사용자 가이드

AWS IAM Identity Center

AWS IAM Identity Center: 사용자 가이드

Table of Contents

IAM Identity Center란 무엇인가요? 1
IAM Identity Center 기능 1
IAM Identity Center 이름 변경 3
기존 네임스페이스는 동일하게 유지 4
IAM Identity Center 활성화 5
필수 조건 및 고려 사항 7
선택 시 고려 사항 AWS 리전 7
IAM ID 센터에서 생성한 IAM 역할의 할당량 9
IAM 아이덴티티 센터 및 AWS Organizations 9
IAM ID 센터에서 ID 소스를 확인하십시오. 10
시작하기 튜토리얼 13
Identity Center 디렉터리 13
Active Directory 19
CyberArk 21
필수 조건 22
SCIM 고려 사항 22
1단계: IAM Identity Center 프로비저닝 활성화 23
2단계: CyberArk에서 프로비저닝 구성 23
(선택 사항) 3단계: IAM Identity Center에서 액세스 제어(ABAC)에 사용되는 CyberArk 사용자 속성 구성 24
(선택 사항) 액세스 제어에 속성 전달 25
Google Workspace 25
JumpCloud 34
사전 조건 35
SCIM 고려 사항 36
1단계: IAM Identity Center 프로비저닝 활성화 36
2단계: JumpCloud에서 프로비저닝 구성 37
(선택 사항) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 JumpCloud 사용자 속성 구성 37
(선택 사항) 액세스 제어에 속성 전달 38
Microsoft Entra ID 39
Okta 54
OneLogin 63
사전 조건 63

1단계: IAM Identity Center 프로비저닝 활성화 64
2단계: OneLogin에서 프로비저닝 구성 64
(선택 사항) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 OneLogin 사용자 속성 구성 65
(선택 사항) 액세스 제어에 속성 전달 66
문제 해결 67
Ping Identity 68
PingFederate 68
PingOne 74
일반적인 작업 79
권한 집합을 생성합니다. 80
최소 권한을 적용하는 권한 세트 생성 81
사용자 액세스 할당 82
AWS 액세스 포털에 로그인 84
그룹 액세스 할당 85
애플리케이션에 대한 액세스 설정 87
사용자 및 그룹 할당 보기 90
관리형 인스턴스 92
IAM Identity Center의 조직 인스턴스 관리 94
조직 인스턴스를 사용하는 경우 94
IAM Identity Center의 계정 인스턴스 94
구성원 계정의 가용성 제한 95
계정 인스턴스를 사용하는 경우 95
계정 인스턴스 고려 사항 96
지원되는 AWS 관리형 애플리케이션 96
계정 인스턴스 활성화 96
계정 인스턴스 생성 제어 97
계정 인스턴스 생성 98
인증 100
인증 세션 100
..... 101
직원 ID 관리 102
사용 사례 102
AWS 애플리케이션에 대한 Single Sign-on 액세스 활성화 102
Amazon EC2 Windows 인스턴스에 대한 Single Sign-On 액세스 활성화 104
사용자, 그룹 및 프로비저닝 104

사용자 이름 및 이메일 주소 고유성 104
그룹 105
사용자 및 그룹 프로비저닝 105
ID 소스 관리 105
ID 소스 변경 시 고려 사항 106
ID 소스 변경 109
모든 ID 소스 유형에 대한 로그인 및 속성 사용 관리 110
IAM Identity Center에서 ID 관리 115
Microsoft AD 디렉터리에 연결 125
외부 ID 제공업체에 연결 146
AWS 액세스 포털 사용 157
IAM Identity Center 가입 초대 수락 158
AWS 액세스 포털에 로그인 159
사용자 암호 재설정 160
AWS CLI 및 SDK 액세스 AWS 161
바로가기 링크 생성 166
디바이스에 MFA 등록 168
AWS 액세스 포털 URL 사용자 지정 170
다중 인증 171
사용 가능한 MFA 유형 172
MFA 구성 175
MFA 관리 181
액세스 관리 AWS 계정 184
AWS 계정 유형 184
액세스 권한 할당 AWS 계정 186
최종 사용자 경험 187
액세스 적용 및 제한 187
액세스 위임 및 적용 188
멤버 계정에서 ID 스토어에 액세스하는 것을 제한합니다. 188
위임된 관리 189
모범 사례 189
필수 조건 190
멤버 계정 등록 190
멤버 계정 해지 191
위임된 관리자로 등록된 멤버 계정을 볼 수 있습니다. 192
임시 권한 상승 192

임시 권한 승격에 대한 검증된 보안 파트너 AWS 193
파트너 검증을 위해 일시적으로 상승된 액세스 기능을 평가했습니다. AWS 194
싱글 사인온 액세스: AWS 계정 195
사용자에게 액세스 권한을 할당하십시오. AWS 계정 195
사용자 및 그룹 액세스 제거 197
활성 권한 집합 세션 취소 198
관리 계정의 사용자 및 그룹에 Single Sign-On 액세스 권한을 할당할 수 있는 사람을 위임합니다. 199
권한 세트 200
사전 정의된 권한 201
사용자 지정 권한 202
권한 세트 생성, 관리 및 삭제 204
권한 집합 속성을 구성합니다. 211
리소스 정책, Amazon EKS의 권한 집합 참조 및 AWS KMS 217
액세스 중단 방지를 위한 권장 사항 218
사용자 지정 신뢰 정책 예 219
속성 기반 액세스 제어 220
이점 221
체크리스트: IAM ID 센터를 사용하여 ABAC 구성 AWS 221
액세스 제어를 위한 속성 223
IAM ID 제공업체 229
IAM ID 제공업체 복구 229
서비스 연결 역할 230
애플리케이션 액세스 관리 231
AWS 관리형 애플리케이션 231
액세스 제어 237
관리 작업 조정 237
ID 정보를 공유하도록 IAM Identity Center 구성 237
ID 정보 공유에 대한 고려 사항 AWS 계정 238
ID 인식 콘솔 세션 활성화 238
관리형 애플리케이션 사용 제한 AWS 241
애플리케이션 세부 정보 보기 241
관리형 AWS 애플리케이션 비활성화 242
고객 관리형 애플리케이션 243
SAML 2.0 및 OAuth 2.0 243
SAML 2.0 애플리케이션 설정 247

신뢰할 수 있는 ID 전파 251
개요 251
사용 사례 252
신뢰할 수 있는 ID 전파 설정 258
신뢰할 수 있는 토큰 발급자 272
인증서 관리 284
인증서 교체 전 고려 사항 284
IAM Identity Center 인증서 교체 284
인증서 만료 상태 표시 287
애플리케이션 속성 구성 287
애플리케이션 시작 URL 287
릴레이 상태 288
세션 지속 시간 289
애플리케이션에 사용자 액세스 권한 할당 289
사용자 액세스 제거 290
속성 매핑 291
복원력 설계 및 리전 동작 292
AWS Management Console에 대한 비상 액세스를 설정합니다. 292
개요 292
비상 액세스 구성 요약 294
중요 운영 역할을 설계하는 방법 294
액세스 모델을 계획하는 방법 295
비상 역할, 계정 및 그룹 매핑을 설계하는 방법 296
비상 액세스 구성을 만드는 방법 296
비상 상황 대비 작업 298
비상 장애 조치 프로세스 298
정상 작동 상태로 복귀합니다. 298
Okta에서 직접 IAM 페더레이션 애플리케이션을 한 번만 설정하면 됩니다. 299
보안 302
IAM Identity Center ID 및 액세스 관리 303
인증 303
액세스 제어 303
액세스 관리 개요 304
자격 증명 기반 정책(IAM 정책) 307
AWS 관리형 정책 315
서비스 링크 역할 사용 330

IAM Identity Center 콘솔 및 API 인증 337
2023년 11월 이후의 API 작업 338
2020년 10월 이후의 API 작업 339
AWS STS IAM 아이덴티티 센터의 조건 키 340
UserId 341
IdentityStoreArn 342
ApplicationArn 342
CredentialId 342
InstanceArn 343
로깅 및 모니터링 343
IAM ID 센터 API 호출을 다음과 같이 로깅합니다. AWS CloudTrail 343
아마존 EventBridge 368
AD 동기화 및 구성 가능한 AD 동기화 오류 로깅 368
규정 준수 확인 371
지원되는 규정 준수 표준 372
복원력 374
인프라 보안 374
리소스에 태그 지정 376
태그 제한 376
콘솔을 사용하여 태그 관리 377
AWS CLI 예제 378
태그 할당 378
태그 보기 378
태그 제거 379
권한 세트를 생성할 때 태그 적용 379
API 작업 379
IAM Identity Center 인스턴스 태그에 대한 API 작업 379
AWS CLI와 IAM Identity Center 통합 381
AWS CLI와 IAM Identity Center 통합 방법 381
리전 가용성 382
IAM Identity Center 리전 데이터 382
크로스 리전 호출 382
옵트인 지역 (기본적으로 비활성화된 지역) 에서 IAM ID 센터 관리 383
IAM Identity Center 구성 삭제 385
할당량 387
애플리케이션 할당량 387

AWS 계정 할당량 387
Active Directory 할당량 388
IAM Identity Center ID 스토어 할당량 389
IAM Identity Center 스로틀 제한 389
추가 할당량 389
문제 해결 391
IAM Identity Center의 계정 인스턴스 생성 문제 391
IAM Identity Center에서 사용하도록 사전 구성된 클라우드 애플리케이션 목록을 보려고 하면 오류가 발생합니다. 391
IAM Identity Center에서 생성된 SAML 어설션 콘텐츠 관련 문제 392
특정 사용자가 외부 SCIM 공급자로부터 IAM Identity Center로 동기화하지 못함 393
사용자 이름이 UPN 형식인 경우 사용자는 로그인할 수 없습니다. 394
IAM 역할을 수정할 때 '보호된 역할에서 작업을 수행할 수 없습니다' 오류가 발생합니다. 395
디렉터리 사용자는 비밀번호를 재설정할 수 없습니다. 395
내 사용자는 권한 집합에서 참조할 수 있지만 할당된 계정이나 애플리케이션에 액세스할 수 없습니다. 396
애플리케이션 카탈로그에서 애플리케이션을 올바르게 구성할 수 없음 396
사용자가 외부 ID 공급업체를 통해 로그인하려고 할 때 “예기치 않은 오류가 발생했습니다” 오류가 표시됩니다. 396
'액세스 제어 속성을 활성화하지 못했습니다' 오류 397
MFA에 디바이스를 등록하려고 할 때 '브라우저가 지원되지 않습니다' 메시지가 표시됩니다. 398
Active Directory “도메인 사용자” 그룹이 IAM Identity Center에 제대로 동기화되지 않습니다. 398
잘못된 MFA 보안 인증 오류 398
인증 앱으로 등록하거나 로그인하려고 시도하면 '예상치 못한 오류가 발생했습니다'라는 메시지가 나타납니다. 398
IAM ID 센터에 로그인하려고 하면 '당신이 아니에요, 우리예요. '라는 오류 메시지가 나타납니다. 399
내 사용자가 IAM Identity Center로부터 이메일을 받지 못하고 있습니다. 399
오류: 관리 계정에 프로비저닝된 권한 집합에 대한 액세스 권한을 삭제/수정/제거/할당할 수 없습니다. 399
오류: 세션 토큰을 찾을 수 없거나 유효하지 않습니다. 400
사용 설명서 기록 401
AWS 용어집 407
..... cdviii

IAM Identity Center란 무엇인가요?

AWS IAM Identity Center AWS 리소스에 AWS 서비스 대한 사용자 액세스를 관리하는 데 권장됩니다. 한 곳에서 직원 사용자(workforce identities), 여러 AWS 계정 및 애플리케이션에 대한 일관적인 액세스를 할당할 수 있습니다. IAM 아이덴티티 센터는 추가 비용 없이 제공됩니다.

IAM Identity Center를 사용하면 인력 사용자를 생성하거나 연결하고 모든 직원 및 애플리케이션에서 직원 액세스를 중앙에서 관리할 수 있습니다 AWS 계정 . 다중 계정 권한을 사용하여 작업 인력 사용자에게 AWS 계정액세스 권한을 할당할 수 있습니다. 애플리케이션 할당을 사용하여 AWS 관리형 및 고객 관리형 애플리케이션에 대한 액세스 권한을 사용자에게 할당할 수 있습니다.

> **Note**
>
> Single AWS Sign-On이라는 서비스 이름은 더 이상 사용되지 않지만 이 안내서에서는 사용자가 한 번에 로그인하여 여러 애플리케이션 및 웹 사이트에 액세스할 수 있도록 하는 인증 체계를 설명하기 위해 여전히 Single Sign-On이라는 용어를 사용하고 있습니다.

IAM Identity Center 기능

IAM Identity Center에는 다음과 같은 핵심 기능이 포함되어 있습니다.

직원 ID 관리

워크로드를 구축하거나 운영하는 휴먼 사용자를 워크포스 사용자 또는 워크포스 ID라고도 합니다. AWS 인력 사용자는 조직 및 내부 비즈니스 AWS 계정 애플리케이션에서 액세스를 허용하는 직원 또는 계약직입니다. 이러한 개인은 내부 및 고객 대상 시스템을 구축하는 개발자나 내부 데이터베이스 시스템 및 애플리케이션 사용자가 될 수 있습니다. IAM Identity Center에서 인력 사용자 및 그룹을 생성하거나 자체 ID 소스의 기존 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 AWS 계정 및 애플리케이션에서 사용할 수 있습니다. 자세한 정보는 ID 소스 관리을 참조하세요.

IAM Identity Center의 인스턴스 관리

IAM Identity Center는 조직 인스턴스와 계정 인스턴스라는 두 가지 유형의 인스턴스를 지원합니다. 조직 인스턴스가 모범 사례입니다. 액세스를 관리할 수 있는 유일한 AWS 계정 인스턴스이며 모든 프로덕션 애플리케이션 사용에 권장됩니다. 조직 인스턴스는 AWS Organizations 관리 계정에 배포되며 AWS 환경 전반의 사용자 액세스를 관리할 수 있는 단일 지점을 제공합니다.

계정 인스턴스는 해당 인스턴스가 활성화된 위치에 바인딩됩니다. AWS 계정 IAM Identity Center의 계정 인스턴스는 AWS 엄선된 관리형 애플리케이션의 격리된 배포를 지원하는 용도로만 사용하십시오. 자세한 정보는 IAM Identity Center의 조직 및 계정 인스턴스 관리을 참조하세요.

여러 곳에 대한 액세스를 관리합니다. AWS 계정

다중 계정 권한을 사용하면 각 계정을 수동으로 구성할 필요 없이 한 AWS 계정 번에 여러 계정에 대한 권한을 계획하고 중앙에서 구현할 수 있습니다. 일반적인 직무를 기반으로 권한을 생성하거나 보안 요구 사항에 맞는 사용자 지정 권한을 정의할 수 있습니다. 그런 다음 작업 인력 사용자에게 해당 권한을 할당하여 특정 계정에 대한 액세스를 제어할 수 있습니다.

이 선택적 기능은 조직 인스턴스에만 사용할 수 있습니다. 환경에서 계정별 IAM 역할 관리를 사용하는 경우 두 시스템이 공존할 수 있습니다. 다중 계정 권한을 시도하려는 경우 먼저 이 시스템을 제한적으로 구현하고 시간이 지남에 따라 사용할 환경을 추가로 마이그레이션할 수 있습니다.

애플리케이션 액세스 관리

IAM Identity Center를 사용하면 애플리케이션 액세스 관리를 간소화할 수 있습니다. IAM Identity Center를 사용하면 IAM Identity Center의 직원 사용자에게 애플리케이션에 대한 Single Sign-On 액세스 권한을 부여할 수 있습니다.

AWS 관리형 애플리케이션

AWS 는 Amazon Managed Grafana Amazon Redshift, Amazon Monitron과 같이 IAM 아이덴티티 센터와 통합되는 애플리케이션을 제공합니다. 이러한 애플리케이션은 인증, 디렉터리 서비스 및 신뢰할 수 있는 ID 전파에 IAM Identity Center를 사용할 수 있습니다. 사용자는 일관적인 Single Sign-On 환경으로부터 이점을 얻게 되고, 애플리케이션은 사용자, 그룹 및 그룹 구성원에 대한 공통된 관점을 공유하므로 사용자는 다른 사람과 애플리케이션 리소스를 공유할 때도 일관된 경험을 할 수 있습니다. 관련 애플리케이션 콘솔 내에서 직접 또는 API를 통해 IAM Identity Center와 작동하도록 AWS 관리형 애플리케이션을 구성할 수 있습니다.

고객 관리형 애플리케이션

IAM Identity Center의 직원 사용자에게 SAML 2.0과의 ID 페더레이션을 지원하는 애플리케이션에 대한 Single Sign-On 액세스 권한을 부여할 수 있습니다. Salesforce 및 Microsoft 365와 같이 일반적으로 사용되는 많은 SAML 2.0 애플리케이션은 IAM Identity Center와 호환되고 IAM Identity Center 콘솔의 애플리케이션 카탈로그에서 사용할 수 있습니다. 이는 이러한 애플리케이션을 사용하고 IAM Identity Center에서 사용자 및 그룹을 생성하거나 Microsoft Active Directory 도메인 서비스를 ID 소스로 사용하는 경우 유용할 수 있는 선택적 기능입니다.

애플리케이션 간 신뢰할 수 있는 ID 전파

신뢰할 수 있는 ID 전파는 서비스의 데이터에 액세스해야 하는 쿼리 도구 및 BI (비즈니스 인텔리전스) 애플리케이션 사용자에게 간소화된 싱글 사인온 경험을 제공합니다. AWS 데이터 액세스 관리는 사용자 ID를 기반으로 하므로 관리자는 사용자의 기존 사용자 및 그룹 구성원 자격을 기반으로 액세스 권한을 부여할 수 있습니다. AWS 서비스 및 기타 이벤트에 대한 사용자 액세스는 서비스별 로그와 CloudTrail 이벤트에 기록되므로 감사자는 사용자가 어떤 작업을 수행했고 어떤 리소스에 액세스했는지 알 수 있습니다.

AWS 사용자의 포털 액세스에 액세스할 수 있습니다.

AWS 액세스 포털은 사용자가 할당된 모든 애플리케이션 AWS 계정 및 애플리케이션에 원활하게 액세스할 수 있도록 하는 간단한 웹 포털입니다.

IAM Identity Center 이름 변경

2022년 7월 26일에 AWS 싱글 사인온의 이름이 로 변경되었습니다. AWS IAM Identity Center기존 고객의 경우 다음 표를 통해 이름 변경으로 인해 이 안내서 전체에서 업데이트된 일반적인 용어 변경 사항 중 일부를 확인할 수 있습니다.

기존 용어	최신 용어
AWS SSO 사용자 또는 SSO 사용자	작업 인력 사용자 또는 사용자
AWS SSO 사용자 포털 또는 사용자 포털	AWS 액세스 포털
AWS SSO 통합 애플리케이션	AWS 관리형 애플리케이션
AWS SSO 디렉터리	Identity Center 디렉터리
AWS SSO 스토어 또는 AWS SSO 아이덴티티 스토어	IAM Identity Center에서 사용된 ID 스토어

다음 표에는 이 이름 변경으로 인해 발생한 해당 사용자, 개발자 및 API 참조 가이드 이름 변경에 대한 설명이 나와 있습니다.

기존 가이드	최신 가이드
AWS 싱글 사인온 사용자 가이드	IAM Identity Center 사용 설명서
AWS 싱글 사인온 SCIM 구현 개발자 가이드	IAM Identity Center SCIM 구현 개발자 가이드
AWS 싱글 사인온 API 참조 가이드	IAM Identity Center API 참조
AWS 싱글 사인온 아이덴티티 스토어 API 참조 가이드	ID 스토어 API 참조
AWS 싱글 사인온 OIDC API 참조 가이드	IAM Identity Center OIDC API 참조
AWS 싱글 사인온 포털 API 참조 가이드	IAM Identity Center 포털 API 참조

기존 네임스페이스는 동일하게 유지

`sso` 및 `identitystore` API 네임스페이스와 다음 관련 네임스페이스는 이전 버전과의 호환성을 위해 변경되지 않은 상태로 유지됩니다.

- CLI 명령
  - `aws configure sso`
  - `identitystore`
  - `sso`
  - `sso-admin`
  - `sso-oidc`
- `AWSSSO` 및 `AWSIdentitySync` 접두사를 포함하는 관리형 정책
- `sso` 및 `identitystore`를 포함하는 서비스 엔드포인트
- `AWS::SSO` 접두사를 포함하는 AWS CloudFormation리소스
- `AWSServiceRoleForSSO`를 포함하는 서비스 연결 역할
- `sso` 및 `singlesignon`를 포함하는 콘솔 URL
- `singlesignon`를 포함하는 설명서 URL

활성화 AWS IAM Identity Center

다음 단계를 완료하여 IAM Identity Center의 조직 인스턴스에 AWS Management Console 로그인하고 활성화하십시오.

1. AWS Management Console에 로그인하려면 다음 중 하나를 수행합니다.
   - 신규 사용자 AWS (루트 사용자) — 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
   - 이미 AWS (IAM 자격 증명) 사용 중 — 관리자 권한이 있는 IAM 자격 증명을 사용하여 로그인합니다.
2. IAM Identity Center 콘솔을 엽니다.
3. IAM Identity Center 활성화에서 AWS Organizations활성화를 선택합니다.
4. 선택 사항: 이 조직 인스턴스와 연결하고자 하는 태그를 추가합니다.
5. 선택 사항: 위임 관리를 구성합니다.

> **Note**
>
> 다중 계정을 사용하는 환경인 경우, 위임 관리를 구성하는 것을 권장합니다. 위임 관리를 사용하면 AWS Organizations의 관리 계정에 액세스해야 하는 사람의 수를 제한할 수 있습니다. 자세한 정보는 위임된 관리을 참조하세요.

> **Important**
>
> IAM Identity Center 계정 인스턴스 생성 기능은 기본적으로 활성화되어 있습니다. IAM Identity Center 계정 인스턴스에는 조직 인스턴스에서 사용할 수 있는 기능의 하위 세트가 포함되어 있습니다. 서비스 제어 정책을 사용하여 사용자가 이 기능에 액세스할 수 있는지 여부를 제어할 수 있습니다.

방화벽과 게이트웨이를 업데이트해야 합니까?

차세대 방화벽 (NGFW) 또는 Secure Web Gateway (SWG) 와 같은 웹 콘텐츠 필터링 솔루션을 사용하여 특정 AWS 도메인이나 URL 엔드포인트에 대한 액세스를 필터링하는 경우 웹 콘텐츠 필터링 솔루션

허용 목록에 다음 도메인 또는 URL 엔드포인트를 추가해야 합니다. 이렇게 하면 액세스 포털에 액세스할 수 있습니다. AWS

- *[Directory ID or alias]*.awsapps.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

도메인 및 URL 엔드포인트 등록 허용 고려 사항

액세스 포털 이외의 AWS 도메인 허용이 미치는 영향을 이해하세요.

- 액세스 포털에서 AWS 계정 AWS Management Console, 및 IAM Identity Center 콘솔에 AWS 액세스하려면 추가 도메인을 허용 목록에 추가해야 합니다. 도메인 목록은 AWS Management Console 시작 안내서의 문제 해결을 참조하십시오. AWS Management Console
- AWS 액세스 포털에서 AWS 관리되는 애플리케이션에 접근하려면 해당 도메인을 허용 목록에 추가해야 합니다. 지침은 해당 서비스 설명서를 참조하십시오.
- 이러한 허용 목록에는 AWS 서비스가 포함됩니다. 외부 소프트웨어 IdPs (예: Okta 및Microsoft Entra ID) 를 사용하는 경우 해당 도메인을 허용 목록에 포함해야 합니다.

이제 IAM Identity Center를 구성할 준비가 되었습니다. IAM Identity Center를 활성화하면 IAM Identity Center 디렉터리를 기본 ID 소스로 사용하여 자동으로 구성되며, 이를 통해 가장 빠르게 IAM Identity Center 사용을 시작할 수 있습니다. 지침은 기본 IAM Identity Center 디렉터리를 사용하여 사용자 액세스를 구성합니다.을 참조하세요.

IAM Identity Center에서 Organizations, ID 소스 및 IAM 역할을 사용하는 방식을 자세히 알아보려면 다음 주제를 참조하세요.

주제

- 필수 조건 및 고려 사항
- IAM ID 센터에서 ID 소스를 확인하십시오.

필수 조건 및 고려 사항

다음 주제에서는 IAM Identity Center를 설정하기 위한 사전 요구 사항 및 기타 고려 사항에 대한 정보를 제공합니다.

선택 시 고려 사항 AWS 리전

원하는 대로 지원되는 AWS 리전 단일 인스턴스에서 IAM Identity Center 인스턴스를 활성화할 수 있습니다. 지역을 선택하려면 사용 사례 및 회사 정책을 기반으로 우선 순위를 평가해야 합니다. IAM Identity Center에서의 클라우드 애플리케이션 액세스는 이 선택에 좌우되지 않습니다. 하지만 AWS 관리형 애플리케이션에 대한 액세스와 ID AWS Managed Microsoft AD 소스로 사용할 수 있는지는 이 선택에 따라 달라질 수 있습니다. AWS 계정 AWS IAM ID 센터가 지원하는 지역 목록은 의 IAM ID 센터 엔드포인트 및 할당량을 참조하십시오. AWS 일반 참조

선택 시 주요 고려 사항. AWS 리전

- 지리적 위치 — 대부분의 최종 사용자와 지리적으로 가장 가까운 지역을 선택하면 액세스 포털 및 Amazon과 같은 AWS 관리형 애플리케이션에 대한 액세스 지연 시간이 짧아집니다. AWS SageMaker Studio
- AWS 관리형 애플리케이션의 가용성 — SageMaker Amazon과 같은 AWS 관리형 애플리케이션은 지원하는 애플리케이션에서만 작동할 수 있습니다. AWS 리전 함께 사용하려는 AWS 관리형 애플리케이션이 지원되는 지역에서 IAM Identity Center를 활성화하십시오. 또한 많은 AWS 관리형 애플리케이션은 IAM Identity Center를 활성화한 지역과 동일한 지역에서만 작동할 수 있습니다.
- 디지털 주권 — 디지털 주권 규정 또는 회사 정책에 따라 특정 항목의 사용이 의무화될 수 있습니다. AWS 리전회사의 법무 부서에 문의하십시오.
- ID 소스 — ID 소스로 AD Connector를 사용하는 AWS Managed Microsoft AD 경우 해당 홈 지역은 IAM Identity Center를 활성화한 지역과 일치해야 합니다. AWS 리전
- 기본적으로 비활성화된 리전 — AWS 원래는 기본적으로 모든 리전에서 새 AWS 리전 리전을 사용할 수 있도록 기본 설정되어 있었으며, 이를 통해 사용자가 어느 지역에서든 리소스를 자동으로 생

성할 수 있게 되었습니다. AWS 계정 이제 새 지역을 AWS 추가하면 모든 계정에서 기본적으로 해당 지역 사용이 비활성화됩니다. 기본적으로 비활성화된 지역에 IAM Identity Center를 배포하는 경우 IAM Identity Center에 대한 액세스를 관리하려는 모든 계정에서 이 지역을 활성화해야 합니다. 이는 해당 계정에서 해당 리전에 리소스를 생성할 계획이 없는 경우에도 필요합니다.

조직의 현재 계정에 대해 지역을 활성화할 수 있으며 나중에 추가할 수 있는 새 계정에 대해서도 이 작업을 반복해야 합니다. 지침은 사용 AWS Organizations 설명서의 조직 내 지역 활성화 또는 비활성화를 참조하십시오. 이러한 추가 단계가 반복되지 않도록 기본적으로 활성화된 지역에 IAM Identity Center를 배포하도록 선택할 수 있습니다. 참고로, 다음 지역은 기본적으로 활성화되어 있습니다.

- 미국 동부(오하이오)
- 미국 동부(버지니아 북부)
- 미국 서부(오리건)
- 미국 서부(캘리포니아 북부)
- 유럽(파리)
- 남아메리카(상파울루)
- 아시아 태평양(뭄바이)
- 유럽(스톡홀름)
- 아시아 태평양(서울)
- 아시아 태평양(도쿄)
- 유럽(아일랜드)
- 유럽(프랑크푸르트)
- 유럽(런던)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 캐나다(중부)
- 아시아 태평양(오사카)

- 지역 간 통화 — 일부 지역에서는 IAM ID 센터가 다른 지역의 Amazon Simple Email Service를 호출하여 이메일을 보낼 수 있습니다. 이러한 지역 간 통화에서 IAM Identity Center는 특정 사용자 속성을 다른 지역으로 전송합니다. 리전에 대한 자세한 내용은 섹션을 참조하세요AWS IAM Identity Center 지역 이용 가능 여부

전환 AWS 리전

현재 인스턴스를 삭제하고 다른 지역에 새 인스턴스를 생성해야만 IAM ID 센터 지역을 전환할 수 있습니다. 기존 AWS 인스턴스로 관리형 애플리케이션을 이미 활성화한 경우, IAM Identity Center를 삭제하기 전에 먼저 관리형 애플리케이션을 삭제해야 합니다. 새 인스턴스에서 사용자, 그룹, 권한 집합, 애플리케이션 및 할당을 다시 생성해야 합니다. IAM Identity Center 계정과 애플리케이션 할당 API를 사용하여 구성의 스냅샷을 가져온 다음 해당 스냅샷을 사용하여 새 지역에서 구성을 재구축할 수 있습니다. 새 인스턴스의 관리 콘솔을 통해 일부 IAM ID 센터 구성을 다시 생성해야 할 수도 있습니다. IAM ID 센터 삭제에 대한 지침은 을 참조하십시오. IAM Identity Center 구성 삭제

IAM ID 센터에서 생성한 IAM 역할의 할당량

IAM Identity Center는 IAM 역할을 생성하여 사용자에게 리소스에 대한 권한을 제공합니다. 권한 세트를 할당하면 IAM Identity Center가 각 계정에 해당되는 IAM Identity Center 제어 역할을 생성하고 권한 세트에 지정된 정책을 해당 역할에 연결합니다. IAM Identity Center는 역할을 관리하고, 액세스 포털 또는 액세스 포털을 사용하여 정의한 인증된 사용자가 역할을 맡을 수 있도록 합니다. AWS AWS CLI 권한 세트를 수정하면 IAM Identity Center에서 해당 IAM 정책 및 역할이 그에 따라 업데이트되도록 합니다.

IAM 역할을 이미 구성한 경우 계정이 IAM 역할 할당량에 근접하고 있는지 확인하는 것이 좋습니다. AWS 계정계정당 IAM 역할의 기본 할당량은 역할 1,000개입니다. 자세한 내용은 IAM 객체 할당량을 참조하세요.

할당량에 근접하고 있으면 할당량 증가를 요청해 보세요. 할당량을 증가시키지 않으면 IAM 역할 할당량을 초과한 계정에 권한 세트를 프로비저닝할 때 IAM Identity Center에 문제가 발생할 수 있습니다. 할당량 증가 요청에 대한 자세한 정보는 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요.

> **Note**
>
> 이미 IAM Identity Center를 사용하는 계정의 IAM 역할을 검토하는 경우 역할 이름이 “AWSReservedSSO_”로 시작하는 것을 알 수 있습니다. 이러한 역할은 IAM Identity Center 서비스가 계정에 생성한 역할로, 계정에 권한 세트를 할당하여 만들어졌습니다.

IAM 아이덴티티 센터 및 AWS Organizations

AWS Organizations IAM ID 센터와 함께 사용하는 것이 좋지만 필수는 아닙니다. 조직을 설정하지 않았어도 설정할 필요는 없습니다. IAM ID 센터를 활성화할 때 서비스를 활성화할지 여부를 선택하게 됩

니다. AWS Organizations조직을 설정하면 조직을 설정한 사용자가 AWS 계정 해당 조직의 관리 계정이 됩니다. AWS 계정 의 루트 사용자는 이제 조직 관리 계정의 소유자입니다. 조직에 추가로 AWS 계정 초대하는 것은 모두 회원 계정입니다. 관리 계정은 조직 리소스, 조직 단위 및 구성원 계정을 관리하는 정책을 생성합니다. 권한은 관리 계정에 의해 구성원 계정에 위임됩니다.

> **Note**
>
> IAM ID 센터의 조직 인스턴스를 생성하는 방법으로 IAM ID 센터를 활성화하는 것이 좋습니다. AWS Organizations조직 인스턴스는 IAM Identity Center의 모든 기능을 지원하고 중앙 관리 기능을 제공하므로 권장되는 모범 사례입니다. 자세한 정보는 IAM Identity Center의 조직 및 계정 인스턴스 관리을 참조하세요.

IAM Identity Center를 이미 AWS Organizations 설정했고 조직에 추가하려는 경우 모든 AWS Organizations 기능이 활성화되어 있는지 확인하십시오. 조직을 생성할 때 모든 기능 활성화가 기본값입니다. 자세한 내용은AWS Organizations 사용 설명서에서 조직 내 모든 기능 활성화를 참조하세요.

IAM Identity Center를 활성화하려면 관리 자격 증명이 있는 사용자 또는 루트 사용자로 AWS Organizations 관리 계정에 로그인하여 로그인해야 합니다. 다른 관리자가 없는 한 사용하지 않는 것이 좋습니다. AWS Management Console AWS Organizations 회원 계정의 관리자 자격 증명으로 로그인한 상태에서는 IAM Identity Center를 활성화할 수 없습니다. 자세한 내용은 AWS Organizations 사용 설명서의 AWS 조직 생성 및 관리를 참조하십시오.

IAM ID 센터에서 ID 소스를 확인하십시오.

IAM Identity Center의 ID 소스는 사용자 및 그룹을 관리하는 위치를 정의합니다. IAM Identity Center를 활성화한 후 선택한 ID 소스를 사용하고 있는지 확인합니다.

ID 소스 확인

1. IAM Identity Center 콘솔을 엽니다.
2. 대시보드 페이지의 권장 설정 단계 섹션 아래에서 ID 소스 확인을 선택합니다. 설정을 선택하고 ID 소스 탭을 선택하여 이 페이지에 액세스할 수도 있습니다.
3. 할당된 ID 소스를 유지하려는 경우에는 별도의 작업을 수행할 필요가 없습니다. 소스를 변경하려면 작업을 선택한 다음 ID 소스 변경을 선택합니다.

   다음 중 하나를 ID 소스로 선택할 수 있습니다.

Identity Center 디렉터리

IAM Identity Center를 처음 활성화하면 Identity Center 디렉터리를 사용하여 자동으로 구성됩니다. 아직 다른 외부 ID 제공업체를 사용하지 않는 경우 사용자 및 그룹을 생성하고, AWS 계정 및 애플리케이션에 대한 액세스 수준을 할당할 수 있습니다. 이 ID 소스 사용에 관한 자습서는 기본 IAM Identity Center 디렉터리를 사용하여 사용자 액세스를 구성합니다.의 내용을 참조하세요.

Active Directory

를 사용하여 AWS Managed Microsoft AD 디렉터리 AWS Directory Service 또는 의 자체 관리형 디렉터리에서 Active Directory (AD) 이미 사용자 및 그룹을 관리하고 있다면 IAM Identity Center를 활성화할 때 해당 디렉터리를 연결하는 것이 좋습니다. 기본 Identity Center 디렉터리에 사용자 및 그룹을 생성하지 마세요. IAM ID 센터는 에서 제공하는 연결을 사용하여 Active Directory의 AWS Directory Service 소스 디렉터리에 있는 사용자, 그룹 및 멤버십 정보를 IAM ID 센터 ID 저장소로 동기화합니다. 자세한 정보는 Microsoft AD 디렉터리에 연결을 참조하세요.

> **Note**
>
> IAM Identity Center는 SAMBA4 기반 Simple AD를 ID 소스로 지원하지 않습니다.

외부 ID 제공업체

Okta또는 같은 외부 ID 공급자 (IdPs) 의 경우Microsoft Entra ID, IAM Identity Center를 사용하여 보안 어설션 마크업 언어 (SAML) 2.0 표준을 IdPs 통해 ID를 인증할 수 있습니다. SAML 프로토콜은 사용자 및 그룹에 대해 알아보기 위해 IdP에 문의하는 방법을 제공하지 않습니다. IAM Identity Center에 해당 사용자와 그룹을 프로비저닝하여 IAM Identity Center에서 해당 사용자와 그룹을 인식합니다. IAM Identity Center는 IdP에서 SCIM(System for Cross-domain Identity Management)을 지원하는 경우 SCIM v2.0 프로토콜을 사용하여 IdP의 사용자 및 그룹 정보를 IAM Identity Center로 자동 프로비저닝(동기화)할 수 있도록 지원합니다. 그렇지 않으면 사용자 이름, 이메일 주소, 그룹을 IAM Identity Center에 수동으로 입력하여 사용자 및 그룹을 수동으로 프로비저닝할 수 있습니다.

ID 소스 설정에 대한 자세한 지침은 을 참조하십시오. 시작하기 튜토리얼

> **Note**
>
> 외부 ID 제공업체를 사용할 계획이라면 IAM Identity Center가 아닌 외부 IdP에서 다중 인증(MFA) 설정을 관리한다는 점에 유의하세요. IAM ID 센터의 MFA는 외부에서 사용할 수 없습니다. IdPs 자세한 정보는 사용자에게 MFA에 대한 메시지 표시을 참조하세요.

선택하는 자격 증명 소스에 따라 IAM Identity Center에서 Single Sign-On 액세스가 필요한 사용자 및 그룹을 검색하는 위치가 결정됩니다. ID 소스를 확인하거나 변경한 후, 사용자를 생성하거나 지정하고 AWS 계정에 관리 권한을 할당합니다.

> **Important**
>
> Active Directory 또는 외부 ID 제공업체(IdP)에서 이미 사용자 및 그룹을 관리하고 있다면, IAM Identity Center를 활성화하고 ID 소스를 선택할 때 이 ID 소스를 연결하는 것을 고려해 보는 것이 좋습니다. 기본 Identity Center 디렉터리에 사용자 및 그룹을 생성하고 할당하기 전에 이 작업을 수행해야 합니다.
>
> 사용자와 그룹을 IAM Identity Center의 한 ID 소스에서 관리하고 있을 때, 다른 ID 소스가 관리하는 것으로 변경하면 IAM Identity Center에서 구성한 모든 사용자 및 그룹 할당이 제거될 수 있습니다. 이 경우 IAM Identity Center의 관리자를 포함한 모든 사용자는 자신과 애플리케이션에 대한 Single Sign-On 액세스 권한을 잃게 됩니다. AWS 계정 자세한 정보는 ID 소스 변경 시 고려 사항을 참조하세요.

ID 소스를 구성한 후에는 사용자 또는 그룹을 검색하여 Single Sign-On 액세스 권한을 부여하거나 클라우드 애플리케이션 또는 둘 다에 AWS 계정액세스할 수 있습니다.

시작하기 튜토리얼

조직당 하나의 ID 소스를 보유할 수 있으므로 시간을 들여 각 ID 소스의 기능을 테스트하는 것이 중요합니다.

이 섹션에서는 다음 자습서 중 하나를 선택하여 원하는 ID 소스로 IAM Identity Center를 설정하고, 관리자를 생성하고, 사용자에게 리소스에 대한 액세스 권한을 부여하도록 권한 세트를 구성할 수 있습니다.

이 자습서를 시작하기 전에 IAM Identity Center를 활성화하십시오. 자세한 내용은 활성화 AWS IAM Identity Center을(를) 참조하세요.

주제

- 기본 IAM Identity Center 디렉터리를 사용하여 사용자 액세스를 구성합니다.
- Active Directory를 ID 소스로 사용
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- Google Workspace 및 IAM Identity Center를 사용하여 SAML 및 SCIM 구성
- IAM Identity Center를 사용하여 JumpCloud Directory Platform에 연결
- Microsoft Entra ID 및 IAM Identity Center를 사용하여 SAML 및 SCIM 구성
- Okta 및 IAM Identity Center를 사용하여 SAML 및 SCIM 구성
- OneLogin 및 IAM Identity Center 간에 SCIM 프로비저닝 설정
- IAM Identity Center에서 Ping Identity 제품 사용

기본 IAM Identity Center 디렉터리를 사용하여 사용자 액세스를 구성합니다.

IAM Identity Center를 처음 활성화하면 기본 ID 소스로 Identity Center 디렉터리가 자동으로 구성되므로 ID 소스를 선택할 필요가 없습니다. 조직에서, 와 같은 다른 ID 공급자를 사용하는 경우 AWS Directory Service for Microsoft Active DirectoryMicrosoft Entra ID, 또는 기본 구성을 사용하는 대신 해당 ID 소스를 IAM Identity Center와 통합하는 것을 Okta 고려해 보십시오.

목표

이 자습서에서는 기본 디렉터리를 ID 소스로 사용하고 사용자 액세스를 설정 및 테스트합니다. 이 시나리오에서는 IAM Identity Center에서 모든 사용자와 그룹을 관리합니다. 사용자는 AWS 액세스 포털을

통해 로그인합니다. 이 자습서는 사용자 및 그룹을 관리하기 위해 IAM을 AWS 처음 사용하거나 IAM을 사용해 본 사용자를 대상으로 합니다. 다음 단계에서는 다음을 생성합니다.

- *Nikki Wolf*라는 관리 사용자
- *Admin team*이라는 그룹
- 이름이 지정된 권한 집합 *AdminAccess*

모든 항목이 올바르게 생성되었는지 확인하려면 로그인하고 관리자 암호를 설정합니다. 이 자습서를 완료한 후에는 관리 사용자를 사용하여 IAM Identity Center에 사용자를 추가하고, 추가 권한 세트를 생성하고, 애플리케이션에 대한 조직 액세스를 설정할 수 있습니다.

IAM Identity Center를 아직 활성화하지 않은 경우 활성화 AWS IAM Identity Center의 내용을 참조하세요.

시작하기 전:

AWS Management Console에 로그인하려면 다음 중 하나를 수행합니다.

- AWS (루트 사용자) 신규 사용자 —AWS 계정 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
- 이미 AWS (IAM 자격 증명) 사용 중 — 관리자 권한이 있는 IAM 자격 증명을 사용하여 로그인합니다.

IAM Identity Center 콘솔을 엽니다.

1단계: 사용자 추가

1. IAM Identity Center 콘솔의 탐색 창에서 사용자를 선택하고 사용자 추가를 선택합니다.
2. 사용자 세부 정보 지정 페이지에서 다음 정보를 입력합니다.
   - 사용자 이름 - 이 자습서에서는 *nikkiw*를 입력합니다.

     사용자를 생성할 때는 기억하기 쉬운 사용자 이름을 선택하세요. 사용자가 AWS 액세스 포털에 로그인하려면 사용자 이름을 기억해야 하며 이름은 나중에 변경할 수 없습니다.
   - 암호 - 이 사용자에게 암호 설정 지침이 포함된 이메일 보내기(권장)를 선택합니다.

     이 옵션은 Amazon Web Services에서 보낸 이메일을 사용자에게 보냅니다. 제목에는 IAM ID 센터 가입 초대 (Single AWS Sign-On의 후속 기능) 라는 제목이 붙어 있습니다. 이메일은 no-

`reply@signin.aws` 또는 `no-reply@login.awsapps.com` 중 하나에서 발송됩니다. 승인된 발신자 목록에 이 이메일 주소를 추가합니다.

