        };

        var response = new ListAccountsResponse();
        try
        {
            do
            {
                response = await client.ListAccountsAsync(request);
                response.Accounts.ForEach(a => DisplayAccounts(a));
            }
        }
    }
}
```



```

        if (response.NextToken is not null)
        {
            request.NextToken = response.NextToken;
        }
    }
    while (response.NextToken is not null);
}
catch (AWSOrganizationsNotInUseException ex)
{
    Console.WriteLine(ex.Message);
}
}

/// <summary>
/// Displays information about an Organizations account.
/// </summary>
/// <param name="account">An Organizations account for which to display
/// information on the console.</param>
private static void DisplayAccounts(Account account)
{
    string accountInfo = $"{account.Id}
{account.Name}\t{account.Status}";

    Console.WriteLine(accountInfo);
}
}

```

- API에 대한 세부 정보는 AWS SDK for .NET API 참조의 [ListAccounts](#)를 참조하세요.

CLI

AWS CLI

조직의 모든 계정 목록을 검색하는 방법

다음 예시에서는 조직의 계정 목록을 요청하는 방법을 보여줍니다.

```
aws organizations list-accounts
```

출력에는 계정 요약 객체 목록이 포함됩니다.

```
{
  "Accounts": [
    {
      "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
      "JoinedMethod": "INVITED",
      "JoinedTimestamp": 1481830215.45,
      "Id": "111111111111",
      "Name": "Master Account",
      "Email": "bill@example.com",
      "Status": "ACTIVE"
    },
    {
      "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/222222222222",
      "JoinedMethod": "INVITED",
      "JoinedTimestamp": 1481835741.044,
      "Id": "222222222222",
      "Name": "Production Account",
      "Email": "alice@example.com",
      "Status": "ACTIVE"
    },
    {
      "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333",
      "JoinedMethod": "INVITED",
      "JoinedTimestamp": 1481835795.536,
      "Id": "333333333333",
      "Name": "Development Account",
      "Email": "juan@example.com",
      "Status": "ACTIVE"
    },
    {
      "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/444444444444",
      "JoinedMethod": "INVITED",
      "JoinedTimestamp": 1481835812.143,
      "Id": "444444444444",
      "Name": "Test Account",
      "Email": "anika@example.com",
      "Status": "ACTIVE"
    }
  ]
}
```

}

- API 세부 정보는 AWS CLI 명령 참조의 [ListAccounts](#)를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations 에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **ListOrganizationalUnitsForParent** 함께 사용

다음 코드 예시는 ListOrganizationalUnitsForParent의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Lists the AWS Organizations organizational units that belong to an
/// organization.
/// </summary>
public class ListOrganizationalUnitsForParent
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// call the ListOrganizationalUnitsForParentAsync method to retrieve
    /// the list of organizational units.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
```

```

        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var parentId = "r-0000";

        var request = new ListOrganizationalUnitsForParentRequest
        {
            ParentId = parentId,
            MaxResults = 5,
        };

        var response = new ListOrganizationalUnitsForParentResponse();
        try
        {
            do
            {
                response = await
client.ListOrganizationalUnitsForParentAsync(request);
                response.OrganizationalUnits.ForEach(u =>
DisplayOrganizationalUnit(u));
                if (response.NextToken is not null)
                {
                    request.NextToken = response.NextToken;
                }
            }
            while (response.NextToken is not null);
        }
        catch (Exception ex)
        {
            Console.WriteLine(ex.Message);
        }
    }

    /// <summary>
    /// Displays information about an Organizations organizational unit.
    /// </summary>
    /// <param name="unit">The OrganizationalUnit for which to display
    /// information.</param>
    public static void DisplayOrganizationalUnit(OrganizationalUnit unit)
    {
        string accountInfo = $"{unit.Id} {unit.Name}\t{unit.Arn}";

        Console.WriteLine(accountInfo);
    }
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [ListOrganizationalUnitsForParent](#)를 참조하세요.

CLI

AWS CLI

상위 OU 또는 루트에서 OU 목록을 검색하려면

다음 예시에서는 지정된 루트에서 OU 목록을 가져오는 방법을 보여줍니다.

```
aws organizations list-organizational-units-for-parent --parent-id r-examplerootid111
```

출력은 지정된 루트에 두 개의 OU가 포함되어 있음과 각각의 세부 정보를 보여줍니다.

```
{
  "OrganizationalUnits": [
    {
      "Name": "AccountingDepartment",
      "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-examplerootid111/ou-examplerootid111-exampleouid111"
    },
    {
      "Name": "ProductionDepartment",
      "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-examplerootid111/ou-examplerootid111-exampleouid222"
    }
  ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 [ListOrganizationalUnitsForParent](#)를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations](#) [에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **ListPolicies** 함께 사용

다음 코드 예시는 ListPolicies의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
```

```

        Filter = "SERVICE_CONTROL_POLICY",
        MaxResults = 5,
    };

    var response = new ListPoliciesResponse();
    try
    {
        do
        {
            response = await client.ListPoliciesAsync(request);
            response.Policies.ForEach(p => DisplayPolicies(p));
            if (response.NextToken is not null)
            {
                request.NextToken = response.NextToken;
            }
        }
        while (response.NextToken is not null);
    }
    catch (AWSOrganizationsNotInUseException ex)
    {
        Console.WriteLine(ex.Message);
    }
}

/// <summary>
/// Displays information about the Organizations policies associated
/// with an organization.
/// </summary>
/// <param name="policy">An Organizations policy summary to display
/// information on the console.</param>
private static void DisplayPolicies(PolicySummary policy)
{
    string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

    Console.WriteLine(policyInfo);
}
}

```

- API 세부 정보는 AWS SDK for .NET API 참조의 [ListPolicies](#)를 참조하십시오.

CLI

AWS CLI

특정 유형의 조직에 있는 모든 정책 목록을 검색하는 방법

다음 예시에서는 필터 파라미터로 지정된 SCP 목록을 가져오는 방법을 보여줍니다.

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

출력에는 요약 정보가 있는 정책 목록이 포함됩니다.

```
{
  "Policies": [
    {
      "Type": "SERVICE_CONTROL_POLICY",
      "Name": "AllowAllS3Actions",
      "AwsManaged": false,
      "Id": "p-examplepolicyid111",
      "Arn": "arn:aws:organizations::111111111111:policy/service_control_policy/p-examplepolicyid111",
      "Description": "Enables account admins to delegate permissions for any S3 actions to users and roles in their accounts."
    },
    {
      "Type": "SERVICE_CONTROL_POLICY",
      "Name": "AllowAllEC2Actions",
      "AwsManaged": false,
      "Id": "p-examplepolicyid222",
      "Arn": "arn:aws:organizations::111111111111:policy/service_control_policy/p-examplepolicyid222",
      "Description": "Enables account admins to delegate permissions for any EC2 actions to users and roles in their accounts."
    },
    {
      "AwsManaged": true,
      "Description": "Allows access to every operation",
      "Type": "SERVICE_CONTROL_POLICY",
      "Id": "p-FullAWSAccess",
      "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess",
      "Name": "FullAWSAccess"
    }
  ]
}
```



```
]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 [ListPolicies](#)를 참조하세요.

Python

SDK for Python (Boto3)

Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 [ListPolicies](#)를 참조하세요.

SAP ABAP

SDK for SAP ABAP API

 Note

GitHub에 더 많은 내용이 있습니다. [AWS 코드 예 리포지토리](#)에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
TRY.
    oo_result = lo_org->listpolicies(          " oo_result is returned for
testing purposes. "
    iv_filter = iv_filter ).
    DATA(lt_policies) = oo_result->get_policies( ).
    MESSAGE 'Retrieved list of policies.' TYPE 'I'.
CATCH /aws1/cx_orgaccessdeniedex.
    MESSAGE 'You do not have permission to list policies.' TYPE 'E'.
CATCH /aws1/cx_orgawsorgsnotinuseex.
    MESSAGE 'Your account is not a member of an organization.' TYPE 'E'.
ENDTRY.
```

- API 세부 정보는 AWS SDK for SAP ABAP API 참조의 [ListPolicies](#)를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDKs를 사용하는 조직에 대한 시나리오

다음 코드 예제에서는 Organizations AWS SDKs에서 일반적인 시나리오를 구현하는 방법을 보여줍니다. 이러한 시나리오는 동일한 Organizations 내에서 또는 다른 AWS 서비스와 결합된 상태에서 여러 함수를 호출하여 특정 태스크를 수행하는 방법을 보여줍니다. 각 시나리오에는 전체 소스 코드에 대한 링크가 포함되어 있습니다. 여기에서 코드를 설정 및 실행하는 방법에 대한 지침을 찾을 수 있습니다.

시나리오는 컨텍스트에 맞는 서비스 작업을 이해하는 데 도움이 되도록 중급 수준의 경험을 대상으로 합니다.

예시

- [AWS Compute Optimizer 자동화 기능이 권장 작업을 적용하도록 허용](#)
- [조직 전반의 자동화를 활성화하는 정책](#)
- [계정의 자동화를 활성화하는 정책](#)
- [조직의 관리 계정에 Compute Optimizer 자동화에 대한 전체 액세스 권한을 부여하기 위한 정책](#)
- [독립 실행형 AWS 계정에 대해 Compute Optimizer Automation에 대한 전체 액세스 권한을 부여하는 정책](#)
- [조직의 관리 계정에 Compute Optimizer 자동화에 대한 읽기 전용 액세스 권한을 부여하기 위한 정책](#)
- [독립 실행형 AWS 계정에 대해 Compute Optimizer Automation에 대한 읽기 전용 액세스 권한을 부여하는 정책](#)
- [컴퓨팅 최적화 자동화에 대한 서비스 연결 역할 권한을 부여하는 정책](#)

AWS Compute Optimizer 자동화 기능이 권장 작업을 적용하도록 허용

다음 코드 예제에서는이 권한 기반 정책을 통해 AWS Compute Optimizer 자동화 기능이 권장 작업을 적용하는 방법을 보여줍니다.

JSON

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

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 [섹션을 참조하세요](#) [AWS SDK for AWS Organizations](#) [에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

조직 전반의 자동화를 활성화하는 정책

다음 코드 예시에서는 이 권한 기반 정책이 어떻게 조직 전반의 자동화를 활성화하는지 보여줍니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/aco-automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation",
      "Condition": {"StringLike": {"iam:AWSServiceName": "aco-automation.amazonaws.com"}}
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PutRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/aco-automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation"
    },
    {
      "Effect": "Allow",
      "Action": "aco-automation:UpdateEnrollmentConfiguration",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "aco-automation:AssociateAccounts",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "aco-automation:DisassociateAccounts",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```

        "Action": "aco-automation:ListAccounts",
        "Resource": "*"
    }
]
}