- 이메일 주소 - 이메일을 받을 수 있는 사용자의 이메일 주소를 입력합니다. 그런 다음 주소를 다시 입력하여 확인합니다. 각 사용자의 이메일 주소는 고유해야 합니다.
- 이름 - 사용자의 이름을 입력합니다. 이 자습서에서는 *Nikki*를 입력합니다.
- 성 - 사용자의 성을 입력합니다. 이 자습서에서는 *Wolf*를 입력합니다.
- 표시 이름 - 기본값은 사용자의 이름과 성입니다. 표시 이름을 변경하려면 다른 이름을 입력할 수 있습니다. 표시 이름은 로그인 포털 및 사용자 목록에서 표시됩니다.
- 원하는 경우 선택 사항인 정보를 입력합니다. 이 자습서에서는 사용되지 않으며 나중에 변경할 수 있습니다.

3. 다음을 선택합니다. 그룹에 사용자 추가 페이지가 표시됩니다. *Nikki*에게 관리 권한을 직접 부여하는 대신 관리 권한을 할당할 그룹을 만들겠습니다.

   그룹 생성을 선택합니다.

   새 브라우저 탭이 열리고 그룹 생성 페이지가 표시됩니다.

   a. 그룹 세부 정보의 그룹 이름에 그룹 이름을 입력합니다. 그룹의 역할을 식별할 수 있는 그룹 이름을 사용하는 것이 좋습니다. 이 자습서에서는 *Admin team*을 입력합니다.
   b. 그룹 생성을 선택합니다.
   c. 그룹 브라우저 탭을 닫고 사용자 추가 브라우저 탭으로 돌아갑니다.
4. 그룹 영역에서 새로 고침 버튼을 선택합니다. *Admin team* 그룹이 목록에 표시됩니다.

   ### # 옆의 확인란을 선택한 후 다음을 선택합니다.
5. 검토 및 사용자 추가 페이지에서 다음을 확인합니다.

   - 기본 정보가 의도한 대로 표시됨
   - 그룹에서 생성한 그룹에 추가된 사용자가 표시됨

   변경하려면 편집을 선택합니다 모든 세부 정보가 정확하면 사용자 추가를 선택합니다.

   사용자가 추가되었다는 알림 메시지가 표시됩니다.

다음으로 *Nikki*가 리소스에 액세스할 수 있도록 *Admin team* 그룹에 관리 권한을 추가합니다.

2단계: 관리 권한 추가

1. IAM Identity Center 탐색 창의 다중 계정 권한에서 AWS 계정을 선택합니다.
2. AWS 계정 페이지의 조직 구조에는 조직이 표시되고 계층 구조에 따라 그 아래에 사용자 계정이 표시됩니다. 관리 계정의 확인란을 선택한 다음 사용자 또는 그룹 할당을 선택합니다.
3. 사용자 및 그룹 할당 워크플로가 표시됩니다. 워크플로는 세 단계로 구성됩니다.

   a. 1단계: 사용자 및 그룹 선택에서 생성한 *Admin team* 그룹을 선택합니다. 다음을 선택합니다.

   b. 2단계: 권한 세트 선택에서 권한 세트 생성을 선택하여 권한 세트 생성과 관련된 3가지 하위 단계를 안내하는 새 탭이 열립니다.

      i. 1단계: 권한 세트 유형 선택에서 다음을 완료합니다.

         - 권한 세트 유형에서 사전 정의된 권한 세트를 선택합니다.
         - 사전 정의된 권한 집합에 대한 정책에서 원하는 항목을 선택합니다 AdministratorAccess.

         다음을 선택합니다.

      ii. 2단계: 권한 세트 세부 정보 지정 페이지에서 기본 설정을 유지하고 다음을 선택합니다.

         기본 설정에서는 세션 시간이 1시간으로 설정된 *AdministratorAccess*이름의 권한 집합을 생성합니다. 사용 권한 집합 이름 필드에 새 이름을 입력하여 사용 권한 집합의 이름을 변경할 수 있습니다.

      iii. 3단계: 검토 및 생성의 경우 권한 집합 유형이 AWS 관리형 정책을 사용하는지 확인하십시오 AdministratorAccess. 생성을 선택합니다. 권한 세트 페이지에 권한 세트가 생성되었음을 알리는 알림이 표시됩니다. 이제 웹 브라우저에서 이 탭을 닫을 수 있습니다.

      사용자 및 그룹 할당 브라우저 탭에서 권한 세트 생성 워크플로를 시작한 2단계: 권한 세트 선택에 여전히 있습니다.

      권한 세트 영역에서 새로 고침 버튼을 선택합니다. 생성한 *AdministratorAccess*권한 집합이 목록에 나타납니다. 해당 권한 집합의 확인란을 선택한 후 다음을 선택합니다.

   c. 3단계: 과제 검토 및 제출 페이지에서 *### #* 그룹이 선택되어 있고 *AdministratorAccess*권한 집합이 선택되었는지 확인한 다음 제출을 선택합니다.

구성 중이라는 메시지와 함께 페이지가 AWS 계정 업데이트됩니다. 프로세스가 완료될 때까지 기다립니다.

AWS 계정 페이지로 돌아옵니다. 다시 프로비전되었으며 업데이트된 권한 집합이 AWS 계정 적용되었음을 알리는 알림 메시지가 나타납니다.

> **축하합니다!**
>
> 첫 번째 사용자, 그룹 및 권한 세트를 성공적으로 설정했습니다.

이 자습서의 다음 부분에서는 *Nikki# ## ## #### ### ### ##### ### #### Nikki#* AWS 액세스 권한을 테스트해 보겠습니다. 이제 콘솔에서 로그아웃합니다.

3단계: 사용자 액세스 테스트

*Nikki Wolf*가 조직의 사용자이므로 로그인하고 권한 세트에 따라 권한이 부여된 리소스에 액세스할 수 있습니다. 사용자가 올바르게 구성되었는지 확인하기 위해 다음 단계에서는 *Nikki*의 보안 인증 정보를 사용하여 로그인하고 암호를 설정합니다. 1단계에서 *Nikki Wolf* 사용자를 추가했을 때 *Nikki*가 암호 설정 지침이 포함된 이메일을 받도록 선택했습니다. 이제 이메일을 열고 다음을 수행합니다.

1. 이메일에서 초대 수락 링크를 선택하여 초대를 수락합니다.

   > **Note**
   >
   > 이메일에는 *Nikki*의 사용자 이름과 조직에 로그인하는 데 사용할 AWS 액세스 포털 URL도 포함되어 있습니다. 나중에 사용할 수 있도록 이 정보를 기록합니다.

   새 사용자 가입 페이지로 이동하면 *Nikki*의 암호를 설정할 수 있습니다.
2. *Nikki*의 암호를 설정하고 나면 로그인 페이지로 이동합니다. *nikkiw*를 입력하고 다음을 선택한 다음 *Nikki*의 암호를 입력하고 로그인을 선택합니다.
3. AWS 접근 포털이 열리고 접근할 수 있는 기관 및 애플리케이션이 표시됩니다.

   조직을 선택하여 목록으로 확장한 AWS 계정 다음 계정을 선택하여 계정의 리소스에 접근하는 데 사용할 수 있는 역할을 표시합니다.

각 권한 집합에는 역할 또는 액세스 키라는 두 가지 관리 방법을 사용할 수 있습니다.

- 역할, *AdministratorAccess*예: 를 엽니다 AWS Console Home.
- 액세스 키 - AWS CLI or 및 AWS SDK와 함께 사용할 수 있는 자격 증명을 제공합니다. 자동으로 갱신되는 단기 보안 인증 정보 또는 단기 액세스 키 사용에 관한 정보가 포함됩니다. 자세한 정보는 AWS CLI 또는 AWS SDK에 대한 IAM Identity Center 사용자 자격 증명 가져오기을 참조하세요.

4. 역할 링크를 선택하여 에 로그인합니다. AWS Console Home

로그인하고 AWS Console Home 페이지로 이동합니다. 콘솔을 탐색하여 예상대로 액세스 권한이 있는지 확인합니다.

다음 단계

이제 IAM Identity Center에서 관리 사용자를 생성했으므로 다음 작업을 수행할 수 있습니다.

- 애플리케이션 할당
- 다른 사용자 추가
- 계정에 사용자 할당
- 추가 권한 세트 구성

> **Note**
>
> 동일한 사용자에게 여러 권한 세트를 할당할 수 있습니다. 최소 권한 적용 모범 사례를 따르려면 관리자를 생성한 후 보다 제한적인 권한 세트를 생성하여 동일한 사용자에게 할당하세요. 이렇게 하면 관리자 권한 대신 필요한 권한만 가지고도 페이지에 액세스할 수 있습니다. AWS 계정

사용자가 계정을 활성화하라는 초대를 수락하고 AWS 액세스 포털에 로그인한 후에는 자신에게 할당된 역할 AWS 계정, 응용 프로그램에 대한 항목만 포털에 표시됩니다.

> **Important**
>
> 사용자에 대해 다중 인증(MFA)을 활성화하는 것도 좋습니다. 자세한 내용은 Identity Center 사용자를 위한 다중 인증을(를) 참조하세요.

Active Directory를 ID 소스로 사용

AWS Directory Service를 사용하여 AWS Managed Microsoft AD 디렉터리 또는 AD(Active Directory)의 자체 관리형 디렉터리에서 사용자를 관리하는 경우 IAM Identity Center ID 소스를 변경하여 이러한 사용자에 사용할 수 있습니다. IAM Identity Center를 활성화하고 ID 소스를 선택할 때는 이 ID 소스의 연결을 고려하는 것이 좋습니다. 기본 Identity Center 디렉터리에 사용자 및 그룹을 생성하기 전에 해당 작업을 수행하면 나중에 ID 소스를 변경할 때 추가 구성 필요해지는 상황을 피할 수 있습니다.

Active Directory를 ID 소스로 사용하려면 구성이 다음 사전 조건을 충족해야 합니다.

- AWS Managed Microsoft AD를 사용하는 경우 AWS Managed Microsoft AD 디렉터리가 설정된 동일한 AWS 리전에서 IAM Identity Center를 활성화해야 합니다. IAM Identity Center는 디렉터리와 동일한 리전에 할당 데이터를 저장합니다. IAM Identity Center를 관리하려면 IAM Identity Center가 구성된 리전으로 전환해야 합니다. 또한, AWS 액세스 포털은 디렉터리와 동일한 액세스 URL을 사용한다는 점에 유의하세요.
- 관리 계정에 있는 Active Directory를 사용합니다.

  기존 AD Connector 또는 AWS Managed Microsoft AD 디렉터리가 AWS Directory Service에 설정되어 있어야 하며, 반드시 AWS Organizations 관리 계정 내에 있어야 합니다. 한 번에 하나의 AD Connector 디렉터리 또는 AWS Managed Microsoft AD의 디렉터리 한 개에만 연결할 수 있습니다. 여러 도메인이나 포리스트를 지원해야 하는 경우 AWS Managed Microsoft AD를 사용합니다. 자세한 내용은 다음을 참조하십시오.

  - AWS Managed Microsoft AD 디렉터리를 IAM ID 센터에 연결
  - Active Directory의 자체 관리형 디렉터리를 IAM Identity Center에 연결
- 위임된 관리자 계정에 있는 Active Directory를 사용합니다.

  IAM Identity Center 위임 관리자를 활성화하고 Active Directory를 IAM Identity Center ID 소스로 사용하려는 경우, 위임된 관리자 계정에 있는 AWS Managed Microsoft AD 디렉터리에 설정된 기존 AD Connector 또는 AWS 디렉터리를 사용할 수 있습니다.

  IAM Identity Center ID 소스를 다른 소스에서 Active Directory로 변경하거나 Active Directory에서 다른 소스로 변경하려는 경우 해당 디렉터리는 IAM Identity Center에서 위임한 관리자 계정(있는 경우)에 있어야 하고 그렇지 않으면 관리 계정에 있어야 합니다.

이 자습서는 Active Directory를 IAM Identity Center ID 소스로 사용하기 위한 기본 설정을 안내합니다.

1단계: Active Directory 연결 및 사용자 지정

이미 Active Directory를 사용 중인 경우 다음 주제가 디렉터리를 IAM Identity Center에 연결하는 데 도움이 될 것입니다.

> **Note**
>
> 최상의 보안을 위해 다중 인증을 사용하는 것을 권장합니다. AWS Managed Microsoft AD 디렉터리 또는 Active Directory의 자체 관리형 디렉터리를 연결하면서 AWS Directory Service와 함께 RADIUS MFA를 사용하지 않는 경우, IAM Identity Center에서 MFA를 활성화합니다.

AWS Managed Microsoft AD

1. Microsoft AD 디렉터리에 연결에서 지침을 검토하세요.
2. AWS Managed Microsoft AD 디렉터리를 IAM ID 센터에 연결 섹션의 단계를 따릅니다.
3. 관리자 권한을 부여하려는 사용자가 IAM Identity Center와 동기화하도록 Active Directory를 구성합니다. 자세한 내용은 관리 사용자의 IAM Identity Center 동기화 섹션을 참조하세요.

Active Directory의 자체 관리형 디렉터리

1. Microsoft AD 디렉터리에 연결에서 지침을 검토하세요.
2. Active Directory의 자체 관리형 디렉터리를 IAM Identity Center에 연결 섹션의 단계를 따릅니다.
3. 관리자 권한을 부여하려는 사용자가 IAM Identity Center와 동기화하도록 Active Directory를 구성합니다. 자세한 내용은 관리 사용자의 IAM Identity Center 동기화 섹션을 참조하세요.

2단계: 관리 사용자의 IAM Identity Center 동기화

디렉터리를 IAM Identity Center에 연결한 후, 관리 권한을 부여할 사용자를 지정한 다음 디렉터리의 해당 사용자를 IAM Identity Center로 동기화할 수 있습니다.

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고, 작업을 선택한 다음 동기화 관리를 선택합니다.
4. 동기화 관리 페이지에서 사용자 탭을 선택한 다음 사용자 및 그룹 추가를 선택합니다.
5. 사용자 탭의 사용자에서 정확한 사용자 이름을 입력하고 추가를 선택합니다.

6. 추가된 사용자 및 그룹에서 다음 작업을 수행합니다.

   a. 관리 권한을 부여하려는 사용자가 지정되었는지 확인합니다.

   b. 사용자 이름 왼쪽의 확인란을 선택합니다.

   c. 제출을 선택합니다.

7. 동기화 관리 페이지에서 지정한 사용자가 동기화 범위의 사용자 목록에 나타납니다.

8. 탐색 창에서 사용자를 선택합니다.

9. 사용자 페이지에서 지정한 사용자가 목록에 나타나는 데 시간이 다소 걸릴 수 있습니다. 새로 고침 아이콘을 선택하여 사용자 목록을 업데이트합니다.

이때 사용자는 관리 계정에 액세스할 수 없습니다. 관리 권한 세트를 만들고, 해당 권한 세트에 사용자를 할당하여 이 계정에 대한 관리 액세스 권한을 설정합니다. 자세한 내용은 권한 집합을 생성합니다. 섹션을 참조하세요.

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center는 CyberArk Directory Platform에서 IAM Identity Center로 들어오는 사용자 정보의 자동 프로비저닝(동기화)을 지원합니다. 이 프로비저닝은 도메인 간 ID 관리 시스템(SCIM) v2.0 프로토콜을 사용합니다. IAM Identity Center SCIM 엔드포인트와 액세스 토큰을 사용하여 CyberArk에서 이 연결을 구성합니다. SCIM 동기화를 구성할 때 CyberArk의 사용자 속성을 IAM Identity Center의 명명된 속성에 매핑합니다. 이로 인해 IAM Identity Center와 CyberArk 간에 예상 속성이 일치하게 됩니다.

CyberArk에 기반한 이 가이드는 2021년 8월 기준입니다. 최신 버전의 단계는 다를 수 있습니다. 이 가이드에는 SAML을 통한 사용자 인증 구성에 관련된 몇 가지 참고 사항이 포함되어 있습니다.

> **Note**
>
> SCIM 배포를 시작하기 전에 먼저 자동 프로비저닝을 사용할 때 고려 사항를 검토하는 것이 좋습니다. 그 후, 다음 섹션에서 추가 고려 사항을 계속 검토합니다.

주제

- 필수 조건
- SCIM 고려 사항

- 1단계: IAM Identity Center 프로비저닝 활성화
- 2단계: CyberArk에서 프로비저닝 구성
- (선택 사항) 3단계: IAM Identity Center에서 액세스 제어(ABAC)에 사용되는 CyberArk 사용자 속성 구성
- (선택 사항) 액세스 제어에 속성 전달

필수 조건

시작하기 전에 다음을 준비해야 합니다.

- CyberArk 구독 또는 무료 평가판. 무료 평가판을 신청하려면 CyberArk를 방문하세요.
- IAM Identity Center 활성화 계정(무료). 자세한 내용은 IAM Identity Center 활성화를 참조하세요.
- IAM Identity Center 센터 CyberArk 설명서에 설명된 대로 CyberArk 계정에서 IAM Identity Center로의 SAML 연결을 수행합니다.
- AWS 계정에 액세스를 허용하려는 역할, 사용자 및 조직과 IAM Identity Center 커넥터를 연결합니다.

SCIM 고려 사항

IAM Identity Center에서 CyberArk 페더레이션을 사용할 때 고려해야 할 사항은 다음과 같습니다.

- 애플리케이션 프로비저닝 섹션에 매핑된 역할만 IAM Identity Center와 동기화됩니다.
- 프로비저닝 스크립트는 기본 상태에서만 지원되며, 이것이 일단 변경되면 SCIM 프로비저닝이 실패할 수 있습니다.
  - 하나의 전화번호 속성만 동기화할 수 있으며 기본값은 “직장 전화”입니다.
- CyberArk IAM Identity Center 애플리케이션의 역할 매핑이 변경되면 다음과 같은 동작이 예상됩니다.
  - 역할 이름이 변경되더라도 IAM Identity Center의 그룹 이름은 변경되지 않습니다.
  - 그룹 이름이 변경되면 IAM Identity Center에 새 그룹이 생성되고 기존 그룹은 유지되지만 구성원은 없습니다.
- 사용자 동기화 및 프로비저닝 해제 동작은 CyberArk IAM Identity Center 애플리케이션에서 설정할 수 있습니다. 조직에 적합한 동작을 설정합니다. 가능한 옵션은 다음과 같습니다.
  - Identity Center 디렉터리의 사용자를 같은 보안 주체 이름으로 덮어쓰지 마세요.
  - 사용자가 CyberArk 역할에서 제거되면 IAM Identity Center에서 사용자 프로비저닝을 해제합니다.

- 사용자 행동 프로비저닝 해제 - 비활성화 또는 삭제.

1단계: IAM Identity Center 프로비저닝 활성화

이 첫 번째 단계에서는 IAM Identity Center 콘솔을 사용하여 자동 프로비저닝을 활성화합니다.

IAM Identity Center에서 자동 프로비저닝을 활성화하려면

1. 사전 필수 조건을 완료한 후 IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 자동 프로비저닝 정보 상자를 찾은 다음 활성화를 선택합니다. 그러면 IAM Identity Center에서 자동 프로비저닝이 즉시 활성화되고 필요한 SCIM 엔드포인트 및 액세스 토큰 정보가 표시됩니다.
4. 인바운드 자동 프로비저닝 대화 상자에서 다음 옵션의 각 값을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.
   a. SCIM 엔드포인트
   b. 액세스 토큰
5. 닫기를 선택하세요.

이제 IAM Identity Center 콘솔에서 프로비저닝을 설정했으므로 CyberArk IAM Identity Center 애플리케이션을 사용하여 나머지 작업을 완료해야 합니다. 다음 절차에서 이 단계를 설명합니다.

2단계: CyberArk에서 프로비저닝 구성

CyberArk IAM Identity Center 애플리케이션의 다음 절차를 사용하여 IAM Identity Center를 통한 프로비저닝을 활성화합니다. 이 절차에서는 웹 앱의 CyberArk 관리 콘솔에 CyberArk IAM Identity Center 애플리케이션을 이미 추가했다고 가정합니다. 아직 이를 수행하지 않은 경우 필수 조건를 참조하고 이 절차를 완료하여 SCIM 프로비저닝을 구성합니다.

CyberArk에서 프로비저닝을 구성하려면

1. CyberArk(앱 > 웹 앱)의 SAML을 구성하는 과정에서 추가한 CyberArk IAM Identity Center 애플리케이션을 엽니다. 필수 조건 단원을 참조하세요.
2. IAM Identity Center 애플리케이션을 선택하고 프로비저닝 섹션으로 이동합니다.
3. 이 애플리케이션에 대한 프로비저닝 활성화 체크박스를 선택하고 라이브 모드를 선택합니다.

4. 이전 절차에서 IAM Identity Center SCIM 엔드포인트 값을 복사했습니다. 해당 값을 SCIM 서비스 URL 필드에 붙여넣고 CyberArk IAM Identity Center 애플리케이션에서 인증 유형을 인증 헤더로 설정합니다. URL 끝에 있는 후행 슬래시를 제거했는지 확인합니다.
5. 헤더 유형을 베어러 토큰으로 설정합니다.
6. 이전 절차에서 IAM Identity Center에서 액세스 토큰 값을 복사했습니다. 해당 값을 CyberArk IAM Identity Center 애플리케이션의 베어러 토큰 필드에 붙여넣습니다.
7. 확인을 클릭하여 구성을 테스트하고 적용합니다.
8. 동기화 옵션에서 CyberArk의 아웃바운드 프로비저닝이 작동하는 데 사용할 올바른 동작을 선택합니다. 보안 주체 이름이 비슷한 기존 IAM Identity Center 사용자를 덮어쓸지 여부 및 프로비저닝 해제 동작을 덮어쓸지 여부를 선택할 수 있습니다.
9. 역할 매핑에서 이름 필드 아래의 CyberArk 역할에서 대상 그룹 아래의 IAM Identity Center 그룹으로의 매핑을 설정합니다.
10. 완료되면 하단의 저장을 클릭합니다.
11. 사용자가 IAM Identity Center와 성공적으로 동기화되었는지 확인하려면 IAM Identity Center 콘솔로 돌아가서 사용자를 선택합니다. CyberArk로부터 동기화된 사용자는 사용자 페이지에 표시됩니다. 이제 이러한 사용자를 계정에 할당하고 IAM Identity Center 내에서 연결할 수 있습니다.

(선택 사항) 3단계: IAM Identity Center에서 액세스 제어(ABAC)에 사용되는 CyberArk 사용자 속성 구성

이 절차는 IAM Identity Center의 속성을 구성하여 AWS 리소스에 대한 액세스를 관리하는 경우 선택할 수 있는 선택적 절차입니다. CyberArk CyberArk에서 정의한 속성은 SAML 어설션을 통해 IAM Identity Center에 전달됩니다. 그런 다음 CyberArk로부터 전달한 속성을 기반으로 액세스를 관리하기 위해 IAM Identity Center에서 권한 세트를 생성해야 합니다.

이 절차를 시작하기 전에 액세스 제어를 위한 속성 기능을 활성화해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 액세스 제어를 위한 속성 활성화 및 구성 단원을 참조하세요.

IAM Identity Center에서 액세스 제어에 사용되는 CyberArk 사용자 속성을 구성하려면

1. CyberArk(앱 > 웹 앱)의 SAML을 구성하는 과정에서 설치된 CyberArk IAM Identity Center 애플리케이션을 엽니다.
2. SAML 응답 옵션으로 이동합니다.
3. 속성 아래에서 논리에 따라 관련 속성을 다음 테이블에 추가합니다.

    a. 속성 이름은 CyberArk의 기존 속성입니다.

b. 속성 값은 SAML 어설션에서 IAM Identity Center로 전송된 속성 이름입니다.

4. 저장을 선택합니다.

(선택 사항) 액세스 제어에 속성 전달

IAM Identity Center의 액세스 제어를 위한 속성 기능을 사용하여 Name 속성이 `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`로 설정된 Attribute 요소를 전달하도록 선택할 수 있습니다. 이 요소를 사용하면 속성을 SAML 어설션에 세션 태그로 전달할 수 있습니다. 세션 태그에 대한 자세한 내용은 IAM 사용 설명서의 AWS STS에서 세션 태그 전달을 참조하세요.

속성을 세션 태그로 전달하려면 태그 값을 지정하는 AttributeValue 요소를 포함합니다. 예를 들어, 태그 키-값 쌍 `CostCenter = blue`를 전달하려면 다음 속성을 사용합니다.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

여러 속성을 추가해야 하는 경우 각 태그마다 별도의 Attribute 요소를 포함합니다.

Google Workspace 및 IAM Identity Center를 사용하여 SAML 및 SCIM 구성

조직에서 을 사용하는 Google Workspace 경우 IAM Identity Google Workspace Center로 사용자와 그룹을 통합하여 AWS 리소스에 대한 액세스 권한을 부여할 수 있습니다. IAM ID 센터 ID 소스를 기본 IAM ID 센터 ID 소스에서 로 변경하여 이러한 통합을 달성할 수 있습니다. Google Workspace

Google Workspace의 사용자 정보는 SCIM(System for Cross-domain Identity Management) 2.0 프로토콜을 사용하여 IAM Identity Center에 동기화됩니다. IAM Identity Center의 SCIM 엔드포인트와 IAM Identity Center 보유자 토큰을 사용하여 Google Workspace에서 연결을 구성할 수 있습니다. SCIM 동기화를 구성할 때 Google Workspace의 사용자 속성을 IAM Identity Center의 명명된 속성에 매핑합니다. 이 매핑은 IAM Identity Center와 Google Workspace 간의 예상 사용자 속성을 일치시킵니다. 이를 위해 Google Workspace를 IAM ID 제공업체와 IAM Identity Center ID 제공업체로 설정해야 합니다.

목표

이 자습서의 단계는 과 (과) 간의 SAML 연결 설정 과정을 안내합니다. Google Workspace AWS나중에 SCIM을 사용하여 Google Workspace에서 사용자를 동기화합니다. 모든 것이 올바르게 구성되었는지 확인하려면 구성 단계를 완료한 후 Google Workspace 사용자로 로그인하여 리소스에 AWS 대한 액세스 권한을 확인합니다. 이 자습서는 소규모 Google Workspace 디렉터리 테스트 환경을 기반으로 합니다. 그룹 및 조직 단위와 같은 디렉터리 구조는 포함되지 않습니다. 이 자습서를 완료한 후 사용자는 Google Workspace 자격 증명으로 AWS 액세스 포털에 액세스할 수 있습니다.

> **Note**
>
> Google Workspace 무료 평가판을 신청하려면 Google's 웹사이트에서 Google Workspace를 방문하세요.
> IAM Identity Center를 아직 활성화하지 않은 경우 활성화 AWS IAM Identity Center의 내용을 참조하세요.

고려 사항

- IAM ID 센터 간의 Google Workspace SCIM 프로비저닝을 구성하기 전에 먼저 검토하는 것이 좋습니다. 자동 프로비저닝을 사용할 때 고려 사항
- SCIM 자동 Google Workspace 동기화는 현재 사용자 프로비저닝으로 제한됩니다. 자동 그룹 프로비저닝은 현재 지원되지 않습니다. 그룹은 AWS CLI ID 스토어 create-group 명령 또는 AWS Identity and Access Management (IAM) API를 사용하여 수동으로 생성할 수 있습니다. CreateGroup 또는 ssosync를 사용하여 Google Workspace 사용자와 그룹을 IAM ID 센터에 동기화할 수 있습니다.
- 모든 Google Workspace 사용자는 이름, 성, 사용자 이름 및 표시 이름 값이 지정되어야 합니다.
- 각 Google Workspace 사용자는 이메일 주소 또는 전화번호와 같은 데이터 속성당 하나의 값만 보유합니다. 값이 여러 개인 사용자는 동기화에 실패합니다. 속성에 여러 개의 값이 있는 사용자가 있는 경우 IAM Identity Center에서 사용자를 프로비저닝하기 전에 중복된 속성을 제거합니다. 예를 들어 전화번호 속성은 하나만 동기화할 수 있습니다. 기본 전화번호 속성이 “회사 전화번호”이므로 사용자의 전화번호가 집이나 휴대폰 전화번호인 경우에도 “회사 전화번호” 속성을 사용하여 사용자의 전화번호를 저장합니다.
- 사용자가 IAM Identity Center에서 비활성화되었지만 Google Workspace에서 여전히 활성 상태인 경우 속성은 여전히 동기화됩니다.
- Identity Center 디렉터리에 동일한 사용자 이름과 이메일을 가진 기존 사용자가 있는 경우 SCIM From을 사용하여 해당 사용자를 덮어쓰고 동기화합니다. Google Workspace
- ID 소스를 변경할 때는 추가 고려 사항이 있습니다. 자세한 정보는 the section called “IAM Identity Center에서 외부 IdP로 변경”을 참조하세요.

1단계Google Workspace: SAML 애플리케이션 구성

1. 슈퍼 Google관리자 권한이 있는 계정을 사용하여 관리 콘솔에 로그인합니다.
2. Google관리 콘솔의 왼쪽 탐색 패널에서 앱을 선택한 다음 웹 및 모바일 앱을 선택합니다.
3. 앱 추가 드롭다운 목록에서 앱 검색을 선택합니다.
4. 검색 상자에 아마존 웹 서비스를 입력한 다음 목록에서 아마존 웹 서비스 (SAML) 앱을 선택합니다.
5. GoogleID 제공자 세부 정보 - Amazon Web Services 페이지에서 다음 중 하나를 수행할 수 있습니다.

   a. IdP 메타데이터를 다운로드합니다.

   b. SSO URL, 엔티티 ID URL 및 인증서 정보를 복사합니다.

   2단계에서 XML 파일 또는 URL 정보가 필요합니다.
6. Google관리 콘솔에서 다음 단계로 이동하기 전에 이 페이지를 열어 두고 IAM Identity Center 콘솔로 이동하십시오.

2단계: IAM ID 센터 및Google Workspace: IAM ID 센터 자격 증명 소스를 변경하고 SAML 자격 증명 Google Workspace 공급자로 설정합니다.

1. 관리자 권한이 있는 역할을 사용하여 IAM ID 센터 콘솔에 로그인합니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 작업을 선택한 다음 ID 소스 변경을 선택합니다.

   - IAM ID 센터를 활성화하지 않은 경우 자세한 내용은 IAM Identity Center 활성화 을 참조하십시오. IAM Identity Center를 처음으로 활성화하고 액세스하면 대시보드에서 ID 소스 선택을 선택할 수 있습니다.
4. ID 소스 선택 페이지에서 외부 ID 제공업체를 선택하고 다음을 선택합니다.
5. 외부 ID 제공업체 구성 페이지가 열립니다. 이 페이지와 1단계의 Google Workspace 페이지를 완료하려면 다음을 완료해야 합니다.

   - IAM Identity Center 콘솔의 ID 제공자 메타데이터 섹션에서 다음 중 하나를 수행해야 합니다.

     i. IAM ID 센터 콘솔에서 GoogleSAML 메타데이터를 IdP SAML 메타데이터로 업로드합니다.

ii. GoogleSSO URL을 IdP 로그인 URL 필드에 복사하여 붙여넣고Google, 발급자 URL을 IdP 발급자 URL 필드에 붙여넣고, 인증서를 IdP 인증서로 업로드합니다. Google

6. IAM ID 센터 콘솔의 ID 공급자 메타데이터 섹션에 메타데이터를 제공한 후AWS 액세스 포털 로그인 URL, IAM ID 어설션 소비자 서비스 (ACS) URL 및 IAM ID 센터 발급자 URL을 복사합니다. Google 다음 단계에서 관리 콘솔에 이러한 URL을 제공해야 합니다. Google
7. IAM ID 센터 콘솔에서 페이지를 열어 두고 Google 관리 콘솔로 돌아가십시오. Amazon Web Services - 서비스 공급자 세부 정보 페이지에 있어야 합니다. 계속을 선택합니다.
8. 서비스 제공자 세부 정보 페이지에서 ACS URL, 엔티티 ID 및 시작 URL 값을 입력합니다. 이 값은 이전 단계에서 복사했으며 IAM Identity Center 콘솔에서 찾을 수 있습니다.
   - IAM ID 센터 어설션 소비자 서비스 (ACS) URL을 ACS URL 필드에 붙여넣습니다.
   - IAM ID 센터 발급자 URL을 개체 ID 필드에 붙여넣습니다.
   - AWS 액세스 포털 로그인 URL을 시작 URL 필드에 붙여넣습니다.
9. 서비스 제공업체 세부정보 페이지에서 다음과 같이 이름 ID 아래의 필드를 작성합니다.
   - 이름 ID 형식의 경우 이메일을 선택합니다.
   - 이름 ID의 경우 기본 정보 > 기본 이메일을 선택합니다.
10. 계속을 선택합니다.
11. 속성 매핑 페이지의 속성에서 매핑 추가를 선택한 다음 Google디렉터리 속성에서 다음 필드를 구성합니다.
    - `https://aws.amazon.com/SAML/Attributes/RoleSessionName`앱 속성의 경우 Google Directory속성에서 기본 정보, 기본 이메일 필드를 선택합니다.
    - `https://aws.amazon.com/SAML/Attributes/Role`앱 속성의 경우 원하는 Google Directory속성을 선택합니다. Google디렉터리 속성은 부서일 수 있습니다.
12. 완료를 클릭합니다.
13. IAM ID 센터 콘솔로 돌아가서 다음을 선택합니다. 검토 및 확인 페이지에서 정보를 검토한 다음 제공된 공간에 ACCEPT를 입력합니다. ID 소스 변경을 선택합니다.

이제 Amazon Web Services 앱을 Google Workspace 활성화하여 사용자를 IAM ID 센터에 프로비저닝할 수 있습니다.

3단계Google Workspace: 앱 활성화

1. Google관리 콘솔로 돌아가서 앱과 웹 및 모바일 앱에서 찾을 수 있는 AWS IAM Identity Center 애플리케이션으로 돌아가십시오.
2. 사용자 액세스 옆의 사용자 액세스 패널에서 아래쪽 화살표를 선택하여 사용자 액세스를 확장하여 서비스 상태 패널을 표시합니다.
3. 서비스 상태 패널에서 모든 사용자 ON을 선택한 다음 SAVE를 선택합니다.

> **Note**
>
> 최소 권한 원칙을 유지하는 데 도움이 되도록 이 자습서를 완료한 후에는 모든 사용자의 서비스 상태를 OFF로 변경하는 것이 좋습니다. 액세스 권한이 필요한 사용자만 서비스를 AWS 활성화해야 합니다. Google Workspace 그룹 또는 조직 단위를 사용하여 특정 사용자 하위 세트에 대한 액세스 권한을 사용자에게 부여할 수 있습니다.

4단계: IAM ID 센터: IAM ID 센터 자동 프로비저닝 설정

1. IAM Identity Center 콘솔로 돌아갑니다.
2. 설정 페이지에서 자동 프로비저닝 정보 상자를 찾은 다음 활성화를 선택합니다. 그러면 IAM Identity Center에서 자동 프로비저닝이 즉시 활성화되고 필요한 SCIM 엔드포인트 및 액세스 토큰 정보가 표시됩니다.
3. 인바운드 자동 프로비저닝 대화 상자에서 다음 옵션의 각 값을 복사합니다. 이 자습서의 5단계에서는 이러한 값을 입력하여 자동 프로비저닝을 구성합니다. Google Workspace
   - SCIM 엔드포인트
   - 액세스 토큰

   > **Warning**
   >
   > SCIM 엔드포인트와 액세스 토큰을 얻을 수 있는 유일한 시간입니다. 진행하기 전에 이 값을 복사해야 합니다.
4. 닫기를 선택하세요.

이제 IAM Identity Center 콘솔에서 프로비저닝을 설정했으니 다음 단계에서 자동 프로비저닝을 구성해 보겠습니다. Google Workspace

5단계Google Workspace: 자동 프로비저닝 구성

1. Google관리 콘솔로 돌아가서 앱과 웹 및 모바일 앱에서 찾을 수 있는 AWS IAM Identity Center 애플리케이션으로 돌아가십시오. 자동 프로비저닝 섹션에서 자동 프로비저닝 구성을 선택합니다.
2. 이전 절차에서는 IAM Identity Center 콘솔의 액세스 토큰 값을 복사했습니다. 해당 값을 액세스 토큰 필드에 붙여넣고 계속을 선택합니다. 또한 이전 절차에서는 IAM ID 센터 콘솔에 SCIM 엔드포인트 값을 복사했습니다. 해당 값을 엔드포인트 URL 필드에 붙여 넣습니다. URL 끝에 있는 후행 슬래시를 제거했는지 확인하고 계속을 선택합니다.
3. 모든 필수 IAM Identity Center 속성(* 표시)이 Google Cloud Directory 속성에 매핑되어 있는지 확인합니다. 그렇지 않은 경우 아래쪽 화살표를 선택하고 적절한 속성에 매핑합니다. 계속을 선택합니다.
4. 프로비저닝 범위 섹션에서 Amazon Web Services 앱에 대한 액세스를 제공할 Google Workspace 디렉터리가 있는 그룹을 선택할 수 있습니다. 이 단계를 건너뛰고 계속을 선택합니다.
5. 프로비저닝 해제 섹션에서는 사용자의 액세스 권한을 제거하는 다양한 이벤트에 응답하는 방법을 선택할 수 있습니다. 각 상황에 대해 프로비저닝 해제가 시작되기까지 걸리는 시간을 다음과 같이 지정할 수 있습니다.

   - 24시간 이내
   - 1일 후
   - 7일 후
   - 30일 후

   각 상황에 따라 계정 액세스를 일시 중단할 시기와 계정을 삭제할 시기를 설정할 수 있습니다.

   > **Tip**
   >
   > 항상 사용자 계정을 삭제하기 전에 사용자 계정을 정지하는 시간보다 더 긴 시간을 설정합니다.

6. 마침을 클릭합니다. Amazon Web Services 앱 페이지로 돌아갑니다.
7. 자동 프로비저닝 섹션에서 토글 스위치를 켜서 비활성에서 활성으로 변경합니다.

> **Note**
>
> 사용자에 대해 IAM Identity Center가 켜져 있지 않으면 활성화 슬라이더가 비활성화됩니다. 사용자 액세스를 선택하고 앱을 켜서 슬라이더를 활성화합니다.

8. 확인 대화 상자에서 켜기를 선택합니다.
9. 사용자가 IAM Identity Center에 성공적으로 동기화되었는지 확인하려면 IAM Identity Center 콘솔로 돌아가서 사용자를 선택합니다. 사용자 페이지에는 SCIM에서 생성한 Google Workspace 디렉터리의 사용자가 나열됩니다. 사용자가 아직 목록에 없는 경우 프로비저닝이 아직 진행 중일 수 있습니다. 프로비저닝은 최대 24시간이 소요될 수 있지만 대부분의 경우 몇 분 내에 완료됩니다. 몇 분마다 브라우저 창을 새로 고쳐야 합니다.

   사용자를 선택하고 세부 정보를 확인합니다. 정보는 디렉터리의 정보와 일치해야 합니다. Google Workspace

> **축하합니다!**
>
> Google Workspace AWS 와 사이에 SAML 연결을 성공적으로 설정하고 자동 프로비저닝이 작동하는지 확인했습니다. 이제 IAM Identity Center에서 계정과 애플리케이션을 사용자에게 할당할 수 있습니다. 이 자습서에서는 다음 단계로 관리 계정에 관리 권한을 부여하여 사용자 중 한 명을 IAM Identity Center 관리자로 지정합니다.

6단계: IAM ID 센터: Google Workspace 사용자에게 계정 액세스 권한 부여

1. IAM ID 센터 콘솔로 돌아가십시오. IAM Identity Center 탐색 창의 다중 계정 권한에서 AWS 계정을 선택합니다.
2. AWS 계정 페이지의 조직 구조에는 조직 루트가 표시되고 계층 구조에 따라 그 아래에 사용자 계정이 표시됩니다. 관리 계정의 확인란을 선택한 다음 사용자 또는 그룹 할당을 선택합니다.
3. 사용자 및 그룹 할당 워크플로가 표시됩니다. 워크플로는 세 단계로 구성됩니다.

   a. 1단계: 사용자 및 그룹 선택에서 관리자 작업을 수행할 사용자를 선택합니다. 다음을 선택합니다.

   b. 2단계: 권한 세트 선택에서 권한 세트 생성을 선택하여 권한 세트 생성과 관련된 3가지 하위 단계를 안내하는 새 탭이 열립니다.

i. 1단계: 권한 세트 유형 선택에서 다음을 완료합니다.

- 권한 세트 유형에서 사전 정의된 권한 세트를 선택합니다.
- 사전 정의된 권한 집합에 대한 정책에서 선택합니다. AdministratorAccess

다음을 선택합니다.

ii. 2단계: 권한 세트 세부 정보 지정 페이지에서 기본 설정을 유지하고 다음을 선택합니다.

기본 설정에서는 세션 시간이 1시간으로 설정된 *AdministratorAccess*이름의 권한 집합을 생성합니다.

iii. 3단계: 검토 및 생성의 경우 권한 집합 유형이 AWS 관리형 정책을 사용하는지 확인하십시오 AdministratorAccess. 생성을 선택합니다. 권한 세트 페이지에 권한 세트가 생성되었음을 알리는 알림이 표시됩니다. 이제 웹 브라우저에서 이 탭을 닫을 수 있습니다.

iv. 사용자 및 그룹 할당 브라우저 탭에서 권한 세트 생성 워크플로를 시작한 2단계: 권한 세트 선택에 여전히 있습니다.

v. 권한 세트 영역에서 새로 고침 버튼을 선택합니다. 생성한 *AdministratorAccess*권한 집합이 목록에 나타납니다. 권한 세트의 확인란을 선택하고 다음을 선택합니다.

c. 3단계: 검토 및 제출에서 선택한 사용자 및 권한 세트를 검토한 다음 제출을 선택합니다.

구성 중이라는 메시지와 함께 페이지가 업데이트됩니다. AWS 계정 프로세스가 완료될 때까지 기다립니다.

AWS 계정 페이지로 돌아옵니다. 다시 프로비전되었으며 업데이트된 권한 집합이 AWS 계정 적용되었음을 알리는 알림 메시지가 나타납니다. 사용자가 로그인하면 역할을 선택할 수 있는 옵션이 제공됩니다. *AdministratorAccess*

> **Note**
>
> SCIM 자동 동기화는 프로비전 Google Workspace 사용자만 지원합니다. 자동 그룹 프로비저닝은 현재 지원되지 않습니다. AWS Management Console을 사용하여 Google Workspace 사용자에 대한 그룹을 생성할 수는 없습니다. 사용자를 프로비저닝한 후에는 AWS CLI Identity Store create-group 명령 또는 IAM API를 사용하여 그룹을 생성할 수 있습니다. CreateGroup

7단계Google Workspace: 리소스에 대한 사용자 액세스 확인 Google WorkspaceAWS

1. 테스트 사용자 계정을 Google 사용하여 로그인합니다. 사용자를 추가하는 방법을 Google Workspace 알아보려면 Google Workspace설명서를 참조하십시오.
2. Google apps런처(와플 모양) 아이콘을 선택합니다.
3. 사용자 지정 Google Workspace 앱이 있는 앱 목록 하단으로 스크롤합니다. Amazon Web Services 및 AWS 액세스 포털이라는 두 개의 앱이 표시됩니다.
4. AWS 액세스 포털 앱을 선택합니다. 포털에 로그인하고 AWS 계정 아이콘을 볼 수 있습니다. 아이콘을 펼치면 사용자가 접근할 수 AWS 계정 있는 목록이 표시됩니다. 이 자습서에서는 단일 계정만 사용했으므로 아이콘을 확장하면 하나의 계정만 표시됩니다.

   > **Note**
   >
   > Amazon Web Services 앱을 선택하면 SAML 오류가 발생합니다. 이 앱은 IAM 사용자로 프로비저닝된 Google Workspace 사용자에 대해 사용되며 이 자습서에서는 Google Workspace 사용자를 IAM Identity Center의 사용자로 프로비저닝합니다.