```

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 [섹션을 참조하세요](#) [AWS SDK AWS Organizations](#) [에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

계정의 자동화를 활성화하는 정책

다음 코드 예시에서는 이 권한 기반 정책이 어떻게 계정의 자동화를 활성화하는지 보여줍니다.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/aco-automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation",
      "Condition": {"StringLike": {"iam:AWSServiceName": "aco-automation.amazonaws.com"}}
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PutRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/aco-automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation"
    },
    {
      "Effect": "Allow",
      "Action": "aco-automation:UpdateEnrollmentConfiguration",
      "Resource": "*"
    }
  ]
}

```

```
    ]
  }
}
```

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 [섹션을 참조하세요](#) [AWS SDK AWS Organizations](#) [에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

조직의 관리 계정에 Compute Optimizer 자동화에 대한 전체 액세스 권한을 부여하기 위한 정책

다음 코드 예시에서는 이 권한 기반 정책이 조직의 관리 계정의 Compute Optimizer 자동화에 대한 전체 액세스 권한을 부여하는 방법을 보여줍니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aco-automation:*",
        "ec2:DescribeVolumes",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations](#) 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

독립 실행형 AWS 계정에 대해 Compute Optimizer Automation에 대한 전체 액세스 권한을 부여하는 정책

다음 코드 예제에서는 이 권한 기반 정책이 독립 실행형 AWS 계정에 대한 Compute Optimizer Automation에 대한 전체 액세스 권한을 부여하는 방법을 보여줍니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aco-automation:*",
        "ec2:DescribeVolumes"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations](#) 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

조직의 관리 계정에 Compute Optimizer 자동화에 대한 읽기 전용 액세스 권한을 부여하기 위한 정책

다음 코드 예시에서는 이 권한 기반 정책이 조직의 관리 계정의 Compute Optimizer 자동화에 대한 읽기 전용 액세스 권한을 부여하는 방법을 보여줍니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aco-automation:GetEnrollmentConfiguration",
        "aco-automation:GetAutomationEvent",
        "aco-automation:GetAutomationRule",
        "aco-automation:ListAccounts",
        "aco-automation:ListAutomationEvents",
        "aco-automation:ListAutomationEventSteps",
        "aco-automation:ListAutomationEventSummaries",
        "aco-automation:ListAutomationRules",
        "aco-automation:ListAutomationRulePreview",
        "aco-automation:ListAutomationRulePreviewSummaries",
        "aco-automation:ListRecommendedActions",
        "aco-automation:ListRecommendedActionSummaries",
        "aco-automation:ListTagsForResource",
        "ec2:DescribeVolumes"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요 [AWS SDK AWS Organizations 에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

독립 실행형 AWS 계정에 대해 Compute Optimizer Automation에 대한 읽기 전용 액세스 권한을 부여하는 정책

다음 코드 예제에서는 이 권한 기반 정책이 독립 실행형 AWS 계정에 대한 Compute Optimizer Automation에 대한 읽기 전용 액세스 권한을 부여하는 방법을 보여줍니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aco-automation:GetEnrollmentConfiguration",
        "aco-automation:GetAutomationEvent",
        "aco-automation:GetAutomationRule",
        "aco-automation:ListAutomationEvents",
        "aco-automation:ListAutomationEventSteps",
        "aco-automation:ListAutomationEventSummaries",
        "aco-automation:ListAutomationRules",
        "aco-automation:ListAutomationRulePreview",
        "aco-automation:ListAutomationRulePreviewSummaries",
        "aco-automation:ListRecommendedActions",
        "aco-automation:ListRecommendedActionSummaries",
        "aco-automation:ListTagsForResource",
        "ec2:DescribeVolumes"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 [섹션을 참조하세요](#) [AWS SDK AWS Organizations](#) [에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

컴퓨팅 최적화 자동화에 대한 서비스 연결 역할 권한을 부여하는 정책

다음 코드 예시에서는 이 권한 기반 정책이 컴퓨팅 최적화 자동화에 대한 서비스 연결 역할 권한을 부여하는 방법을 보여줍니다.

JSON

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

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": "iam:CreateServiceLinkedRole",  
    "Resource": "arn:aws:iam::*:role/aws-service-role/aco-  
automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation",  
    "Condition": {"StringLike": {"iam:AWSServiceName": "aco-  
automation.amazonaws.com"}}  
  },  
  {  
    "Effect": "Allow",  
    "Action": "iam:PutRolePolicy",  
    "Resource": "arn:aws:iam::*:role/aws-service-role/aco-  
automation.amazonaws.com/AWSServiceRoleForComputeOptimizerAutomation"  
  }  
]  
}
```