5. 계정을 선택하면 사용자에게 제공되는 권한 세트가 표시됩니다. 이 자습서에서는 AdministratorAccess권한 집합을 만들었습니다.
6. 권한 세트 옆에는 해당 권한 세트에 사용할 수 있는 액세스 유형에 대한 링크가 있습니다. 권한 세트를 생성할 때 관리 콘솔과 프로그래밍 방식 액세스를 모두 활성화하도록 지정했으므로 두 가지 옵션이 제공됩니다. 관리 콘솔을 선택하면 AWS Management Console이 열립니다.
7. 사용자가 콘솔에 로그인합니다.

(선택 사항) 액세스 제어에 속성 전달

IAM Identity Center의 액세스 제어를 위한 속성 기능을 사용하여 `Name` 속성이 `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`로 설정된 `Attribute` 요소를 전달하도록 선택할 수 있습니다. 이 요소를 사용하면 속성을 SAML 어설션에 세션 태그로 전달할 수 있습니다. 세션 태그에 대한 자세한 내용은 IAM 사용 설명서의 AWS STS에서 세션 태그 전달을 참조하세요.

속성을 세션 태그로 전달하려면 태그 값을 지정하는 `AttributeValue` 요소를 포함합니다. 예를 들어, 태그 키-값 쌍 `CostCenter = blue`를 전달하려면 다음 속성을 사용합니다.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
```

```
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

여러 속성을 추가해야 하는 경우 각 태그마다 별도의 `Attribute` 요소를 포함합니다.

다음 단계

이제 Google Workspace를 ID 제공업체로 구성하고 IAM Identity Center의 사용자를 프로비저닝했기 때문에 다음을 수행할 수 있습니다.

- AWS CLI 아이덴티티 스토어 create-group 명령 또는 IAM API를 CreateGroup사용하여 사용자를 위한 그룹을 생성합니다.

  그룹은 애플리케이션에 대한 액세스 권한을 할당할 때 유용합니다. AWS 계정 각 사용자를 개별적으로 할당하는 대신 그룹에 권한을 부여합니다. 나중에 그룹에 사용자를 추가하거나 그룹에서 사용자를 제거하면 해당 사용자는 그룹에 할당한 계정 및 애플리케이션에 대한 액세스 권한을 동적으로 얻거나 잃게 됩니다.
- 직무에 따라 권한을 구성합니다. 권한 세트 생성을 참조하세요.

  권한 집합은 사용자와 그룹이 AWS 계정에 대해 보유할 수 있는 액세스 수준을 정의합니다. 권한 집합은 IAM Identity Center에 저장되며 하나 이상의 AWS 계정에 프로비저닝할 수 있습니다. 한 사용자에게 두 개 이상의 권한 집합을 할당할 수 있습니다.

> **Note**
>
> IAM Identity Center 관리자는 이전 IdP 인증서를 새 인증서로 교체해야 하는 경우가 있습니다. 예를 들어, 인증서 만료 날짜가 다가올 경우 IdP 인증서를 교체해야 할 수도 있습니다. 이전 인증서를 새 인증서로 교체하는 프로세스를 인증서 교체라고 합니다. Google Workspace에 대한 SAML 인증서를 관리하는 방법을 검토하세요.

IAM Identity Center를 사용하여 JumpCloud Directory Platform에 연결

IAM Identity Center는 JumpCloud Directory Platform에서 IAM Identity Center로 들어오는 사용자 정보의 자동 프로비저닝(동기화)을 지원합니다. 이 프로비저닝은 도메인 간 ID 관리 시스템(SCIM) v2.0 프

로토콜을 사용합니다. IAM Identity Center SCIM 엔드포인트와 액세스 토큰을 사용하여 JumpCloud에서 이 연결을 구성합니다. SCIM 동기화를 구성할 때 JumpCloud의 사용자 속성을 IAM Identity Center의 명명된 속성에 매핑합니다. 이로 인해 IAM Identity Center와 JumpCloud 간에 예상 속성이 일치하게 됩니다.

JumpCloud에 기반한 이 가이드는 2021년 6월 기준입니다. 최신 버전의 단계는 다를 수 있습니다. 이 가이드에는 SAML을 통한 사용자 인증 구성에 관련된 몇 가지 참고 사항이 포함되어 있습니다.

다음 단계는 SCIM 프로토콜을 사용하여 JumpCloud에서 IAM Identity Center으로 사용자 및 그룹을 자동으로 프로비저닝하도록 활성화하는 방법을 안내합니다.

> **Note**
>
> SCIM 배포를 시작하기 전에 먼저 자동 프로비저닝을 사용할 때 고려 사항를 검토하는 것이 좋습니다. 그 후, 다음 섹션에서 추가 고려 사항을 계속 검토합니다.

주제

- 사전 조건
- SCIM 고려 사항
- 1단계: IAM Identity Center 프로비저닝 활성화
- 2단계: JumpCloud에서 프로비저닝 구성
- (선택 사항) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 JumpCloud 사용자 속성 구성
- (선택 사항) 액세스 제어에 속성 전달

사전 조건

시작하기 전에 다음을 준비해야 합니다.

- JumpCloud 구독 또는 무료 평가판. 무료 평가판을 신청하려면 JumpCloud를 방문하십시오.
- IAM Identity Center 활성화 계정(무료). 자세한 내용은 IAM Identity Center 활성화를 참조하십시오.
- IAM Identity Center 센터 JumpCloud 설명서에 설명된 대로 JumpCloud 계정에서 IAM Identity Center로의 SAML 연결을 수행합니다.
- AWS 계정에 액세스를 허용하려는 그룹과 IAM Identity Center 커넥터를 연결합니다.

SCIM 고려 사항

IAM Identity Center에서 JumpCloud 페더레이션을 사용할 때 고려해야 할 사항은 다음과 같습니다.

- JumpCloud 의 AWS Single Sign-On 커넥터와 연결된 그룹만 SCIM과 동기화됩니다.
- 하나의 전화번호 속성만 동기화할 수 있으며 기본값은 “직장 전화”입니다.
- JumpCloud 디렉터리의 사용자는 SCIM을 사용하여 IAM Identity Center와 동기화되도록 구성된 이름과 성을 가지고 있어야 합니다.
- 사용자가 IAM Identity Center에서 비활성화되었지만 JumpCloud에서 여전히 활성 상태인 경우 속성은 여전히 동기화됩니다.
- 커넥터에서 “사용자 그룹 및 그룹 구성원 관리 활성화”를 선택 취소하여 사용자 정보에 대해서만 SCIM 동기화를 활성화하도록 선택할 수 있습니다.
- Identity Center 디렉터리에 동일한 사용자 이름과 이메일을 가진 기존 사용자가 있는 경우 JumpCloud의 SCIM을 사용하여 해당 사용자를 덮어쓰고 동기화합니다.

1단계: IAM Identity Center 프로비저닝 활성화

이 첫 번째 단계에서는 IAM Identity Center 콘솔을 사용하여 자동 프로비저닝을 활성화합니다.

IAM Identity Center에서 자동 프로비저닝을 활성화하려면

1. 사전 필수 조건을 완료한 후 IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 자동 프로비저닝 정보 상자를 찾은 다음 활성화를 선택합니다. 그러면 IAM Identity Center에서 자동 프로비저닝이 즉시 활성화되고 필요한 SCIM 엔드포인트 및 액세스 토큰 정보가 표시됩니다.
4. 인바운드 자동 프로비저닝 대화 상자에서 다음 옵션의 각 값을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.
   a. SCIM 엔드포인트
   b. 액세스 토큰
5. 닫기를 선택하세요.

이제 IAM Identity Center 콘솔에서 프로비저닝을 설정했으므로 JumpCloud IAM Identity Center 커넥터를 사용하여 나머지 작업을 완료해야 합니다. 다음 절차에서 이 단계를 설명합니다.

2단계: JumpCloud에서 프로비저닝 구성

JumpCloud IAM Identity Center 커넥터의 다음 절차를 사용하여 IAM Identity Center를 통한 프로비저닝을 활성화합니다. 이 절차에서는 JumpCloud 관리 포털 및 그룹에 JumpCloud IAM Identity Center 커넥터를 이미 추가했다고 가정합니다. 아직 이를 수행하지 않은 경우 사전 조건를 참조하고 이 절차를 완료하여 SCIM 프로비저닝을 구성합니다.

JumpCloud에서 프로비저닝을 구성하려면

1. JumpCloud(사용자 인증 > IAM Identity Center)의 SAML을 구성하는 과정에서 설치한 JumpCloud IAM Identity Center 커넥터를 엽니다. 사전 조건 단원을 참조하십시오.
2. IAM Identity Center 커넥터를 선택한 다음 세 번째 탭 ID 관리를 선택합니다.
3. 그룹을 SCIM 동기화하려면 이 애플리케이션에서 사용자 그룹 및 그룹 구성원 관리 활성화 체크박스를 선택합니다.
4. 구성을 클릭합니다.
5. 이전 절차에서 IAM Identity Center에서 SCIM 엔드포인트 값을 복사했습니다. 해당 값을 JumpCloud IAM Identity Center 커넥터의 기본 URL 필드에 붙여넣습니다. URL 끝에 있는 후행 슬래시를 제거했는지 확인합니다.
6. 이전 절차에서 IAM Identity Center에서 액세스 토큰 값을 복사했습니다. 해당 값을 JumpCloud IAM Identity Center 커넥터의 토큰 키 필드에 붙여넣습니다.
7. 활성화를 클릭하여 구성을 적용합니다.
8. 녹색 표시기 옆에 Single Sign-On 활성화가 있는지 확인합니다.
9. 네 번째 탭인 사용자 그룹으로 이동하여 SCIM으로 프로비저닝하려는 그룹을 선택합니다.
10. 완료되면 하단의 저장을 클릭합니다.
11. 사용자가 IAM Identity Center와 성공적으로 동기화되었는지 확인하려면 IAM Identity Center 콘솔로 돌아가서 사용자를 선택합니다. JumpCloud로부터 동기화된 사용자는 사용자 페이지에 표시됩니다. 이제 이러한 사용자를 IAM Identity Center 내에서 계정에 할당할 수 있습니다.

(선택 사항) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 JumpCloud 사용자 속성 구성

이는 AWS 리소스에 대한 액세스를 관리하기 위해 IAM Identity Center의 속성을 구성하도록 선택하는 경우에 사용할 수 있는 JumpCloud의 선택적 절차입니다. JumpCloud에서 정의한 속성은 SAML 어설션을 통해 IAM Identity Center에 전달됩니다. 그런 다음 JumpCloud로부터 전달한 속성을 기반으로 액세스를 관리하기 위해 IAM Identity Center에서 권한 세트를 생성해야 합니다.

이 절차를 시작하기 전에 먼저 액세스 제어용 속성 기능을 활성화해야 합니다. 이에 대한 자세한 방법은 액세스 제어 속성 활성화 및 구성을 참조하십시오.

IAM Identity Center에서 액세스 제어에 사용되는 JumpCloud 사용자 속성을 구성하려면

1. JumpCloud(사용자 인증 > IAM Identity Center)의 SAML을 구성하는 과정에서 설치한 JumpCloud IAM Identity Center 커넥터를 엽니다.
2. IAM Identity Center 커넥터를 선택합니다. 그런 다음 IAM Identity Center의 두 번째 탭을 선택합니다.
3. 이 탭 하단의 사용자 속성 매핑에서 새 속성 추가를 선택한 후 다음을 수행합니다. IAM Identity Center에서 액세스 제어용으로 사용하기 위해 추가할 각 속성에 대해 다음 단계를 수행해야 합니다.

   a. 서비스 제공 속성 이름 필드에서 IAM Identity Center에서 예상하는 속성 이름 **AttributeName**로 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**`.` 바꾸기를 입력합니다. 예를 들어 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**입니다.

   b. JumpCloud속성 이름 필드에서 JumpCloud 디렉터리의 사용자 속성을 선택합니다. 예제로 이메일(직장).
4. 저장을 선택합니다.

(선택 사항) 액세스 제어에 속성 전달

IAM Identity Center의 액세스 제어를 위한 속성 기능을 사용하여 `Name` 속성이 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**로 설정된 `Attribute` 요소를 전달하도록 선택할 수 있습니다. 이 요소를 사용하면 속성을 SAML 어설션에 세션 태그로 전달할 수 있습니다. 세션 태그에 대한 자세한 내용은 IAM 사용 설명서의 AWS STS에서 세션 태그 전달을 참조하십시오.

속성을 세션 태그로 전달하려면 태그 값을 지정하는 `AttributeValue` 요소를 포함합니다. 예를 들어, 태그 키-값 쌍 `CostCenter = blue`를 전달하려면 다음 속성을 사용합니다.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

여러 속성을 추가해야 하는 경우 각 태그마다 별도의 `Attribute` 요소를 포함합니다.

Microsoft Entra ID 및 IAM Identity Center를 사용하여 SAML 및 SCIM 구성

AWS IAM Identity Center에서는 SAML(Security Assertion Markup Language) 2.0과의 통합은 물론 SCIM(System for Cross-domain Identity Management) 2.0 프로토콜을 사용하여 Microsoft Entra ID(이전 Azure Active Directory 또는 Azure AD)에서 IAM Identity Center로의 사용자 및 그룹 정보 자동 프로비저닝(동기화)을 지원합니다.

목표

이 자습서에서는 테스트 랩을 설정하고 Microsoft Entra ID 및 IAM Identity Center 간에 SAML 연결 및 SCIM 프로비저닝을 구성합니다. 초기 준비 단계에서는 양방향으로 SAML 연결을 테스트하는 데 사용할 Microsoft Entra ID 및 IAM Identity Center 모두에 테스트 사용자(Nikki Wolf)를 생성합니다. 나중에 SCIM 단계의 일부로 다른 테스트 사용자(Richard Roe)를 생성하여 Microsoft Entra ID의 새 속성이 예상대로 IAM Identity Center와 동기화되고 있는지 확인합니다.

사전 조건

이 자습서를 시작하려면 먼저 다음을 설정해야 합니다.

- Microsoft Entra ID 테넌트. 자세한 내용은 Microsoft 웹사이트에서 퀵스타트: 테넌트 설정을 참조하십시오.
- AWS IAM Identity Center 활성화 계정. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 IAM Identity Center 활성화를 참조하세요.

1단계: Microsoft 테넌트 준비

이 단계에서는 AWS IAM Identity Center 엔터프라이즈 애플리케이션을 설치 및 구성하고 새로 만든 Microsoft Entra ID 테스트 사용자에게 액세스 권한을 할당하는 방법을 안내합니다.

Step 1.1 >

1.1단계: Microsoft Entra ID에서 AWS IAM Identity Center 엔터프라이즈 애플리케이션 설정

이 절차에서는 Microsoft Entra ID에 AWS IAM Identity Center 엔터프라이즈 애플리케이션을 설치합니다. 나중에 AWS와의 SAML 연결을 구성하려면 이 애플리케이션이 필요합니다.

1. Microsoft Entra 관리 센터에 클라우드 애플리케이션 관리자 이상의 권한으로 로그인합니다.

2. ID > 애플리케이션 > 엔터프라이즈 애플리케이션으로 이동한 다음 새 애플리케이션을 선택합니다.
3. Microsoft Entra 갤러리 찾아보기 페이지의 검색 상자에 **AWS IAM Identity Center**을 입력합니다.
4. 결과 영역에서 AWS IAM Identity Center을 선택합니다.
5. 생성을 선택합니다.

Step 1.2 >

1.2단계: Microsoft Entra ID에서 테스트 사용자 생성

Nikki Wolf는 이 절차에서 생성할 Microsoft Entra ID 테스트 사용자의 이름입니다.

1. Microsoft Entra 관리 센터 콘솔에서 ID > 사용자 > 모든 사용자로 이동합니다.
2. 새 사용자를 선택한 다음 화면 상단에서 새 사용자 생성을 선택합니다.
3. 사용자 보안 주체 이름에 **NikkiWolf**를 입력하고 원하는 도메인과 확장자를 선택합니다. NikkiWolf@*example.org*를 예로 들 수 있습니다.
4. 표시 이름에 **NikkiWolf**를 입력합니다.
5. 암호 강력한 암호를 입력하거나 눈 모양 아이콘을 선택하여 자동 생성된 암호를 표시한 다음 표시된 값을 복사하거나 기록해 둡니다.
6. 속성 을 선택하고 이름에 **Nikki**를 입력합니다. 성에 **Wolf**를 입력합니다.
7. 검토 + 생성을 선택한 후 생성을 선택합니다.

Step 1.3

1.3단계: AWS IAM Identity Center에 권한을 부여하기 전에 Nikki의 환경 테스트

이 절차에서는 Nikki가 Microsoft 내 계정 포털에 성공적으로 로그인할 수 있는지 확인합니다.

1. 동일한 브라우저에서 새 탭을 열고 내 계정 포털 로그인 페이지로 이동한 다음 Nikki의 전체 이메일 주소를 입력합니다. NikkiWolf@*example.org*를 예로 들 수 있습니다.
2. 메시지가 표시되면 Nikki의 암호를 입력한 다음 로그인을 선택합니다. 자동 생성된 암호인 경우 암호를 변경하라는 메시지가 표시됩니다.
3. 작업 필요 페이지에서 나중에 물어보기를 선택하여 추가 보안 방법 메시지를 건너뜁니다.
4. 내 계정 페이지의 왼쪽 탐색 메뉴에서 내 앱을 선택합니다. 지금은 추가 기능 외에는 앱이 표시되지 않습니다. 이후 단계에서 여기에 표시될 AWS IAM Identity Center 앱을 추가하게 됩니다.

Step 1.4

1.4단계: Microsoft Entra ID에서 Nikki에게 권한 할당

이제 Nikki가 내 계정 포털에 성공적으로 액세스할 수 있음을 확인했으니 이 절차를 사용하여 Nikki의 사용자를 AWS IAM Identity Center 앱에 할당합니다.

1. Microsoft Entra 관리 센터 콘솔에서 ID > 애플리케이션 > 엔터프라이즈 애플리케이션으로 이동한 다음 목록에서 AWS IAM Identity Center을 선택합니다.
2. 왼쪽에서 사용자 및 그룹을 선택합니다.
3. 사용자/그룹 추가(Add user/group)를 선택합니다. 그룹을 할당할 수 없다는 메시지는 무시해도 좋습니다. 이 자습서에서는 할당에 그룹을 사용하지 않습니다.
4. 할당 추가 페이지의 사용자에서 선택된 항목 없음을 선택합니다.
5. NikkiWolf를 선택하고 선택을 선택합니다.
6. Add Assignment(할당 추가) 페이지에서 Assign(할당)을 선택합니다. 이제 AWS IAM Identity Center 앱에 할당된 사용자 목록에 NikkiWolf가 표시됩니다.

2단계: AWS 계정 준비

이 단계에서는 IAM Identity Center를 사용하여 권한 세트를 통해 액세스 권한을 구성하고, Nikki Wolf 사용자를 수동으로 생성하고, AWS에서 리소스를 관리하는 데 필요한 권한을 할당하는 방법을 안내합니다.

Step 2.1 >

2.1단계: IAM Identity Center에서 RegionalAdmin 권한 세트 생성

이 권한 세트는 AWS Management Console 내 계정 페이지에서 리전을 관리하는 데 필요한 AWS 계정 권한을 Nikki에게 부여하는 데 사용됩니다. Nikki 계정에서 다른 정보를 보거나 관리할 수 있는 기타 모든 권한은 기본적으로 거부됩니다.

1. IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한 아래에서 권한 집합을 선택합니다.
3. 권한 집합 생성을 선택합니다.
4. 권한 세트 유형 선택 페이지에서 사용자 지정 권한 세트를 선택하고 다음을 선택합니다.
5. 인라인 정책을 선택하여 확장하고, 다음 단계에 따라 권한 세트에 대한 정책을 생성합니다.

a. 새 문 추가를 선택하여 정책 문을 생성합니다.

b. 문 편집의 목록에서 계정을 선택하고 다음 확인란을 선택합니다.

- **ListRegions**
- **GetRegionOptStatus**
- **DisableRegion**
- **EnableRegion**

c. 리소스 추가 옆에 있는 추가를 선택합니다.

d. 리소스 추가 페이지의 리소스 유형에서 모든 리소스를 선택한 다음 리소스 추가를 선택합니다. 정책이 다음과 같은지 확인합니다.

```
{
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
                "account:DisableRegion",
                "account:EnableRegion",
                "account:GetRegionOptStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. 다음을 선택합니다.
7. 권한 세트 세부 정보 지정 페이지의 권한 세트 이름에서 **RegionalAdmin**을 입력하고 다음을 선택합니다.
8. 검토 및 생성(Review and create) 페이지에서 생성(Create)을 선택합니다. 권한 세트 목록에 RegionalAdmin이 표시될 것입니다.

Step 2.2 >

2.2단계: IAM Identity Center에서 해당 NikkiWolf 사용자 생성

SAML 프로토콜은 IdP(Microsoft Entra ID)를 쿼리하고 IAM Identity Center에서 사용자를 자동으로 생성하는 메커니즘을 제공하지 않으므로 다음 절차를 사용하여 IAM Identity Center에서 Microsoft Entra ID의 Nikki Wolfs 사용자의 핵심 속성을 미러링하는 사용자를 수동으로 생성합니다.

1. IAM Identity Center 콘솔을 엽니다.
2. 사용자를 선택하고 사용자 추가를 선택한 후 다음 정보를 입력합니다.
   a. 사용자 이름과 이메일 주소 모두 – Microsoft Entra ID 사용자 생성 시 사용한 **NikkiWolf@*yourcompanydomain.extension***을 입력합니다. NikkiWolf@*example.org*를 예로 들 수 있습니다.
   b. 이메일 주소 확인 - 이전 단계에서 사용한 이메일 주소를 다시 입력
   c. 이름 – **Nikki** 입력
   d. 성 – **Wolf** 입력
   e. 표시 이름 – **Nikki Wolf** 입력
3. 다음을 두 번 선택하고, 사용자 추가를 선택합니다.
4. Close(닫기)를 선택합니다.

Step 2.3

2.3단계: IAM Identity Center에 설정된 RegionalAdmin 권한에 Nikki 할당

여기에서 Nikki가 리전을 관리할 AWS 계정을 찾고, AWS 액세스 포털에 액세스하는 데 필요한 권한을 할당합니다.

1. IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한에서 AWS 계정를 선택합니다.
3. Nikki에게 리전을 관리할 수 있는 액세스 권한을 부여하려는 계정 이름(예: *Sandbox*) 옆의 확인란을 선택한 다음 사용자 및 그룹 할당을 선택합니다.
4. 사용자 및 그룹 할당 페이지에서 사용자 탭을 선택하고, Nikki 옆에 있는 확인란을 찾아 선택하고, 다음을 선택합니다.

3단계: SAML 연결 구성 및 테스트

이 단계에서는 IAM Identity Center의 외부 IdP 설정과 함께 Microsoft Entra ID에서 AWS IAM Identity Center 엔터프라이즈 애플리케이션을 사용하여 SAML 연결을 구성합니다.

Step 3.1 >

3.1단계: IAM Identity Center에서 필수 서비스 공급자 메타데이터 수집

이 단계에서는 IAM Identity Center 콘솔 내에서 ID 소스 변경 마법사를 시작하고 다음 단계에서 Microsoft Entra ID 연결을 구성할 때 입력해야 하는 메타데이터 파일과 AWS 관련 로그인 URL을 검색합니다.

1. IAM Identity Center 콘솔에서 설정을 선택합니다.
2. 설정 페이지에서 ID 소스 탭을 선택한 다음 작업 > ID 소스 변경을 선택합니다.
3. ID 소스 선택 페이지에서 외부 ID 제공업체를 선택하고 다음을 선택합니다.
4. 외부 ID 제공자 구성 페이지의 서비스 공급자 메타데이터에서 메타데이터 파일 다운로드를 선택하여 시스템에 다운로드합니다.
5. 같은 섹션에서 AWS 액세스 포털 로그인 URL 값을 찾아 복사합니다. 다음 단계에서 메시지가 표시될 때 이 값을 입력해야 합니다.
6. 이 페이지를 열어 두고 다음 단계(**`Step 3.2`**)로 이동하여 Microsoft Entra ID에서 AWS IAM Identity Center 엔터프라이즈 애플리케이션을 구성합니다. 나중에 이 페이지로 돌아와 프로세스를 완료하게 됩니다.

Step 3.2 >

3.2단계: Microsoft Entra ID에서 AWS IAM Identity Center 엔터프라이즈 애플리케이션 구성

이 절차에서는 지난 단계에서 얻은 메타데이터 파일 및 Sign-On URL의 값을 사용하여 Microsoft 측에서 SAML 연결의 절반을 설정합니다.

1. Microsoft Entra 관리 센터 콘솔에서 ID > 애플리케이션 > 엔터프라이즈 애플리케이션으로 이동한 다음 AWS IAM Identity Center을 선택합니다.
2. 왼쪽에서 Single Sign-On을 선택합니다.
3. SAML로 Single Sign-On 설정 페이지에서 메타데이터 파일 업로드를 선택하고 폴더 아이콘을 선택하고 이전 단계에서 다운로드한 서비스 공급자 메타데이터 파일을 선택한 다음 추가를 선택합니다.
4. 기본 SAML 구성 페이지에서 식별자 및 응답 URL 값이 이제 `https://<REGION>.signin.aws.amazon.com/platform/saml/`로 시작하는 AWS의 엔드포인트를 가리키는지 확인합니다.

5. Sign-On URL(선택 사항)에서 이전 단계(**Step 3.1**)에서 복사한 AWS 액세스 포털 로그인 URL 값을 붙여 넣고 저장을 선택한 다음 X를 선택하여 창을 닫습니다.
6. AWS IAM Identity Center을 사용한 Single Sign-On 테스트 메시지가 표시되면 아니요, 나중에 테스트하겠습니다를 선택합니다. 이 확인 작업은 이후 단계에서 수행하게 됩니다.
7. SAML로 Single Sign-On 설정 페이지의 SAML 인증서 섹션에 있는 페더레이션 메타데이터 XML 옆에서 다운로드를 선택하여 메타데이터 파일을 시스템에 저장합니다. 다음 단계에서 메시지가 표시될 때 이 파일을 업로드해야 합니다.

Step 3.3 >

3.3단계: AWS IAM Identity Center에서 Microsoft Entra ID 외부 IdP 구성

여기에서 IAM Identity Center 콘솔의 ID 소스 변경 마법사로 돌아가 AWS에서의 SAML 연결 후반부를 완료합니다.

1. IAM Identity Center 콘솔의 **Step 3.1**에서 열어 둔 브라우저 세션으로 돌아갑니다.
2. 외부 ID 제공업체 구성 페이지의 ID 제공업체 메타데이터 섹션에 있는 IdP SAML 메타데이터에서 파일 선택 버튼을 선택하고, 이전 단계에서 Microsoft Entra ID로부터 다운로드한 ID 제공업체 메타데이터 파일을 선택한 다음 열기를 선택합니다.
3. 다음을 선택합니다.
4. 고지 사항을 읽고 진행할 준비가 되면 **ACCEPT**를 입력합니다.
5. ID 소스 변경을 선택하여 변경 사항을 적용합니다.

Step 3.4 >

3.4단계: Nikki가 AWS 액세스 포털로 리디렉션되는지 테스트

이 절차에서는 Nikki의 보안 인증 정보로 Microsoft의 내 계정 포털에 로그인하여 SAML 연결을 테스트합니다. 인증이 완료되면 Nikki를 AWS 액세스 포털로 리디렉션할 AWS IAM Identity Center 애플리케이션을 선택합니다.

1. 내 계정 포털 로그인 페이지로 이동한 다음 Nikki의 전체 이메일 주소를 입력합니다. **NikkiWolf**@*example.org*를 예로 들 수 있습니다.
2. 메시지가 표시되면 Nikki의 암호를 입력한 다음 로그인을 선택합니다.
3. 내 계정 페이지의 왼쪽 탐색 메뉴에서 내 앱을 선택합니다.
4. 내 앱 페이지에서 이름이 AWS IAM Identity Center인 앱을 선택합니다. 그러면 추가 인증을 요구하는 메시지가 표시됩니다.

5. Microsoft 로그인 페이지에서 NikkiWolf의 보안 인증 정보를 선택합니다. 인증을 요구하는 메시지가 다시 표시되면 NikkiWolf의 보안 인증 정보를 다시 선택합니다. 그러면 자동으로 AWS 액세스 포털로 리디렉션됩니다.

> **Tip**
>
> 성공적으로 리디렉션되지 않는 경우 **Step 3.2**에서 입력한 AWS 액세스 포털 로그인 URL 값이 **Step 3.1**에서 복사한 원본 값과 일치하는지 확인합니다.

6. AWS 계정 아이콘

( )
이 표시되는지 확인합니다.

> **Tip**
>
> 페이지가 비어 있고 AWS 계정 아이콘이 표시되지 않는 경우 Nikki가 RegionalAdmin 권한 세트에 성공적으로 할당되었는지 확인합니다(**Step 2.3** 참조).

Step 3.5

3.5단계: Nikki의 액세스 수준을 테스트하여 AWS 계정 관리

이 단계에서는 Nikki의 액세스 수준을 확인하여 AWS 계정의 리전 설정을 관리합니다. Nikki는 계정 페이지에서 리전을 관리할 수 있는 충분한 관리자 권한만 보유해야 합니다.

1. AWS 액세스 포털에서 AWS 계정 아이콘

( )
선택하여 계정 목록을 확장합니다. 아이콘을 선택하면 권한 세트를 정의한 계정과 연결된 계정 이름, 계정 ID, 이메일 주소가 표시됩니다.

2. 권한 세트를 적용한 계정 이름(예: *Sandbox*)을 선택합니다(**Step 2.3** 참조). 그러면 Nikki가 계정을 관리하기 위해 선택할 수 있는 권한 세트 목록이 확장됩니다.
3. RegionalAdmin 옆에 있는 관리 콘솔을 선택하여 RegionalAdmin 권한 세트에서 정의한 역할을 맡을 관리 콘솔을 선택합니다. 그러면 AWS Management Console 홈 페이지로 리디렉션됩니다.

4. 콘솔의 오른쪽 상단 모서리 부분에서 계정 이름을 선택한 후 계정을 선택합니다. 그러면 계정 페이지로 이동합니다. 이 페이지의 다른 모든 섹션에는 해당 설정을 보거나 수정하는 데 필요한 권한이 없다는 메시지가 표시됩니다.
5. 계정 페이지에서 AWS 리전 섹션으로 이동합니다. 표에서 사용 가능한 리전의 확인란을 선택합니다. Nikki에게 계정의 리전 목록을 활성화 또는 비활성화하는 데 필요한 권한이 있습니다.

> 좋습니다!
>
> 1~3단계는 SAML 연결을 성공적으로 구현하고 테스트하는 데 도움이 되었습니다. 이제 자습서를 완료하려면 4단계로 이동하여 자동 프로비저닝을 구현하는 것이 좋습니다.

4단계: SCIM 동기화 구성 및 테스트

이 단계에서는 SCIM v2.0 프로토콜을 사용하여 Microsoft Entra ID에서 IAM Identity Center로 사용자 정보를 자동 프로비저닝(동기화)하도록 설정합니다. IAM Identity Center의 SCIM 엔드포인트와 IAM Identity Center에서 자동으로 생성한 베어러 토큰을 사용하여 Microsoft Entra ID에서 이 연결을 구성합니다.

SCIM 동기화를 구성할 때 Microsoft Entra ID의 사용자 속성을 IAM Identity Center의 명명된 속성에 매핑합니다. 이로 인해 IAM Identity Center와 Microsoft Entra ID 간에 예상 속성이 일치하게 됩니다.

다음 단계는 Microsoft Entra ID의 IAM Identity Center 앱을 사용하여 Microsoft Entra ID에 상주하는 사용자를 IAM Identity Center로 자동 프로비저닝하도록 활성화하는 방법을 안내합니다.

Step 4.1 >

4.1단계: Microsoft Entra ID에서 두 번째 테스트 사용자 생성

테스트 목적으로 Microsoft Entra ID에서 새 사용자(Richard Roe)를 생성합니다. 나중에 SCIM 동기화를 설정한 후 이 사용자와 모든 관련 속성이 IAM Identity Center에 성공적으로 동기화되었는지 테스트합니다.

1. Microsoft Entra 관리 센터 콘솔에서 ID > 사용자 > 모든 사용자로 이동합니다.
2. 새 사용자를 선택한 다음 화면 상단에서 새 사용자 생성을 선택합니다.
3. 사용자 보안 주체 이름에 **`RichRoe`**를 입력하고 원하는 도메인과 확장자를 선택합니다. RichRoe@*`example.org`*를 예로 들 수 있습니다.
4. 표시 이름에 **`RichRoe`**를 입력합니다.

5. 암호 강력한 암호를 입력하거나 눈 모양 아이콘을 선택하여 자동 생성된 암호를 표시한 다음 표시된 값을 복사하거나 기록해 둡니다.
6. 속성을 선택하고 다음 값을 입력합니다.
   - 이름 – **`Richard`** 입력
   - 성 – **`Roe`** 입력
   - 직책 - **`Marketing Lead`** 입력
   - 부서 - **`Sales`** 입력
   - 직원 ID - **`12345`** 입력
7. 검토 + 생성을 선택한 후 생성을 선택합니다.

Step 4.2 >

4.2단계: IAM Identity Center에서 자동 프로비저닝 활성화

이 절차에서는 IAM Identity Center 콘솔을 사용하여 Microsoft Entra ID에서 IAM Identity Center로 들어오는 사용자 및 그룹의 자동 프로비저닝을 활성화합니다.

1. IAM Identity Center 콘솔을 열고, 왼쪽 탐색 창에서 설정을 선택합니다.
2. 설정 페이지의 ID 소스 탭에서 프로비저닝 방법이 수동으로 설정되어 있는지 확인합니다.
3. 자동 프로비저닝 정보 상자를 찾은 다음 활성화를 선택합니다. 그러면 IAM Identity Center에서 자동 프로비저닝이 즉시 활성화되고 필요한 SCIM 엔드포인트 및 액세스 토큰 정보가 표시됩니다.
4. 인바운드 자동 프로비저닝 대화 상자에서 다음 옵션의 각 값을 복사합니다. 다음 단계에서 Microsoft Entra ID에서 프로비저닝을 구성할 때 이를 붙여 넣어야 합니다.
   a. SCIM 엔드포인트 - 예: https://scim.*us-east-2*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2/
   b. 액세스 토큰 - 토큰 표시를 선택하여 값을 복사합니다.
5. 닫기를 선택하세요.
6. ID 소스 탭에서 프로비저닝 방법이 이제 SCIM으로 설정된 것을 확인할 수 있습니다.

Step 4.3 >

4.3단계: Microsoft Entra ID에서 자동 프로비저닝 구성

이제 RichRoe 테스트 사용자가 있고 IAM Identity Center에서 SCIM을 활성화했으므로 Microsoft Entra ID에서 SCIM 동기화 설정을 구성할 수 있습니다.

1. Microsoft Entra 관리 센터 콘솔에서 ID > 애플리케이션 > 엔터프라이즈 애플리케이션으로 이동한 다음 AWS IAM Identity Center을 선택합니다.
2. 프로비저닝을 선택하고 관리에서 프로비저닝을 다시 선택합니다.
3. 프로비저닝 모드에서 자동을 선택합니다.
4. 관리자 보안 인증 정보의 테넌트 URL에서 이전 **Step 4.1**에서 복사한 SCIM 엔드포인트 URL 값을 붙여 넣습니다. 비밀 토큰에 액세스 토큰 값을 붙여 넣습니다.
5. [Test Connection]을 선택합니다. 테스트된 보안 인증 정보에 프로비저닝 활성화가 성공적으로 승인되었다는 메시지가 표시되어야 합니다.
6. 저장을 선택합니다.
7. 관리에서 사용자 및 그룹을 선택한 다음 사용자/그룹 추가를 선택합니다.
8. 할당 추가 페이지의 사용자에서 선택된 항목 없음을 선택합니다.
9. RichRoe를 선택하고 선택을 선택합니다.
10. Add Assignment(할당 추가) 페이지에서 Assign(할당)을 선택합니다.
11. 개요를 선택한 다음 프로비저닝 시작을 선택합니다.

Step 4.4

4.4단계: 동기화가 발생했는지 확인

이 섹션에서는 Richard의 사용자가 성공적으로 프로비저닝되었고 모든 속성이 IAM Identity Center에 표시되는지 확인합니다.

1. IAM Identity Center 콘솔에서 사용자를 선택합니다.
2. 사용자 페이지에 RichRoe 사용자가 표시되어야 합니다. 생성 열에서 값이 SCIM으로 설정되어 있는지 확인합니다.
3. 프로필에서 RichRoe를 선택하고 다음 속성이 Microsoft Entra ID에서 복사되었는지 확인합니다.
   - 이름 - **Richard**
   - 성 - **Roe**
   - 부서 - **Sales**

- 직책 - **`Marketing Lead`**
- 직원 번호 - **`12345`**

이제 IAM Identity Center에서 Richard의 사용자가 생성되었으므로, 모든 권한 세트를 할당하여 AWS 리소스에 대한 액세스 수준을 제어할 수 있습니다. 예를 들어 이전에 사용한 **`RegionalAdmin`** 권한 세트에 RichRoe를 할당하여 Nikki에게 리전을 관리할 권한을 부여(**`Step 2.3`** 참조)한 다음 **`Step 3.5`**를 사용하여 액세스 수준을 테스트할 수 있습니다.

> 축하합니다!
>
> Microsoft와 AWS 간에 SAML 연결을 성공적으로 설정하고 자동 프로비저닝이 작동하여 모든 것이 동기화된 것을 확인했습니다. 이제 학습한 내용을 적용하여 프로덕션 환경을 보다 원활하게 설정할 수 있습니다.

프로덕션 환경에서 Microsoft Entra ID와 SCIM 사용 시 고려할 사항

다음은 SCIM v2 프로토콜을 사용하여 프로덕션 환경에서 IAM Identity Center를 통해 자동 프로비저닝을 구현하는 방법에 영향을 미칠 수 있는 Microsoft Entra ID 관련 중요 고려 사항입니다.

> Note
>
> SCIM 배포를 시작하기 전에 먼저 자동 프로비저닝을 사용할 때 고려 사항의 내용을 검토하는 것이 좋습니다.

액세스 제어를 위한 속성

액세스 제어 속성은 ID 소스에서 AWS 리소스에 액세스할 수 있는 사용자를 결정하는 권한 정책에 사용됩니다. Microsoft Entra ID의 사용자로부터 속성을 제거해도 IAM Identity Center의 해당 사용자에서는 해당 속성이 제거되지 않습니다. 이것은 Microsoft Entra ID의 알려진 문제입니다. 사용자의 속성이 비어 있지 않은 다른 값으로 변경하면 해당 변경 내용이 IAM Identity Center에 동기화됩니다.

중첩된 그룹

Microsoft Entra ID 사용자 프로비저닝 서비스는 중첩된 그룹의 사용자를 읽거나 프로비저닝할 수 없습니다. 명시적으로 할당된 그룹의 직계 구성원인 사용자만 읽고 프로비저닝할 수 있습니다. Microsoft

Entra ID는 간접적으로 할당된 사용자 또는 그룹(직접 할당된 그룹의 구성원인 사용자 또는 그룹)의 그룹 구성원 자격을 반복적으로 해제하지 않습니다. 자세한 내용은 Microsoft Entra ID 설명서의 할당 기반 범위 지정을 참조하세요.

동적 그룹

Microsoft Entra ID 사용자 프로비저닝 서비스는 동적 그룹의 사용자를 읽거나 프로비저닝할 수 없습니다. 동적 그룹을 사용하는 동안의 사용자 및 그룹 구조와 IAM Identity Center에 표시되는 방식을 보여주는 예는 아래를 참조하십시오. 이러한 사용자 및 그룹은 SCIM을 통해 Microsoft Entra ID에서 IAM Identity Center로 프로비저닝되었습니다.

예를 들어 동적 그룹의 Microsoft Entra ID 구조는 다음과 같습니다.

1. 구성원 ua1, ua2로 구성된 그룹 A
2. 구성원 ub1의 그룹 B
3. 구성원 uc1의 그룹 C
4. 그룹 A, B, C의 구성원을 포함하는 규칙이 있는 그룹 K
5. 그룹 B, C의 구성원을 포함하는 규칙이 있는 그룹 L

사용자 및 그룹 정보가 SCIM을 통해 Microsoft Entra ID에서 IAM Identity Center로 제공된 후 구조는 다음과 같습니다.

1. 구성원 ua1, ua2로 구성된 그룹 A
2. 구성원 ub1의 그룹 B
3. 구성원 uc1의 그룹 C
4. 구성원 ua1, ua2, ub1, uc1로 구성된 그룹 K
5. 구성원 ub1, uc1의 그룹 L

동적 그룹을 사용하여 자동 프로비저닝을 구성할 때는 다음 사항을 명심하십시오.

- 동적 그룹에는 중첩된 그룹이 포함될 수 있습니다. 하지만 Microsoft Entra ID 프로비저닝 서비스는 중첩된 그룹을 단순화하지 않습니다. 예를 들어 다음 Microsoft Entra ID 구조의 동적 그룹을 가지고 있습니다.
  - 그룹 A는 그룹 B의 부모입니다.
  - 그룹 A에는 ua1이 구성원으로 있습니다.
  - 그룹 B에는 ub1이 구성원으로 있습니다.

그룹 A를 포함하는 동적 그룹에는 그룹 A의 직속 구성원(즉, ua1)만 포함됩니다. 그룹 B의 구성원은 반복적으로 포함되지 않습니다.

- 동적 그룹은 다른 동적 그룹을 포함할 수 없습니다. 자세한 내용은 Microsoft Entra ID 설명서의 미리 보기 제한 사항을 참조하세요.

Microsoft Entra ID 관련 SCIM 문제 해결

Microsoft Entra ID 사용자가 IAM Identity Center와 동기화되지 않는 문제가 발생하는 경우, IAM Identity Center에 새 사용자를 추가할 때 IAM Identity Center에서 플래그를 지정한 구문 문제 때문일 수 있습니다. Microsoft Entra ID 감사 로그에서 `'Export'`와 같은 실패한 이벤트가 있는지 검토하여 이를 확인할 수 있습니다. 이 이벤트의 상태 설명에는 다음과 같은 내용이 나와 있습니다.

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is
 unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

실패한 이벤트가 있는지 AWS CloudTrail를 확인할 수도 있습니다. 이 작업은 CloudTrail의 이벤트 기록 콘솔에서 다음 필터를 사용하여 검색하면 됩니다.

```
"eventName":"CreateUser"
```

CloudTrail 이벤트의 오류는 다음과 같이 표시됩니다.

```
"errorCode": "ValidationException",
        "errorMessage": "Currently list attributes only allow single item“
```

궁극적으로 이 예외는 Microsoft Entra ID에서 전달된 값 중 하나에 예상보다 많은 값이 포함되어 있음을 의미합니다. 해결 방법은 Microsoft Entra ID에서 사용자 속성을 검토하여 중복된 값을 포함하지 않는지 확인하는 것입니다. 값이 중복되는 일반적인 예로는 휴대폰, 회사, 팩스 등의 연락처 번호에 여러 개의 값이 있는 경우를 들 수 있습니다. 값은 별개이지만 모두 단일 상위 속성인 phoneNumbers에 따라 IAM Identity Center에 전달됩니다.

일반 SCIM 문제 해결 팁은 IAM Identity Center 문제 해결 섹션을 참조하세요.

5단계: (선택 사항) ABAC 구성

SAML과 SCIM을 구성했으므로 ABAC(속성 기반 액세스 제어)를 구성할 수도 있습니다. ABAC는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다.

Microsoft Entra ID를 통해 다음 두 가지 방법 중 하나를 사용하여 IAM Identity Center에서 사용할 ABAC를 구성할 수 있습니다.

Method 1

방법 1: IAM Identity Center에서 액세스 제어에 사용되는 Microsoft Entra ID 사용자 속성 구성

다음 절차에서는 IAM Identity Center에서 AWS 리소스 액세스를 관리하기 위해 사용해야 하는 Microsoft Entra ID의 속성을 확인합니다. 정의가 완료되면 Microsoft Entra ID는 SAML 어설션을 통해 이러한 속성을 IAM Identity Center로 전송합니다. 그런 다음 Microsoft Entra ID로부터 전달한 속성을 기반으로 액세스를 관리하기 위해 IAM Identity Center에서 권한 집합을 생성합니다. 해야 합니다.

이 절차를 시작하기 전에 먼저 액세스 제어를 위한 속성 기능을 활성화해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 액세스 제어를 위한 속성 활성화 및 구성 단원을 참조하십시오.

1. Microsoft Entra 관리 센터 콘솔에서 ID > 애플리케이션 > 엔터프라이즈 애플리케이션으로 이동한 다음 AWS IAM Identity Center을 선택합니다.
2. Single Sign-On을 선택합니다.
3. 속성 및 클레임 섹션에서 편집을 선택합니다.
4. 속성 및 클레임 페이지에서 다음을 수행합니다.
   a. 새 클레임 추가를 선택합니다.
   b. 이름에 `AccessControl:`*`AttributeName`*를 입력합니다. IAM Identity Center에서 *`AttributeName`*을 예상하는 속성의 이름으로 바꿉니다. 예: `AccessControl:`**`Department`**.
   c. 네임스페이스(Namespace)에**`https://aws.amazon.com/SAML/Attributes`**를 입력합니다.
   d. 소스에서 속성를 선택합니다.
   e. 소스 속성의 경우 드롭다운 목록을 사용하여 Microsoft Entra ID 사용자 속성을 선택합니다. 예: `user.`**`department`**.
5. SAML 어설션에서 IAM Identity Center로 전송해야 하는 각 속성에 대해 이전 단계를 반복합니다.
6. 저장을 선택합니다.

Method 2

방법 2: IAM Identity Center를 사용하여 ABAC 구성

이 방법을 사용하면 IAM Identity Center의 액세스 제어를 위한 속성 기능을 사용하여 `Name` 속성이 `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`로 설정된 `Attribute` 요소를 전달합니다. 이 요소를 사용해 SAML 어설션에 속성을 세션 태그로 전달할 수 있습니다. 세션 태그에 대한 자세한 내용은 IAM 사용 설명서의 AWS STS에서 세션 태그 전달을 참조하십시오.

속성을 세션 태그로 전달하려면 태그 값을 지정하는 `AttributeValue` 요소를 포함합니다. 예를 들어, 태그 키-값 쌍 `CostCenter = blue`를 전달하려면 다음 속성을 사용합니다.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

여러 속성을 추가해야 하는 경우 각 태그마다 별도의 `Attribute` 요소를 포함합니다.

Okta 및 IAM Identity Center를 사용하여 SAML 및 SCIM 구성

SCIM(System for Cross-domain Identity Management) v2.0 프로토콜을 사용하여 Okta의 사용자 및 그룹 정보를 IAM Identity Center로 자동 프로비저닝(동기화)할 수 있습니다. Okta에서 이 연결을 구성하려면 IAM Identity Center의 SCIM 엔드포인트와 IAM Identity Center에서 자동으로 생성한 베어러 토큰을 사용합니다. SCIM 동기화를 구성할 때 Okta의 사용자 속성을 IAM Identity Center의 명명된 속성에 매핑합니다. 이 매핑은 IAM Identity Center와 Okta 간의 예상 사용자 속성을 일치시킵니다.

Okta는 SCIM을 통해 IAM Identity Center에 연결할 경우 다음과 같은 프로비저닝 기능을 지원합니다.

- 사용자 생성 - Okta에서 IAM Identity Center 애플리케이션에 할당된 사용자는 IAM Identity Center에서 프로비저닝됩니다.
- 사용자 속성 업데이트 — Okta에서 IAM Identity Center 애플리케이션에 할당된 사용자의 속성 변경 사항이 IAM Identity Center에서 업데이트됩니다.
- 사용자 비활성화 - Okta에서 IAM Identity Center 애플리케이션에 할당을 취소된 사용자는 IAM Identity Center에서 비활성화됩니다.

- 그룹 푸시 - Okta에서 그룹 (및 해당 구성원)이 IAM Identity Center에 동기화됩니다.

> **Note**
>
> Okta과 IAM Identity Center 모두에서 관리 오버헤드를 최소화하려면 개별 사용자 대신 그룹을 할당하고 푸시하는 것이 좋습니다.

IAM Identity Center를 아직 활성화하지 않은 경우 활성화 AWS IAM Identity Center의 내용을 참조하세요.

목표

이 자습서에서는 Okta IAM Identity Center와의 SAML 연결 설정 방법을 안내합니다. 나중에 SCIM을 사용하여 Okta에서 사용자를 동기화합니다. 이 시나리오에서는 Okta에서 모든 사용자와 그룹을 관리합니다. Okta 포털을 통해 로그인합니다. 모든 것이 올바르게 구성되었는지 확인하려면 구성 단계를 완료한 후 Okta 사용자로 로그인하고 AWS 리소스에 대한 액세스 권한을 확인합니다.

> **Note**
>
> Okta's IAM Identity Center 애플리케이션이 설치된 Okta 계정(무료 평가판)을 등록할 수 있습니다. 유료 Okta 제품의 경우 Okta 라이선스가 라이프사이클 관리 또는 아웃바운드 프로비저닝을 활성화하는 유사 기능을 지원하는지 확인해야 할 수도 있습니다. 이러한 기능은 Okta에서 IAM Identity Center로 SCIM을 구성하는 데 필요할 수 있습니다.

시작하기 전 준비 사항

IAM ID 센터 간의 Okta SCIM 프로비저닝을 구성하기 전에 먼저 검토하는 것이 좋습니다. 자동 프로비저닝을 사용할 때 고려 사항

시작하기 전에 확인할 사항:

- 모든 Okta 사용자는 이름, 성, 사용자 이름 및 표시 이름 값이 지정되어야 합니다.
- 각 Okta 사용자는 이메일 주소 또는 전화번호와 같은 데이터 속성당 하나의 값만 보유합니다. 값이 여러 개인 사용자는 동기화에 실패합니다. 속성에 여러 개의 값이 있는 사용자가 있는 경우 IAM Identity Center에서 사용자를 프로비저닝하기 전에 중복된 속성을 제거합니다. 예를 들어 전화번호 속성은 하나만 동기화할 수 있습니다. 기본 전화번호 속성이 “회사 전화번호”이므로 사용자의 전화번

호가 집이나 휴대폰 전화번호인 경우에도 “회사 전화번호” 속성을 사용하여 사용자의 전화번호를 저장합니다.

- 사용자 주소를 업데이트하는 경우 streetAddress, city, state, zipCode 및 countryCode 값을 지정해야 합니다. 동기화 시 Okta 사용자에 대해 이러한 값이 지정되지 않은 경우, 사용자 또는 사용자에 대한 변경 내용은 프로비저닝되지 않습니다.

> **Note**
>
> 권한 및 역할 속성은 지원되지 않으며 IAM Identity Center와 동기화할 수 없습니다.
> 할당과 그룹 푸시 모두에 동일한 Okta 그룹을 사용하는 것은 현재 지원되지 않습니다. Okta와 IAM Identity Center 간에 일관된 그룹 구성원 자격을 유지하려면 별도의 그룹을 생성하고 그룹을 IAM Identity Center로 푸시하도록 구성합니다.

1단계: Okta 계정에서 SAML 메타데이터 획득

1. Okta admin dashboard에 로그인하고, 애플리케이션을 확장한 다음 애플리케이션을 선택합니다.
2. 애플리케이션(Applications) 페이지에서 앱 카탈로그 찾아보기(Browse App Catalog)를 선택합니다.
3. 검색 상자에 IAM Identity Center 앱을 추가할 앱을 입력하고 AWS IAM Identity Center선택합니다.
4. 로그인 탭을 선택합니다.
5. SAML 서명 인증서에서 작업을 선택한 다음 IdP 메타데이터 보기를 선택합니다. 새 브라우저 탭이 열리고 XML 파일의 문서 트리를 보여줍니다. `<md:EntityDescriptor>`에서 `</md:EntityDescriptor>`까지 XML 전체를 선택하고 텍스트 파일에 복사합니다.
6. 텍스트 파일을 `metadata.xml`로 저장합니다.

Okta admin dashboard를 열려 있는 상태로 두고, 이후 단계에서는 콘솔을 계속 사용합니다.

2단계: IAM Identity Center의 ID 소스로 Okta 구성

1. 관리 권한이 있는 사용자로 IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 작업을 선택한 다음 ID 소스 변경을 선택합니다.
4. ID 소스 선택에서 외부 ID 제공업체를 선택하고 다음을 선택합니다.

5. 외부 ID 제공업체 구성 에서 다음을 수행합니다.

   a. 서비스 공급자 메타데이터에서 메타데이터 파일 다운로드를 선택하여 IAM Identity Center 메타데이터 파일을 다운로드하고 시스템에 저장합니다. 이후 자습서에서 IAM Identity Center SAML 메타데이터 파일을 Okta에 제공합니다.

      쉽게 액세스할 수 있도록 다음 항목을 텍스트 파일에 복사합니다.

      - IAM Identity Center Assertion Consumer Service(ACS) URL
      - IAM Identity Center 발급자 URL

      이후 자습서에서는 이러한 값을 업데이트합니다.

   b. ID 제공자 메타데이터의 IdP SAML 메타에서 파일 선택을 선택한 다음 이전 단계에서 만든 `metadata.xml` 파일을 선택합니다.

   c. 다음을 선택합니다.

6. 고지 사항을 읽고 진행할 준비가 되면 ACCEPT를 입력합니다.
7. ID 소스 변경을 선택합니다.

   AWS 콘솔을 열린 상태로 두면 다음 단계에서 해당 콘솔을 계속 사용하게 됩니다.

8. Okta admin dashboard로 돌아가 AWS IAM Identity Center 앱의 로그인 탭을 선택하고 편집을 클릭합니다.
9. 고급 로그인 설정에서 다음을 입력합니다.

   - ACS URL의 경우 IAM Identity Center ACS(Assertion Consumer Service) URL에서 복사한 값을 입력합니다.
   - 발급자 URL의 경우 IAM Identity Center 발급자 URL에서 복사한 값을 입력합니다.
   - 애플리케이션 사용자 이름 형식의 경우 드롭다운 메뉴에서 옵션 중 하나를 선택합니다.

     선택한 값이 각 사용자마다 고유해야 합니다. 이 자습서에서는 Okta 사용자 이름을 선택합니다.

10. 저장을 선택합니다.

이제 IAM Identity Center에서 Okta의 사용자를 프로비저닝할 준비가 되었습니다. Okta admin dashboard열린 상태로 두고 IAM Identity Center 콘솔로 돌아가 다음 단계를 진행하십시오.

3단계: Okta에서 사용자 프로비저닝

1. IAM Identity Center의 설정 페이지에서 자동 프로비저닝 정보 상자를 찾은 다음 활성화를 선택합니다. 그러면 IAM Identity Center에서 자동 프로비저닝이 활성화되고 필요한 SCIM 엔드포인트 및 액세스 토큰 정보가 표시됩니다.
2. 인바운드 자동 프로비저닝 대화 상자에서 다음 옵션의 값을 각각 복사합니다.

   - SCIM 엔드포인트
   - 액세스 토큰

   이 자습서의 뒷부분에서는 이러한 값을 입력하여 프로비저닝을 구성해 보겠습니다. Okta
3. 닫기를 선택하세요.
4. Okta admin dashboard로 돌아가서 IAM Identity Center 앱으로 이동합니다.
5. IAM Identity Center 앱 페이지에서 프로비저닝 탭을 선택한 다음 왼쪽 탐색 메뉴의 설정에서 통합을 선택합니다.
6. 편집을 선택한 다음 API 통합 활성화 옆의 확인란을 선택하여 프로비저닝을 활성화합니다.
7. 이 자습서의 앞부분에서 복사한 IAM Identity Center의 SCIM 프로비저닝 값을 사용하여 Okta를 구성합니다.

   a. 기본 URL 필드에 SCIM 엔드포인트 값을 입력합니다. URL 끝에 있는 후행 슬래시를 제거했는지 확인합니다.

   b. API 토큰 필드에 액세스 토큰 값을 입력합니다.
8. API 보안 인증 테스트를 선택하여 입력한 보안 인증 정보가 유효한지 확인합니다.

   AWS IAM Identity Center 확인 완료! 메시지가 표시됩니다.
9. 저장을 선택합니다. 통합이 선택된 상태로 설정 영역으로 이동합니다.
10. 설정에서 To App을 선택한 다음 활성화하려는 각 앱 프로비저닝 기능에 대해 활성화 확인란을 선택합니다. 이 자습서에서는 모든 옵션을 선택합니다.
11. 저장을 선택합니다.

이제 Okta의 사용자를 IAM Identity Center와 동기화할 준비가 되었습니다.

4단계: Okta의 사용자를 IAM Identity Center와 동기화

기본적으로 Okta IAM Identity Center 앱에는 어떤 사용자 또는 그룹도 할당되지 않습니다. 프로비저닝 그룹은 그룹 구성원인 사용자를 프로비저닝합니다. 다음 단계를 완료하여 그룹 및 사용자를 IAM Identity Center와 동기화합니다.

1. OktaIAM Identity Center 앱 페이지에서 할당 탭을 선택합니다. 사람과 그룹을 모두 IAM Identity Center 앱에 할당할 수 있습니다.

   a. 사람 할당:

      - 할당 페이지에서 할당을 선택한 다음 사람에게 할당을 선택합니다.
      - IAM Identity Center 앱에 대한 액세스 권한을 보유하려는 Okta 사용자를 선택합니다. 할당 및 저장 후 뒤로 가기를 선택한 다음 완료를 선택합니다.

      그러면 사용자를 IAM Identity Center에 프로비저닝하는 프로세스가 시작됩니다.

   b. 그룹 할당:

      - 할당 페이지에서 할당을 선택한 다음 그룹에 할당을 선택합니다.
      - IAM Identity Center 앱에 대한 액세스 권한을 보유하려는 Okta 그룹을 선택합니다. 할당 및 저장 후 뒤로 가기를 선택한 다음 완료를 선택합니다.

      그러면 그룹의 사용자를 IAM Identity Center에 프로비저닝하는 프로세스가 시작됩니다.

      > **Note**
      >
      > 일부 사용자 레코드에 없는 경우 그룹에 대한 추가 속성을 지정해야 할 수 있습니다. 그룹에 지정된 속성은 모든 개별 속성 값보다 우선합니다.

2. 푸시 그룹 탭을 선택합니다. IAM Identity Center 앱에 할당한 모든 그룹이 포함된 Okta 그룹을 선택합니다. 저장을 선택합니다.

   그룹과 구성원이 IAM Identity Center로 푸시되면 그룹 상태가 활성으로 변경됩니다.

3. 할당 탭으로 돌아갑니다.
4. IAM Identity Center에 푸시한 그룹의 구성원이 아닌 사용자가 있는 경우 다음 단계를 사용하여 사용자를 개별적으로 추가합니다.

   할당 페이지에서 할당을 선택한 다음 사람에게 할당을 선택합니다.

5. IAM Identity Center 앱에 대한 액세스 권한을 보유하려는 Okta 사용자를 선택합니다. 할당 및 저장 후 뒤로 가기를 선택한 다음 완료를 선택합니다.

   그러면 개별 사용자를 IAM Identity Center에 프로비저닝하는 프로세스가 시작됩니다.

   > **Note**
   >
   > 의 애플리케이션 페이지에서 AWS IAM Identity Center 앱에 사용자와 그룹을 할당할 수도 있습니다. Okta admin dashboard 이를 위해 설정 아이콘을 선택하고 사용자에게 할당 또는 그룹에 할당을 선택한 다음 사용자나 그룹을 지정합니다.

6. IAM Identity Center 콘솔로 돌아갑니다. 왼쪽 탐색 창에서 사용자를 선택하면 Okta 사용자가 입력한 사용자 목록이 표시됩니다.

> **축하합니다!**
>
> Okta AWS 와 사이에 SAML 연결을 성공적으로 설정하고 자동 프로비저닝이 작동하는지 확인했습니다. 이제 IAM Identity Center에서 계정과 애플리케이션을 사용자에게 할당할 수 있습니다. 이 자습서에서는 다음 단계로 관리 계정에 관리 권한을 부여하여 사용자 중 한 명을 IAM Identity Center 관리자로 지정합니다.

5단계: 계정에 Okta 사용자 액세스 권한 부여

1. IAM Identity Center 탐색 창의 다중 계정 권한에서 AWS 계정을 선택합니다.
2. AWS 계정 페이지의 조직 구조에는 조직 루트가 표시되고 계층 구조에 따라 그 아래에 사용자 계정이 표시됩니다. 관리 계정의 확인란을 선택한 다음 사용자 또는 그룹 할당을 선택합니다.
3. 사용자 및 그룹 할당 워크플로가 표시됩니다. 워크플로는 세 단계로 구성됩니다.

   a. 1단계: 사용자 및 그룹 선택에서 관리자 작업을 수행할 사용자를 선택합니다. 다음을 선택합니다.

   b. 2단계: 권한 세트 선택에서 권한 세트 생성을 선택하여 권한 세트 생성과 관련된 3가지 하위 단계를 안내하는 새 탭이 열립니다.

      i. 1단계: 권한 세트 유형 선택에서 다음을 완료합니다.

         - 권한 세트 유형에서 사전 정의된 권한 세트를 선택합니다.

- 사전 정의된 권한 집합에 대한 정책에서 원하는 항목을 선택합니다. AdministratorAccess

다음을 선택합니다.

ii. 2단계: 권한 세트 세부 정보 지정 페이지에서 기본 설정을 유지하고 다음을 선택합니다.

기본 설정에서는 세션 시간이 1시간으로 설정된 *AdministratorAccess*이름의 권한 집합을 생성합니다.

iii. 3단계: 검토 및 생성의 경우 권한 집합 유형이 AWS 관리형 정책을 사용하는지 확인하십시오 AdministratorAccess. 생성을 선택합니다. 권한 세트 페이지에 권한 세트가 생성되었음을 알리는 알림이 표시됩니다. 이제 웹 브라우저에서 이 탭을 닫을 수 있습니다.

사용자 및 그룹 할당 브라우저 탭에서 권한 세트 생성 워크플로를 시작한 2단계: 권한 세트 선택에 여전히 있습니다.

권한 세트 영역에서 새로 고침 버튼을 선택합니다. 생성한 *AdministratorAccess*권한 집합이 목록에 나타납니다. 권한 세트의 확인란을 선택하고 다음을 선택합니다.

c. 3단계: 검토 및 제출에서 선택한 사용자 및 권한 세트를 검토한 다음 제출을 선택합니다.

구성 중이라는 메시지와 함께 페이지가 업데이트됩니다. AWS 계정 프로세스가 완료될 때까지 기다립니다.

AWS 계정 페이지로 돌아옵니다. 다시 프로비전되었으며 업데이트된 권한 집합이 AWS 계정 적용되었음을 알리는 알림 메시지가 나타납니다. 사용자가 로그인하면 역할을 선택할 수 있는 옵션이 제공됩니다. *AdministratorAccess*

> **Note**
>
> Okta의 SCIM 자동 동기화는 사용자 프로비저닝만 지원하며 그룹은 자동으로 프로비저닝되지 않습니다. AWS Management Console을 사용하여 Okta 사용자에 대한 그룹을 생성할 수는 없습니다. 사용자를 프로비저닝한 후 CLI 또는 API 작업을 사용하여 그룹을 생성할 수 있습니다.

6단계: 리소스에 대한 Okta 사용자 액세스 확인 AWS

1. 테스트 사용자 계정을 사용하여 Okta dashboard에 로그인합니다.

2. 내 앱에서 AWS IAM Identity Center 아이콘을 선택합니다.
3. 포털에 로그인하고 AWS 계정 아이콘을 볼 수 있습니다. 아이콘을 펼치면 사용자가 접근할 수 AWS 계정 있는 목록이 표시됩니다. 이 자습서에서는 단일 계정만 사용했으므로 아이콘을 확장하면 하나의 계정만 표시됩니다.
4. 계정을 선택하면 사용자에게 제공되는 권한 세트가 표시됩니다. 이 자습서에서는 AdministratorAccess권한 집합을 만들었습니다.
5. 권한 세트 옆에는 해당 권한 세트에 사용할 수 있는 액세스 유형에 대한 링크가 있습니다. 권한 세트를 생성할 때 관리 콘솔과 프로그래밍 방식 액세스를 모두 활성화하도록 지정했으므로 두 가지 옵션이 제공됩니다. 관리 콘솔을 선택하면 AWS Management Console이 열립니다.
6. 사용자가 콘솔에 로그인합니다.

(선택 사항) 액세스 제어에 속성 전달

IAM Identity Center의 액세스 제어를 위한 속성 기능을 사용하여 `Name` 속성이 `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`로 설정된 `Attribute` 요소를 전달하도록 선택할 수 있습니다. 이 요소를 사용하면 속성을 SAML 어설션에 세션 태그로 전달할 수 있습니다. 세션 태그에 대한 자세한 내용은 IAM 사용 설명서의 AWS STS에서 세션 태그 전달을 참조하세요.

속성을 세션 태그로 전달하려면 태그 값을 지정하는 `AttributeValue` 요소를 포함합니다. 예를 들어, 태그 키-값 쌍 `CostCenter = blue`를 전달하려면 다음 속성을 사용합니다.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

여러 속성을 추가해야 하는 경우 각 태그마다 별도의 `Attribute` 요소를 포함합니다.

다음 단계

이제 Okta를 ID 제공업체로 구성하고 IAM Identity Center의 사용자를 프로비저닝했기 때문에 다음을 수행할 수 있습니다.

- 에 대한 액세스 권한 부여 AWS 계정, 참조사용자에게 액세스 권한을 할당하십시오. AWS 계정.

- 클라우드 애플리케이션에 대한 액세스 권한을 부여하려면 IAM Identity Center 콘솔에서 애플리케이션에 사용자 액세스 권한 할당의 내용을 참조하세요.
- 직무에 따라 권한을 구성합니다. 권한 세트 생성을 참조하세요.

OneLogin 및 IAM Identity Center 간에 SCIM 프로비저닝 설정

IAM Identity Center는 도메인 간 ID 관리 시스템(SCIM) v2.0 프로토콜을 사용하여 OneLogin의 사용자 및 그룹 정보를 IAM Identity Center로 자동 프로비저닝(동기화)할 수 있도록 지원합니다. IAM Identity Center의 SCIM 엔드포인트와 IAM Identity Center에서 자동으로 생성한 베어러 토큰을 사용하여 OneLogin에서 이 연결을 구성합니다. SCIM 동기화를 구성할 때 OneLogin의 사용자 속성을 IAM Identity Center의 명명된 속성에 매핑합니다. 이로 인해 IAM Identity Center와 OneLogin 간에 예상 속성이 일치하게 됩니다.

다음 단계는 SCIM 프로토콜을 사용하여 OneLogin에서 IAM Identity Center으로 사용자 및 그룹을 자동으로 프로비저닝하도록 활성화하는 방법을 안내합니다.

> **Note**
>
> SCIM 배포를 시작하기 전에 먼저 자동 프로비저닝을 사용할 때 고려 사항를 검토하는 것이 좋습니다.

주제

- 사전 조건
- 1단계: IAM Identity Center 프로비저닝 활성화
- 2단계: OneLogin에서 프로비저닝 구성
- (선택 사항) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 OneLogin 사용자 속성 구성
- (선택 사항) 액세스 제어에 속성 전달
- 문제 해결

사전 조건

시작하기 전에 다음을 준비해야 합니다.

- OneLogin 계정. 기존 계정이 없는 경우 OneLogin웹사이트에서 무료 평가판 또는 개발자 계정을 얻을 수 있습니다.

- IAM Identity Center 활성화 계정(무료). 자세한 내용은 IAM Identity Center 활성화를 참조하십시오.
- OneLogin 계정에서 IAM Identity Center로 SAML 연결을 수행합니다. 자세한 내용은 AWS Partner Network Blog에서 OneLogin 및 AWS 간의 Single Sign-On 활성화를 참조하십시오.

1단계: IAM Identity Center 프로비저닝 활성화

이 첫 번째 단계에서는 IAM Identity Center 콘솔을 사용하여 자동 프로비저닝을 활성화합니다.

IAM Identity Center에서 자동 프로비저닝을 활성화하려면

1. 사전 필수 조건을 완료한 후 IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 자동 프로비저닝 정보 상자를 찾은 다음 활성화를 선택합니다. 그러면 IAM Identity Center에서 자동 프로비저닝이 즉시 활성화되고 필요한 SCIM 엔드포인트 및 액세스 토큰 정보가 표시됩니다.
4. 인바운드 자동 프로비저닝 대화 상자에서 다음 옵션의 각 값을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.
   a. SCIM 엔드포인트
   b. 액세스 토큰
5. 닫기를 선택하세요.

이제 IAM Identity Center 콘솔에서 프로비저닝을 설정했습니다. 이제 다음 절차에 설명된 대로 OneLogin 관리 콘솔을 사용하여 나머지 작업을 수행해야 합니다.

2단계: OneLogin에서 프로비저닝 구성

OneLogin 관리 콘솔에서 다음 절차를 사용하여 IAM Identity Center와 IAM Identity Center 앱 간의 통합을 활성화합니다. 이 절차에서는 SAML 인증을 위해 OneLogin에서 AWS Single Sign-On 애플리케이션을 이미 구성했다고 가정합니다. 이 SAML 연결을 아직 생성하지 않은 경우 이를 먼저 생성한 다음 여기로 돌아와 SCIM 프로비저닝 프로세스를 완료합니다. OneLogin로 SAML을 구성하는 것에 대한 자세한 내용은 AWS Partner Network Blog에서 OneLogin 및 AWS 간의 Single Sign-On 활성화를 참조하십시오.

OneLogin에서 프로비저닝을 구성하려면

1. OneLogin에 로그인한 다음 애플리케이션 > 애플리케이션으로 이동합니다.

2. 애플리케이션 페이지에서 이전에 생성한 애플리케이션을 검색하여 IAM Identity Center와 SAML 연결을 구성합니다. 선택한 다음 왼쪽 탐색 바에서 구성을 선택합니다.
3. 이전 절차에서 IAM Identity Center에서 SCIM 엔드포인트 값을 복사했습니다. 해당 값을 OneLogin의 SCIM 기본 URL 필드에 붙여넣습니다. URL 끝에 있는 후행 슬래시를 제거했는지 확인합니다. 또한 이전 절차에서 IAM Identity Center에서 액세스 토큰 값을 복사했습니다. 해당 값을 OneLogin의 SCIM 베어러 토큰 필드에 붙여넣습니다.
4. API 연결 옆의 활성화를 클릭한 다음 저장을 클릭하여 구성을 완료합니다.
5. 왼쪽 탐색 모음에서 프로비저닝을 선택합니다.
6. 프로비저닝 활성화, 사용자 생성, 사용자 삭제 및 사용자 업데이트 체크박스를 선택한 다음 저장을 선택합니다.
7. 왼쪽 탐색 바에서 사용자를 선택합니다.
8. 추가 작업을 클릭하고 로그인 동기화를 선택합니다. AWS Single Sign-On(SSO)로 사용자 동기화 중이라는 메시지가 표시되어야 합니다.
9. 추가 작업을 다시 클릭한 다음 권한 매핑 재적용을 선택합니다. 매핑이 재적용되는 중이라는 메시지가 표시되어야 합니다.
10. 이제 프로비저닝 프로세스가 시작되어야 합니다. 이를 확인하려면 활동 > 이벤트로 이동하여 진행 상황을 모니터링합니다. 성공적인 프로비저닝 이벤트와 오류는 이벤트 스트림에 나타나야 합니다.
11. 사용자 및 그룹이 IAM Identity Center와 모두 성공적으로 동기화되었는지 확인하려면 IAM Identity Center 콘솔로 돌아가서 사용자를 선택합니다. OneLogin로부터 동기화된 사용자는 사용자 페이지에 표시됩니다. 그룹 페이지에서도 동기화된 그룹을 볼 수 있습니다.
12. 사용자 변경 내용을 IAM Identity Center에 자동으로 동기화하려면 프로비저닝 페이지로 이동하여 이 작업을 수행하기 전에 관리자 승인 필요 섹션을 찾아 사용자 생성, 사용자 삭제 및/또는 사용자 업데이트 선택을 취소하고 저장을 클릭합니다.

(선택 사항) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 OneLogin 사용자 속성 구성

이는 AWS 리소스에 대한 액세스를 관리하기 위해 IAM Identity Center의 속성을 구성하도록 선택하는 경우를 위한 OneLogin의 선택 절차입니다. OneLogin에서 정의한 속성은 SAML 어설션을 통해 IAM Identity Center에 전달됩니다. 그런 다음 OneLogin로부터 전달한 속성을 기반으로 액세스를 관리하기 위해 IAM Identity Center에서 권한 세트를 생성해야 합니다.

이 절차를 시작하기 전에 액세스 제어를 위한 속성 기능을 활성화해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 액세스 제어를 위한 속성 활성화 및 구성 단원을 참조하십시오.

IAM Identity Center에서 액세스 제어에 사용되는 OneLogin 사용자 속성을 구성하려면

1. OneLogin에 로그인한 다음 애플리케이션 > 애플리케이션으로 이동합니다.
2. 애플리케이션 페이지에서 이전에 생성한 애플리케이션을 검색하여 IAM Identity Center와 SAML 연결을 구성합니다. 선택한 다음 왼쪽 탐색 바에서 파라미터를 선택합니다.
3. 필수 파라미터 섹션에서 IAM Identity Center에서 사용하려는 각 속성에 대해 다음을 수행합니다.
   a. +를 선택합니다.
   b. 필드 이름에서 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**를 입력하고, IAM Identity Center에서 예상하는 속성 이름 **`AttributeName`**로 교체합니다. 예를 들어 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**입니다.
   c. 플래그에서 SAML 어설션에 포함 옆의 체크박스를 선택하고 저장을 선택합니다.
   d. 값 필드에서 드롭다운 목록을 사용하여 OneLogin 사용자 속성을 선택합니다. 예를 들어 부서입니다.
4. 저장을 선택합니다.

(선택 사항) 액세스 제어에 속성 전달

IAM Identity Center의 액세스 제어를 위한 속성 기능을 사용하여 `Name` 속성이 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**로 설정된 `Attribute` 요소를 전달하도록 선택할 수 있습니다. 이 요소를 사용하면 속성을 SAML 어설션에 세션 태그로 전달할 수 있습니다. 세션 태그에 대한 자세한 내용은 IAM 사용 설명서의 AWS STS에서 세션 태그 전달을 참조하십시오.

속성을 세션 태그로 전달하려면 태그 값을 지정하는 `AttributeValue` 요소를 포함합니다. 예를 들어, 태그 키-값 쌍 `CostCenter = blue`를 전달하려면 다음 속성을 사용합니다.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

여러 속성을 추가해야 하는 경우 각 태그마다 별도의 `Attribute` 요소를 포함합니다.

문제 해결

다음은 OneLogin로 자동 프로비저닝을 설정하는 동안 발생할 수 있는 몇 가지 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

IAM Identity Center에 프로비저닝되지 않는 그룹

기본적으로 그룹은 OneLogin에서 IAM Identity Center로 프로비저닝할 수 없습니다. OneLogin에서 IAM Identity Center 애플리케이션에 대한 그룹 프로비저닝을 활성화했는지 확인합니다. 이렇게 하려면 OneLogin 관리 콘솔에 로그인하고 IAM Identity Center 애플리케이션(IAM Identity Center 애플리케이션 > 파라미터 > 그룹)의 속성에서 사용자 프로비저닝에 포함 옵션이 선택되어 있는지 확인합니다. SCIM에서 OneLogin 역할을 그룹으로 동기화하는 방법을 포함하여 OneLogin에서 그룹을 생성하는 방법에 대한 자세한 내용은 OneLogin웹사이트를 참조하십시오.

모든 설정이 정확함에도 불구하고 OneLogin에서 IAM Identity Center로 아무 것도 동기화되지 않음

관리자 승인과 관련된 위의 참고 사항 외에도 많은 구성 변경 사항을 적용하려면 권한 매핑을 재적용해야 합니다. 이는 애플리케이션 > 애플리케이션 > IAM Identity Center 애플리케이션 > 추가 작업에서 찾을 수 있습니다. 활동 > 이벤트에서 동기화 이벤트를 비롯한 OneLogin의 대부분 작업에 대한 세부 정보와 로그를 볼 수 있습니다.

OneLogin에서 그룹을 삭제하거나 비활성화했지만 여전히 IAM Identity Center에 표시됨

현재 OneLogin는 그룹에 대한 SCIM DELETE 작업을 지원하지 않습니다. 즉, 그룹은 IAM Identity Center에 계속 존재합니다. 따라서 IAM Identity Center에서 해당 그룹에 대한 해당 권한이 모두 제거되도록 하려면 IAM Identity Center에서 그룹을 직접 제거해야 합니다.

OneLogin에서 먼저 삭제하지 않고 IAM Identity Center에서 그룹을 삭제했는데, 이제 사용자/그룹 동기화 문제가 발생함

이 상황을 해결하려면 먼저 OneLogin에 중복된 그룹 프로비저닝 규칙 또는 구성이 없는지 확인합니다. 예를 들어, 동일한 그룹에 게시하는 규칙과 함께 애플리케이션에 직접 할당된 그룹이 여기에 해당합니다. 다음으로, IAM Identity Center에서 원하지 않는 그룹을 모두 삭제합니다. 마지막으로 OneLogin에서 권한(IAM Identity Center 앱 > 프로비저닝 > 사용 권한)을 새로 고침하고 권한 매핑을 재적용(IAM Identity Center 앱 > 추가 작업)합니다. 나중에 이 문제가 발생하지 않도록 하려면 먼저 OneLogin에서 그룹 프로비저닝을 중지하도록 변경한 다음 IAM Identity Center에서 그룹을 삭제합니다.

IAM Identity Center에서 Ping Identity 제품 사용

다음 Ping Identity 제품은 IAM Identity Center에서 테스트되었습니다.

주제

- PingFederate
- PingOne

PingFederate

IAM Identity Center는 Ping Identity의 PingFederate 제품(이하 “Ping”)에서 IAM Identity Center로 들어오는 사용자 및 그룹 정보의 자동 프로비저닝(동기화)을 지원합니다. 이 프로비저닝은 도메인 간 ID 관리 시스템(SCIM) v2.0 프로토콜을 사용합니다. IAM Identity Center SCIM 엔드포인트와 액세스 토큰을 사용하여 PingFederate에서 이 연결을 구성합니다. SCIM 동기화를 구성할 때 PingFederate의 사용자 속성을 IAM Identity Center의 명명된 속성에 매핑합니다. 이로 인해 IAM Identity Center와 PingFederate 간에 예상 속성이 일치하게 됩니다.

이 가이드는 PingFederate 버전 10.2를 기반으로 합니다. 이외 버전의 단계는 다를 수 있습니다. PingFederate의 이외 버전에 대한 IAM Identity Center 프로비저닝 구성 방법의 자세한 내용은 Ping에 문의하십시오.

다음 단계는 SCIM 프로토콜을 사용하여 PingFederate에서 IAM Identity Center으로 사용자 및 그룹을 자동으로 프로비저닝하도록 활성화하는 방법을 안내합니다.

> **Note**
>
> SCIM 배포를 시작하기 전에 먼저 자동 프로비저닝을 사용할 때 고려 사항를 검토하는 것이 좋습니다. 그 후, 다음 섹션에서 추가 고려 사항을 계속 검토합니다.

주제

- 사전 조건
- 추가 고려 사항
- 1단계: IAM Identity Center 프로비저닝 활성화
- 2단계: PingFederate에서 프로비저닝 구성

- (선택 사항) 3단계: IAM ID 센터의 액세스 제어를 위한 PingFed erate의 사용자 속성 구성
- (선택 사항) 액세스 제어에 속성 전달

사전 조건

시작하기 전에 다음을 준비해야 합니다.

- 작동 중인 PingFederate 서버. 기존 PingFederate 서버가 없는 경우 Ping Identity 웹사이트에서 무료 평가판 또는 개발자 계정을 얻을 수 있습니다. 평가판에는 라이선스, 소프트웨어 다운로드 및 관련 문서가 포함됩니다.
- PingFederate 서버에 설치된 PingFederate IAM Identity Center 커넥터 소프트웨어 사본. 이 소프트웨어를 구하는 방법에 대한 자세한 내용은 Ping Identity 웹사이트의 IAM Identity Center 커넥터를 참조하십시오.
- IAM Identity Center 활성화 계정(무료). 자세한 내용은 IAM Identity Center 활성화를 참조하십시오.
- PingFederate 인스턴스스에서 IAM Identity Center로 SAML 연결을 수행합니다. 이 연결을 구성하는 방법에 대한 지침은 PingFederate 설명서를 참조하십시오. 요약하면, 권장 경로는 IAM Identity Center 커넥터를 사용하여 PingFederate에 “브라우저 SSO”를 구성하고, 양쪽 끝의 “다운로드” 및 “가져오기” 메타데이터 기능을 사용하여 PingFederate 및 IAM Identity Center 간에 SAML 메타데이터를 교환하는 것입니다.

추가 고려 사항

다음은 IAM Identity Center를 사용하여 프로비저닝을 구현하는 방법에 영향을 미칠 수 있는 PingFederate에 대한 중요한 고려 사항입니다.

- PingFederate에서 구성된 데이터 스토어의 사용자로부터 (전화번호와 같은) 속성을 제거해도 IAM Identity Center의 해당 사용자에서는 해당 속성이 제거되지 않습니다. 이는 PingFederate’s 프로비저닝 구현의 알려진 문제입니다. 사용자의 속성이 비어 있지 않은 다른 값으로 변경하면 해당 변경 내용이 IAM Identity Center에 동기화됩니다.

1단계: IAM Identity Center 프로비저닝 활성화

이 첫 번째 단계에서는 IAM Identity Center 콘솔을 사용하여 자동 프로비저닝을 활성화합니다.

IAM Identity Center에서 자동 프로비저닝을 활성화하려면

1. 사전 필수 조건을 완료한 후 IAM Identity Center 콘솔을 엽니다.

2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 자동 프로비저닝 정보 상자를 찾은 다음 활성화를 선택합니다. 그러면 IAM Identity Center에서 자동 프로비저닝이 즉시 활성화되고 필요한 SCIM 엔드포인트 및 액세스 토큰 정보가 표시됩니다.
4. 인바운드 자동 프로비저닝 대화 상자에서 다음 옵션의 각 값을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.

   a. SCIM 엔드포인트

   b. 액세스 토큰
5. 닫기를 선택하세요.

이제 IAM Identity Center 콘솔에서 프로비저닝을 설정했으므로 PingFederate 관리 콘솔을 사용하여 나머지 작업을 완료해야 합니다. 단계는 다음 절차에 설명되어 있습니다.

2단계: PingFederate에서 프로비저닝 구성

PingFederate 관리 콘솔에서 다음 절차를 사용하여 IAM Identity Center와 IAM Identity Center 커넥터 간의 통합을 활성화합니다. 이 절차에서는 IAM Identity Center 커넥터 소프트웨어를 이미 설치했다고 가정합니다. 아직 이를 수행하지 않은 경우 사전 조건를 참조하고 이 절차를 완료하여 SCIM 프로비저닝을 구성합니다.

> **Important**
>
> PingFederate 서버가 이전에 아웃바운드 SCIM 프로비저닝용으로 구성되지 않은 경우, 프로비저닝을 활성화하려면 구성 파일을 변경해야 할 수 있습니다. 자세한 내용은 Ping 설명서를 참조하십시오. 요약하면, pingfederate-<version>/pingfederate/bin/run.properties 파일의 `pf.provisioner.mode` 설정을 `OFF`(기본값)이 아닌 다른 값으로 수정하고 현재 실행 중인 경우 서버를 다시 시작해야 합니다. 예를 들어, 현재 PingFederate와 고가용성 구성을 사용하지 않는 경우 `STANDALONE`를 사용하도록 선택할 수 있습니다.

PingFederate에서 프로비저닝을 구성하려면

1. PingFederate 관리 콘솔에 로그인합니다.
2. 페이지 상단에서 애플리케이션을 선택한 다음 SP 연결을 클릭합니다.
3. IAM Identity Center와 SAML 연결을 구성하기 위해 이전에 생성한 애플리케이션을 찾아 연결 이름을 클릭합니다.

4. 페이지 상단 근처의 어두운 탐색 제목에서 연결 유형을 선택합니다. 이전 SAML 구성에서 이미 선택된 브라우저 SSO가 보일 것입니다. 그렇지 않은 경우, 계속하기 위해 먼저 해당 단계를 완료해야 합니다.
5. 아웃바운드 프로비저닝 체크박스를 선택하고 유형으로 IAM Identity Center 클라우드 커넥터를 선택한 다음 저장을 클릭합니다. IAM Identity Center 클라우드 커넥터가 옵션으로 표시되지 않는 경우 IAM Identity Center 커넥터를 설치하고 PingFederate 서버를 다시 시작했는지 확인합니다.
6. 아웃바운드 프로비저닝 페이지가 표시될 때까지 다음을 반복해서 클릭한 후 프로비저닝 구성 버튼을 클릭합니다.
7. 이전 절차에서 IAM Identity Center에서 SCIM 엔드포인트 값을 복사했습니다. 해당 값을 PingFederate 콘솔의 SCIM URL 필드에 붙여넣습니다. URL 끝에 있는 후행 슬래시를 제거했는지 확인합니다. 또한 이전 절차에서 IAM Identity Center에서 액세스 토큰 값을 복사했습니다. 해당 값을 PingFederate 콘솔의 액세스 토큰 필드에 붙여넣습니다. 저장을 클릭합니다.
8. 채널 구성 페이지에서 생성을 클릭합니다.
9. 해당 새 프로비저닝 채널의 채널 이름 (예: **`AWSIAMIdentityCenterchannel`**)을 입력하고 다음을 클릭합니다.
10. 소스페이지에서 IAM Identity Center 연결에 사용할 활성 데이터 스토어를 선택하고 다음을 클릭합니다.

> **Note**
>
> 데이터 소스를 아직 구성하지 않았다면 지금 구성해야 합니다. PingFederate에서 데이터 소스를 선택하고 구성하는 방법에 대한 자세한 내용은 Ping 제품 설명서를 참조하십시오.

11. 소스 설정 페이지에서 모든 값이 설치에 일치하는지 확인한 후 다음을 클릭합니다.
12. 소스 위치 페이지에서 데이터 소스에 적합한 설정을 입력하고 다음을 클릭합니다. 예를 들어 Active Directory를 LDAP 디렉터리로 사용하는 경우:

    a. AD 포리스트(예: **`DC=myforest,DC=mydomain,DC=com`**)의 기본 DN을 입력합니다.

    b. 사용자 > 그룹 DN에서 IAM Identity Center에 프로비저닝하려는 모든 사용자를 포함하는 단일 그룹을 지정합니다. 그러한 단일 그룹이 없는 경우 AD에서 해당 그룹을 생성하고 이 설정으로 돌아간 다음 해당 DN을 입력합니다.

    c. 하위 그룹을 검색할지 여부(중첩 검색)와 필요한 LDAP 필터를 지정합니다.

    d. 그룹 > 그룹 DN에서 IAM Identity Center에 프로비저닝하려는 모든 그룹을 포함하는 단일 그룹을 지정합니다. 대부분의 경우 이 DN은 사용자 섹션에서 지정한 것과 동일한 DN일 수 있습니다. 필요에 따라 중첩 검색 및 필터 값을 입력합니다.

13. 속성 매핑 페이지에서 다음을 확인한 후 다음을 클릭합니다.

    a. 사용자 이름 필드는 이메일(user@domain.com) 형식의 속성에 매핑되어야 합니다. 또한 사용자가 Ping에 로그인할 때 사용할 값과 일치해야 합니다. 이 값은 연동 인증 중에 SAML `nameId` 클레임에 차례로 채워지고 IAM Identity Center에서 사용자와 매칭하는 데 사용됩니다. 예를 들어 Active Directory를 사용하는 경우 `UserPrincipalName`를 userName으로 지정할 수 있습니다.

    b. * 접미사가 붙은 다른 필드는 사용자의 null이 아닌 속성에 매핑되어야 합니다.

14. 활성화 및 요약 페이지에서 채널 상태를 활성으로 설정하여 구성을 저장한 후 즉시 동기화가 시작되도록 합니다.

15. 페이지의 모든 구성 값이 올바른지 확인하고 완료를 클릭합니다.

16. 채널 관리 페이지에서 저장을 클릭합니다.

17. 이제 프로비저닝이 시작됩니다. 기본적으로 PingFederate 서버의 pingfederate-<version>/pingfederate/log 디렉터리에 있는 provisioner.log 파일을 보면 활동을 확인할 수 있습니다.

18. 사용자 및 그룹이 IAM Identity Center와 성공적으로 동기화되었는지 확인하려면 IAM Identity Center 콘솔로 돌아가서 사용자를 선택합니다. PingFederate로부터 동기화된 사용자는 사용자 페이지에 표시됩니다. 그룹 페이지에서도 동기화된 그룹을 볼 수 있습니다.

(선택 사항) 3단계: IAM ID 센터의 액세스 제어를 위한 PingFed erate의 사용자 속성 구성

이는 AWS 리소스에 대한 액세스를 관리하기 위해 IAM Identity Center의 속성을 구성하도록 선택하는 경우를 위한 PingFederate의 선택 절차입니다. PingFederate에서 정의한 속성은 SAML 어설션을 통해 IAM Identity Center에 전달됩니다. 그런 다음 PingFederate로부터 전달한 속성을 기반으로 액세스를 관리하기 위해 IAM Identity Center에서 권한 세트를 생성해야 합니다.

이 절차를 시작하기 전에 액세스 제어를 위한 속성 기능을 활성화해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 액세스 제어를 위한 속성 활성화 및 구성 단원을 참조하십시오.

IAM Identity Center에서 액세스 제어에 사용되는 PingFederate 사용자 속성을 구성하려면

1. PingFederate 관리 콘솔에 로그인합니다.
2. 페이지 상단에서 애플리케이션을 선택한 다음 SP 연결을 클릭합니다.
3. IAM Identity Center와 SAML 연결을 구성하기 위해 이전에 생성한 애플리케이션을 찾아 연결 이름을 클릭합니다.

4. 페이지 상단 근처의 어두운 탐색 제목에서 브라우저 SSO를 선택합니다. 그런 다음 브라우저 SSO 구성을 클릭합니다.
5. 브라우저 SSO 구성 페이지에서 어설션 생성을 선택한 다음 어설션 생성 구성을 클릭합니다.
6. 어설션 생성 구성 페이지에서 속성 계약을 선택합니다.
7. 속성 계약 페이지의 계약 확장 섹션에서 다음 단계를 수행하여 새 속성을 추가합니다.

   a. 텍스트 박스에 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**를 입력하고, IAM Identity Center에서 예상하는 속성 이름으로 **`AttributeName`**를 교체합니다. 예를 들어 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**입니다.

   b. 속성 이름 형식에서 urn:oasis:names:tc:SAML:2.0:attrname-format:uri을 선택합니다.

   c. 추가를 선택한 후 다음을 선택합니다.
8. 인증 소스 매핑 페이지에서 애플리케이션으로 구성된 어댑터 인스턴스를 선택합니다.
9. 속성 계약 이행 페이지에서 속성 계약 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**의 소스(데이터 스토어)와 값(데이터 스토어 속성)을 선택합니다.

   > **Note**
   >
   > 데이터 소스를 아직 구성하지 않았다면 지금 구성해야 합니다. PingFederate에서 데이터 소스를 선택하고 구성하는 방법에 대한 자세한 내용은 Ping 제품 설명서를 참조하십시오.

10. 활성화 및 요약 페이지가 표시될 때까지 다음을 반복해서 클릭한 다음 저장을 클릭합니다.

(선택 사항) 액세스 제어에 속성 전달

IAM Identity Center의 액세스 제어를 위한 속성 기능을 사용하여 Name 속성이 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**로 설정된 `Attribute` 요소를 전달하도록 선택할 수 있습니다. 이 요소를 사용하면 속성을 SAML 어설션에 세션 태그로 전달할 수 있습니다. 세션 태그에 대한 자세한 내용은 IAM 사용 설명서의 AWS STS에서 세션 태그 전달을 참조하십시오.

속성을 세션 태그로 전달하려면 태그 값을 지정하는 `AttributeValue` 요소를 포함합니다. 예를 들어, 태그 키-값 쌍 `CostCenter = blue`를 전달하려면 다음 속성을 사용합니다.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
```

```
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

여러 속성을 추가해야 하는 경우 각 태그마다 별도의 `Attribute` 요소를 포함합니다.

PingOne