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 [섹션을 참조하세요](#) [AWS SDK AWS Organizations](#) [에서 사용](#). 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

에 대한 문서 기록 AWS Organizations

다음 표에서는 본 AWS Organizations관련 주요 설명서 업데이트를 설명합니다.

- API 버전: 2016-11-28
- 최종 설명서 업데이트: 2026년 3월 30일

변경 사항	설명	날짜
계정 및 OU 객체에 경로 필드 추가	이제 계정 및 조직 단위(OU) 객체가 API 응답에 경로 정보를 포함합니다. 계정 APIs(예: DescribeAccount 및 ListAccounts) 및 OU APIs(예: DescribeOrganizationalUnit)는 조직 내에 엔터티가 있는 위치를 보여주는 경로 필드를 반환합니다.	2026년 3월 30일
RCPs에서 지원되는 새로운 서비스	RCPs.	2026년 1월 23일
새 모니터링 계정 상태 주제	콘솔, CLI 및 SDKs에서 AWS Organizations 를 사용하여 활성, 일시 중지 또는 종료와 같은 조직의 모든 계정에서 계정 상태를 중앙에서 모니터링하는 방법에 대한 지침이 추가되었습니다.	2025년 9월 9일
Security Hub 정책 추가	Security Hub 정책을 사용하여 에서 Security Hub 구성을 중앙에서 관리할 수 있습니다 AWS Organizations. 이러한 정책은 조직의 다중 계정에서 기능을	2025년 6월 17일

활성화하고 일관된 보안 제어를 유지하는 데 도움이 됩니다.

[AWSOrganizationsFullAccess](#) [관리형 정책을 업데이트했습니다](#)

조직 내 계정의 계정 이름을 볼 수 있는 액세스 권한을 활성화하는 `account:GetAccountInformation` 작업과 조직의 계정 이름을 수정할 수 있는 액세스 권한을 활성화하는 `account:PutAccountName` 작업이 추가되었습니다.

2025년 4월 22일

[와 Organizations 통합 AWS User Notifications](#)

사용자 알림 와 AWS Organizations 를 통합하여 조직의 여러 계정에서 알림을 중앙에서 구성하고 볼 수 있습니다.

2025년 1월 24일

[Organizations와 AWS Managed Services \(AMS\) Self-Service Reporting\(SSR\)의 통합](#)

AMS SSR을와 통합하여 집계 셀프 서비스 보고(SSR) AWS Organizations 를 활성화할 수 있습니다. 이는 Advanced 및 Accelerate 고객이 조직 수준, 교차 계정에서 집계된 기존 셀프 서비스 보고서를 보도록 AMS 기능입니다.

2025년 1월 21일

[선언적 정책 추가](#)

선언적 정책을 사용하여 조직 전체에서 지정된에 대해 원하는 구성을 중앙 AWS 서비스 에서 선언하고 적용할 수 있습니다. 연결되면 서비스가 새 기능 또는 API를 추가할 때 구성이 항상 유지됩니다.