IAM Identity Center는 Ping Identity의 PingOne 제품(이하 “Ping”)에서 IAM Identity Center로 들어오는 사용자 정보의 자동 프로비저닝(동기화)을 지원합니다. 이 프로비저닝은 도메인 간 ID 관리 시스템(SCIM) v2.0 프로토콜을 사용합니다. IAM Identity Center SCIM 엔드포인트와 액세스 토큰을 사용하여 PingOne에서 이 연결을 구성합니다. SCIM 동기화를 구성할 때 PingOne의 사용자 속성을 IAM Identity Center의 명명된 속성에 매핑합니다. 이로 인해 IAM Identity Center와 PingOne 간에 예상 속성이 일치하게 됩니다.

PingOne에 기반한 이 가이드는 2020년 10월 기준입니다. 최신 버전의 단계는 다를 수 있습니다. PingOne의 이외 버전에 대한 IAM Identity Center 프로비저닝 구성 방법의 자세한 내용은 Ping에 문의하십시오. 또한 이 가이드에는 SAML을 통한 사용자 인증 구성에 관련된 몇 가지 참고 사항이 포함되어 있습니다.

다음 단계는 SCIM 프로토콜을 사용하여 PingOne에서 IAM Identity Center으로 사용자를 자동으로 프로비저닝하도록 활성화하는 방법을 안내합니다.

> **Note**
>
> SCIM 배포를 시작하기 전에 먼저 자동 프로비저닝을 사용할 때 고려 사항를 검토하는 것이 좋습니다. 그 후, 다음 섹션에서 추가 고려 사항을 계속 검토합니다.

주제

- 사전 조건
- 추가 고려 사항
- 1단계: IAM Identity Center 프로비저닝 활성화
- 2단계: PingOne에서 프로비저닝 구성
- (선택 사항) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 PingOne 사용자 속성 구성
- (선택 사항) 액세스 제어에 속성 전달

사전 조건

시작하기 전에 다음을 준비해야 합니다.

- 페더레이션 인증 및 프로비저닝 기능이 모두 포함된 PingOne 구독 또는 무료 평가판 무료 평가판 사용 방법에 대한 자세한 내용은 Ping Identity 웹사이트를 참조하십시오.
- IAM Identity Center 활성화 계정(무료). 자세한 내용은 IAM Identity Center 활성화를 참조하십시오.
- PingOne IAM Identity Center 애플리케이션이 PingOne 관리 포털에 추가되었습니다. PingOne IAM Identity Center 애플리케이션은 PingOne 애플리케이션 카탈로그에서 구할 수 있습니다. 기본 정보는 Ping Identity 웹 사이트의 애플리케이션 카탈로그에서 애플리케이션 추가를 참조하십시오.
- PingOne 인스턴스스에서 IAM Identity Center로 SAML 연결을 수행합니다. PingOne IAM Identity Center 애플리케이션을 PingOne 관리 포털에 추가한 후에는 이 애플리케이션을 사용하여 PingOne 인스턴스에서 IAM Identity Center로의 SAML 연결을 구성해야 합니다. 양쪽 끝의 “다운로드” 및 “가져오기” 메타데이터 기능을 사용하여 PingOne 및 IAM Identity Center 간에 SAML 메타데이터를 교환할 수 있습니다. 이 연결을 구성하는 방법에 대한 지침은 PingOne 설명서를 참조하십시오.

추가 고려 사항

다음은 IAM Identity Center를 사용하여 프로비저닝을 구현하는 방법에 영향을 미칠 수 있는 PingOne에 대한 중요한 고려 사항입니다.

- 2020년 10월부터 PingOne는 SCIM을 통한 그룹 프로비저닝을 지원하지 않습니다. Ping의 SCIM 그룹 지원에 대한 최신 정보는 PingOne로 문의하십시오.
- 사용자는 PingOne 관리 포털에서 프로비저닝을 비활성화한 이후에도 PingOne로부터 계속 프로비저닝을 받을 수 있습니다. 프로비저닝을 즉시 종료해야 하는 경우 관련 SCIM 베어러 토큰을 삭제하거나 IAM Identity Center에서 자동 프로비저닝를 비활성화합니다.
- 사용자 속성이 PingOne에서 구성된 데이터 스토어로부터 제거되어도, IAM Identity Center의 해당 사용자에서는 해당 속성이 제거되지 않습니다. 이는 PingOne’s 프로비저닝 구현의 알려진 문제입니다. 속성이 수정되면 변경 내용이 IAM Identity Center에 동기화됩니다.
- 다음은 PingOne의 SAML 구성과 관련된 중요 참고 사항입니다.
  - IAM Identity Center는 `NameId` 형식으로만 `emailaddress`를 지원합니다. 즉, PingOne의 SAML_SUBJECT 매핑을 위해 PingOne 디렉토리 내에서 고유하고 null이 아닌 이메일/UPN(예: user@domain.com) 형식의 사용자 속성을 선택해야 합니다 이메일(직장)은 PingOne 내장형 디렉터리로 테스트 구성에 사용하기에 적합한 값입니다.
  - PingOne에서 + 문자가 포함된 이메일 주소를 사용하는 사용자는 `'SAML_215'` 또는 `'Invalid input'` 등의 오류가 발생하여 IAM Identity Center에 로그인하지 못할 수 있습니다. 이 문제를 해

결하려면 PingOne에서 속성 매핑의 SAML_SUBJECT 매핑에 대한 고급 옵션을 선택합니다. 그런 다음 드롭다운 메뉴에서 SP 로 전송할 이름의 ID 형식:을 urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress로 설정합니다.

1단계: IAM Identity Center 프로비저닝 활성화

이 첫 번째 단계에서는 IAM Identity Center 콘솔을 사용하여 자동 프로비저닝을 활성화합니다.

IAM Identity Center에서 자동 프로비저닝을 활성화하려면

1. 사전 필수 조건을 완료한 후 IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 자동 프로비저닝 정보 상자를 찾은 다음 활성화를 선택합니다. 그러면 IAM Identity Center에서 자동 프로비저닝이 즉시 활성화되고 필요한 SCIM 엔드포인트 및 액세스 토큰 정보가 표시됩니다.
4. 인바운드 자동 프로비저닝 대화 상자에서 다음 옵션의 각 값을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.
   a. SCIM 엔드포인트
   b. 액세스 토큰
5. 닫기를 선택하세요.

이제 IAM Identity Center 콘솔에서 프로비저닝을 설정했으므로 PingOne IAM Identity Center 애플리케이션을 사용하여 나머지 작업을 완료해야 합니다. 다음 절차에서 이 단계를 설명합니다.

2단계: PingOne에서 프로비저닝 구성

PingOne IAM Identity Center 애플리케이션의 다음 절차를 사용하여 IAM Identity Center를 통한 프로비저닝을 활성화합니다. 이 절차에서는 PingOne 관리 포털에 PingOne IAM Identity Center 애플리케이션을 이미 추가했다고 가정합니다. 아직 이를 수행하지 않은 경우 사전 조건를 참조하고 이 절차를 완료하여 SCIM 프로비저닝을 구성합니다.

PingOne에서 프로비저닝을 구성하려면

1. PingOne(애플리케이션 > 내 애플리케이션)의 SAML을 구성하는 과정에서 설치된 PingOne IAM Identity Center 애플리케이션을 엽니다. 사전 조건 단원을 참조하십시오.

2. 페이지 하단으로 스크롤합니다. 사용자 프로비저닝에서 링크 완료를 선택하여 연결의 사용자 프로비저닝 구성으로 이동합니다.
3. 프로비전 지침 페이지에서 다음 단계로 계속을 선택합니다.
4. 이전 절차에서 IAM Identity Center에서 SCIM 엔드포인트 값을 복사했습니다. 해당 값을 PingOne IAM Identity Center 애플리케이션의 SCIM URL 필드에 붙여넣습니다. URL 끝에 있는 후행 슬래시를 제거했는지 확인합니다. 또한 이전 절차에서 IAM Identity Center에서 액세스 토큰 값을 복사했습니다. 해당 값을 PingOne IAM Identity Center 애플리케이션의 ACCESS_TOKEN 필드에 붙여넣습니다.
5. REMOVE_ACTION의 경우 비활성화 또는 삭제를 선택합니다(자세한 내용은 페이지의 설명 텍스트 참조).
6. 속성 매핑 페이지에서 이 페이지 앞부분 추가 고려 사항 지침에 따라 SAML_SUBJECT(`NameId`) 어설션에 사용할 값을 선택합니다. 그런 뒤 다음 단계로 계속을 선택합니다.
7. PingOne앱 사용자 지정 - IAM Identity Center 페이지에서 원하는 대로 사용자 지정을 변경(선택 사항)하고 다음 단계로 계속을 클릭합니다.
8. 그룹 액세스 페이지에서 IAM Identity Center에 프로비저닝 및 Single Sign-on을 활성화하려는 사용자가 포함된 그룹을 선택합니다. 다음 단계로 계속을 선택합니다.
9. 페이지 하단으로 스크롤하고 완료를 선택하여 프로비저닝을 시작합니다.
10. 사용자가 IAM Identity Center와 성공적으로 동기화되었는지 확인하려면 IAM Identity Center 콘솔로 돌아가서 사용자를 선택합니다. PingOne로부터 동기화된 사용자는 사용자 페이지에 표시됩니다. 이제 이러한 사용자를 IAM Identity Center 내에서 계정 및 애플리케이션에 할당할 수 있습니다.

    단, PingOne는 SCIM을 통한 그룹 또는 그룹 구성원 프로비저닝은 지원하지 않습니다. 자세한 정보는 Ping에 문의하십시오.

(선택 사항) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 PingOne 사용자 속성 구성

이는 AWS 리소스에 대한 액세스를 관리하기 위해 IAM Identity Center의 속성을 구성하도록 선택하는 경우에 사용할 수 있는 PingOne의 선택적 절차입니다. PingOne에서 정의한 속성은 SAML 어설션을 통해 IAM Identity Center에 전달됩니다. 그런 다음 PingOne로부터 전달한 속성을 기반으로 액세스를 관리하기 위해 IAM Identity Center에서 권한 세트를 생성해야 합니다.

이 절차를 시작하기 전에 액세스 제어를 위한 속성 기능을 활성화해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 액세스 제어를 위한 속성 활성화 및 구성 단원을 참조하십시오.

IAM Identity Center에서 액세스 제어에 사용되는 PingOne 사용자 속성을 구성하려면

1. PingOne(애플리케이션 > 내 애플리케이션)의 SAML을 구성하는 과정에서 설치된 PingOne IAM Identity Center 애플리케이션을 엽니다.
2. 편집을 선택한 다음 속성 매핑 페이지가 표시될 때까지 다음 단계로 계속 을 선택합니다.
3. 속성 매핑 페이지에서 새 속성 추가를 선택하고 다음을 수행합니다. 액세스 제어를 위해 IAM Identity Center에서 추가하여 사용할 각 속성에 대해 다음 단계를 수행해야 합니다.

    a. 애플리케이션 속성 필드에 `https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`*를 입력합니다. IAM Identity Center에서 *`AttributeName`*을 예상하는 속성의 이름으로 바꿉니다. 예를 들어 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**입니다.

    b. Identity Bridge Attribute 또는 Literal Value 필드에서 PingOne 디렉터리의 사용자 속성을 선택합니다. 예제로 이메일(직장).
4. 다음을 몇 번 선택한 후 완료를 선택합니다.

(선택 사항) 액세스 제어에 속성 전달

IAM Identity Center의 액세스 제어를 위한 속성 기능을 사용하여 Name 속성이 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**로 설정된 `Attribute` 요소를 전달하도록 선택할 수 있습니다. 이 요소를 사용하면 속성을 SAML 어설션에 세션 태그로 전달할 수 있습니다. 세션 태그에 대한 자세한 내용은 IAM 사용 설명서의 AWS STS에서 세션 태그 전달을 참조하십시오.

속성을 세션 태그로 전달하려면 태그 값을 지정하는 `AttributeValue` 요소를 포함합니다. 예를 들어, 태그 키-값 쌍 `CostCenter = blue`를 전달하려면 다음 속성을 사용합니다.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

여러 속성을 추가해야 하는 경우 각 태그마다 별도의 `Attribute` 요소를 포함합니다.

IAM Identity Center에서 일반 작업 시작

IAM Identity Center를 처음 사용하는 경우 서비스를 사용하기 위한 기본 워크플로는 다음과 같습니다.

1. IAM Identity Center의 조직 인스턴스를 사용하는 경우 관리 계정의 콘솔에 로그인하고 IAM Identity Center의 계정 인스턴스를 사용하는 AWS 계정 경우 관리 계정의 콘솔에 로그인하고 IAM ID 센터 콘솔로 이동하십시오.
2. IAM Identity Center 콘솔에서 사용자 및 그룹의 ID를 저장하는 데 사용할 디렉터리를 선택합니다. IAM Identity Center는 기본적으로 사용자 액세스를 구성하는 데 사용할 수 있는 디렉터리를 제공합니다. 다른 ID 소스를 사용하려는 경우 Active Directory 또는 외부 ID 제공업체를 연결할 수 있습니다.
3. 조직 인스턴스의 경우 조직의 계정을 선택한 다음 디렉터리에서 사용자 또는 그룹과 이들에게 부여할 권한을 선택하여 AWS 계정에 사용자 액세스 권한을 할당합니다.
4. 사용자에게 애플리케이션에 대한 액세스 권한 부여:
   a. 애플리케이션 카탈로그에서 사전 통합된 애플리케이션 중 하나를 선택하거나 자체 SAML 2.0 애플리케이션을 추가하여 고객 관리형 SAML 2.0 애플리케이션을 설정합니다.
   b. 애플리케이션 속성을 구성합니다.
   c. 애플리케이션에 대한 사용자 액세스 권한을 할당합니다. 개별 사용자 권한을 추가하는 대신 그룹 구성원 자격을 통해 사용자 액세스 권한을 할당하는 것이 좋습니다. 그룹을 사용하면 각 개인에게 권한을 적용하는 대신 사용자 그룹에 권한을 부여하거나 거부할 수 있습니다. 사용자가 다른 조직으로 이동하면 해당 사용자를 다른 그룹으로 이동하기만 하면 됩니다. 그러면 사용자는 새 조직에 필요한 권한을 자동으로 받게 됩니다.
5. 기본 IAM Identity Center 디렉터리를 사용하는 경우 사용자에게 액세스 포털에 로그인하는 방법을 알려주세요. AWS IAM Identity Center의 신규 사용자는 먼저 사용자 자격 증명을 활성화해야 AWS 액세스 포털에 로그인하는 데 사용할 수 있습니다. 자세한 내용은 AWS 로그인 사용 AWS 설명서의 액세스 포털에 로그인을 참조하십시오.

이 섹션의 주제는 IAM Identity Center의 초기 구성을 완료한 후 수행하는 일반 작업을 익히는 데 도움이 됩니다.

IAM Identity Center를 아직 활성화하지 않은 경우 활성화 AWS IAM Identity Center의 내용을 참조하세요.

주제

- 권한 집합을 생성합니다.

- IAM ID 센터 사용자에게 AWS 계정 액세스 권한을 할당합니다.
- IAM ID 센터 자격 증명으로 AWS 액세스 포털에 로그인합니다.
- 그룹에 AWS 계정 액세스 권한을 할당하십시오.
- 애플리케이션에 대한 Single Sign-On 액세스 설정
- 사용자 및 그룹 할당 보기

권한 집합을 생성합니다.

권한 집합은 IAM Identity Center에 저장되며 사용자 및 그룹이 AWS 계정에 대해 보유할 수 있는 액세스 수준을 정의합니다. 가장 먼저 생성하는 권한 세트는 관리 권한 세트입니다. 시작하기 튜토리얼 가운데 하나를 완료한 경우 이미 관리 권한 세트를 생성한 것입니다. 이 절차를 사용하여 IAM 사용 설명서의 직무에 대한AWS 관리형 정책에서 설명하는 것과 같이 권한 세트를 생성할 수 있습니다.

1. AWS Management Console에 로그인하려면 다음 중 하나를 수행합니다.
   - AWS (루트 사용자) 신규 사용자 - 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
   - 이미 AWS (IAM 자격 증명) 사용 중 — 관리자 권한이 있는 IAM 자격 증명을 사용하여 로그인합니다.
2. IAM Identity Center 콘솔을 엽니다.
3. IAM Identity Center 탐색 창의 다중 계정 권한에서 권한 세트를 선택합니다.
4. 권한 세트 생성을 선택합니다.
   a. 권한 세트 유형 선택 페이지의 권한 세트 유형 섹션에서 사전 정의된 권한 세트를 선택합니다.
   b. 사전 정의된 권한 세트 정책 섹션에서 다음 중 하나를 선택합니다.
      - AdministratorAccess
      - 결제
      - DatabaseAdministrator
      - DataScientist
      - NetworkAdministrator
      - PowerUserAccess
      - ReadOnlyAccess
      - SecurityAudit

- SupportUser
- SystemAdministrator
- ViewOnlyAccess

5. 권한 세트 세부 정보 지정 페이지에서 기본 설정을 유지하고 다음을 선택합니다. 기본 설정은 세션을 1시간으로 제한합니다.
6. 검토 및 생성 페이지에서 다음을 확인합니다.

   1. 1단계: 권한 집합 유형 선택의 경우 선택한 권한 집합의 유형이 표시됩니다.
   2. 2단계: 사용 권한 집합 세부 정보 정의의 경우 선택한 사용 권한 집합의 이름을 표시합니다.
   3. 생성을 선택합니다.

최소 권한을 적용하는 권한 세트 생성

최소 권한 적용 모범 사례를 따르려면 관리 권한 세트를 생성한 후 보다 제한적인 권한 세트를 생성하여 한 명 이상의 사용자에게 할당합니다. 이전 절차에서 생성한 권한 세트는 사용자가 필요로 하는 리소스에 대한 액세스 범위를 평가하는 출발점 역할을 합니다. 최소 권한으로 전환하려면 IAM Access Analyzer를 실행하여 AWS 관리형 정책으로 보안 주체를 모니터링합니다. 사용하는 권한을 학습한 후 사용자 지정 정책을 작성하거나 팀에 필요한 권한만 있는 정책을 생성할 수 있습니다.

IAM Identity Center를 사용하여 동일한 사용자에게 여러 권한 세트를 할당할 수 있습니다. 또한 관리자에게 더 제한적인 추가 권한 세트를 할당해야 합니다. 이렇게 하면 관리 권한을 항상 사용하는 대신 필요한 권한만 AWS 계정 사용하여 사용자 권한에 액세스할 수 있습니다.

예를 들어 개발자인 경우 IAM Identity Center에서 관리자를 생성한 후 `PowerUserAccess` 권한을 허용하는 새 권한 세트를 만든 다음 해당 권한 세트를 직접 할당할 수 있습니다. `AdministratorAccess`권한을 사용하는 관리 권한 집합과 달리, `PowerUserAccess` 권한 집합은 IAM 사용자 및 그룹을 관리할 수 없습니다. AWS 액세스 포털에 로그인하여 계정에 접근할 때 `PowerUserAccess` 대신 AWS 계정에서 개발 작업을 `AdministratorAccess` 수행하도록 선택할 수 있습니다.

다음 사항에 유의하세요.

- 보다 제한적인 권한 세트를 빠르게 생성하려면 사용자 지정 권한 세트 대신 미리 정의된 권한 세트를 사용하세요.

  사전 정의된 권한을 사용하는 사전 정의된 권한 집합의 경우 사용 가능한 정책 목록에서 단일 AWS 관리형 정책을 선택할 수 있습니다. 각 정책은 AWS 서비스 및 리소스에 대한 특정 수준의 액세스 권

한 또는 공통 직무에 대한 권한을 부여합니다. 각 정책에 대한 자세한 내용은 직무 역할에 대한AWS 관리형 정책을 참조하세요.

- 권한 세트의 세션 기간을 구성하여 사용자가 AWS 계정에 로그인하는 시간을 제어할 수 있습니다.

  사용자가 AWS 관리 콘솔 또는AWS CLI (AWS 명령줄 인터페이스) 에 통합하여 사용하는 경우 IAM Identity Center는 권한 세트의 세션 기간 설정을 사용하여 세션 기간을 제어합니다. AWS 계정 기본적으로 세션 기간 값은 사용자가 세션에서 AWS 계정 로그아웃하기 전에 AWS 로그인할 수 있는 시간을 결정하는 1시간으로 설정됩니다. 최대 12시간까지 값을 지정할 수 있습니다. 자세한 정보는 세션 기간 설정을 참조하세요.
- 또한 AWS 액세스 포털 세션 기간을 구성하여 직원 사용자가 포털에 로그인하는 시간을 제어할 수 있습니다.

  기본적으로 최대 세션 지속 시간 값은 직원 사용자가 다시 인증하기 전에 AWS 액세스 포털에 로그인할 수 있는 시간을 결정하는 8시간입니다. 최대 90일까지 값을 지정할 수 있습니다. 자세한 정보는 AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 구성합니다.을 참조하세요.
- AWS 액세스 포털에 로그인할 때 최소 권한을 제공하는 역할을 선택하십시오.

  생성하여 사용자에게 할당한 각 권한 집합은 액세스 포털에서 사용 가능한 역할로 표시됩니다. AWS 해당 사용자로 포털에 로그인할 때는 계정에서 작업을 수행하는 데 사용할 수 있는 가장 제한적인 권한 세트에 해당하는 역할을 대신 `AdministratorAccess`를 선택하세요.
- IAM Identity Center에 다른 사용자를 추가하고 해당 사용자에게 기존 또는 새 권한 세트를 할당할 수 있습니다.

  자세한 내용은 그룹에 AWS 계정 액세스 권한을 할당하십시오.의 내용을 참조하세요.

IAM ID 센터 사용자에게 AWS 계정 액세스 권한을 할당합니다.

IAM Identity Center 사용자에 대한 AWS 계정 액세스를 설정하려면 사용자에게 AWS 계정 및 권한 집합을 할당해야 합니다.

1. AWS Management Console에 로그인하려면 다음 중 하나를 수행합니다.

   - 신규 사용자 AWS (루트 사용자) — 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
   - 이미 AWS (IAM 자격 증명) 사용 중 — 관리자 권한이 있는 IAM 자격 증명을 사용하여 로그인합니다.

2. IAM Identity Center 콘솔을 엽니다.
3. 탐색 창의 다중 계정 권한에서 AWS 계정을 선택합니다.
4. AWS 계정 페이지에는 조직의 트리 뷰 목록이 나타납니다. 액세스 권한을 AWS 계정 할당하려는 대상 옆의 체크박스를 선택합니다. IAM Identity Center에 대한 관리 액세스를 설정하는 경우 관리 계정 옆의 확인란을 선택합니다.
5. 사용자 또는 그룹 할당을 선택합니다.
6. 1단계: 사용자 및 그룹 선택의 경우 “***AWS ## ###*** 사용자 및 그룹 할당" 페이지에서 다음을 수행하십시오.

    1. 사용자 탭에서 관리 권한을 부여하려는 사용자를 선택합니다.

        결과를 필터링하려면 검색 상자에 원하는 사용자 이름을 순서대로 입력합니다.

    2. 올바른 사용자가 선택되었는지 확인한 후, 다음을 선택합니다.
7. 2단계: 사용 권한 집합 선택의 경우, “***AWS ## ##*** “에 사용 권한 집합 할당 페이지의 사용 권한 집합에서 사용 권한 집합을 선택하여 사용자 및 그룹이 이에 대해 갖는 액세스 수준을 정의합니다 AWS 계정.
8. 다음을 선택합니다.
9. 3단계: 검토 및 제출의 경우 “***AWS ## ##*** “에 대한 할당 검토 및 제출 페이지에서 다음을 수행하십시오.

    1. 선택한 사용자 및 권한 세트를 검토합니다.
    2. 권한 집합에 올바른 사용자가 할당되었는지 확인한 후 제출을 선택합니다.

    > **Important**
    >
    > 사용자 할당 프로세스를 완료하는 데 몇 분이 걸릴 수 있습니다. 프로세스가 성공적으로 완료될 때까지 이 페이지를 열어둡니다.

10. 다음 중 하나에 해당하는 경우, IAM Identity Center 다중 인증(MFA)을 활성화하기 위해 사용자에게 MFA에 대한 메시지 표시에서 다음 단계를 따릅니다.

    - 기본 Identity Center 디렉터리를 ID 소스로 사용하고 있습니다.
    - Active Directory의 AWS Managed Microsoft AD 디렉터리 또는 자체 관리형 디렉터리를 ID 소스로 사용하고 RADIUS AWS Directory Service MFA와 함께 사용하지는 않습니다.

> **Note**
>
> 외부 ID 제공업체(IdP)를 사용하는 경우, IAM Identity Center가 아닌 외부 ID 제공업체가 MFA 설정을 관리한다는 점에 유의하세요. IAM ID 센터의 MFA는 외부에서 사용할 수 없습니다. IdPs

관리 사용자에 대한 계정 액세스를 설정하면 IAM Identity Center에서 해당 IAM 역할을 생성합니다. IAM Identity Center에서 제어하는 이 역할은 관련 AWS 계정위치에서 생성되며 권한 집합에 지정된 정책이 역할에 연결됩니다.

IAM ID 센터 자격 증명으로 AWS 액세스 포털에 로그인합니다.

AWS 액세스 포털은 IAM Identity Center 사용자에게 웹 포털을 통해 할당된 모든 애플리케이션 AWS 계정 및 애플리케이션에 대한 Single Sign-On 액세스를 제공합니다.

다음 단계를 완료하여 IAM Identity Center 사용자가 액세스 포털에 로그인하여 AWS 액세스 포털에 액세스할 수 있는지 확인하십시오. AWS 계정

1. AWS Management Console에 로그인하려면 다음 중 하나를 수행합니다.
   - 신규 사용자 AWS (루트 사용자) — 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
   - AWS (IAM 자격 증명) 이미 사용 중 — IAM 자격 증명으로 로그인하고 관리자 역할을 선택합니다.
2. IAM Identity Center 콘솔을 엽니다.
3. 탐색 창에서 대시보드를 선택합니다.
4. 대시보드 페이지의 설정 요약에서 AWS 액세스 포털 URL을 선택합니다.
5. 다음 중 하나를 사용하여 로그인합니다.
   - Active Directory 또는 외부 ID 제공업체(IdP)를 ID 소스로 사용하는 경우, Active Directory 또는 IdP 사용자의 보안 인증 정보를 사용하여 로그인합니다.
   - 기본 Identity Center 디렉터리를 ID 소스로 사용하는 경우, 사용자를 생성할 때 지정한 사용자 이름과 해당 사용자에 지정한 새 암호를 사용하여 로그인합니다.

1. 계정 탭에서 내 계정을 AWS 계정 찾아 펼치십시오.
2. 사용할 수 있는 역할이 표시됩니다. 예를 들어 권한 집합과 청구 AdministratorAccess권한 집합이 모두 할당된 경우 해당 역할이 AWS 액세스 포털에 표시됩니다. 세션에 사용할 IAM 역할 이름을 선택합니다.
3. AWS Management Console로 리디렉션되면 에 대한 액세스 설정을 성공적으로 완료한 AWS 계정것입니다.

> **Note**
>
> 목록에 AWS 계정가 표시되지 않으면 사용자에게 해당 계정에 대한 권한 세트가 아직 할당되지 않았을 가능성이 높습니다. 권한 세트에 사용자를 할당하는 방법에 대한 지침은 사용자에게 액세스 권한을 할당하십시오. AWS 계정을 참조하세요.

이제 IAM Identity Center 자격 증명을 사용하여 로그인할 수 있음을 확인했으므로 로그인할 때 사용한 브라우저로 AWS Management Console 전환하고 루트 사용자 또는 IAM 사용자 자격 증명에서 로그아웃하십시오.

> **Important**
>
> 관리 작업을 수행하기 위해 AWS 액세스 포털에 로그인할 때는 IAM 사용자 또는 루트 사용자 자격 증명을 사용하는 대신 IAM Identity Center 관리 사용자의 자격 증명을 사용하는 것이 좋습니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 다른 사용자가 계정과 애플리케이션에 액세스하고 IAM Identity Center를 관리하도록 활성화하려면 IAM Identity Center로만 권한 세트를 생성하고 할당합니다.

그룹에 AWS 계정 액세스 권한을 할당하십시오.

IAM Identity Center에서 관리자를 생성하고 최소 권한으로 작업을 수행하는 데 사용할 수 있는 추가 권한 집합을 생성한 후에는 사용자 그룹에 액세스 권한을 제공할 수 있습니다. AWS 계정

개별 사용자에게 할당하는 대신 그룹에 직접 액세스 권한을 할당하는 것이 좋습니다. 예를 들어 조직 단위를 기반으로 그룹과 권한 세트를 생성하는 경우 사용자가 다른 조직 단위로 이동하면 해당 사용자를 다른 그룹으로 이동하기만 하면 새 조직 단위에 필요한 권한을 자동으로 받게 되며 이전 조직 단위의 권한은 잃게 됩니다.

사용자 그룹 액세스 권한을 할당하려면 AWS 계정

1. IAM Identity Center 콘솔을 엽니다.

   > **Note**
   >
   > ID 소스가 있는 경우 다음 단계로 넘어가기 전에 IAM Identity Center 콘솔이 AWS Managed Microsoft AD 디렉터리가 위치한 지역을 사용하고 있는지 AWS Managed Microsoft AD 확인하십시오.

2. 탐색 창의 다중 계정 권한에서 AWS 계정을 선택합니다.
3. AWS 계정 페이지에는 조직의 트리 뷰 목록이 표시됩니다. Single Sign-On 액세스를 할당하려는 하나 이상의 AWS 계정 옆에 있는 확인란을 선택합니다.

   > **Note**
   >
   > 권한 AWS 계정 집합당 최대 10개까지 선택할 수 있습니다.

4. 사용자 또는 그룹 할당을 선택합니다.
5. 1단계: 사용자 및 그룹 선택의 "***AWS-account-name***"으로 사용자 및 그룹 할당 페이지에서 그룹 탭을 선택한 다음 하나 이상의 그룹을 선택합니다.

   결과를 필터링하려면 검색 상자에 원하는 그룹 이름을 순서대로 입력합니다.

   선택한 그룹을 표시하려면 선택한 사용자 및 그룹 옆에 있는 옆의 삼각형을 선택합니다.

   올바른 그룹이 선택되었는지 확인한 후 다음을 선택합니다.

6. 2단계: 권한 세트 선택의 "***AWS-account-name***"으로 권한 세트 할당 페이지에서 하나 이상의 권한 세트를 선택합니다.

   > **Note**
   >
   > 이 절차를 시작하기 전에 원하는 권한 세트를 생성하지 않은 경우 권한 세트 생성을 선택하고 권한 집합을 생성합니다.의 단계를 따릅니다. 적용하려는 권한 집합을 생성한 후 IAM Identity Center 콘솔에서 AWS 계정로 돌아가 2단계: 권한 집합 선택에 도달할 때까지 지침을 따릅니다. 이 단계에 도달하면 생성한 새 권한 집합을 선택하고 이 절차의 다음 단계를 진행합니다.

올바른 권한 집합이 선택되었는지 확인한 후 다음을 선택합니다.

7. 3단계: 검토 및 제출의 경우 "***AWS-account-name***"에 대한 할당 검토 및 제출 페이지에서 다음을 수행합니다.

   1. 선택한 그룹 및 권한 세트를 검토합니다.
   2. 올바른 그룹 및 권한 세트가 선택되었는지 확인한 후 제출을 선택합니다.

> **Important**
>
> 그룹 할당 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 프로세스가 성공적으로 완료될 때까지 이 페이지를 열어둡니다.

> **Note**
>
> AWS Organizations 관리 계정에서 작업하려면 사용자 또는 그룹에 권한을 부여해야 할 수 있습니다. 권한이 높은 계정이므로 추가 보안 제한을 적용하려면 먼저 IAM FullAccess 정책 또는 이에 상응하는 권한이 있어야 설정할 수 있습니다. 조직의 구성원 AWS 계정에는 이러한 추가 보안 제한이 필요하지 않습니다.

또는 AWS CloudFormation를 사용하여 권한 세트를 생성 및 할당하고 해당 권한 세트에 사용자를 할당할 수 있습니다. 그러면 사용자는 AWS 액세스 포털에 로그인하거나AWS Command Line Interface (AWS CLI) 명령을 사용할 수 있습니다.

애플리케이션에 대한 Single Sign-On 액세스 설정

IAM Identity Center는 관리형 애플리케이션과 고객 AWS 관리형 애플리케이션이라는 두 가지 애플리케이션 유형을 지원합니다.

AWS 관리형 애플리케이션은 관련 애플리케이션 콘솔 내에서 직접 또는 애플리케이션 API를 통해 구성됩니다.

고객 관리형 애플리케이션은 IAM Identity Center 콘솔에 추가되고 IAM Identity Center 및 서비스 공급자 모두에 적합한 메타데이터로 구성되어야 합니다. SAML 2.0을 지원하는 일반적으로 사용되는 애플

리케이션 카탈로그에서 선택하거나 자체 SAML 2.0 애플리케이션 또는 OAuth 2.0 애플리케이션을 설정할 수 있습니다.

애플리케이션에 대한 Single Sign-On 액세스를 설정하는 구성 단계는 애플리케이션 유형에 따라 다릅니다.

관리형 애플리케이션 설정 AWS

AWS Amazon Managed Grafana 및 Amazon Monitron과 같은 관리형 애플리케이션은 IAM ID 센터와 통합되어 인증 및 디렉터리 서비스에 사용할 수 있습니다. IAM Identity Center와 함께 작동하도록 AWS 관리형 애플리케이션을 설정하려면 해당 서비스에 맞게 콘솔에서 직접 애플리케이션을 구성하거나 애플리케이션 API를 사용해야 합니다.

애플리케이션 카탈로그에서 애플리케이션 설정

IAM Identity Center 콘솔의 일반적으로 사용되는 애플리케이션 카탈로그에서 SAML 2.0 애플리케이션을 선택할 수 있습니다. IAM Identity Center와 애플리케이션의 서비스 공급자 간에 SAML 2.0 신뢰 관계를 설정해야 하는 경우 이 절차를 사용합니다.

애플리케이션 카탈로그에서 애플리케이션 설정

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 고객 관리형 탭을 선택합니다.
4. 애플리케이션 추가를 선택합니다.
5. 애플리케이션 유형 선택 페이지의 설정 기본 설정에서 카탈로그에서 애플리케이션을 선택하겠습니다를 선택합니다.
6. 애플리케이션 카탈로그에서 검색 상자에 추가하려는 애플리케이션 이름을 입력하기 시작합니다.
7. 검색 결과에 나타나는 목록에서 애플리케이션 이름을 선택한 후 다음을 선택합니다.
8. 애플리케이션 구성 페이지에서 표시 이름 및 설명 필드에 애플리케이션 관련 세부 정보가 미리 채워집니다. 이 정보를 편집할 수 있습니다.
9. IAM Identity Center 메타데이터에서 다음 작업을 수행합니다.

    a. IAM Identity Center SAML 메타데이터 파일에서 다운로드를 선택하여 ID 제공자 메타데이터를 다운로드합니다.

    b. IAM Identity Center 인증서에서 인증서 다운로드를 선택하여 ID 제공자 인증서를 다운로드합니다.

> **Note**
>
> 이러한 파일은 나중에 서비스 공급자의 웹 사이트에서 애플리케이션을 설정할 때 필요합니다. 해당 제공업체의 지침을 따르세요.

10. (선택 사항) 애플리케이션 속성에서 애플리케이션 시작 URL, 릴레이 상태 및 세션 지속 시간을 지정할 수 있습니다. 자세한 정보는 IAM Identity Center 콘솔의 애플리케이션 속성 구성을 참조하세요.
11. 애플리케이션 메타데이터에서 다음 작업 중 하나를 수행합니다.
    a. 메타데이터 파일이 있는 경우 애플리케이션 SAML 메타데이터 파일 업로드를 선택합니다. 그런 다음 파일 선택에서 메타데이터 파일을 찾아 선택합니다.
    b. 메타데이터 파일이 없는 경우 메타데이터 값 수동 입력을 선택한 다음 애플리케이션 ACS URL 및 애플리케이션 SAML 대상 값을 입력합니다.
12. 제출을 선택합니다. 방금 추가한 애플리케이션의 세부정보 페이지로 이동합니다.

자체 SAML 2.0 애플리케이션 설정

IAM Identity Center와 SAML 2.0 애플리케이션의 서비스 공급자 간에 자체 SAML 2.0 신뢰 관계를 설정해야 하는 경우 이 절차를 사용합니다. 이 절차를 시작하기 전에 신뢰 설정을 완료할 수 있도록 서비스 제공업체의 인증서 및 메타데이터 교환 파일이 있는지 확인하세요.

자체 SAML 2.0 애플리케이션 설정

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 고객 관리형 탭을 선택합니다.
4. 애플리케이션 추가를 선택합니다.
5. 애플리케이션 유형 선택 페이지의 설정 기본 설정에서 설정하고자 하는 애플리케이션이 있습니다를 선택합니다.
6. 애플리케이션 유형에서 SAML 2.0을 선택합니다.
7. 다음을 선택합니다.
8. 애플리케이션 구성 페이지의 애플리케이션 구성에서 **MyApp**와 같이 애플리케이션의 표시 이름을 입력합니다. 그런 다음 설명을 입력합니다.

9. IAM Identity Center 메타데이터에서 다음 작업을 수행합니다.

   a. IAM Identity Center SAML 메타데이터 파일에서 다운로드를 선택하여 ID 제공자 메타데이터를 다운로드합니다.

   b. IAM Identity Center 인증서에서 다운로드를 선택하여 ID 제공업체 인증서를 다운로드합니다.

> **Note**
>
> 이러한 파일은 나중에 서비스 제공자의 웹 사이트에서 사용자 지정 애플리케이션을 설정할 때 필요합니다.

10. (선택 사항) 애플리케이션 속성에서 애플리케이션 시작 URL, 릴레이 상태 및 세션 지속 시간을 지정할 수도 있습니다. 자세한 정보는 IAM Identity Center 콘솔의 애플리케이션 속성 구성을 참조하세요.
11. 애플리케이션 메타데이터에서 메타데이터 값 수동 입력을 선택합니다. 그런 다음 애플리케이션 ACS URL과 애플리케이션 SAML 대상 값을 제공합니다.
12. 제출을 선택합니다. 방금 추가한 애플리케이션의 세부정보 페이지로 이동합니다.

애플리케이션을 설정하고 나면 사용자는 할당된 권한에 따라 AWS 액세스 포털 내에서 애플리케이션에 액세스할 수 있습니다.

OAuth 2.0을 지원하는 고객 관리형 애플리케이션이 있고 사용자가 이러한 애플리케이션에서 AWS 서비스에 액세스해야 하는 경우 신뢰할 수 있는 ID 전파를 사용할 수 있습니다. 신뢰할 수 있는 ID 전파를 사용하면 사용자가 애플리케이션에 로그인할 수 있으며, 해당 애플리케이션은 서비스의 데이터에 액세스하기 위한 요청에 사용자의 ID를 전달할 수 있습니다. AWS 자세한 정보는 고객 관리형 애플리케이션에서 신뢰할 수 있는 ID 전파 사용을 참조하세요.

지원되는 애플리케이션 유형에 대한 자세한 내용은 애플리케이션 액세스 관리을 참조하세요.

사용자 및 그룹 할당 보기

사용자 및 그룹 페이지에서 IAM Identity Center의 내용에 누가 액세스할 수 있는지 확인할 수 있습니다. 이 절차를 사용하여 AWS 계정, 권한 집합, 애플리케이션 및 그룹에 대한 사용자의 액세스 수준을 확인할 수 있습니다.

1. IAM Identity Center 콘솔을 엽니다.

2. 사용자 그룹을 편집할지 아니면 개별적으로 할당된 한 명의 사용자를 편집할지에 따라 사용자 또는 그룹을 선택합니다.
3. 목록에서 사용자 또는 그룹을 선택합니다.
4. 계정 할당을 볼지, 애플리케이션 할당을 볼지, 그룹 할당을 볼지 선택합니다.

   - AWS 계정 및 권한 집합 할당
     1. [Accounts] 탭을 선택합니다.
     2. 목록에서 계정을 선택하면 사용자 및 그룹 권한 집합 할당을 볼 수 있습니다.
     3. 보려는 권한 집합을 선택하면 정책 및 할당 세부 정보를 볼 수 있습니다.
   - 애플리케이션 할당
     1. 애플리케이션 탭을 선택하면 사용자 또는 그룹에 할당된 애플리케이션을 볼 수 있습니다.
     2. 목록에서 애플리케이션을 선택하면 과제 세부 정보를 볼 수 있습니다.
   - 그룹 과제
     1. 사용자 페이지에서 그룹 탭을 선택합니다.
     2. 그룹을 선택하면 사용자에 대한 그룹 할당을 볼 수 있습니다.

IAM Identity Center의 조직 및 계정 인스턴스 관리

인스턴스는 IAM Identity Center의 단일 배포입니다. IAM Identity Center에서 사용할 수 있는 두 가지 인스턴스 유형은 조직 인스턴스와 계정 인스턴스입니다.

AWS 계정 IAM ID 센터를 활성화할 수 있는 유형

IAM Identity Center를 활성화하려면 생성하려는 인스턴스 유형에 따라 다음 자격 증명 중 하나를 사용하여 로그인합니다. AWS Management Console

- AWS Organizations 관리 계정 (권장) - IAM Identity Center의 조직 인스턴스를 생성하는 데 필요합니다. 조직 인스턴스를 사용하여 조직 전체에 걸쳐 다중 계정 권한 및 애플리케이션 할당을 수행할 수 있습니다.
- AWS Organizations 멤버 계정 - IAM Identity Center의 계정 인스턴스를 생성하여 해당 멤버 계정 내에서 애플리케이션을 할당할 수 있도록 하는 데 사용합니다. 구성원 수준 인스턴스가 있는 하나 이상의 계정이 조직에 존재할 수 있습니다.
- 독립형 AWS 계정 — IAM Identity Center의 조직 인스턴스 또는 계정 인스턴스를 생성하는 데 사용합니다. 독립형은 에서 AWS 계정 관리되지 않습니다. AWS Organizations IAM Identity Center의 인스턴스 하나만 독립 실행형과 연결할 수 AWS 계정 있으며 해당 독립 실행형 내에서 애플리케이션 할당에 인스턴스를 사용할 수 있습니다. AWS 계정

기능	AWS Organizations 관리 계정의 인스턴스 (권장)	구성원 계정의 인스턴스	독립형 인스턴스 AWS 계정
사용자 관리	 예	 예	 예
AWS 관리 애플리케이션에 AWS 싱글 사인온 액세스를 위한 액세스 포털	 예	 예	 예

기능	AWS Organizations 관리 계정의 인스턴스 (권장)	구성원 계정의 인스턴스	독립형 인스턴스 AWS 계정
OAuth 2.0 (OIDC) 고객 관리형 애플리케이션	 여	 너	 네
다중 계정 권한	 여	 니요	 니요
AWS 싱글 사인온 액세스를 위한 액세스 포털 AWS 계정	 여	 니요	 니요
SAML 2.0 고객 관리형 애플리케이션	 여	 니요	 니요
위임된 관리자가 인스턴스 관리 가능	 여	 니요	 니요

주제

- IAM Identity Center의 조직 인스턴스 관리
- IAM Identity Center의 계정 인스턴스
- IAM ID 센터 콘솔에서 계정 인스턴스를 활성화합니다.
- 서비스 제어 정책으로 계정 인스턴스 생성 제어
- IAM Identity Center의 계정 인스턴스 생성

IAM Identity Center의 조직 인스턴스 관리

IAM ID 센터와 함께 AWS Organizations활성화하면 IAM ID 센터의 조직 인스턴스가 생성됩니다. 관리 계정에서 조직 인스턴스를 활성화해야 하고 단일 조직 인스턴스로 사용자와 그룹의 액세스를 중앙에서 관리할 수 있습니다. AWS Organizations의 각 관리 계정에 대해 단 하나의 조직 인스턴스만 보유할 수 있습니다.

2023년 11월 15일 이전에 IAM Identity Center를 활성화한 경우 IAM Identity Center의 조직 인스턴스를 보유합니다.

조직 인스턴스를 사용하는 경우

조직 인스턴스는 IAM Identity Center를 활성화하는 기본 방법으로, 대부분의 경우 조직 인스턴스 사용이 권장됩니다. 조직 인스턴스가 제공하는 이점:

- IAM Identity Center의 모든 기능 지원 — 조직 AWS 계정 내 여러 명의 권한 관리 및 고객 관리 애플리케이션에 대한 액세스 권한 할당을 포함합니다.
- 관리 지점 수 감소 - 조직 인스턴스에는 단일 관리 지점인 관리 계정이 있습니다. 계정 인스턴스 대신 조직 인스턴스를 활성화하여 관리 지점 수를 줄이는 것이 좋습니다.
- 계정 인스턴스 생성 제어 - 옵트인 지역 (AWS 리전 기본적으로 비활성화됨) 에서 조직에 IAM Identity Center 인스턴스를 배포하지 않았다면 조직의 구성원 계정으로 계정 인스턴스를 생성할 수 있는지 여부를 제어할 수 있습니다.

IAM Identity Center의 계정 인스턴스

IAM Identity Center의 계정 인스턴스를 사용하여 지원되는 AWS 관리형 애플리케이션과 OIDC 기반 고객 관리형 애플리케이션을 배포할 수 있습니다. 계정 인스턴스는 IAM Identity Center 직원 ID 및 액세스 포털 기능을 활용하여 애플리케이션을 한 번에 AWS 계정격리하여 배포할 수 있도록 지원합니다.

계정 인스턴스는 AWS 계정 단일에 바인딩되며 동일한 계정에서 지원되는 애플리케이션의 사용자 및 그룹 액세스를 관리하는 데만 사용됩니다. AWS 리전계정 인스턴스당 1개로 제한됩니다 AWS 계정. 다음 중 하나에서 계정 인스턴스 생성 가능:

- 의 멤버 계정 AWS Organizations.
- 에서 관리하지 AWS 계정 않는 독립형 계정입니다. AWS Organizations

구성원 계정의 가용성 제한

다음 조건에 해당하는 경우 조직의 구성원 계정에 계정 인스턴스를 배포할 수 있습니다.

- 2023년 11월 15일 이전에 IAM ID 센터 인스턴스를 조직에 배포하지 않았습니다.
- 2023년 11월 15일 이전에 IAM Identity Center 인스턴스가 이미 조직에 배포되어 있고 관리자가 구성원 계정을 활성화하여 IAM ID 센터의 계정 인스턴스를 생성할 수 있도록 했습니다.
- 관리자는 회원 계정이 계정 인스턴스를 생성하지 못하도록 하는 서비스 제어 정책을 만들지 않았습니다.
- 여부와 상관없이 동일한 계정에 IAM Identity Center 인스턴스가 이미 있는 것은 AWS 리전아닙니다.
- IAM ID 센터를 사용할 수 없는 AWS 리전 곳에서 일하고 있습니다. 리전에 대한 자세한 내용은 AWS IAM Identity Center 지역 이용 가능 여부의 내용을 참조하세요.

주제

- 계정 인스턴스를 사용하는 경우
- 계정 인스턴스 고려 사항
- AWS 계정 인스턴스를 지원하는 관리형 애플리케이션

계정 인스턴스를 사용하는 경우

대부분의 경우 조직 인스턴스가 권장됩니다. 계정 인스턴스는 다음 시나리오 중 하나에 해당하는 경우에만 사용해야 합니다.

- 지원되는 AWS 관리형 애플리케이션의 임시 평가판을 실행하여 애플리케이션이 비즈니스 요구 사항에 적합한지 확인하고 싶습니다.
- 조직 전체에 IAM Identity Center를 도입할 계획은 없지만 하나 이상의 AWS 관리형 애플리케이션을 지원하려는 경우
- IAM Identity Center의 조직 인스턴스가 있지만 지원되는 AWS 관리형 애플리케이션을 조직 인스턴스의 사용자와 구별되는 격리된 사용자 집합에 배포하려고 합니다.

> **Important**
>
> IAM Identity Center를 사용하여 여러 계정의 애플리케이션을 지원하려는 경우 조직 인스턴스를 생성하고 계정 인스턴스는 사용하지 마세요.

계정 인스턴스 고려 사항

계정 인스턴스는 특수 사용 사례에 맞게 설계되어 조직 인스턴스에서 사용할 수 있는 기능 하위 세트를 제공합니다. 계정 인스턴스를 생성하기 전에 고려할 사항:

- 계정 인스턴스는 권한 집합을 지원하지 않으므로 액세스를 AWS 계정지원하지 않습니다.
- 계정 인스턴스를 조직 인스턴스로 변환할 수 없습니다.
- 계정 인스턴스를 조직 인스턴스로 병합할 수 없습니다.
- 일부 AWS 관리형 애플리케이션 지원 계정 인스턴스만 가능합니다.
- 단일 계정에서만, 그리고 애플리케이션이 사용되는 기간 동안 애플리케이션을 사용할 격리된 사용자에 대해 계정 인스턴스를 사용합니다.
- 계정 인스턴스에 연결된 애플리케이션은 애플리케이션과 해당 리소스를 삭제할 때까지 계정 인스턴스에 연결된 상태로 유지되어야 합니다.
- 계정 인스턴스는 생성된 AWS 계정 위치에 그대로 남아 있어야 합니다.

AWS 계정 인스턴스를 지원하는 관리형 애플리케이션

IAM Identity Center의 계정 인스턴스를 지원하는 AWS 관리형 애플리케이션을 AWS 관리형 애플리케이션 알아보려면 을 참조하십시오. AWS 관리형 애플리케이션으로 계정 인스턴스 생성 가능 여부를 확인하십시오.

IAM ID 센터 콘솔에서 계정 인스턴스를 활성화합니다.

2023년 11월 15일 이전에 IAM Identity Center를 활성화한 경우 IAM Identity Center의 조직 인스턴스가 생성되며 구성원 계정으로 계정 인스턴스를 생성할 수 있는 기능은 기본적으로 비활성화됩니다. AWS Management Console에서 계정 인스턴스 기능을 활성화하여 구성원 계정이 계정 인스턴스를 생성할 수 있는지 여부를 선택할 수 있습니다.

> **Note**
>
> 배포 날짜와 상관없이 옵트인 지역 (AWS 리전 기본적으로 비활성화됨) 에서 조직에 IAM Identity Center 인스턴스를 배포하지 않았다면 구성원 계정은 계정 인스턴스를 생성할 수 있습니다. 옵트인으로 AWS 리전 배포된 IAM Identity Center의 조직 인스턴스는 계정 인스턴스 생성을 차단합니다. 리전에 대한 자세한 내용은 AWS IAM Identity Center 지역 이용 가능 여부의 내용을 참조하세요.

조직의 구성원 계정에서 계정 인스턴스의 생성 활성화

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택한 다음 관리 탭을 선택합니다.
3. IAM Identity Center의 계정 인스턴스 섹션에서 IAM Identity Center의 계정 인스턴스 활성화를 선택합니다.
4. IAM Identity Center의 계정 인스턴스 활성화 대화 상자에서 활성화를 선택하여 조직의 구성원 계정에서 계정 인스턴스를 생성할 수 있도록 허용할지 여부를 확인합니다.

> **Important**
>
> 회원 계정에 대해 IAM Identity Center의 계정 인스턴스를 활성화하는 작업은 한 번만 하면 됩니다. 즉, 이 작업은 되돌릴 수 없습니다. 활성화한 후에는 서비스 제어 정책 (SCP) 을 생성하여 계정 인스턴스 생성을 제한할 수 있습니다. 지침은 서비스 제어 정책을 사용한 계정 인스턴스 생성 제어를 참조하십시오.

서비스 제어 정책으로 계정 인스턴스 생성 제어

사용자는 IAM ID 센터의 계정 인스턴스라고 하는 단일 AWS 계정인스턴스에 바인딩되는 IAM ID 센터 인스턴스를 생성할 수 있습니다. 서비스 제어 정책(SCP)으로 계정 인스턴스 생성을 제어할 수 있습니다.

1. IAM Identity Center 콘솔을 엽니다.
2. 대시보드의 중앙 관리 섹션에서 계정 인스턴스 방지 버튼을 선택합니다.
3. 새 계정 인스턴스가 생성되지 않도록 SCP 연결 대화 상자에 SCP가 제공됩니다. SCP를 복사하고 SCP 대시보드로 이동 버튼을 선택합니다. AWS Organizations 콘솔로 이동하여 SCP를 생성하거나 이를 기존 SCP에 명령문으로 연결할 수 있게 됩니다.

   서비스 제어 정책은 의 기능입니다. AWS Organizations SCP 연결에 대한 지침은 AWS Organizations 사용 설명서의 서비스 제어 정책 연결 및 분리를 참조하세요.

계정 인스턴스 생성을 방지하는 대신 조직 AWS 계정 내 특정 인스턴스로 계정 인스턴스 생성을 제한할 수 있습니다.

Example : 인스턴스 생성을 제어하는 SCP