2024년 12월 1일

새로운 AWS 관리형 정책

declarative-policies-ec2.amazonaws.com 서비스 링크 역할의 기능을 활성화하는 DeclarativePoliciesEC2Report 정책을 추가했습니다.

2024년 11월 22일

백업 정책 업데이트

AWS Backup 정책이 selections 정책 키를 포함하도록 conditions 정책 키를 업데이트하고 스키마에 새 resources 정책 키를 추가했습니다. 새 스키마를 사용하면 백업 정책에 대한 리소스 선택의 유연성을 높일 수 있습니다.

2024년 11월 14일

중앙에서 멤버 계정에 대한 루트 액세스 관리

이제 중앙 집중식 루트 액세스를 통해 AWS Organizations의 멤버 계정 전체에서 권한 있는 루트 사용자 자격 증명을 관리할 수 있습니다. 를 사용하여 AWS 계정 관리형의 루트 사용자 자격 증명을 중앙에서 보호 AWS Organizations 하여 루트 사용자 자격 증명 복구 및 대규모 액세스를 방지하세요.

2024년 11월 14일

리소스 제어 정책(RCP) 추가

리소스 제어 정책(RCP)은 조직의 리소스에 사용할 수 있는 최대 권한을 정의합니다.

2024년 11월 13일

채팅 애플리케이션 정책 추가

채팅 정책을 사용하여 Slack 및 Microsoft Teams와 같은 채팅 애플리케이션에서 조직의 계정에 대한 액세스를 제어할 수 있습니다.

2024년 9월 26일

[시나리오 기반 콘텐츠 업데이트](#)

AWS Organizations 설명서는 전체 가이드에서 시나리오를 중심으로 업데이트되었으며 가독성과 검색을 개선하기 위해 내용이 재구성되었습니다. 이러한 변경 사항에 대한 피드백이 있는 경우 페이지 하단의 피드백 제공 버튼을 사용하세요.

2024년 9월 4일

[새로운 모든 AI 서비스 주제 옅트아웃](#)

지원되는 모든 AWS AI 서비스를 옅트아웃하는 방법에 대한 설명서가 추가되었습니다.

2024년 8월 16일

[이제 Organizations가 조직 내에서 10,000개의 계정 지원](#)

이제 조직 내에서 이전 한도인 5,000개의 계정에서 두 배로 늘어난 최대 10,000개의 멤버 계정을 관리할 수 있습니다. 유효한 요구 사항과 비즈니스 요구 사항이 있는 경우 Organizations 또는 기타 통합 AWS 서비스의 서비스 한도 확인 없이 10,000개의 계정 할당량을 요청하고 승인받을 수 있습니다.

2024년 8월 14일

[새 계정 마이그레이션 주제](#)

한 조직에서 다른 조직으로 계정을 마이그레이션하는 방법에 대한 설명서가 추가되었습니다.

2024년 8월 1일

[백업 정책 업데이트](#)

AWS Backup 이제 정책은 Amazon Elastic Block Store(Amazon EBS) 스냅샷 아카이브를 지원합니다. 업데이트된 예제는 [백업 정책 업데이트](#) 및 [백업 정책 구문 및 예제](#)를 참조하세요.

2024년 7월 9일

[AWSOrganizationsReadOnlyAccess 관리형 정책 업데이트](#)

AWSOrganizationsReadOnlyAccess 정책에 조직 내 멤버 계정에 대한 루트 사용자 이메일 주소를 볼 수 있는 액세스 권한을 활성화하는 `account:GetPrimaryEmail` 작업과 조직 내 멤버 계정에 대해 활성화된 리전을 볼 수 있는 액세스 권한을 활성화하는 `account:GetRegionOptStatus` 작업이 추가되었습니다.

2024년 6월 6일

[루트 사용자 이메일 주소 주제 새 업데이트](#)

조직은 이제 모든 구성원 계정에 대한 루트 사용자 이메일 주소를 중앙에서 업데이트하는 기능을 제공합니다.

2024년 6월 6일

[정책 설명 업데이트](#)

AWS Organizations 관리형 정책 문서에 새 Sid 요소를 추가했습니다.

2024년 2월 6일

[새 관리 계정 해지 주제](#)

관리 계정을 해지하는 방법을 안내하는 고려 사항 및 자세한 단계에 대한 링크가 추가되었습니다.

2024년 2월 1일

[추가된 모범 사례](#)

IAM 모범 사례에 부합할 수 있도록 유용하고 새로운 정보가 모범 사례 섹션에 추가되었습니다.