```
{
    "Version": "2012-10-17",
    "Statement" : [
        {
            "Sid": "DenyMemberAccountInstances",
            "Effect": "Deny",
            "Action": "sso:CreateInstance",
            "Resource": "*",
            "Condition": {
                 "StringNotEquals": {
                    "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
                }
            }
        }
    ]
}
```

IAM Identity Center의 계정 인스턴스 생성

조직 인스턴스는 IAM Identity Center를 활성화하는 기본이자 권장되는 방법입니다. 사용 사례가 계정 인스턴스 생성을 지원해야 하고 고려 사항을 파악해야 합니다.

조직 구성원 계정 또는 독립형 AWS 계정에서 계정 인스턴스를 생성합니다.

1. AWS Management Console에 로그인하려면 다음 중 하나를 수행합니다.
   - 신규 사용자 AWS (루트 사용자) — 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
   - 이미 AWS (IAM 자격 증명) 사용 중 — 관리자 권한이 있는 IAM 자격 증명을 사용하여 로그인합니다.
2. IAM Identity Center 콘솔을 엽니다.
3. IAM Identity Center 활성화에서 활성화를 선택합니다.
4. 계정 인스턴스 생성 계속을 선택하고 계속을 선택합니다.

> **Note**
>
> IAM Identity Center의 조직 인스턴스가 있는 경우 사용 사례에 자체적인 IAM Identity Center의 계정 인스턴스가 필요한지 확인합니다. 그렇지 않은 경우 취소 후 조직 인스턴스 사용을 선택합니다.

5. 선택 사항. 이 계정 인스턴스와 연결하고자 하는 태그를 추가합니다.

콘솔의 알림은 계정 인스턴스가 생성되었음을 나타내며 인스턴스 ID도 포함됩니다. 설정 요약에서 인스턴스 이름을 지정할 수 있습니다.

> **Note**
>
> 기본적으로 다중 인증(MFA)이 계정 인스턴스에서 활성화됩니다. 디바이스, 브라우저 또는 위치가 변경되면 사용자에게 MFA로 로그인하라는 메시지가 표시됩니다. 보안 모범 사례로 직원 ID에 MFA가 강력하게 권장됩니다. IAM Identity Center에서 MFA 디바이스 관리에 대해 알아봅니다.

ID 소스 확인, 다단계 인증 설정 조정, AWS 관리형 애플리케이션 추가와 같은 관리 기능은 IAM Identity Center 콘솔에서 완료해야 합니다.

인증

사용자는 사용자 이름을 사용하여 AWS 액세스 포털에 로그인합니다. 로그인하면 IAM Identity Center는 사용자 이메일 주소와 연결된 디렉터리를 기반으로 요청을 IAM Identity Center 인증 서비스로 리디렉션합니다. 인증을 받으면 사용자는 추가 로그인 메시지 없이 포털에 표시되는 모든 AWS 계정과 타사 (software-as-a-service SaaS) 애플리케이션에 싱글 사인온 (Single Sign-On) 액세스할 수 있습니다. 즉, 사용자는 매일 사용하는 다양한 할당된 AWS 애플리케이션에 대한 여러 계정 자격 증명을 더 이상 추적할 필요가 없습니다.

인증 세션

IAM ID 센터에서 유지 관리하는 인증 세션에는 두 가지 유형이 있습니다. 하나는 IAM ID 센터에 대한 사용자의 로그인을 나타내는 것이고 다른 하나는 Amazon Studio SageMaker 또는 Amazon AWS Managed Grafana와 같은 관리형 애플리케이션에 대한 사용자의 액세스를 나타내는 것입니다. 사용자가 IAM Identity Center에 로그인할 때마다 IAM Identity Center에 구성된 기간(최대 90일) 동안 로그인 세션이 생성됩니다. 자세한 정보는 AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 관리합니다.을 참조하세요. 사용자가 애플리케이션에 액세스할 때마다 IAM Identity Center 로그인 세션을 사용하여 해당 애플리케이션에 대한 IAM Identity Center 애플리케이션 세션을 확보합니다. IAM Identity Center 애플리케이션 세션의 수명은 1시간으로 갱신할 수 있습니다. 즉, IAM Identity Center 애플리케이션 세션은 생성된 IAM Identity Center 로그인 세션이 여전히 유효하다면 1시간마다 자동으로 새로 고침됩니다. 사용자가 IAM Identity Center를 사용하여 AWS Management Console 또는 CLI에 액세스하는 경우, IAM ID 센터 로그인 세션을 사용하여 해당 IAM ID 센터 권한 집합에 지정된 대로 IAM 세션을 획득합니다 (특히, IAM ID 센터는 대상 계정에서 IAM ID 센터가 관리하는 IAM 역할을 맡습니다).

IAM Identity Center에서 사용자를 비활성화하거나 삭제하면, 해당 사용자는 즉시 로그인하여 새로운 IAM Identity Center 로그인 세션을 생성할 수 없게 됩니다. IAM Identity Center 로그인 세션은 1시간 동안 저장됩니다. 즉, 활성화된 IAM Identity Center 로그인 세션이 있는 동안 사용자를 비활성화하거나 삭제하면 로그인 세션이 마지막으로 갱신된 시기에 따라 기존 IAM Identity Center 로그인 세션이 최대 1시간 동안 유지됩니다. 이 기간 동안 사용자는 새 IAM Identity Center 애플리케이션 및 IAM 역할 세션을 시작할 수 있습니다.

IAM Identity Center 로그인 세션이 만료된 후에는 사용자가 더 이상 새 IAM Identity Center 애플리케이션 또는 IAM 역할 세션을 시작할 수 없습니다. 하지만 IAM Identity Center 애플리케이션 세션을 최대 1시간 동안 저장할 수도 있으므로 사용자는 IAM Identity Center 로그인 세션이 만료된 후 최대 1시간 동안 애플리케이션에 대한 액세스 권한을 유지할 수 있습니다. 기존의 모든 IAM 역할 세션은 IAM Identity Center 권한 세트에 구성된 기간(관리자 구성 가능, 최대 12시간)에 따라 지속됩니다.

아래 표에는 이러한 행동이 요약되어 있습니다.

사용자 경험/시스템 행동	사용자 비활성화/삭제 후 남은 시간
사용자는 더 이상 IAM Identity Center에 로그인할 수 없으며 새 IAM Identity Center 로그인 세션을 가져올 수 없습니다.	없음(즉시 적용)
사용자는 더 이상 IAM Identity Center를 통해 새 애플리케이션 또는 IAM 역할 세션을 시작할 수 없습니다.	최대 1시간
사용자는 더 이상 애플리케이션에 액세스할 수 없습니다(모든 애플리케이션 세션이 종료됨).	최대 2시간 (IAM Identity Center 로그인 세션 만료의 경우 최대 1시간, IAM Identity Center 애플리케이션 세션 만료의 경우 최대 1시간)
사용자는 더 이상 IAM ID 센터를 통해 어떤 것에도 액세스할 수 없습니다. AWS 계정	최대 13시간 (IAM Identity Center 로그인 세션 만료의 경우 최대 1시간, 권한 세트의 IAM Identity Center 세션 기간 설정에 따라 관리자가 구성한 IAM 역할 세션 만료의 경우 최대 12시간)

세션에 대한 자세한 내용은 세션 기간 설정 단원을 참조하세요.

직원 ID 관리

AWS Identity and Access Management(IAM)을(를) 사용하면 ID와 AWS 서비스 및 리소스에 대한 액세스를 안전하게 관리할 수 있습니다. IAM 서비스로서 AWS IAM Identity Center는 AWS에서 작업 인력 ID를 한 번에 생성하거나 연결하고 여러 AWS 계정 및 애플리케이션에 대한 액세스를 중앙 관리하는 곳입니다.

IAM Identity Center 고객의 경우 여러 AWS 계정 또는 애플리케이션에 대한 액세스를 중앙에서 관리하는 방법은 변경되지 않습니다. IAM Identity Center를 처음 사용하는 고객의 경우 IAM Identity Center를 IAM을 사용한 단일 AWS 계정 액세스 관리와 함께 실행하거나 이를 대체하도록 유연하게 구성할 수 있습니다.

주제

- 사용 사례
- 사용자, 그룹 및 프로비저닝
- ID 소스 관리
- AWS 액세스 포털 사용
- Identity Center 사용자를 위한 다중 인증

사용 사례

다음은 IAM Identity Center를 사용하여 다양한 비즈니스 요구 사항을 충족하는 방법을 보여주는 사용 사례입니다.

주제

- AWS 애플리케이션에 대한 Single Sign-on 액세스 활성화(애플리케이션 관리자 역할)
- Amazon EC2 Windows 인스턴스에 대한 Single Sign-On 액세스 활성화

AWS 애플리케이션에 대한 Single Sign-on 액세스 활성화(애플리케이션 관리자 역할)

이 사용 사례는 귀하가 Amazon SageMaker, 또는 AWS IoT SiteWise와 같은 AWS 관리형 애플리케이션을 관리하는 애플리케이션 관리자이고, 사용자에게 Single Sign-on 액세스를 제공해야 하는 경우 제공되는 사용 사례 지침입니다.

시작하기 전에 다음을 고려하십시오.

- AWS Organizations에서 별도의 조직에 테스트 또는 프로덕션 환경을 만들고 싶으신가요?
- 조직에 이미 IAM Identity Center가 활성화되어 있습니까? AWS Organizations의 관리 계정에서 IAM Identity Center를 활성화할 권한이 있습니까?

다음 지침을 검토하여 비즈니스 요구 사항에 따라 다음 단계를 결정합니다.

AWS 애플리케이션을 독립형 AWS 계정으로 구성

AWS 애플리케이션에 대한 Single Sign-On 액세스를 제공해야 하고 IT 부서에서 아직 IAM Identity Center를 사용하지 않는다는 사실을 알고 있다면 독립형 AWS 계정 애플리케이션을 생성하여 시작해야 할 수 있습니다. 기본적으로 자체 AWS 계정 조직을 만들면 이러한 자체 AWS 조직을 만들고 관리하는 데 필요한 권한을 갖게 됩니다. IAM Identity Center를 활성화하려면 AWS 계정 루트 사용자 권한이 있어야 합니다.

IAM Identity Center 및 AWS Organizations은 AWS 애플리케이션(예: Amazon Managed Grafana)의 설정 중에 자동으로 활성화될 수 있습니다. AWS 애플리케이션에서 이러한 서비스를 활성화하는 옵션을 제공하지 않는 경우 애플리케이션에 Single Sign-on 액세스를 제공하기 전에 먼저 AWS Organizations 및 IAM Identity Center를 설정해야 합니다.

조직에 IAM Identity Center가 구성되어 있지 않음

애플리케이션 관리자의 역할에서는 권한에 따라 IAM Identity Center를 활성화하지 못할 수도 있습니다. IAM Identity Center를 사용하려면 AWS Organizations 관리 계정의 특정 권한이 필요합니다. 이 경우 해당 관리자에게 문의하여 조직 관리 계정에서 IAM Identity Center를 활성화합니다.

IAM Identity Center를 활성화할 수 있는 충분한 권한이 있는 경우 먼저 이 작업을 수행한 다음 애플리케이션 설정을 진행합니다. 자세한 내용은 IAM Identity Center에서 일반 작업 시작 단원을 참조하십시오.

조직에 IAM Identity Center가 구성되어 있음

이 경우, 추가 조치를 취하지 않고도 AWS 애플리케이션을 계속 배포할 수 있습니다.

> **Note**
>
> 조직이 2019년 11월 25일 이전에 관리 계정에서 IAM Identity Center를 활성화한 경우 관리 계정(선택적으로 구성원 계정)에서 AWS 관리형 애플리케이션을 활성화해야 합니다. 관리 계정에서만 활성화하면 구성원 계정에서는 이후에 활성화할 수 있습니다. 이러한 애플리케이션을

활성화하려면 IAM Identity Center 콘솔의 설정 페이지 내의 AWS 관리형 애플리케이션 섹션에서 액세스 활성화를 선택합니다. 자세한 내용은 ID 정보를 공유하도록 IAM Identity Center 구성 섹션을 참조하세요.

Amazon EC2 Windows 인스턴스에 대한 Single Sign-On 액세스 활성화

Identity Center 디렉터리(IAM Identity Center의 기본 ID 소스)에서 사용자를 관리하는 애플리케이션 관리자이거나 지원되는 외부 ID 제공업체(IdP)인 경우 Amazon EC2 Windows 인스턴스에 대한 Single Sign-on 액세스를 활성화할 수 있으며, AWS Fleet Manager 콘솔에서 Amazon EC2 Windows 데스크톱에 대한 IAM Identity Center 액세스 권한을 제공해야 합니다.

이 구성을 사용하면 기존 기업 보안 인증 정보로 Amazon EC2 Windows 인스턴스에 안전하게 액세스할 수 있습니다. 관리자 보안 인증 정보 및 액세스 보안 인증 정보를 여러 번 공유하거나 원격 액세스 클라이언트 소프트웨어를 구성할 필요가 없습니다. 여러 AWS 계정에 걸쳐 Amazon EC2 Windows 인스턴스에 대한 액세스 권한을 대규모로 중앙에서 부여하고 취소할 수 있습니다. 예를 들어, IAM Identity Center 통합 ID 소스에서 직원을 제거하면 해당 직원은 Amazon EC2 Windows 인스턴스를 포함한 모든 AWS 리소스에 대한 액세스 권한을 자동으로 잃게 됩니다.

자세한 내용은 IAM Identity Center를 사용하여 Amazon EC2 Windows 인스턴스에 안전하고 원활한 Single Sign-on을 활성화하는 방법을 참조하십시오.

이 기능을 활성화하도록 IAM Identity Center를 구성하는 방법에 대한 데모는 IAM Identity Center를 사용하여 Amazon EC2 Windows에 Single Sign-on 활성화를 참조하십시오.

사용자, 그룹 및 프로비저닝

IAM Identity Center에서 사용자 및 그룹을 사용할 때 다음 사항을 고려하세요.

사용자 이름 및 이메일 주소 고유성

IAM Identity Center의 사용자는 고유하게 식별할 수 있어야 합니다. IAM Identity Center는 사용자의 기본 식별자인 사용자 이름을 구현합니다. 대부분의 사람들이 사용자 이름을 사용자의 이메일 주소와 동일하게 설정하지만 IAM Identity Center 및 SAML 2.0 표준에서는 이를 요구하지 않습니다. 하지만 많은 SAML 2.0 기반 애플리케이션은 이메일 주소를 사용자의 고유 식별자로 사용합니다. 이러한 애플리케이션은 SAML 2.0 ID 제공업체가 인증 중에 전송하는 어설션을 통해 이 정보를 얻습니다. 이러한 애플리케이션은 각 사용자의 이메일 주소 고유성에 따라 달라집니다. 이런 이유로 IAM Identity Center에서는 사용자 로그인에 사용할 이메일 주소 이외의 다른 주소를 지정할 수 있습니다. IAM Identity Center에서는 사용자의 모든 사용자 이름과 이메일 주소가 NULL이 아니며 고유해야 합니다.

그룹

그룹은 귀하가 정의한 사용자의 논리적 조합입니다. 그룹을 생성하고 사용자를 그룹에 추가할 수 있습니다. IAM Identity Center는 그룹(중첩된 그룹)에 그룹을 추가하는 것을 지원하지 않습니다. 그룹은 AWS 계정 및 애플리케이션에 대한 액세스 권한을 할당할 때 유용합니다. 각 사용자를 개별적으로 할당하는 대신 그룹에 권한을 부여합니다. 나중에 그룹에 사용자를 추가하거나 그룹에서 사용자를 제거하면 해당 사용자는 그룹에 할당한 계정 및 애플리케이션에 대한 액세스 권한을 동적으로 얻거나 잃게 됩니다.

사용자 및 그룹 프로비저닝

프로비저닝은 IAM Identity Center 및 AWS 관리형 애플리케이션 또는 고객 관리형 애플리케이션에서 사용자 및 그룹 정보를 사용할 수 있도록 하는 프로세스입니다. IAM Identity Center에서 사용자 및 그룹을 직접 생성하거나 Active Directory 또는 외부 ID 제공업체에서 사용자 및 그룹과 함께 작업할 수 있습니다. IAM Identity Center가 AWS 계정에서 사용자 및 그룹에 액세스 권한을 할당하려면 먼저 IAM Identity Center에서 사용자와 그룹을 인식해야 합니다. 마찬가지로 AWS 관리형 애플리케이션 및 고객 관리형 애플리케이션은 IAM Identity Center가 인식하는 사용자 및 그룹에서 사용됩니다.

IAM Identity Center에서의 프로비저닝은 사용하는 ID 소스에 따라 달라집니다. 자세한 내용은 ID 소스 관리 섹션을 참조하세요.

ID 소스 관리

IAM Identity Center의 ID 소스는 사용자 및 그룹을 관리하는 위치를 정의합니다. ID 소스를 구성한 후 사용자 또는 그룹을 검색하여 AWS 계정, 애플리케이션 또는 둘 다에 대한 Single Sign-On 액세스 권한을 부여할 수 있습니다.

AWS Organizations에서 조직당 하나의 ID 소스만 가질 수 있습니다. 다음 중 하나를 ID 소스로 선택할 수 있습니다.

- ID Center 디렉터리 - IAM Identity Center를 처음 활성화하면 자동으로 Identity Center 디렉터리가 기본 ID 소스로 구성됩니다. 여기에서 사용자와 그룹을 생성하고 AWS 계정 및 애플리케이션에 대한 액세스 수준을 할당할 수 있습니다.
- Active Directory - AWS Directory Service을 사용하는 AWS Managed Microsoft AD 디렉터리 또는 Active Directory (AD)의 자체 관리 디렉터리에서 사용자를 계속 관리하려면 이 옵션을 선택합니다.
- 외부 ID 제공업체(idP) - Okta 또는 Microsoft Entra ID와 외부 ID 제공업체(idP)에서 사용자를 관리하려는 경우 이 옵션을 선택합니다.

> **Note**
>
> IAM Identity Center는 SAMBA4 기반 Simple AD를 ID 소스로 지원하지 않습니다.

주제

- ID 소스 변경 시 고려 사항
- ID 소스 변경
- 모든 ID 소스 유형에 대한 로그인 및 속성 사용 관리
- IAM Identity Center에서 ID 관리
- Microsoft AD 디렉터리에 연결
- 외부 ID 제공업체에 연결

ID 소스 변경 시 고려 사항

ID 소스는 언제든지 변경할 수 있지만, 이러한 변경이 현재 배포에 어떤 영향을 미칠 수 있는지 고려하는 것이 좋습니다.

이미 하나의 ID 소스에서 사용자 및 그룹을 관리하고 있는 경우, 다른 ID 소스로 변경하면 IAM Identity Center에서 구성한 모든 사용자 및 그룹 할당이 제거될 수 있습니다. 이 경우 IAM Identity Center의 관리자를 포함한 모든 사용자는 자신과 애플리케이션에 대한 Single Sign-On 액세스 권한을 AWS 계정 잃게 됩니다.

IAM Identity Center의 ID 소스를 변경하기 전에 다음 고려 사항을 검토한 후 진행하세요. ID 소스 변경을 계속 진행하려면 ID 소스 변경에서 자세한 내용을 확인하세요.

IAM Identity Center와 Active Directory 간 변경

이미 Active Directory에서 사용자와 그룹을 관리하고 있다면 IAM Identity Center를 활성화하고 ID 소스를 선택할 때 디렉터리 연결을 고려하는 것이 좋습니다. 기본 Identity Center 디렉터리에 사용자 및 그룹을 생성하고 할당하기 전에 먼저 이 작업을 수행합니다.

기본 Identity Center 디렉터리에서 이미 사용자 및 그룹을 관리하고 있다면 다음 사항을 고려합니다.

- 할당 제거 및 사용자 및 그룹 삭제 - ID 소스를 Active Directory로 변경하면 Identity Center 디렉터리에서 사용자 및 그룹이 삭제됩니다. 이 변경 사항으로 인해 할당도 제거됩니다. 이 경우 Active Directory로 변경한 후에는 Active Directory의 사용자 및 그룹을 Identity Center 디렉터리로 동기화한 다음 할당을 다시 적용해야 합니다.

Active Directory를 사용하지 않는 경우 Identity Center 디렉터리에 사용자 및 그룹을 만든 다음 할당해야 합니다.

- ID가 삭제되어도 할당은 삭제되지 않음 – Identity Center 디렉터리에서 ID를 삭제하면 IAM Identity Center에서도 해당 할당이 삭제됩니다. 하지만 Active Directory에서는 ID가 삭제해도(Active Directory 또는 동기화된 ID에서) 해당 할당은 삭제되지 않습니다.
- API에 대한 아웃바운드 동기화 없음 - AActive Directory를 ID 소스로 사용하는 경우에는 생성, 업데이트 및 삭제 API를 주의해서 사용하는 것이 좋습니다. IAM Identity Center는 아웃바운드 동기화를 지원하지 않으므로 이러한 API를 사용하여 사용자 또는 그룹을 변경해도 이에 따라 ID 소스가 자동으로 업데이트되지 않습니다.
- 액세스 포털 URL 변경 — IAM ID 센터와 Active Directory 간에 ID 소스를 변경하면 액세스 포털의 URL도 변경됩니다. AWS

IAM Identity Center에서 사용자 및 그룹을 프로비저닝하는 방법에 대한 자세한 내용은 Microsoft AD 디렉터리에 연결을 참조하세요.

IAM Identity Center에서 외부 IdP로 변경

ID 소스를 IAM Identity Center에서 외부 ID 제공업체(idP)로 변경하는 경우 다음 사항을 고려합니다.

- 과제 및 멤버십은 올바른 어설션으로 작동합니다. 새 IdP가 올바른 어설션 (예: SAML NameID) 을 보내는 한 사용자 할당, 그룹 할당, 그룹 멤버십은 계속 작동합니다. 이러한 어설션은 IAM Identity Center의 사용자 이름 및 그룹과 일치해야 합니다.
- 아웃바운드 동기화 없음 — IAM Identity Center는 아웃바운드 동기화를 지원하지 않으므로 IAM Identity Center에서 사용자 및 그룹을 변경해도 외부 IdP가 자동으로 업데이트되지 않습니다.
- SCIM 프로비저닝 — SCIM 프로비저닝을 사용하는 경우 ID 제공자의 사용자 및 그룹에 대한 변경 사항은 ID 제공자가 해당 변경 사항을 IAM Identity Center로 전송한 후에만 IAM Identity Center에 반영됩니다. 자동 프로비저닝을 사용할 때 고려 사항 섹션을 참조하십시오.
- 롤백 — 언제든지 ID 소스를 다시 IAM Identity Center를 사용하도록 되돌릴 수 있습니다. 외부 IdP에서 IAM Identity Center로 변경 섹션을 참조하십시오.

IAM Identity Center에서 사용자 및 그룹을 프로비저닝하는 방법에 대한 자세한 내용은 외부 ID 제공업체에 연결을 참조하세요.

외부 IdP에서 IAM Identity Center로 변경

ID 소스를 외부 ID 제공업체(idP)에서 IAM Identity Center로 변경하는 경우 다음 사항을 고려합니다.

- IAM Identity Center는 모든 할당을 그대로 유지합니다.
- 비밀번호 강제 재설정 - IAM Identity Center에 비밀번호를 설정한 사용자는 이전 비밀번호로 계속 로그인할 수 있습니다. 외부 IdP에 있고 IAM Identity Center에 있지 않은 사용자 관리자가 비밀번호를 강제로 재설정해야 합니다.

IAM Identity Center에서 사용자 및 그룹을 프로비저닝하는 방법에 대한 자세한 내용은 IAM Identity Center에서 ID 관리을 참조하세요.

하나의 외부 IdP에서 다른 외부 IdP로 변경

이미 외부 IdP를 IAM Identity Center의 ID 소스로 사용 중이고 다른 외부 IdP로 변경하는 경우 다음 사항을 고려합니다.

- 할당 및 멤버십은 올바른 어설션으로 작동 – IAM Identity Center는 모든 할당을 그대로 유지합니다. 사용자 할당, 그룹 할당 및 그룹 멤버십은 새 IdP가 올바른 어설션(예: SAML nameIDs)을 보내는 한 계속 작동합니다.

  이러한 어설션은 사용자가 새 외부 IdP를 통해 인증할 때 IAM Identity Center의 사용자 이름과 일치해야 합니다.
- SCIM 프로비저닝 – SCIM을 사용하여 IAM Identity Center에 프로비저닝하는 경우, 이 가이드의 IdP 관련 정보 및 IdP에서 제공한 설명서를 읽고, SCIM이 활성화되었을 때 새 제공업체가 사용자와 그룹을 올바르게 매칭하는지 확인하는 것이 좋습니다.

IAM Identity Center에서 사용자 및 그룹을 프로비저닝하는 방법에 대한 자세한 내용은 외부 ID 제공업체에 연결을 참조하세요.

Active Directory와 외부 IdP 간 변경

ID 소스를 외부 IdP에서 Active Directory로 또는 Active Directory에서 외부 IdP로 변경하는 경우 다음 사항을 고려합니다.

- 사용자, 그룹 및 할당이 삭제됨 - 모든 사용자, 그룹 및 할당이 IAM Identity Center에서 삭제됩니다. 외부 IdP 또는 Active Directory의 사용자 또는 그룹 정보에는 영향을 미치지 않습니다.
- 사용자 프로비저닝 - 외부 IdP로 변경하는 경우 사용자를 프로비저닝하도록 IAM Identity Center를 구성해야 합니다. 또는 외부 IdP에 대한 사용자 및 그룹을 수동으로 프로비저닝한 후에야 할당을 구성할 수 있습니다.
- 할당 및 그룹 생성 - Active Directory로 변경하는 경우 Active Directory의 디렉터리에 있는 사용자 및 그룹으로 할당을 생성해야 합니다.

IAM Identity Center에서 사용자 및 그룹을 프로비저닝하는 방법에 대한 자세한 내용은 Microsoft AD 디렉터리에 연결을 참조하세요.

ID 소스 변경

다음 절차는 IAM Identity Center에서 제공하는 디렉터리(기본 Identity Center 디렉터리)에서 Active Directory 또는 외부 ID 공급자로 변경하거나 그 반대로 변경하는 방법에 대해 설명합니다. 계속하기 전에 ID 소스 변경 시 고려 사항에 있는 정보를 검토하십시오. 현재 배포에 따라 이 변경으로 인해 IAM Identity Center에서 구성한 모든 사용자 및 그룹 할당이 제거될 수 있습니다. 이 경우 IAM Identity Center의 관리자를 포함한 모든 사용자는 자신의 AWS 계정 애플리케이션에 대한 Single Sign-On 액세스 권한을 잃게 됩니다.

ID 소스를 변경하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택합니다. 작업을 선택한 다음 ID 소스 변경을 선택합니다.
4. ID 소스 선택에서 변경할 소스를 선택한 후 다음을 선택합니다.

   Active Directory로 변경하는 경우 다음 페이지의 메뉴에서 사용 가능한 디렉터리를 선택합니다.

   > **Important**
   >
   > ID 소스를 Active Directory로 또는 Active Directory에서 변경하면 Identity Center 디렉터리에서 사용자와 그룹이 삭제됩니다. 또한 이 변경으로 인해 IAM Identity Center에서 구성한 모든 할당이 제거됩니다.

   외부 ID 공급자로 전환하는 경우 외부 ID 제공업체에 연결하는 방법의 단계를 따르는 것이 좋습니다.
5. 고지 사항을 읽고 진행할 준비가 되면 ACCEPT를 입력합니다.
6. ID 소스 변경을 선택합니다. ID 소스를 Active Directory로 변경하는 경우 다음 단계로 진행합니다.
7. ID 소스를 Active Directory로 변경하면 설정 페이지로 이동합니다. 설정 페이지를 사용하여 다음 중 하나를 수행하십시오.

   - 안내에 따른 설정 시작을 선택합니다. 안내된 설정 프로세스를 완료하는 방법에 대한 자세한 내용은 설정 안내을 참조하십시오.

- ID 소스 섹션에서 작업을 선택한 다음 동기화 관리를 선택하여 동기화 범위, 동기화할 사용자 및 그룹 목록을 구성합니다.

모든 ID 소스 유형에 대한 로그인 및 속성 사용 관리

IAM Identity Center는 관리자가 AWS 액세스 포털 사용을 제어하고, 액세스 포털 및 애플리케이션의 사용자에 대한 세션 기간을 설정하고, AWS 액세스 제어를 위한 속성을 사용할 수 있는 다음과 같은 기능 세트를 제공합니다. 이러한 기능은 Identity Center 디렉터리 또는 외부 ID 공급자를 ID 소스로 사용할 수 있습니다.

> **Note**
>
> Active Directory를 IAM Identity Center의 ID 소스로 사용하는 경우 세션 관리는 지원되지 않습니다.

주제

- AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 관리합니다.
- AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 구성합니다.
- AWS 액세스 포털 및 AWS 통합 애플리케이션의 세션을 삭제합니다.
- 지원되는 사용자 및 그룹 속성

AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 관리합니다.

IAM ID 센터 관리자는 IAM Identity Center와 통합된 두 애플리케이션 및 의 세션 기간을 구성할 수 있습니다. AWS 액세스 포털세션 기간 구성에 따라 사용자가 재인증해야 하는 빈도가 결정됩니다. IAM Identity Center 관리자는 활성 AWS 액세스 포털 세션을 종료할 수 있으며, 이를 통해 통합 애플리케이션의 세션도 종료할 수 있습니다.

자세한 정보는 AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 구성합니다.을 참조하세요. 최종 사용자 세션을 관리하는 방법에 대한 자세한 내용은 을 참조하십시오AWS 액세스 포털 및 AWS 통합 애플리케이션의 세션을 삭제합니다..

> **Note**
>
> AWS 액세스 포털 세션 기간을 수정하고 AWS 액세스 포털 세션을 종료해도 권한 집합에 정의한 AWS Management Console 세션 기간에는 영향을 주지 않습니다.

AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 구성합니다.

IAM Identity Center 통합 애플리케이션 AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션에 대한 인증 세션 기간은 사용자가 재인증 없이 로그인할 수 있는 최대 시간입니다. 기본 세션 지속 시간은 8시간입니다. IAM ID 센터 관리자는 최소 15분에서 최대 90일까지 다른 기간을 지정할 수 있습니다. 인증 세션 기간 및 사용자 동작에 대한 자세한 내용은 을 참조하십시오인증.

다음 항목에서는 AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간 구성에 대한 정보를 제공합니다.

주제

- 필수 조건 및 고려 사항
- 세션 기간을 구성하는 방법

필수 조건 및 고려 사항

다음은 AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 구성하기 위한 사전 요구 사항 및 고려 사항입니다.

외부 ID 제공업체(idP)

IAM Identity Center는 SAML 어설션의 `SessionNotOnOrAfter` 속성을 사용하여 세션의 유효 기간을 결정하는 데 도움을 줍니다.

- SAML 어설션에서 전달되지 않은 경우 `SessionNotOnOrAfter` AWS 액세스 포털 세션 기간은 외부 IdP 세션 기간의 영향을 받지 않습니다. 예를 들어 IdP 세션 기간이 24시간이고 IAM Identity Center에서 세션 기간을 18시간으로 설정한 경우 사용자는 18시간 후에 액세스 포털에서 다시 인증해야 합니다. AWS
- `SessionNotOnOrAfter`가 SAML 어설션으로 전달되면 세션 기간 값은 AWS 액세스 포털 세션 기간과 SAML IdP 세션 기간 중 더 짧은 시간으로 설정됩니다. IAM Identity Center에서 72시간 세션 기

간을 설정하고 IdP의 세션 지속 시간이 18시간인 경우 사용자는 IdP에 정의된 18시간 동안 AWS 리소스에 액세스할 수 있습니다.

- IdP의 세션 기간이 IAM Identity Center에 설정된 기간보다 길면 사용자는 자격 증명을 다시 입력하지 않고도 IdP와의 유효한 로그인 세션을 기반으로 새 IAM Identity Center 세션을 시작할 수 있습니다.

> **Note**
>
> Active Directory를 IAM Identity Center의 ID 소스로 사용하는 경우 세션 관리는 지원되지 않습니다.

AWS CLI 및 SDK 세션

AWS Command Line Interface, AWS 소프트웨어 개발 키트 (SDK) 또는 기타 AWS 개발 도구를 사용하여 프로그래밍 방식으로 AWS 서비스에 액세스하는 경우 AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 설정하려면 다음 사전 요구 사항을 충족해야 합니다.

- IAM Identity Center 콘솔에서 AWS 액세스 포털 세션 기간을 구성해야 합니다.
- 공유 AWS 구성 파일에서 Single Sign-On 설정을 위한 프로필을 정의해야 합니다. 이 프로파일은 AWS 액세스 포털에 연결하는 데 사용됩니다. SSO 토큰 제공업체 구성을 사용하는 것이 좋습니다. 이 구성을 사용하면 AWS SDK 또는 도구가 새로 고쳐진 인증 토큰을 자동으로 검색할 수 있습니다. 자세한 내용은AWS SDK 및 도구 참조 설명서의 SSO 토큰 공급자 구성을 참조하세요.
- 사용자는 세션 관리를 지원하는 버전 AWS CLI 또는 SDK를 실행해야 합니다.

세션 관리를 지원하는 AWS CLI 의 최소 버전

다음은 세션 관리를 AWS CLI 지원하는 의 최소 버전입니다.

- AWS CLI V2 2.9 이상
- AWS CLI V1 1.27.10 이상

최신 버전을 설치하거나 업데이트하는 방법에 대한 자세한 내용은 최신 AWS CLI 버전 설치 또는 업데이트를 참조하십시오. AWS CLI

사용자가 를 실행 중인 경우 IAM Identity Center 세션이 만료되기 직전에 권한 집합을 새로 고치고 세션 지속 시간이 20시간으로 설정되고 권한 설정 기간은 12시간으로 설정된 상태에서 AWS CLI 세션은

최대 20시간에 12시간을 더한 총 32시간 동안 실행됩니다. AWS CLI IAM Identity Center CLI에 대한 자세한 내용은 AWS CLI 명령 참조를 참조하세요.

IAM Identity Center 세션 관리를 지원하는 SDK의 최소 버전

다음은 IAM Identity Center 세션 관리를 지원하는 SDK의 최소 버전입니다.

SDK	최소 버전
Python	1.26.10
PHP	3.245.0
Ruby	aws-sdk-core 3.167.0
Java V2	AWS Java v2용 SDK (2.18.13)
Go V2	전체 SDK: release-2022-11-11 및 특정 Go 모듈: credentials/v1.13.0, config/v1.18.0
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

세션 기간을 구성하는 방법

다음 절차를 사용하여 AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 구성하십시오.

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 인증에서 세션 설정 옆의 구성을 선택합니다. 세션 설정 구성 대화 상자가 나타납니다.
5. 세션 설정 구성 대화 상자에서 드롭다운 화살표를 선택하여 사용자의 최대 세션 기간을 분, 시간, 일 단위로 선택합니다. 세션 길이를 선택한 다음 저장을 선택합니다. 설정 페이지로 돌아갑니다.

AWS 액세스 포털 및 AWS 통합 애플리케이션의 세션을 삭제합니다.

다음 절차를 사용하여 IAM Identity Center 사용자의 활성 세션을 보고 삭제할 수 있습니다.

AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 활성 세션을 삭제하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 사용자를 선택하세요.
3. 사용자 페이지에서 세션을 관리할 사용자의 ID를 선택합니다. 그러면 사용자 정보가 있는 페이지로 이동합니다.
4. 사용자 페이지에서 활성 세션 탭을 선택합니다. 활성 세션 옆의 괄호 안의 숫자는 이 사용자의 현재 활성 세션 수를 나타냅니다.
5. 삭제하고 싶은 세션 옆의 체크박스를 선택하고 세션 삭제를 선택합니다. 이 사용자의 활성 세션을 삭제할지 확인하는 대화 상자가 나타납니다. 대화 상자의 정보를 읽고 계속하려면 세션 삭제를 선택합니다.
6. 사용자 페이지로 돌아갑니다. 선택한 세션이 성공적으로 삭제되었음을 나타내는 녹색 플래시 바가 나타납니다.

취소된 인증 세션의 동작에 대한 자세한 내용은 을 참조하십시오. 인증 세션

지원되는 사용자 및 그룹 속성

속성은 개별 사용자 또는 그룹 개체를 정의하고 식별하는 데 도움이 되는 정보(예: `name`, `email` 또는 `members`)입니다. 사용자 생성 시 수동으로 입력하든, 교차 도메인 자격 증명 관리용 시스템(SCIM) 사양에 정의된 것과 같은 동기화 엔진을 사용하여 자동으로 프로비저닝하든 관계없이 IAM Identity Center는 가장 일반적으로 사용되는 속성을 지원합니다. 이 사양에 대한 자세한 내용은 https://tools.ietf.org/html/rfc7642을 참조하세요. 수동 및 자동 프로비저닝에 대한 자세한 내용은 사용자가 외부 IdP일 경우 프로비저닝 섹션을 참조하세요.

IAM Identity Center는 자동 프로비저닝 사용 사례에서 SCIM을 지원하므로몇 가지 예외를 제외하고 Identity Center 디렉터리는 SCIM 사양에 나와 있는 동일한 사용자 및 그룹 속성을 모두 지원합니다. 다음 섹션에서는 IAM Identity Center에서 지원되지 않는 속성에 대해 설명합니다.

사용자 객체

SCIM 사용자 스키마(https://tools.ietf.org/html/rfc7643#section-8.3)의 모든 속성은 다음을 제외하고 IAM Identity Center ID Store에서 지원됩니다.

- password
- ims
- photos
- entitlements
- x509Certificates

사용자의 하위 속성은 다음을 제외하고 모두 지원됩니다.

- 다중 값 속성의 'display' 하위 속성(예: emails 또는 phoneNumbers)
- 'meta' 속성의 'version' 하위 속성

그룹 객체

SCIM 그룹 스키마(https://tools.ietf.org/html/rfc7643#section-8.4)의 모든 속성이 지원됩니다.

그룹의 하위 속성은 다음을 제외하고 모두 지원됩니다.

- 다중 값 속성의 'display' 하위 속성(예: 멤버)

IAM Identity Center에서 ID 관리

IAM Identity Center는 사용자 및 그룹에 다음과 같은 기능을 제공합니다.

- 사용자 및 그룹을 생성합니다.
- 사용자를 그룹에 구성원으로 추가합니다.
- 사용자 AWS 계정 및 애플리케이션에 원하는 수준의 액세스 권한을 가진 그룹을 할당합니다.

IAM Identity Center 스토어의 사용자 및 그룹을 관리하기 위해 ID 센터 작업에 나열된 API 작업을 AWS 지원합니다.

IAM Identity Center에서의 프로비저닝

IAM Identity Center에서 직접 사용자 및 그룹을 생성하는 경우 자동으로 프로비저닝이 이루어집니다. 이러한 ID는 즉시 할당에 사용할 수 있고 애플리케이션에서 사용할 수 있습니다. 자세한 정보는 사용자 및 그룹 프로비저닝을 참조하세요.

ID 소스 변경

에서 AWS Managed Microsoft AD사용자를 관리하려는 경우 언제든지 ID 센터 디렉터리 사용을 중지하고 대신 를 사용하여 IAM Identity Center를 Microsoft AD의 디렉터리에 연결할 수 있습니다. AWS Directory Service자세한 내용은 IAM Identity Center와 Active Directory 간 변경의 고려 사항을 참조하세요.

외부 ID 제공업체(idP)에서 사용자를 관리하려는 경우 IAM Identity Center를 IdP에 연결하고 자동 프로비저닝을 활성화할 수 있습니다. 자세한 내용은 IAM Identity Center에서 외부 IdP로 변경의 고려 사항을 참조하세요.

주제

- 사용자 추가
- 그룹 추가
- 그룹에 사용자 추가
- IAM Identity Center에서 그룹 삭제
- IAM Identity Center에서 사용자 삭제
- IAM Identity Center에서 사용자 액세스 비활성화
- 사용자 속성 편집
- IAM Identity Center 최종 사용자 암호 재설정
- API에서 생성한 사용자에게 이메일 OTP 전송
- IAM Identity Center에서 ID를 관리할 때 암호 요구 사항

사용자 추가

IAM Identity Center 디렉터리에 생성한 사용자 및 그룹은 IAM Identity Center에서만 사용할 수 있습니다. 다음 절차에 따라 IAM Identity Center 콘솔을 사용하여 Identity Center 디렉터리에 사용자를 추가할 수 있습니다. 또는 AWS API 작업을 호출하여 사용자를 CreateUser추가할 수도 있습니다.

사용자를 추가하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 사용자를 선택하세요.
3. 필요한 다음 정보를 입력한 다음 사용자 추가를 선택합니다.

a. 사용자 이름 - 이 사용자 이름은 AWS 액세스 포털에 로그인하는 데 필요하며 나중에 변경할 수 없습니다. 이는 1~100자여야 합니다.

b. 암호 - 이 암호를 통해 설정 지침(기본 옵션)이 포함된 이메일을 보내거나 일회용 암호를 생성할 수 있습니다. 관리자를 만들 때 이메일을 보내기로 선택한 경우 액세스할 수 있는 이메일 주소를 지정해야 합니다.

   i. 암호 설정 지침이 포함된 이메일을 이 사용자에게 보냅니다. — 이 옵션은 가입 초대 AWS IAM Identity Center (Single AWS Sign-On 후속) 라는 제목이 붙은 Amazon Web Services의 이메일 주소를 사용자에게 자동으로 보냅니다. 이 이메일은 회사를 대신하여 사용자가 IAM Identity Center 액세스 포털에 액세스하도록 초대합니다. AWS

   > **Note**
   >
   > 특정 리전에서는 IAM Identity Center가 다른 AWS 리전의 Amazon Simple Email Service를 사용하는 사용자에게 이메일을 보냅니다. 이메일 전송 방법에 대한 자세한 내용은 크로스 리전 호출 단원을 참조하세요.
   > IAM Identity Center 서비스에서 보내는 모든 이메일은 주소 `no-reply@signin.aws.com` 또는 `no-reply@login.awsapps.com` 에서 발송됩니다. 이러한 발신자 이메일 주소의 이메일은 수신하고 정크 또는 스팸으로 처리하지 않도록 이메일 시스템을 구성하는 것이 좋습니다.

   ii. 이 사용자와 공유할 수 있는 일회용 암호를 생성합니다. — 이 옵션은 이메일 주소를 통해 사용자에게 수동으로 보낼 수 있는 AWS 액세스 포털 URL 및 암호 세부 정보를 제공합니다.

c. 이메일 주소 - 이메일 주소는 고유해야 합니다.

d. 이메일 주소 확인

e. 이름 — 자동 프로비저닝이 작동하려면 여기에 이름을 입력해야 합니다. 자세한 내용은 자동 프로비저닝 단원을 참조하세요.

f. 성 — 자동 프로비저닝이 작동하려면 여기에 이름을 입력해야 합니다.

g. 표시 이름

> **Note**
>
> (선택 사항) 해당하는 경우 사용자의 Microsoft 365 변경 불가 ID와 같은 추가 특성 값을 지정하여 사용자에게 특정 비즈니스 응용 프로그램에 대한 Single Sign-On 액세스를 제공할 수 있습니다.

4. 다음을 선택합니다.
5. 해당하는 경우 사용자를 추가할 그룹을 하나 이상 선택하고 다음을 선택합니다.
6. 1단계: 사용자 세부 정보 지정 및 2단계: 그룹에 사용자 추가(선택 사항)에서 지정한 정보를 검토합니다. 변경하려면 두 단계 중 하나에서 편집을 선택합니다. 두 단계 모두에 올바른 정보가 지정되었는지 확인한 후 사용자 추가를 선택합니다.

그룹 추가

다음 절차에 따라 IAM Identity Center 콘솔을 사용하여 Identity Center 디렉터리에 그룹을 추가할 수 있습니다. 또는 AWS API 작업을 호출하여 그룹을 CreateGroup추가할 수도 있습니다.

그룹을 추가하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 그룹을 선택합니다.
3. 그룹 생성을 선택합니다.
4. 그룹 이름 및 설명 (선택 사항)을 입력합니다. 설명에는 그룹에 할당되었거나 할당될 권한에 대한 세부 정보가 제공되어야 합니다. 그룹에 사용자 추가 - 선택 사항이며, 구성원으로 추가할 사용자를 찾습니다. 그런 다음 옆의 확인란을 선택합니다.
5. 그룹 생성을 선택합니다.

이 그룹을 Identity Center 디렉터리에 추가한 후 이 그룹에 Single Sign-On 액세스 권한을 할당할 수 있습니다. 자세한 내용은 사용자에게 액세스 권한을 할당하십시오. AWS 계정 단원을 참조하세요.

그룹에 사용자 추가

다음 절차에 따라 IAM Identity Center 콘솔을 사용하여 이전에 Identity Center 디렉터리에 생성한 그룹의 구성원으로 사용자를 추가할 수 있습니다. 또는 AWS API 작업을 CreateGroupMembership호출하여 사용자를 그룹 구성원으로 추가할 수도 있습니다.

사용자를 그룹의 구성원으로 추가하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 그룹을 선택합니다.
3. 업데이트할 그룹 이름을 선택합니다.
4. 그룹 세부 정보 페이지 내의 이 그룹의 사용자에서 그룹에 사용자 추가를 선택합니다.
5. 그룹에 사용자 추가 페이지 내의 기타 사용자에서 구성원으로 추가할 사용자를 찾습니다. 그런 다음 옆의 확인란을 선택합니다.
6. 사용자 추가를 선택합니다.

IAM Identity Center에서 그룹 삭제

IAM Identity Center 디렉터리에서 그룹을 삭제하면 이 그룹의 구성원인 모든 사용자의 AWS 계정 및 애플리케이션에 대한 액세스가 제거됩니다. 그룹을 삭제한 후에는 실행 취소할 수 없습니다. 다음 절차에 따라 IAM Identity Center 콘솔을 사용하여 Identity Center 디렉터리에서 그룹을 삭제할 수 있습니다.

IAM Identity Center에서 그룹을 삭제하려면

> **Important**
>
> 이 페이지의 지침은 AWS IAM Identity Center에 적용됩니다. AWS Identity and Access Management(IAM)에는 적용되지 않습니다. IAM 사용자, 그룹 및 IAM 사용자 보안 인증은 IAM Identity Center 사용자, 그룹 및 사용자 보안 인증과 다릅니다. IAM에서 그룹을 삭제하는 방법에 대한 지침을 찾으려면 AWS Identity and Access Management 사용 설명서의 IAM 사용자 그룹 삭제를 참조하세요.

1. IAM Identity Center 콘솔을 엽니다.
2. 그룹을 선택합니다.
3. 그룹을 삭제하는 방법에는 다음 두 가지 방법이 있습니다.
   - 그룹 페이지에서 삭제할 그룹을 여러 개 선택할 수 있습니다. 삭제하려는 그룹 이름을 선택하고 그룹 삭제를 선택합니다.
   - 삭제할 그룹 이름을 선택합니다. 그룹의 세부 정보 페이지에서 그룹 삭제를 선택합니다.
4. 그룹 삭제 의사를 확인하라는 메시지가 표시될 수 있습니다.

- 한 번에 여러 그룹을 삭제하는 경우 그룹 삭제 대화 상자에 **Delete**을 입력하여 의사를 확인합니다.
- 사용자가 포함된 단일 그룹을 삭제하는 경우 그룹 삭제 대화 상자에 삭제하려는 그룹의 이름을 입력하여 의사를 확인합니다.

5. 그룹 삭제를 선택합니다. 삭제할 그룹을 여러 개 선택한 경우 # 그룹 삭제를 선택합니다.

IAM Identity Center에서 사용자 삭제

IAM Identity Center 디렉터리에서 사용자를 삭제하면 AWS 계정 및 애플리케이션에 대한 액세스가 제거됩니다. 사용자를 삭제한 후에는 실행 취소할 수 없습니다. 다음 절차에 따라 IAM Identity Center 콘솔을 사용하여 Identity Center 디렉터리에서 사용자를 삭제할 수 있습니다.

> **Note**
>
> IAM Identity Center에서 사용자 액세스를 비활성화하거나 사용자를 삭제하면 해당 사용자는 즉시 AWS 액세스 포털에 로그인할 수 없으며 새 로그인 세션을 생성할 수 없게 됩니다. 자세한 정보는 인증 세션을 참조하세요.

IAM Identity Center에서 사용자를 삭제하려면

> **Important**
>
> 이 페이지의 지침은 AWS IAM Identity Center에 적용됩니다. AWS Identity and Access Management(IAM)에는 적용되지 않습니다. IAM 사용자, 그룹 및 IAM 사용자 보안 인증은 IAM Identity Center 사용자, 그룹 및 사용자 보안 인증과 다릅니다. IAM에서 사용자를 삭제하는 방법에 대한 지침을 찾으려면 AWS Identity and Access Management 사용 설명서의 IAM 사용자 삭제를 참조하세요.

1. IAM Identity Center 콘솔을 엽니다.
2. 사용자를 선택하세요.
3. 사용자를 삭제하는 방법에는 다음 두 가지 방법이 있습니다.

   - 사용자 페이지에서 삭제할 사용자를 여러 명 선택할 수 있습니다. 삭제하려는 사용자 이름을 선택하고 사용자 삭제를 선택합니다.

- 삭제하려는 사용자 이름을 선택합니다. 사용자 세부 정보 페이지에서 사용자 삭제를 선택합니다.

4. 한 번에 여러 사용자를 삭제하는 경우 사용자 삭제 대화 상자에 **Delete**을 입력하여 의사를 확인합니다.
5. 사용자 삭제를 선택합니다. 삭제할 사용자를 여러 명 선택한 경우 # 사용자 삭제를 선택합니다.

IAM Identity Center에서 사용자 액세스 비활성화

IAM Identity Center 디렉터리에서 사용자 액세스를 비활성화하면 사용자 세부 정보를 편집하거나, 암호를 재설정하거나, 사용자를 그룹에 추가하거나, 그룹 멤버십을 볼 수 없습니다. 다음 절차에 따라 IAM Identity Center 콘솔을 사용하여 Identity Center 디렉터리에서 사용자 액세스를 비활성화할 수 있습니다.

> **Note**
>
> IAM Identity Center에서 사용자 액세스를 비활성화하거나 사용자를 삭제하면 해당 사용자는 즉시 AWS 액세스 포털에 로그인할 수 없으며 새 로그인 세션을 생성할 수 없게 됩니다. 자세한 정보는 인증 세션을 참조하세요.

IAM Identity Center에서 사용자 액세스를 비활성화하려면

1. IAM Identity Center 콘솔을 엽니다.

   > **Important**
   >
   > 이 페이지의 지침은 AWS IAM Identity Center에 적용됩니다. AWS Identity and Access Management(IAM)에는 적용되지 않습니다. IAM 사용자, 그룹 및 IAM 사용자 보안 인증은 IAM Identity Center 사용자, 그룹 및 사용자 보안 인증과 다릅니다. IAM에서 사용자를 비활성화하는 방법에 대한 지침을 찾으려면 AWS Identity and Access Management 사용 설명서의 IAM 사용자 관리를 참조하세요.

2. 사용자를 선택하세요.
3. 액세스를 비활성화하려는 사용자의 사용자 이름을 선택합니다.
4. 액세스를 비활성화하려는 사용자의 사용자 이름 아래에 있는 일반 정보 섹션에서 사용자 액세스 비활성화를 선택합니다.
5. 사용자 액세스 비활성화 대화 상자에서 비활성화를 선택합니다.

사용자 속성 편집

다음 절차에 따라 IAM Identity Center 콘솔을 사용하여 Identity Center 디렉터리에서 사용자 속성을 편집할 수 있습니다. 또는 AWS API 작업을 UpdateUser호출하여 사용자 속성을 업데이트할 수도 있습니다.

IAM Identity Center에서 사용자 속성을 편집하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 사용자를 선택하세요.
3. 편집할 사용자를 선택합니다.
4. 사용자 프로필 페이지에서 프로필 세부 정보 옆의 편집을 선택합니다.
5. 프로필 세부 정보 편집 페이지에서 필요에 따라 속성을 업데이트합니다. 그런 다음 변경 사항 저장을 선택합니다.

> **Note**
>
> (선택 사항) 직원 번호 및 Office 365 변경 불가 ID와 같은 추가 특성을 수정하여 IAM Identity Center의 사용자 ID를 사용해야 하는 특정 비즈니스 애플리케이션에 매핑하는 데 도움이 되도록 할 수 있습니다.

> **Note**
>
> 이메일 주소 속성은 편집 가능한 필드이지만 제공하는 값은 고유해야 합니다.

IAM Identity Center 최종 사용자 암호 재설정

이 절차는 IAM Identity Center 디렉터리에 있는 사용자의 암호를 재설정해야 하는 관리자를 위한 것입니다. IAM Identity Center 콘솔을 사용하여 암호를 재설정합니다.

ID 제공업체 및 사용자 유형에 대한 고려 사항

- MicrosoftActive Directory 또는 외부 제공업체 - IAM Identity Center를 Microsoft Active Directory 또는 외부 제공업체에 연결하는 경우 Active Directory 또는 외부 제공업체를 통해 사용자 암호를 재설정해야 합니다. 즉, IAM Identity Center 콘솔에서는 해당 사용자의 암호를 재설정할 수 없습니다.

- IAM ID 센터 디렉터리의 사용자 - IAM Identity Center 사용자인 경우 IAM Identity Center 암호를 직접 재설정할 수 있으며, IAM Identity Center의 사용자 암호 재설정하기 단원을 참조하세요.

IAM Identity Center 최종 사용자 암호를 재설정하려면

> **Important**
>
> 이 페이지의 지침은 AWS IAM Identity Center에 적용됩니다. AWS Identity and Access Management(IAM)에는 적용되지 않습니다. IAM 사용자, 그룹 및 IAM 사용자 보안 인증은 IAM Identity Center 사용자, 그룹 및 사용자 보안 인증과 다릅니다. IAM 사용자의 암호를 변경하는 방법에 대한 지침을 찾으려면 AWS Identity and Access Management 사용 설명서의 IAM 사용자 암호 관리를 참조하세요.

1. IAM Identity Center 콘솔을 엽니다.
2. 사용자를 선택하세요.
3. 암호를 재설정하려는 사용자의 이름을 선택합니다.
4. 사용자 세부 정보 페이지에서 암호 재설정을 선택합니다.
5. 암호 재설정 대화 상자에서 다음 선택 사항 중 하나를 선택한 다음 암호 재설정을 선택합니다.

   a. 암호 재설정 지침이 포함된 이메일을 사용자에게 전송 — 이 옵션은 암호 재설정 방법을 안내하는 Amazon Web Services의 이메일을 사용자에게 자동으로 보냅니다.

   > **Warning**
   >
   > 보안 모범 사례로서 이 옵션을 선택하기 전에 이 사용자의 이메일 주소가 올바른지 확인합니다. 이 암호 재설정 이메일이 잘못되거나 잘못 구성된 이메일 주소로 전송되면 악의적인 수신자가 이를 사용하여 사용자 AWS 환경에 무단으로 액세스할 수 있습니다.

   b. 일회용 암호를 생성하여 사용자와 암호 공유 — 이 옵션은 전자 메일 주소를 통해 수동으로 사용자에게 보낼 수 있는 암호 세부 정보를 제공합니다.

API에서 생성한 사용자에게 이메일 OTP 전송

CreateUserAPI 작업을 사용하여 사용자를 생성하면 해당 사용자에게는 비밀번호가 없습니다. API로 사용자를 생성할 때 사용자에게 이메일 일회용 암호(OTP)를 보내도록 선택하여 이를 변경할 수 있습

니다. 사용자는 처음 로그인을 시도할 때 이메일 OTP를 받게 됩니다. 이메일 OTP 수신 후 로그인할 때 새 암호를 설정해야 합니다. 이 설정을 활성화하지 않으면 CreateUser API를 사용하여 생성한 사용자와 OTP를 생성하고 공유해야 합니다.

CreateUser API로 만든 사용자에게 이메일 OTP를 보내려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 표준 인증 섹션에서 구성을 선택합니다.
5. 대화 상자가 나타납니다. 이메일 OTP 전송 옆의 체크박스를 선택합니다. 그런 다음 저장을 선택합니다. 상태가 비활성화에서 활성화로 업데이트됩니다.

IAM Identity Center에서 ID를 관리할 때 암호 요구 사항

> **Note**
>
> 이러한 요구 사항은 Identity Center 디렉터리에 생성된 사용자에게만 적용됩니다. 인증을 위해 IAM Identity Center 이외의 ID 소스 (예: 외부 ID 공급자) 를 구성한 경우 사용자에 대한 암호 정책은 IAM Identity Center가 아닌 해당 시스템에서 정의되고 적용됩니다. Active Directory ID 소스가 다음과 AWS Managed Microsoft AD같은 경우 자세한 내용은 AWS Managed Microsoft AD비밀번호 정책 관리를 참조하십시오.

IAM Identity Center를 ID 소스로 사용하는 경우 사용자는 다음 암호 요구 사항을 준수하여 암호를 설정하거나 변경해야 합니다.

- 암호는 대/소문자를 구분합니다.
- 암호 길이는 8~64자여야 합니다.
- 암호는 각각의 다음 네 가지 범주의 문자를 최소 1자씩 포함해야 합니다.
  - 소문자(a~z)
  - 대문자(A-Z)
  - 숫자(0-9)
  - 영숫자 외의 특수 문자(~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- 최근 사용한 세 개의 암호는 다시 사용할 수 없습니다.

- 제3자로부터 유출된 데이터 세트를 통해 공개적으로 알려진 암호는 사용할 수 없습니다.

Microsoft AD 디렉터리에 연결

를 사용하여 AWS IAM Identity CenterActive Directory (AD) 의 자체 관리 디렉터리 또는 내부 디렉터리에 AWS Managed Microsoft AD 연결할 수 있습니다. AWS Directory Service이 Microsoft AD 디렉터리는 관리자가 IAM Identity Center 콘솔을 사용하여 싱글 사인 온 액세스를 할당할 때 가져올 수 있는 자격 증명 풀을 정의합니다. 기업 디렉터리를 IAM Identity Center에 연결한 후 AD 사용자 또는 그룹에 AWS 계정, 애플리케이션 또는 둘 다에 대한 액세스 권한을 부여할 수 있습니다.

AWS Directory Service 클라우드에서 호스팅되는 독립형 AWS Managed Microsoft AD 디렉터리를 설정하고 실행할 수 있도록 도와줍니다. AWS 를 사용하여 기존 자체 관리형 AD에 AWS 리소스를 AWS Directory Service 연결할 수도 있습니다. 자체 관리형 AD와 함께 AWS Directory Service 작동하도록 구성하려면 먼저 신뢰 관계를 설정하여 인증을 클라우드로 확장해야 합니다.

IAM Identity Center는 에서 제공하는 연결을 사용하여 AWS Directory Service 원본 AD 인스턴스에 대한 패스스루 인증을 수행합니다. 를 ID AWS Managed Microsoft AD 소스로 사용하는 경우 IAM Identity Center는 AD 트러스트를 통해 연결된 모든 도메인의 사용자 AWS Managed Microsoft AD 또는 도메인의 사용자와 작업할 수 있습니다. 4개 이상의 도메인에서 사용자를 찾으려는 경우 사용자는 IAM Identity Center에 로그인할 때 `DOMAIN\user` 구문을 사용자 이름으로 사용해야 합니다.

> **참고**
>
> - 필수 단계로, IN의 AD Connector 또는 디렉터리가 관리 AWS Managed Microsoft AD 계정 내에 AWS Directory Service 있는지 확인하십시오. AWS Organizations 자세한 설명은 IAM ID 센터에서 ID 소스를 확인하십시오. 섹션을 참조하세요.
> - IAM Identity Center는 SAMBA 4 기반 Simple AD를 연결된 디렉터리로 지원하지 않습니다.

Active Directory 사용 시 고려 사항

Active Directory를 ID 소스로 사용하려면 구성이 다음과 같은 사전 요구 사항을 충족해야 합니다.

- 를 사용하는 경우 AWS Managed Microsoft AD 디렉터리가 AWS Managed Microsoft AD설정된 AWS 리전 곳과 동일한 위치에서 IAM Identity Center를 활성화해야 합니다. IAM Identity Center는 디렉터리와 동일한 리전에 할당 데이터를 저장합니다. IAM Identity Center를 관리하려면 IAM Identity Center가 구성된 리전으로 전환해야 합니다. 또한 AWS 액세스 포털은 디렉터리와 동일한 액세스 URL을 사용한다는 점에 유의하세요.

- 관리 계정에 있는 Active Directory를 사용합니다.

  에 기존 AD Connector 또는 AWS Managed Microsoft AD 디렉터리가 설정되어 있어야 AWS Directory Service하며 AWS Organizations 관리 계정 내에 있어야 합니다. 한 번에 하나의 AD Connector 디렉터리 또는 하나의 디렉터리만 연결할 수 있습니다. AWS Managed Microsoft AD 여러 도메인이나 포리스트를 지원해야 하는 경우 AWS Managed Microsoft AD를 사용합니다. 자세한 내용은 다음을 참조하세요.

  - AWS Managed Microsoft AD 디렉터리를 IAM ID 센터에 연결
  - Active Directory의 자체 관리형 디렉터리를 IAM Identity Center에 연결
- 위임된 관리자 계정에 있는 Active Directory를 사용합니다.

  IAM Identity Center 위임 관리자를 활성화하고 Active Directory를 IAM ID 센터 ID 소스로 사용하려는 경우 위임된 관리자 계정에 있는 AWS Managed Microsoft AD 디렉터리에 설정된 기존 AD Connector 또는 AWS 디렉터리를 사용할 수 있습니다.

  IAM Identity Center ID 소스를 다른 소스에서 Active Directory로 변경하거나 Active Directory에서 다른 소스로 변경하려는 경우, 해당 디렉터리는 IAM Identity Center에서 위임한 관리자 계정(있는 경우)에 있어야 하며, 그렇지 않으면 관리 계정에 있어야 합니다.

Active Directory 연결 및 사용자 지정

이미 Active Directory를 사용 중인 경우 다음 주제가 디렉터리를 IAM Identity Center에 연결하는 데 도움이 될 것입니다.

AWS Managed Microsoft AD Active Directory의 디렉터리 또는 자체 관리형 디렉터리를 IAM ID 센터에 연결할 수 있습니다. Active AWS Managed Microsoft AD Directory의 디렉터리 또는 자체 관리 디렉터리를 연결하려는 경우 Active Directory 구성이 의 사전 요구 사항을 충족하는지 확인하십시오. IAM ID 센터에서 ID 소스를 확인하십시오.

> **Note**
>
> 최상의 보안을 위해 다중 인증을 사용하는 것을 권장합니다. Active AWS Managed Microsoft AD Directory의 디렉터리 또는 자체 관리형 디렉터리를 연결하려는 경우 RADIUS MFA를 AWS Directory Service함께 사용하지 않는 경우 IAM ID 센터에서 MFA를 활성화하십시오.

AWS Managed Microsoft AD

1. Microsoft AD 디렉터리에 연결에서 지침을 검토하세요.
2. AWS Managed Microsoft AD 디렉터리를 IAM ID 센터에 연결 단원의 단계를 따르세요.
3. 관리자 권한을 부여하려는 사용자가 IAM Identity Center와 동기화하도록 Active Directory를 구성합니다. 자세한 설명은 관리 사용자의 IAM Identity Center 동기화 섹션을 참조하세요.

Active Directory의 자체 관리형 디렉터리

1. Microsoft AD 디렉터리에 연결에서 지침을 검토하세요.
2. Active Directory의 자체 관리형 디렉터리를 IAM Identity Center에 연결 단원의 단계를 따르세요.
3. 관리자 권한을 부여하려는 사용자가 IAM Identity Center와 동기화하도록 Active Directory를 구성합니다. 자세한 설명은 관리 사용자의 IAM Identity Center 동기화 섹션을 참조하세요.

외부 ID 제공업체(IdP)

1. 외부 ID 제공업체에 연결에서 지침을 검토하세요.
2. 외부 ID 제공업체에 연결하는 방법 단원의 단계를 따르세요.
3. 사용자를 IAM Identity Center에 프로비저닝하도록 ID 제공업체를 구성합니다.

> **Note**
>
> IdP의 모든 직원 ID를 IAM Identity Center에 자동으로 그룹 기반으로 프로비저닝하도록 설정하기 전에 관리 권한을 부여하려는 한 명의 사용자를 IAM Identity Center와 동기화하는 것이 좋습니다.

관리 사용자의 IAM Identity Center 동기화

디렉터리를 IAM Identity Center에 연결한 후, 관리 권한을 부여할 사용자를 지정한 다음 디렉터리의 해당 사용자를 IAM Identity Center로 동기화할 수 있습니다.

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 동기화 관리를 선택합니다.
4. 동기화 관리 페이지에서 사용자 탭을 선택한 다음 사용자 및 그룹 추가를 선택합니다.
5. 사용자 탭의 사용자에 정확한 사용자 이름을 입력하고 추가를 선택합니다.

6. 추가된 사용자 및 그룹에서 다음 작업을 수행합니다.

   a. 관리 권한을 부여하려는 사용자가 지정되었는지 확인합니다.

   b. 사용자 이름 왼쪽의 확인란을 선택합니다.

   c. 제출을 선택합니다.

7. 동기화 관리 페이지에서 지정한 사용자가 동기화 범위의 사용자 목록에 나타납니다.

8. 탐색 창에서 사용자를 선택합니다.

9. 사용자 페이지에서 지정한 사용자가 목록에 나타나는 데 시간이 걸릴 수 있습니다. 새로 고침 아이콘을 선택하여 사용자 목록을 업데이트합니다.

이때 사용자는 관리 계정에 액세스할 수 없습니다. 관리 권한 세트를 만들고, 해당 권한 세트에 사용자를 할당하여 이 계정에 대한 관리 액세스 권한을 설정합니다. 자세한 설명은 권한 집합을 생성합니다. 섹션을 참조하세요.

Active Directory에서 사용자를 가져올 때 프로비저닝

IAM ID 센터는 에서 제공하는 연결을 사용하여 Active Directory의 AWS Directory Service 소스 디렉터리에 있는 사용자, 그룹 및 구성원 정보를 IAM ID 센터 ID 저장소로 동기화합니다. 사용자 인증은 Active Directory의 소스 디렉터리에서 직접 수행되므로 암호 정보는 IAM Identity Center에 동기화되지 않습니다. 이 ID 데이터는 애플리케이션에서 LDAP 작업을 Active Directory의 소스 디렉터리로 다시 전달하지 않고도 인앱 조회, 권한 부여 및 협업 시나리오를 용이하게 하는 데 사용됩니다.

프로비저닝에 대한 자세한 내용은 사용자 및 그룹 프로비저닝 단원을 참조하세요.

주제

- AWS Managed Microsoft AD 디렉터리를 IAM ID 센터에 연결
- Active Directory의 자체 관리형 디렉터리를 IAM Identity Center에 연결
- AWS Managed Microsoft AD 디렉터리의 속성 매핑
- Active Directory에서 사용자 및 그룹 프로비전

AWS Managed Microsoft AD 디렉터리를 IAM ID 센터에 연결

에서 관리하는 디렉터리를 IAM ID AWS Managed Microsoft AD 센터에 AWS Directory Service 연결하려면 다음 절차를 사용하십시오.

IAM ID AWS Managed Microsoft AD 센터에 연결하려면

1. IAM Identity Center 콘솔을 엽니다.

> **Note**
>
> 다음 단계로 넘어가기 전에 IAM Identity Center 콘솔이 AWS Managed Microsoft AD 디렉터리가 위치한 리전 중 하나를 사용하고 있는지 확인합니다.

2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택한 다음 작업 > ID 소스 변경을 선택합니다.
4. ID 소스 선택에서 Active Directory를 선택하고 다음을 선택합니다.
5. 활성 디렉터리 연결 아래의 목록에서 AWS Managed Microsoft AD 의 디렉터리를 선택한 후 다음을 선택합니다.
6. 변경 확인에서 정보를 검토하고 준비가 되면 ACCEPT를 입력한 다음 ID 소스 변경을 선택합니다.

> **Important**
>
> Active Directory의 사용자를 IAM Identity Center의 관리 사용자로 지정하려면 먼저 Active Directory에서 관리 권한을 부여하려는 사용자를 IAM Identity Center로 동기화해야 합니다. 이렇게 하려면 관리 사용자의 IAM Identity Center 동기화 단원의 절차를 따르세요.

Active Directory의 자체 관리형 디렉터리를 IAM Identity Center에 연결

Active Directory (AD) 의 자체 관리형 디렉터리에 있는 사용자는 액세스 포털의 애플리케이션 AWS 계정 및 애플리케이션에 대한 싱글 사인온 액세스를 가질 수도 있습니다. AWS 이러한 사용자에 대한 Single Sign-On 액세스를 구성하려면 다음 중 하나를 수행할 수 있습니다.

- 양방향 신뢰 관계 생성 — AD의 자체 관리형 디렉터리 간에 양방향 신뢰 관계가 생성되면 AD의 자체 관리형 디렉터리에 있는 사용자가 회사 자격 증명을 사용하여 다양한 서비스 AWS Managed Microsoft AD 및 비즈니스 애플리케이션에 로그인할 수 있습니다. AWS 단방향 신뢰는 IAM Identity Center에서 작동하지 않습니다.

  AWS IAM Identity Center 사용자 및 그룹 메타데이터를 동기화하기 위해 도메인에서 사용자 및 그룹 정보를 읽을 수 있는 권한을 가지려면 양방향 트러스트가 필요합니다. IAM Identity Center는 권한 집합 또는 애플리케이션에 액세스 권한을 할당할 때 이 메타데이터를 사용합니다. 사용자 및 그룹 메타데이터는 애플리케이션에서 다른 사용자 또는 그룹과 대시보드를 공유하는 경우와 같이 협업용으로

도 사용됩니다. Microsoft Active Directory가 사용자 도메인에 AWS Directory Service 대한 트러스트 양식을 통해 IAM ID 센터는 인증을 위해 해당 도메인을 신뢰할 수 있습니다. 반대 방향의 트러스트는 사용자 및 그룹 메타데이터를 읽을 수 있는 AWS 권한을 부여합니다.

양방향 신뢰를 설정하는 방법에 대한 자세한 내용은 AWS Directory Service 관리 가이드의 신뢰 관계를 생성해야 하는 경우를 참조하세요.

- AD 커넥터 생성 - AD Connector는 클라우드에 정보를 캐싱하지 않고도 디렉터리 요청을 자체 관리형 AD로 리디렉션할 수 있는 디렉터리 게이트웨이입니다. 자세한 정보는 AWS Directory Service 관리 가이드의 디렉터리에 연결을 참조하세요.

> **Note**
>
> IAM Identity Center를 AD Connector 디렉터리에 연결하는 경우 향후 사용자 암호 재설정은 AD 내에서 수행해야 합니다. 즉, 사용자는 AWS 액세스 포털에서 비밀번호를 재설정할 수 없습니다.
> AD 커넥터를 사용하여 Active Directory 도메인 서비스를 IAM Identity Center에 연결하는 경우 IAM Identity Center는 AD 커넥터가 연결된 단일 도메인의 사용자 및 그룹에만 액세스할 수 있습니다. 여러 도메인이나 포리스트를 지원해야 하는 경우 Microsoft Active Directory에는 AWS Directory Service 를 사용합니다.

> **Note**
>
> IAM Identity Center는 SAMBA4 기반 Simple AD 디렉터리에서는 작동하지 않습니다.

AWS Managed Microsoft AD 디렉터리의 속성 매핑

속성 매핑은 IAM Identity Center에 있는 속성 유형을 디렉터리의 유사한 속성과 매핑하는 데 사용됩니다. AWS Managed Microsoft AD IAM Identity Center는 Microsoft AD 디렉터리에서 사용자 속성을 검색하여 IAM Identity Center 사용자 속성에 매핑합니다. 이러한 IAM Identity Center 사용자 속성 매핑은 애플리케이션에 대한 SAML 2.0 어설션을 생성하는 데에도 사용됩니다. 각 애플리케이션은 성공적인 Single Sign-On에 필요한 SAML 2.0 속성 목록을 결정합니다.

IAM Identity Center는 애플리케이션 구성 페이지에 있는 속성 매핑 탭에서 속성 세트를 자동으로 채웁니다. IAM Identity Center는 이러한 사용자 속성을 사용하여 애플리케이션으로 전송되는 SAML 어설션(SAML 속성으로)을 채웁니다. 이러한 사용자 속성은 Microsoft AD 디렉터리에서 검색됩니다. 자세한 내용은 애플리케이션의 속성을 IAM Identity Center 속성에 매핑 단원을 참조하세요.

또한 IAM Identity Center는 디렉터리 구성 페이지의 속성 매핑 섹션에서 속성 세트를 관리합니다. 자세한 내용은 IAM Identity Center의 속성을 디렉터리의 속성에 매핑합니다. AWS Managed Microsoft AD 단원을 참조하세요.

지원되는 디렉터리 속성

다음 표에는 지원되는 AWS Managed Microsoft AD 디렉터리 속성 및 IAM Identity Center의 사용자 속성에 매핑할 수 있는 모든 디렉터리 속성이 나열되어 있습니다.

Microsoft AD 디렉터리에서 지원되는 속성
`${dir:email}`
`${dir:displayname}`
`${dir:distinguishedName}`
`${dir:firstname}`
`${dir:guid}`
`${dir:initials}`
`${dir:lastname}`
`${dir:proxyAddresses}`
`${dir:proxyAddresses:smtp}`
`${dir:proxyAddresses:SMTP}`
`${dir:windowsUpn}`

지원되는 Microsoft AD 디렉터리 속성의 조합을 IAM Identity Center의 단일 가변 속성에 매핑하도록 지정할 수 있습니다. 예를 들어, IAM Identity Center 열의 사용자 속성 아래에서 `subject` 속성을 선택할 수 있습니다. 그런 다음 `${dir:displayname}` 또는 `${dir:lastname}${dir:firstname }` 또는 지원되는 단일 속성이나 지원되는 속성의 임의 조합중 하나에 매핑합니다. IAM Identity Center의 사용자 속성에 대한 기본 매핑 목록은 기본 매핑 단원을 참조하세요.

> **Warning**
>
> 특정 IAM Identity Center 속성은 변경할 수 없고 기본적으로 특정 Microsoft AD 디렉터리 속성에 매핑되므로 수정할 수 없습니다.
> 예를 들어, “사용자 이름”은 IAM ID 센터의 필수 속성입니다. 값이 비어 있는 AD 디렉터리 속성에 “사용자 이름”을 매핑하면 IAM Identity Center는 해당 `windowsUpn` 값을 “사용자 이름”의 기본값으로 간주합니다. 현재 매핑에서 “사용자 이름”에 대한 속성 매핑을 변경하려면 변경하기 전에 “사용자 이름”에 종속된 IAM Identity Center 흐름이 예상대로 계속 작동하는지 확인하십시오.

ListUsers또는 ListGroupsAPI 작업 또는 list-users및 list-groups AWS CLI 명령을 사용하여 사용자 및 그룹에 애플리케이션에 대한 액세스 권한을 할당하는 AWS 계정 경우 의 값을 `AttributeValue` FQDN으로 지정해야 합니다. 이 값은 user@example.com 형식이어야 합니다. 다음 예에서 `AttributeValue`가 `janedoe@example.com`으로 설정됩니다.