2023년 6월 12일

[AWSOrganizationsFullAccess 및 AWSOrganizationsReadOnlyAccess 관리형 정책을 업데이트했습니다](#)

두 관리형 정책 모두 계정의 연락처에 대한 쓰기 또는 읽기 액세스를 허용하도록 업데이트되었습니다.

2022년 10월 21일

[AWSOrganizationsFullAccess](#) [관리형 정책을 업데이트했습니다](#)

새 조직에 필요한 서비스 연결 역할을 만드는 데 필요한 권한을 추가하여 조직을 만들 수 있도록 관리형 정책이 업데이트되었습니다.

2022년 8월 24일

[AWS Organizations 콘솔에서](#) [조직 계정 기능 닫기](#)

관리 계정의 보안 주체는 AWS Organizations 콘솔을 통해 멤버 계정을 해지하고 IAM 정책을 사용하여 실수로 해지되지 않도록 멤버 계정을 보호합니다.

2022년 3월 29일

[AWS Organizations 콘솔을 사](#) [용하여 대체 연락처를 업데이](#) [트하도록 공지 업데이트](#)

이제 Organizations는 AWS Organizations 콘솔을 사용하여 조직 내 계정의 대체 연락처를 업데이트할 수 있는 기능을 제공합니다. 새로운 기능을 발표하고 지침으로 계정 관리 참조를 제공하십시오.

2022년 2월 8일

[Organizations 관리형 정책 업](#) [데이트 - 기존 정책에 대한 업데](#) [이트](#)

AWS Organizations 콘솔을 통해 계정 대체 연락처를 업데이트하거나 보는 데 필요한 계정 API 권한을 허용하도록 AWSOrganizationsFullAccess 및 AWSOrganizationsReadOnlyAccess 관리형 정책을 업데이트했습니다.

2022년 2월 7일

[Organizations와 Amazon](#) [DevOps Guru 통합](#)

Amazon DevOps Guru AWS Organizations 를와 통합하여 모든 조직 계정에서 애플리케이션 상태를 전체적으로 모니터링하고 인사이트를 얻을 수 있습니다.

2022년 1월 3일

Organizations와 Amazon Detective 통합

Amazon Detective AWS Organizations 를와 통합하여 Detective 동작 그래프가 모든 조직 계정의 활동에 대한 가시성을 제공하도록 할 수 있습니다.

2021년 12월 16일

와의 조직 통합은 AWS Config 이제 다중 계정 다중 리전 데이터 집계를 지원합니다.

위임된 관리자 계정을 사용하여 조직 내 모든 멤버 계정의 리소스 구성 및 규정 준수 데이터를 집계할 수 있습니다. 자세한 내용은 AWS Config 개발자 안내서에서 [다중 계정 다중 리전 데이터 집계](#)를 참조하세요.

2021년 6월 16일

AWS Firewall Manager 이제와의 조직 통합에 위임된 관리자에 대한 지원이 포함됩니다.

이제 조직의 멤버 계정을 전체 조직의 Firewall Manager 관리자로 지정할 수 있습니다. 이를 통해 조직의 관리 계정으로부터 권한을 더 잘 분리할 수 있습니다.

2021년 4월 30일

Organizations 백업 정책이 이제 연속 백업을 지원합니다

조직의 백업 정책과 함께 AWS Backup 연속 백업 기능을 사용할 수 있습니다.

2021년 3월 10일

이제 Organizations와 AWS CloudFormation StackSets 통합에 위임된 관리자에 대한 지원이 포함됩니다.

이제 조직의 멤버 계정을 전체 조직의 CloudFormation StackSets 관리자로 지정할 수 있습니다. 이를 통해 조직의 관리 계정으로부터 권한을 더 잘 분리할 수 있습니다.

2021년 2월 18일

[모든 기능을 활성화하는 동안 계정 계속 초대](#)

AWS 는 조직의 모든 기능을 활성화하도록 프로세스를 업데이트했습니다. 이제 기존 계정이 초대장에 응답할 때까지 기다리는 동안 조직에 가입할 새 계정을 계속 초대할 수 있습니다.

2021년 2월 3일

[AWS Organizations 콘솔 버전 2.0 도입](#)

AWS 는 AWS 콘솔의 새 버전을 도입했습니다. 새 작업 수행 방법을 반영하도록 모든 설명서를 업데이트했습니다.

2021년 1월 21일

[이제 Organizations는 와의 통합을 지원합니다. AWS Marketplace](#)

이제 AWS Marketplace 를 활성화하여 조직의 모든 계정에서 소프트웨어 라이선스를 보다 쉽게 공유할 수 있습니다.

2020년 12월 3일

[이제 Organizations에서 Amazon S3 Lens와의 통합을 지원](#)

Amazon S3 Lens는 Organizations에서 신뢰할 수 있는 액세스와 위임된 관리자를 지원합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [Amazon S3 Storage Lens](#)를 참조하세요.

2020년 11월 18일

[교차 계정 백업 복사본](#)

백업 정책을 사용하여 조직의 리소스를 백업하는 경우 이제 백업 사본을 AWS 계정 조직의 다른에 저장할 수 있습니다.

2020년 11월 18일

[AWS 리전 중국에서 이제 Organizations 신뢰할 수 AWS Resource Access Manager 있 는 서비스로 지원](#)

이제 중국 AWS RAM 에서 Organizations 및를 사용할 때 Organizations와 통합되는 AWS RAM 기능을 신뢰할 수 있는 서비스로 사용할 수 있습니다.

2020년 11월 18일

[이제 Organizations는 와의 통합을 지원합니다. AWS Security Hub CSPM](#)

조직의 모든 계정에서 Security Hub CSPM을 활성화하고 조직의 멤버 계정 중 하나를 Security Hub CSPM의 위임된 관리자 계정으로 지정할 수 있습니다.

2020년 11월 12일

[마스터 계정의 이름이 변경됨](#)

AWS Organizations 에서 “마스터 계정”의 이름을 “관리 계정”으로 변경했습니다. 이름만 변경되었을 뿐 기능은 바뀌지 않았습니다.

2020년 10월 20일

[새로운 모범 사례 단원 및 주제](#)

AWS Organizations의 모범 사례에 대한 새로운 단원을 추가했습니다. 새 단원에는 관리 계정/멤버 계정 루트 사용자 및 암호 관리에 대한 모범 사례를 설명하는 주제가 포함되었습니다.

2020년 10월 6일

[새로운 모범 사례 단원과 처음 두 페이지 추가됨](#)

AWS Organizations의 모범 사례를 설명하는 주제를 위한 새로운 단원이 생겼습니다. 이 업데이트에는 조직의 관리 계정의 모범 사례에 대한 주제와, 멤버 계정의 모범 사례에 대한 주제가 포함되었습니다.

2020년 10월 2일

[Organizations 백업 정책이 이제 Windows EC2 인스턴스에 VSS\(Volume Shadow Copy Service\)를 사용한 애플리케이션 일관성 보장 백업을 지원합니다.](#)

백업 정책에서 새로운 advanced_backup_settings " 섹션이 지원됩니다. 새로운 이 섹션의 첫 번째 항목은 WindowsVSS 라는 ec2 설정이며, 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 AWS Backup 개발자 안내서의 [VSS 지원 Windows 백업 생성](#)을 참조하세요.

2020년 9월 24일

[Organizations에서 생성 시점 태그\(tag-on-create\) 및 태그 기반\(tag-based\) 액세스 제어 지원](#)

Organizations 리소스를 만들 때 태그를 해당 리소스에 추가할 수 있습니다. [태그 정책](#)을 사용하여 Organizations 리소스에 대한 태그 사용을 표준화할 수 있습니다. [태그 키 및 값을 지정한 리소스로만 액세스를 제한하는 IAM 정책](#)을 사용할 수 있습니다.

2020년 9월 15일

[신뢰할 수 있는 AWS Health 있는 서비스로 추가됨](#)

조직의 계정 간에 AWS Health 이벤트를 집계할 수 있습니다.

2020년 8월 4일

[인공 지능\(AI\) 서비스 옵트아웃 정책](#)

AI 서비스 옵트아웃 정책을 사용하여 AWS AI 서비스가 AI 서비스 및 기술의 개발 및 지속적인 개선을 위해 해당 서비스에서 처리한 고객 콘텐츠(AI 콘텐츠)를 저장 AWS 하고 사용할 수 있는지 여부를 제어할 수 있습니다.

2020년 7월 8일

[백업 정책 및 와의 통합 추가 AWS Backup](#)

백업 정책을 사용하여 조직 내 모든 계정에서 백업 정책을 만들고 적용할 수 있습니다.

2020년 6월 24일

<u>IAM Access Analyzer의 위임된 관리를 지원합니다</u>	조직의 액세스 분석기에 대한 관리 액세스를 지정된 멤버 계정에 위임할 수 있습니다.	2020년 3월 30일
<u>CloudFormation StackSets와 통합</u>	서비스 관리형 스택 세트를 생성하여 AWS Organizations에서 관리되는 계정에 스택 인스턴스를 배포할 수 있습니다.	2020년 2월 11일
<u>Compute Optimizer와의 통합</u>	Compute Optimizer가 조직 내 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2020년 2월 4일
<u>- 태그 정책</u>	태그 정책을 사용하여 조직의 계정에 있는 리소스 전체에서 태그를 표준화할 수 있습니다.	2019년 11월 26일
<u>Systems Manager와의 통합</u>	Systems Manager Explorer AWS 계정에서 조직의 모든에서 작업 데이터를 동기화할 수 있습니다.	2019년 11월 26일
<u>aws:PrincipalOrgPaths</u>	새 전역 조건 키는 요청을 수행하는 IAM 사용자, IAM 역할 또는 AWS 계정 루트 사용자의 AWS Organizations 경로를 확인합니다.	2019년 11월 20일
<u>AWS Config 규칙과 통합</u>	AWS Config API 작업을 사용하여 조직의 모든 AWS 계정에 AWS Config 규칙을 관리할 수 있습니다.	2019년 7월 8일
<u>신뢰할 수 있는 액세스를 위한 새로운 서비스</u>	Service Quotas가 사용자 조직 내 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2019년 6월 24일

<u>AWS Control Tower와 통합</u>	AWS Control Tower가 조직의 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2019년 6월 24일
<u>와 통합 AWS Identity and Access Management</u>	IAM은 조직의 엔터티(조직 루트, OU 및 계정)에 대해 마지막으로 액세스한 데이터를 서비스에 제공합니다. 이 데이터를 사용하여 필요한 로만 액세스를 제한할 수 AWS 서비스 있습니다.	2019년 6월 20일
<u>계정 태그 지정</u>	조직의 계정에 태그를 지정 및 지정 취소하여 조직의 계정에 지정된 태그를 볼 수 있습니다.	2019년 6월 6일
<u>서비스 제어 정책(SCP)의 리소스, 조건 및 NotAction 요소</u>	이제 SCP에서 리소스, 조건 및 <u>NotAction</u> 요소를 지정하여 조직 또는 조직 단위(OU)의 계정 전체에서 액세스를 거부할 수 있습니다.	2019년 3월 25일
<u>신뢰할 수 있는 액세스를 위한 새로운 서비스</u>	AWS License Manager 및 Service Catalog가 조직의 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2018년 12월 21일
<u>신뢰할 수 있는 액세스를 위한 새로운 서비스</u>	AWS CloudTrail 및가 조직의 계정으로 작업할 수 있는 서비스로 AWS RAM 추가되었습니다.	2018년 12월 4일
<u>신뢰할 수 있는 액세스를 위한 새로운 서비스</u>	Directory Service 가 조직의 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2018년 9월 25일

<u>이메일 주소 확인</u>	기존 계정을 조직에 초대하려면 먼저 관리 계정과 연결된 이메일 주소의 소유자임을 입증해야 합니다.	2018년 9월 20일
<u>CreateAccount 알림</u>	CreateAccount 알림이 관리 계정의 CloudTrail 로그에 게시됩니다.	2018년 6월 28일
<u>신뢰할 수 있는 액세스를 위한 새로운 서비스</u>	AWS Artifact가 조직의 계정으로 작업할 수 있는 서비스로 추가되었습니다.	2018년 6월 20일
<u>신뢰할 수 있는 액세스를 위한 새로운 서비스</u>	AWS Config 및가 조직의 계정으로 작업할 수 있는 서비스로 AWS Firewall Manager 추가되었습니다.	2018년 4월 18일
<u>신뢰할 수 있는 서비스 액세스</u>	이제 조직의 계정에서 작동 AWS 서비스 하도록 선택에 대한 액세스를 활성화하거나 비활성화할 수 있습니다. IAM Identity Center는 일차적으로 지원되는 신뢰할 수 있는 서비스입니다.	2018년 3월 29일
<u>계정 제거가 이제는 셀프 서비스</u>	이제 연락 AWS Organizations 없이 내에서 생성된 계정을 제거할 수 있습니다 AWS Support.	2017년 12월 19일
<u>새 서비스에 대한 지원 추가 AWS IAM Identity Center</u>	AWS Organizations는 이제 AWS IAM Identity Center (IAM Identity Center)와의 통합을 지원합니다.	2017년 12월 7일

[AWS 모든 조직 계정에 서비스 연결 역할 추가](#)

라는 서비스 연결 역할(AWSServiceRoleForOrganizations)이 조직의 모든 계정에 추가되어 AWS Organizations와 다른 간의 통합을 활성화합니다 AWS 서비스.

2017년 10월 11일

[이제 생성된 계정 제거 가능](#)

고객은 이제 AWS Support의 도움을 통해 조직에서 생성된 계정을 제거할 수 있습니다.

2017년 6월 15일

[서비스 시작](#)

새 서비스 출시와 함께 제공된 AWS Organizations 설명서의 초기 버전입니다.

2017년 2월 17일

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