```
aws identitystore list-users --identity-store-id d-12345a678b --filters
 AttributePath=UserName,AttributeValue=janedoe@example.com
```

지원되는 IAM Identity Center 속성

다음 표에는 지원되고 디렉터리의 사용자 속성에 매핑할 수 있는 모든 IAM Identity Center 속성이 나열되어 있습니다. AWS Managed Microsoft AD 애플리케이션 속성 매핑을 설정한 후 동일한 IAM Identity Center 속성을 사용하여 해당 애플리케이션에서 사용하는 실제 속성에 매핑할 수 있습니다.

IAM Identity Center에서 지원되는 속성
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`
`${user:middleName}`
`${user:name}`

IAM Identity Center에서 지원되는 속성
${user:preferredUsername}
${user:subject}

지원되는 외부 ID 제공업체 속성

다음 표에는 지원되고 IAM Identity Center에서 액세스 제어를 위한 속성을(를) 구성할 때 사용할 수 있는 속성에 매핑할 수 있는 모든 외부 ID 제공업체(idP) 속성이 나열되어 있습니다. SAML 어설션을 사용할 때는 IdP가 지원하는 모든 속성을 사용할 수 있습니다.

IdP에서 지원되는 속성
${path:userName}
${path:name.familyName}
${path:name.givenName}
${path:displayName}
${path:nickName}
${path:emails[primary eq true].value}
${path:addresses[type eq "work"].streetAddress}
${path:addresses[type eq "work"].locality}
${path:addresses[type eq "work"].region}
${path:addresses[type eq "work"].postalCode}
${path:addresses[type eq "work"].country}
${path:addresses[type eq "work"].formatted}
${path:phoneNumbers[type eq "work"].value}

IdP에서 지원되는 속성
`${path:userType}`
`${path:title}`
`${path:locale}`
`${path:timezone}`
`${path:enterprise.employeeNumber}`
`${path:enterprise.costCenter}`
`${path:enterprise.organization}`
`${path:enterprise.division}`
`${path:enterprise.department}`
`${path:enterprise.manager.value}`

기본 매핑

다음 표에는 IAM Identity Center의 사용자 속성과 디렉터리의 사용자 속성에 대한 기본 매핑이 나와 있습니다. AWS Managed Microsoft AD IAM Identity Center는 IAM Identity Center 열의 사용자 속성에 있는 속성 목록만 지원합니다.

> **Note**
>
> 구성 가능한 AD 동기화를 활성화할 때 IAM Identity Center의 사용자 및 그룹에 대한 할당이 없는 경우 다음 표의 기본 매핑이 사용됩니다. 이러한 매핑을 사용자 지정하는 방법은 동기화를 위한 속성 매핑을 구성합니다. 단원을 참조하세요.

IAM Identity Center의 사용자 속성	Microsoft AD 디렉터리의 이 속성에 매핑됩니다.
`AD_GUID`	`${dir:guid}`

IAM Identity Center의 사용자 속성	Microsoft AD 디렉터리의 이 속성에 매핑됩니다.
email *	${dir:windowsUpn}
familyName	${dir:lastname}
givenName	${dir:firstname}
middleName	${dir:initials}
name	${dir:displayname}
preferredUsername	${dir:displayname}
subject	${dir:windowsUpn}

* IAM Identity Center의 이메일 속성은 디렉터리 내에서 고유해야 합니다. 그렇지 않으면 JIT 로그인 프로세스가 실패할 수 있습니다.

요구 사항에 따라 기본 매핑을 변경하거나 SAML 2.0 어설션에 더 많은 속성을 추가할 수 있습니다. 예를 들어, 애플리케이션의 `User.Email` SAML 2.0 속성에 사용자 이메일이 필요하다고 가정해 보겠습니다. 또한 Microsoft AD 디렉터리의 `windowsUpn` 속성에 이메일 주소가 저장되어 있다고 가정해 보겠습니다. 이 매핑을 수행하려면 IAM Identity Center 콘솔의 다음 두 위치를 변경해야 합니다.

1. 디렉터리 페이지의 속성 매핑 섹션에서 사용자 속성 **`email`**을 **`${dir:windowsUpn}`** 속성에 매핑해야 합니다(디렉터리의 이 속성에 매핑 열).
2. 애플리케이션 페이지의 표에서 애플리케이션을 선택합니다. 속성 매핑 탭을 선택합니다. 그런 다음 `User.Email` 속성을 **`${user:email}`** 속성(IAM Identity Center의 이 문자열 값 또는 사용자 속성에 매핑 열)에 매핑합니다.

참고로 각 디렉터리 속성은 ${dir:**`AttributeName`**} 형식으로 제공해야 합니다. 예를 들어, Microsoft AD 디렉터리의 `firstname` 속성은 `${dir:firstname}`이(가) 됩니다. 모든 디렉터리 속성에는 실제 값이 할당되어 있어야 합니다. `${dir:` 뒤에 속성 값이 누락되면 사용자 로그인 문제가 발생할 수 있습니다.

IAM Identity Center의 속성을 디렉터리의 속성에 매핑합니다. AWS Managed Microsoft AD

다음 절차를 사용하여 IAM Identity Center의 사용자 속성을 Microsoft AD 디렉터리의 해당 속성에 매핑하는 방법을 지정할 수 있습니다.

IAM Identity Center의 속성을 디렉터리의 속성에 매핑하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 액세스 제어용 속성 탭을 선택한 다음 속성 관리를 선택합니다.
4. 액세스 제어용 속성 관리 페이지에서 매핑하려는 IAM Identity Center의 속성을 찾은 다음 텍스트 상자에 값을 입력합니다. 예를 들어 IAM Identity Center 사용자 속성 **email**을 Microsoft AD 디렉터리 **${dir:windowsUpn}** 속성에 매핑하는 게 좋을 수 있습니다.
5. 변경 사항 저장을 선택합니다.

Active Directory에서 사용자 및 그룹 프로비전

IAM Identity Center는 Active Directory에서 사용자와 그룹을 프로비전하는 다음 두 가지 방법을 제공합니다.

- IAM Identity Center 구성 가능 Active Director(AD) 동기화(권장) - 이 동기화 방법을 사용하면 다음 작업을 수행할 수 있습니다.
  - Microsoft Active Directory에서 IAM Identity Center에 자동으로 동기화되는 사용자 및 그룹을 명시적으로 정의하여 데이터 경계를 제어합니다. 언제든지 사용자 및 그룹을 추가하거나 사용자 및 그룹을 제거하여 동기화 범위를 변경할 수 있습니다.
  - 동기화된 사용자 및 그룹에 AWS 계정에 대한 Single Sign-On 액세스 권한 또는 애플리케이션에 대한 액세스 권한을 할당합니다. 애플리케이션은 관리형 애플리케이션 또는 고객 AWS 관리형 애플리케이션일 수 있습니다.
  - 필요에 따라 동기화를 일시 중지했다가 다시 시작하여 동기화 프로세스를 제어합니다. 이를 통해 프로덕션 시스템의 부하를 조절할 수 있습니다.
- IAM Identity Center AD 동기화 - 이 동기화 방법을 사용하면 IAM Identity Center를 사용하여 Active Directory의 사용자 및 그룹에 AWS 계정 및 애플리케이션에 대한 액세스 권한을 할당할 수 있습니다. 할당된 모든 ID는 IAM Identity Center에 자동으로 동기화됩니다.

IAM Identity Center 구성 가능 AD 동기화

IAM Identity Center 구성 가능한 Active Directory(AD) 동기화를 사용하면 Microsoft Active Directory에서 IAM Identity Center에 자동으로 동기화되는 자격 증명을 명시적으로 구성하고 동기화 프로세스를 제어할 수 있습니다.

다음 항목에서는 구성 가능한 AD 동기화를 구성하고 관리하는 데 필요한 정보를 제공합니다.

주제

- 필수 조건 및 고려 사항
- 구성 가능한 AD 동기화의 작동 방식
- 동기화 범위 구성 및 관리

필수 조건 및 고려 사항

구성 가능한 AD 동기화를 사용하기 전에 다음의 사전 조건 및 고려 사항에 주의하세요.

- Active Directory에서 동기화할 사용자 및 그룹 지정

  IAM Identity Center를 사용하여 AWS 관리형 애플리케이션 또는 고객 관리형 애플리케이션에 대한 액세스 권한을 새 사용자 AWS 계정 및 그룹에 할당하려면 먼저 Active Directory에서 동기화할 사용자 및 그룹을 지정한 다음 IAM Identity Center에 동기화해야 합니다.

  - AD 동기화 – IAM Identity Center 콘솔 또는 관련 할당 API 작업을 사용하여 새 사용자 및 그룹을 할당하면 IAM Identity Center는 도메인 컨트롤러에서 지정된 사용자 또는 그룹을 직접 검색하여 할당을 완료한 다음 사용자 또는 그룹 메타데이터를 IAM Identity Center에 정기적으로 동기화합니다.
  - 구성 가능한 AD 동기화 – IAM Identity Center는 도메인 컨트롤러에서 사용자와 그룹을 직접 검색하지 않습니다. 대신 먼저 동기화할 사용자 및 그룹 목록을 지정해야 합니다. IAM Identity Center에 이미 동기화된 사용자 및 그룹이 있는지 또는 구성 가능한 AD 동기화를 사용하여 처음으로 동기화하는 새 사용자 및 그룹이 있는지에 따라 다음 방법 중 하나로 이 목록(동기화 범위라고도 함)을 구성할 수 있습니다.
    - 기존 사용자 및 그룹: IAM Identity Center에 이미 동기화된 사용자 및 그룹이 있는 경우 구성 가능한 AD Sync의 동기화 범위는 해당 사용자 및 그룹 목록으로 미리 채워집니다. 새 사용자 또는 그룹을 할당하려면 동기화 범위에 구체적으로 추가해야 합니다. 자세한 내용은 동기화 범위에 사용자 및 그룹 추가 단원을 참조하세요.
    - 새 사용자 및 그룹: AWS 계정 및 애플리케이션에 대한 액세스 권한을 새 사용자 및 그룹에 할당하려면 먼저 구성 가능한 AD 동기화에서 동기화 범위에 추가할 사용자와 그룹을 지정해야 IAM Identity Center를 사용하여 할당할 수 있습니다. 자세한 내용은 동기화 범위에 사용자 및 그룹 추가 단원을 참조하세요.

- Active Directory의 중첩된 그룹에 할당하기

다른 그룹의 구성원인 그룹을 중첩 그룹 (또는 하위 그룹) 이라고 합니다. Active Directory에서 중첩된 그룹이 포함된 그룹에 할당하는 경우 할당이 적용되는 방식은 AD 동기화를 사용하는지 구성 가능한 AD 동기화를 사용하는지에 따라 달라집니다.

- AD 동기화 - Active Directory에서 중첩된 그룹이 포함된 그룹에 할당하는 경우 그룹의 직속 구성원만 계정에 액세스할 수 있습니다. 예를 들어 그룹 A에 액세스 권한을 할당하고 그룹 B가 그룹 A의 멤버인 경우 그룹 A의 직속 멤버만 계정에 액세스할 수 있습니다. 그룹 B의 구성원은 액세스 권한을 상속받지 않습니다.
- 구성 가능한 AD 동기화 - 구성 가능한 AD 동기화를 사용하여 Active Directory에서 중첩된 그룹이 포함된 그룹에 할당하면 응용 프로그램에 액세스하거나 응용 프로그램에 액세스할 수 있는 사용자의 범위가 늘어날 수 있습니다. AWS 계정 이 경우 할당은 중첩된 그룹에 있는 사용자를 포함한 모든 사용자에게 적용됩니다. 예를 들어 그룹 A에 액세스 권한을 할당하고 그룹 B가 그룹 A의 멤버인 경우 그룹 B의 멤버도 이 액세스 권한을 상속합니다.

- 자동화된 워크플로 업데이트

  IAM Identity Center ID 스토어 API 작업과 IAM Identity Center 할당 API 작업을 사용하여 새 사용자 및 그룹에 계정 및 애플리케이션에 대한 액세스 권한을 할당하고 IAM Identity Center와 동기화하는 자동화된 워크플로가 있는 경우, 구성 가능한 AD 동기화로 예상대로 작동하도록 2022년 4월 15일까지 해당 워크플로를 조정해야 합니다. 구성 가능한 AD Sync는 사용자 및 그룹 할당 및 프로비저닝이 발생하는 순서와 쿼리 수행 방식을 변경합니다.

  - AD 동기화 – 할당 프로세스가 먼저 발생합니다. 사용자 및 그룹에 응용 프로그램에 대한 액세스 권한을 AWS 계정 할당합니다. 사용자 및 그룹에 액세스 권한이 할당되면 자동으로 프로비저닝(IAM Identity Center에 동기화)됩니다. 자동화된 워크플로를 사용하는 경우 Active Directory에 새 사용자를 추가하면 자동화된 워크플로에서 ID 스토어 `ListUser` API 작업을 사용하여 Active Directory에서 사용자를 쿼리한 다음 IAM Identity Center 할당 API 작업을 사용하여 사용자 액세스 권한을 할당할 수 있습니다. 사용자에게 할당이 있으므로 해당 사용자는 자동으로 IAM Identity Center에 프로비저닝됩니다.
  - 구성 가능한 AD 동기화 – 프로비저닝이 먼저 수행되며 자동으로 수행되지는 않습니다. 대신 먼저 사용자 및 그룹을 동기화 범위에 추가하여 ID 스토어에 명시적으로 추가해야 합니다. 구성 가능한 AD 동기화의 동기화 구성을 자동화하기 위한 권장 단계에 대한 자세한 내용은 구성 가능한 AD 동기화를 위한 동기화 구성을 자동화합니다. 단원을 참조하세요.

구성 가능한 AD 동기화의 작동 방식

IAM Identity Center는 다음 프로세스를 사용하여 ID 스토어의 AD 기반 ID 데이터를 새로 고칩니다.

생성

Active Directory의 자체 관리형 디렉터리 또는 관리되는 AWS Managed Microsoft AD 디렉터리를 IAM ID 센터에 연결한 후, IAM ID 센터 ID 저장소에 동기화할 Active Directory 사용자 및 그룹을 명시적으로 구성할 수 있습니다. AWS Directory Service 선택한 ID는 약 3시간 정도마다 IAM Identity Center ID 스토어에 동기화됩니다. 디렉터리 크기에 따라 동기화 프로세스가 더 오래 걸릴 수 있습니다.

다른 그룹의 구성원인 그룹 (중첩 그룹 또는 하위 그룹이라고 함) 도 ID 저장소에 기록됩니다. 중첩된 그룹이 포함된 Active Directory의 그룹에 할당하는 경우 할당이 적용되는 방식은 AD 동기화를 사용하는지 구성 가능한 AD 동기화를 사용하는지에 따라 달라집니다. 자세한 설명은 Making assignments to nested groups in Active Directory 섹션을 참조하세요.

새 사용자 또는 그룹이 IAM Identity Center ID 스토어와 동기화된 후에만 액세스 권한을 할당할 수 있습니다.

업데이트

IAM Identity Center ID 스토어의 ID 데이터는 Active Directory의 소스 디렉터리에서 데이터를 정기적으로 읽어 최신 상태로 유지됩니다. IAM ID 센터는 기본적으로 동기화 주기에 따라 1시간마다 Active Directory의 데이터를 동기화합니다. Active Directory의 크기에 따라 데이터가 IAM ID 센터에 동기화되는 데 30분에서 2시간이 걸릴 수 있습니다.

동기화 범위에 있는 사용자 및 그룹 객체와 해당 구성원 자격은 IAM Identity Center에서 생성되거나 업데이트되어 Active Directory의 소스 디렉터리에 있는 해당 객체에 매핑됩니다. 사용자 속성의 경우 IAM Identity Center 콘솔의 액세스 제어 속성 섹션에 나열된 속성의 하위 집합만 IAM Identity Center에서 업데이트됩니다. Active Directory에서 수행한 모든 속성 업데이트가 IAM ID 센터에 반영되려면 동기화 주기가 한 번 걸릴 수 있습니다.

또한 IAM Identity Center ID 스토어와 동기화하는 사용자 및 그룹의 하위 집합을 업데이트할 수 있습니다. 새 사용자 또는 그룹을 이 하위 집합에 추가하거나 제거하도록 선택할 수 있습니다. 추가하는 모든 ID는 다음 예약 동기화 시 동기화됩니다. 하위 집합에서 제거한 ID는 IAM Identity Center ID 스토어에서 더 이상 업데이트되지 않습니다. 28일 이상 동기화되지 않은 사용자는 IAM Identity Center ID 스토어에서 비활성화됩니다. 해당 사용자 객체는 아직 동기화 범위에 속해 있는 다른 그룹에 속하지 않는 한 다음 동기화 주기 동안 IAM Identity Center ID 스토어에서 자동으로 비활성화됩니다.

삭제

Active Directory의 소스 디렉터리에서 해당 사용자 또는 그룹 객체가 삭제되면 IAM Identity Center ID 스토어에서 사용자와 그룹이 삭제됩니다. 또는 IAM Identity Center 콘솔을 사용하여 IAM Identity Center ID 스토어에서 사용자 객체를 명시적으로 삭제할 수 있습니다. IAM Identity Center 콘솔을 사용

하는 경우 동기화 범위에서도 사용자를 제거하여 다음 동기화 주기 동안 IAM Identity Center로 다시 동기화되지 않도록 해야 합니다.

언제든지 동기화를 일시 중지하고 다시 시작할 수도 있습니다. 28일 이상 동기화를 일시 중지하면 모든 사용자가 비활성화됩니다.

동기화 범위 구성 및 관리

다음 방법 중 하나를 사용하여 동기화 범위를 구성할 수 있습니다.

- 설정 안내: Active Directory의 사용자 및 그룹을 IAM Identity Center로 처음으로 동기화하는 경우 설정 안내의 단계에 따라 동기화 범위를 구성합니다. 설정 안내를 완료한 후에는 이 섹션의 다른 절차에 따라 언제든지 동기화 범위를 수정할 수 있습니다.
- 이미 IAM Identity Center와 동기화된 사용자 및 그룹이 있거나 설정 안내를을 따르지 않으려면 동기화 관리를 선택합니다. 설정 안내 절차를 건너뛰고 필요에 따라 이 섹션의 다른 절차에 따라 동기화 범위를 구성하고 관리합니다.

절차

- 설정 안내
- 동기화 범위에 사용자 및 그룹 추가
- 동기화 범위에서 사용자 및 그룹을 제거합니다.
- 동기화 일시 중지 및 다시 시작
- 동기화를 위한 속성 매핑을 구성합니다.
- 구성 가능한 AD 동기화를 위한 동기화 구성을 자동화합니다.

설정 안내

1. IAM Identity Center 콘솔을 엽니다.

   > **Note**
   >
   > 다음 단계로 넘어가기 전에 IAM Identity Center 콘솔이 AWS Managed Microsoft AD 디렉터리가 AWS 리전 있는 곳 중 하나를 사용하고 있는지 확인하십시오.

2. 설정을 선택합니다.
3. 페이지 상단의 알림 메시지에서 설정 안내 시작을 선택합니다.

4. 1단계 – 선택 사항: 속성 매핑 구성에서 기본 사용자 및 그룹 속성 매핑을 검토합니다. 변경이 필요하지 않은 경우 다음을 선택합니다. 변경이 필요한 경우 변경한 후 변경 내용 저장을 선택합니다.
5. 2단계 – 선택 사항: 동기화 범위 구성에서 사용자 탭을 선택합니다. 그런 다음 동기화 범위에 추가할 사용자의 사용자 이름을 정확히 입력하고 추가를 선택합니다. 다음으로 그룹 탭을 선택합니다. 동기화 범위에 추가하려는 그룹의 정확한 그룹 이름을 입력하고 추가를 선택합니다. 그리고 다음을 선택합니다. 나중에 동기화 범위에 사용자와 그룹을 추가하려면 변경하지 않고 다음을 선택합니다.
6. 3단계: 구성 검토 및 저장에서 1단계: 속성 매핑의 속성 매핑을 확인하고 2단계: 동기화 범위에서 사용자 및 그룹을 확인합니다. 구성 저장을 선택합니다. 그러면 동기화 관리 페이지로 이동합니다.

동기화 범위에 사용자 및 그룹 추가

사용자를 추가하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 동기화 관리를 선택합니다.
4. 동기화 관리 페이지에서 사용자 탭을 선택한 다음 사용자 및 그룹 추가를 선택합니다.
5. 사용자 탭의 사용자에서 정확한 사용자 이름을 입력하고 추가를 선택합니다.
6. 추가된 사용자 및 그룹에서 추가하려는 사용자를 검토합니다.
7. 제출을 선택합니다.
8. 탐색 창에서 사용자를 선택합니다.
9. 사용자 페이지에서 지정한 사용자가 목록에 나타나는 데 시간이 걸릴 수 있습니다. 새로 고침 아이콘을 선택하여 사용자 목록을 업데이트합니다.

그룹을 추가하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 동기화 관리를 선택합니다.
4. 동기화 관리 페이지에서 그룹 탭을 선택한 다음 사용자 및 그룹 추가를 선택합니다.
5. 그룹 탭을 선택합니다. 그룹에서 정확한 그룹 이름을 입력하고 추가를 선택합니다.
6. 추가된 사용자 및 그룹에서 추가하려는 그룹을 검토합니다.

7. 제출을 선택합니다.
8. 탐색 창에서 그룹을 선택합니다.
9. 그룹 페이지에서 지정한 그룹이 목록에 나타나는 데 시간이 다소 걸릴 수 있습니다. 새로 고침 아이콘을 선택하여 그룹 목록을 업데이트합니다.

동기화 범위에서 사용자 및 그룹을 제거합니다.

동기화 범위에서 사용자 및 그룹을 제거하면 어떤 일이 발생하는지에 대한 자세한 내용은 구성 가능한 AD 동기화의 작동 방식 단원을 참조하세요.

사용자를 제거하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 동기화 관리를 선택합니다.
4. 사용자 탭을 선택합니다.
5. 동기화 범위의 사용자 아래에서 삭제할 사용자 옆의 확인란을 선택합니다. 모든 사용자를 삭제하려면 사용자 이름 옆의 확인란을 선택합니다.
6. 제거를 선택합니다.

그룹을 제거하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 동기화 관리를 선택합니다.
4. 그룹 탭을 선택합니다.
5. 동기화 범위 내 그룹에서 삭제할 사용자 옆의 확인란을 선택합니다. 그룹을 모두 삭제하려면 그룹 이름 옆의 확인란을 선택합니다.
6. 제거를 선택합니다.

동기화 일시 중지 및 다시 시작

동기화를 일시 중지하면 향후의 모든 동기화 주기가 일시 중지되며 Active Directory의 사용자 및 그룹에 대한 변경 사항이 IAM Identity Center에 반영되지 않습니다. 동기화를 재개하면 동기화 주기에 따라 다음 예약된 동기화에서 이러한 변경 사항이 적용됩니다.

동기화를 일시 중지하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 동기화 관리를 선택합니다.
4. 동기화 관리에서 동기화 일시 중지를 선택합니다.

동기화를 재개하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 동기화 관리를 선택합니다.
4. 동기화 관리에서 동기화 재개를 선택합니다.

> **Note**
>
> 동기화 재개 대신 동기화 일시 중지가 표시되면 Active Directory에서 IAM Identity Center로의 동기화가 이미 재개된 것입니다.

동기화를 위한 속성 매핑을 구성합니다.

사용 가능한 속성에 대한 자세한 내용은 AWS Managed Microsoft AD 디렉터리의 속성 매핑 단원을 참조하세요.

IAM Identity Center의 속성을 디렉터리에 매핑하도록 구성하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 동기화 관리를 선택합니다.
4. 동기화 관리에서 속성 매핑 보기를 선택합니다.
5. Active Directory 사용자 속성에서 IAM Identity Center ID 스토어 속성과 Active Directory 사용자 속성을 구성합니다. 예를 들어 IAM Identity Center ID 스토어 속성 `email`을 Active Directory 사용자 디렉터리 속성 `${objectguid}`에 매핑하는 게 좋을 수 있습니다.

> **Note**
>
> 그룹 속성에서 IAM Identity Center ID 스토어 속성과 Active Directory 그룹 속성을 변경할 수 없습니다.

6. 변경 사항 저장를 선택합니다. 그러면 동기화 관리 페이지로 돌아갑니다.

구성 가능한 AD 동기화를 위한 동기화 구성을 자동화합니다.

구성 가능한 AD 동기화를 사용하여 자동화된 워크플로가 예상대로 작동하도록 하려면 다음 단계를 수행하여 동기화 구성을 자동화하는 것이 좋습니다.

구성 가능한 AD 동기화의 동기화 구성을 자동화하려면

1. Active Directory에서 IAM Identity Center에 동기화하려는 모든 사용자 및 그룹을 포함하는 상위 동기화 그룹을 생성합니다. 예를 들어 그룹 이름을 IdentityCenterAllUsersAndGroupsIAM으로 지정할 수 있습니다.
2. IAM Identity Center에서 상위 동기화 그룹을 구성 가능한 동기화 목록에 추가합니다. IAM Identity Center는 상위 동기화 그룹 내에 포함된 모든 사용자, 그룹, 하위 그룹 및 모든 그룹의 구성원을 동기화합니다.
3. Microsoft에서 제공하는 Active Directory 사용자 및 그룹 관리 API 작업을 사용하여 상위 동기화 그룹에서 사용자 및 그룹을 추가하거나 제거할 수 있습니다.

IAM Identity Center 광고 동기화

IAM ID 센터 AD 동기화를 사용하면 IAM ID 센터를 사용하여 Active Directory의 사용자 및 그룹에 AWS 관리형 애플리케이션 또는 고객 관리 애플리케이션에 대한 액세스 권한을 할당할 수 있습니다. AWS 계정 할당된 모든 ID는 IAM Identity Center에 자동으로 동기화됩니다.

IAM Identity Center AD 동기화 작동 방식

IAM Identity Center는 다음 프로세스를 사용하여 ID 스토어의 AD 기반 ID 데이터를 새로 고칩니다.

생성

AWS 콘솔 또는 할당 API 호출을 사용하여 사용자 AWS 계정 또는 그룹을 애플리케이션에 할당하면 사용자, 그룹 및 멤버십에 대한 정보가 IAM Identity Center ID 저장소에 정기적으로 동기화됩니다. IAM

Identity Center 할당에 추가된 사용자 또는 그룹은 일반적으로 2시간 이내에 AWS ID 저장소에 표시됩니다. 동기화되는 데이터의 양에 따라 이 프로세스는 더 오래 걸릴 수 있습니다. 액세스 권한이 직접 할당되거나 액세스 권한이 할당된 그룹의 구성원인 사용자 및 그룹만 동기화됩니다.

다른 그룹의 구성원인 그룹(중첩 그룹이라고 함)도 ID 스토어에 기록됩니다. 중첩된 그룹이 포함된 Active Directory의 그룹에 할당하는 경우 할당이 적용되는 방식은 AD 동기화를 사용하는지 구성 가능한 AD 동기화를 사용하는지에 따라 달라집니다.

- AD 동기화 - Active Directory에서 중첩된 그룹이 포함된 그룹에 할당하는 경우 그룹의 직속 구성원만 계정에 액세스할 수 있습니다. 예를 들어 그룹 A에 액세스 권한을 할당하고 그룹 B가 그룹 A의 멤버인 경우 그룹 A의 직속 멤버만 계정에 액세스할 수 있습니다. 그룹 B의 구성원은 액세스 권한을 상속받지 않습니다.
- 구성 가능한 AD 동기화 - 구성 가능한 AD 동기화를 사용하여 Active Directory에서 중첩된 그룹이 포함된 그룹에 할당하면 응용 프로그램에 액세스하거나 응용 프로그램에 액세스할 수 있는 사용자의 범위가 늘어날 수 있습니다. AWS 계정 이 경우 할당은 중첩된 그룹에 있는 사용자를 포함한 모든 사용자에게 적용됩니다. 예를 들어 그룹 A에 액세스 권한을 할당하고 그룹 B가 그룹 A의 멤버인 경우 그룹 B의 멤버도 이 액세스 권한을 상속합니다.

사용자 객체가 처음으로 동기화되기 전에 사용자가 IAM Identity Center에 액세스하는 경우 해당 사용자의 ID 저장소 객체는 JIT just-in-time () 프로비저닝을 사용하여 온디맨드 방식으로 생성됩니다. JIT 프로비저닝으로 생성된 사용자는 직접 할당되거나 그룹 기반 IAM Identity Center 사용 권한이 없는 한 동기화되지 않습니다. JIT로 프로비전한 사용자의 그룹 멤버십은 동기화가 완료될 때까지 사용할 수 없습니다.

사용자에게 액세스 권한을 할당하는 방법에 대한 지침은 을 참조하십시오. AWS 계정싱글 사인온 액세스: AWS 계정

업데이트

IAM Identity Center ID 스토어의 ID 데이터는 Active Directory의 소스 디렉터리에서 데이터를 정기적으로 읽어 최신 상태로 유지됩니다. Active Directory에서 변경된 ID 데이터는 일반적으로 4시간 이내에 AWS ID 저장소에 표시됩니다. 동기화되는 데이터의 양에 따라 이 프로세스는 더 오래 걸릴 수 있습니다.

사용자 및 그룹 객체와 해당 구성원은 IAM Identity Center에서 생성되거나 업데이트되어 Active Directory의 소스 디렉터리에 있는 해당 객체에 매핑됩니다. 사용자 속성의 경우 IAM Identity Center 콘솔의 액세스 제어 속성 관리 섹션에 나열된 속성의 하위 집합만 IAM Identity Center 콘솔에서 업데이트됩니다. 또한 사용자 속성은 각 사용자 인증 이벤트와 함께 업데이트됩니다.

삭제

Active Directory의 소스 디렉터리에서 해당 사용자 또는 그룹 객체가 삭제되면 IAM Identity Center ID 스토어에서 사용자와 그룹이 삭제됩니다.

외부 ID 제공업체에 연결

Active Directory 또는 에서 자체 관리되는 디렉터리를 사용하는 AWS Managed Microsoft AD경우 을 참조하십시오Microsoft AD 디렉터리에 연결. 다른 외부 ID 공급자 (IdPs) 의 경우 SAML (보안 어설션 마크업 언어) 2.0 표준을 IdPs 통해 ID를 인증하는 AWS IAM Identity Center 데 사용할 수 있습니다. 이렇게 하면 사용자가 회사 자격 증명으로 AWS 액세스 포털에 로그인할 수 있습니다. 그러면 외부에서 호스팅되는 할당된 계정, 역할 및 애플리케이션으로 이동할 수 IdPs 있습니다.

예를 들어 Okta 또는 Microsoft Entra ID와 같은 외부 IdP를 IAM Identity Center에 연결할 수 있습니다. 그러면 사용자는 기존 Okta 또는 Microsoft Entra ID 자격 증명으로 AWS 액세스 포털에 로그인할 수 있습니다. 사용자가 로그인한 후 수행할 수 있는 작업을 제어하려면 AWS 조직의 모든 계정과 애플리케이션에서 사용자에게 중앙에서 액세스 권한을 할당할 수 있습니다. 또한 개발자는 기존 자격 증명을 사용하여 AWS Command Line Interface (AWS CLI) 에 간단히 로그인할 수 있으며, 자동 단기 자격 증명 생성 및 교체 기능을 활용할 수 있습니다.

SAML 프로토콜은 사용자 및 그룹에 대해 알아보기 위해 IdP에 문의하는 방법을 제공하지 않습니다. 따라서 IAM Identity Center에 해당 사용자와 그룹을 프로비저닝하여 IAM Identity Center에서 해당 사용자와 그룹을 인식하도록 해야 합니다.

사용자가 외부 IdP일 경우 프로비저닝

외부 IdP를 사용하는 경우 애플리케이션에 할당하려면 먼저 해당하는 모든 사용자 및 그룹을 IAM Identity Center에 프로비저닝해야 합니다. AWS 계정 이를 위해 사용자 및 그룹에 대해 자동 프로비저닝 구성을 수행하거나 수동 프로비저닝을 사용할 수 있습니다. 사용자를 프로비저닝하는 방법에 관계없이 IAM Identity Center는 명령줄 인터페이스 및 애플리케이션 인증을 외부 IdP로 리디렉션합니다. AWS Management Console그러면 IAM Identity Center에서 생성한 정책을 기반으로 IAM Identity Center에서 해당 리소스에 대한 액세스 권한을 부여합니다. 프로비저닝에 대한 자세한 내용은 사용자 및 그룹 프로비저닝 단원을 참조하세요.

외부 ID 제공업체에 연결하는 방법

지원되는 사용자를 위한 step-by-step 자습서는 다음과 같습니다. IdPs

- CyberArk

- Google Workspace
- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Ping Identity

지원되는 외부마다 서로 다른 사전 요구 사항, 고려 사항 및 프로비전 절차가 있습니다. IdPs 다음 절차는 모든 외부 ID 제공업체에서 사용되는 절차에 대한 일반적인 개요를 제공합니다.

외부 ID 제공업체에 연결하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택한 다음 작업 > ID 소스 변경을 선택합니다.
4. ID 소스 선택에서 외부 ID 제공업체를 선택하고 다음을 선택합니다.
5. 외부 ID 제공업체 구성 에서 다음을 수행합니다.

   a. 서비스 제공업체 메타데이터에서 메타데이터 파일 다운로드를 선택하여 메타데이터 파일을 다운로드하고 시스템에 저장합니다. IAM Identity Center SAML 메타데이터 파일은 외부 ID 제공업체에 필요합니다.

   b. ID 제공업체 메타데이터에서 파일 선택에서 외부 ID 제공업체로부터 다운로드한 메타데이터 파일을 찾습니다. 그런 다음 파일을 업로드합니다. 이 메타데이터 파일에는 IdP에서 보낸 메시지를 신뢰하는 데 사용되는 필수 공개 x509 인증서가 들어 있습니다.

   c. 다음을 선택합니다.

> **Important**
>
> 소스를 Active Directory로 또는 Active Directory에서 변경하면 기존의 모든 사용자 및 그룹 할당이 제거됩니다. 소스를 성공적으로 변경한 후에는 할당을 수동으로 다시 적용해야 합니다.

6. 고지 사항을 읽고 진행할 준비가 되면 ACCEPT를 입력합니다.
7. ID 소스 변경을 선택합니다. ID 소스를 성공적으로 변경했음을 알리는 상태 메시지가 표시됩니다.

주제

- 외부 ID 공급자와의 SAML 및 SCIM ID 페더레이션 사용
- SCIM 프로필 및 SAML 2.0 구현

외부 ID 공급자와의 SAML 및 SCIM ID 페더레이션 사용

IAM Identity Center는 ID 페더레이션을 위해 다음과 같은 표준 기반 프로토콜을 구현합니다.

- 사용자 인증을 위한 SAML 2.0
- 프로비저닝을 위한 SCIM

이러한 표준 프로토콜을 구현하는 모든 ID 제공업체(idP)는 다음과 같은 특수 고려 사항을 고려하여 IAM Identity Center와 성공적으로 상호 운용되어야 합니다.

- SAML
  - IAM Identity Center에는 `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`와 같은 SAML NameID 형식의 이메일 주소가 필요합니다.
  - 어설션의 NameID 필드 값은 RFC 2822(https://tools.ietf.org/html/rfc2822) 추가 사양 준수(“`name@domain.com`”) 문자열(https://tools.ietf.org/html/rfc2822#section-3.4.1)이어야 합니다.
  - 메타데이터 파일은 75,000자를 초과할 수 없습니다.
  - 메타데이터에는 EntityID, X509 인증서 및 SingleSignOnService 로그인 URL의 일부가 포함되어야 합니다.
  - 암호화 키는 지원되지 않습니다.

- SCIM
  - IAM 아이덴티티 센터 SCIM 구현은 SCIM RFC 7642 (https://tools.ietf.org/html/rfc7642), 7643 (https://tools.ietf.org/html/rfc7643) 및 7644 (https://tools.ietf.org/html/rfc7644) 와 2020년 3월 기본 SCIM 프로필 1.0 초안 (https://tools.ietf.org/html/rfc7644) 에 명시된 상호 운용성 요구 사항을 기반으로 합니다. FastFed https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4 현재 구현에 있어 이러한 문서와 IAM Identity Center 간의 차이점은 IAM Identity Center SCIM 구현 개발자 가이드의 지원되는 API 운영 섹션에 설명되어 있습니다.

IdPs 위에서 언급한 표준 및 고려 사항을 준수하지 않는 것은 지원되지 않습니다. 해당 제품의 이러한 표준 및 고려 사항 준수와 관련된 질문이나 설명이 필요하면 IdP에 문의하세요.

IdP를 IAM Identity Center에 연결하는 데 문제가 있는 경우 다음을 확인하는 것이 좋습니다.

- AWS CloudTrail 이벤트 이름 ExternalId P를 기준으로 필터링하여 로깅합니다. DirectoryLogin
- IdP 관련 로그 및/또는 디버그 로그
- IAM Identity Center 문제 해결

> **Note**
>
> 에 있는 것과 같은 일부는 IdPs IAM Identity Center용으로 특별히 구축된 “애플리케이션” 또는 “커넥터”의 형태로 IAM Identity Center에 대한 간소화된 구성 환경을 제공합니다. 시작하기 튜토리얼 IdP가 이 옵션을 제공하는 경우 IAM Identity Center용으로 특별히 구축된 항목을 신중하게 선택하면서 이 옵션을 사용하는 것이 좋습니다. “AWS”, “AWS 페더레이션” 또는 유사한 일반AWS""이라는 다른 항목은 다른 페더레이션 접근 방식 및/또는 엔드포인트를 사용할 수 있으며, IAM Identity Center에서는 예상대로 작동하지 않을 수 있습니다.

SCIM 프로필 및 SAML 2.0 구현

SCIM과 SAML은 모두 IAM Identity Center를 구성할 때 중요한 고려 사항입니다.

SAML 2.0 구현

IAM Identity Center는 Security Assertion Markup Language(SAML) 2.0을 사용하여 ID 페더레이션을 지원합니다. 이를 통해 IAM Identity Center는 외부 ID 제공자의 ID를 인증할 수 있습니다 (). IdPs SAML 2.0은 SAML 어설션을 안전하게 교환하는 데 사용되는 개방형 표준입니다. SAML 2.0은 SAML 기관(ID 제공업체 또는 IdP라고 함)과 SAML 소비자(서비스 제공업체 또는 SP라고 함) 간에 사용자에 대한 정보를 전달합니다. IAM Identity Center 서비스는 이 정보를 사용하여 페더레이션된 Single Sign-on을 제공합니다. Single Sign-On을 통해 사용자는 기존 ID 제공자 자격 증명을 기반으로 애플리케이션에 AWS 계정 액세스하고 구성할 수 있습니다.

IAM ID 센터는 IAM ID 센터 스토어 또는 외부 ID 공급자에 SAML IdP 기능을 추가합니다. AWS Managed Microsoft AD그러면 사용자는 SAML을 지원하는 서비스 (예:,,) AWS Management Console와 같은 타사 애플리케이션을 포함하여 SAML을 지원하는 서비스에 싱글 사인온할 수 있습니다. Microsoft 365 Concur Salesforce

그러나 SAML 프로토콜은 사용자 및 그룹에 대해 알아보기 위해 IdP에 문의하는 방법을 제공하지 않습니다. 따라서 IAM Identity Center에 해당 사용자와 그룹을 프로비저닝하여 IAM Identity Center에서 해당 사용자와 그룹을 인식하도록 해야 합니다.

SCIM 프로필

IAM Identity Center는 도메인 간 ID 관리 시스템(SCIM) v2.0 표준을 지원합니다. SCIM은 IAM Identity Center ID를 IdP의 자격 증명과 동기화합니다. 여기에는 IdP와 IAM Identity Center 간의 모든 사용자 프로비저닝, 업데이트 및 디프로비저닝이 포함됩니다.

SCIM 구현하는 방법에 대한 자세한 내용은 자동 프로비저닝 단원을 참조하세요. IAM Identity Center의 SCIM 구현에 대한 자세한 내용은 IAM Identity Center SCIM 구현 개발자 가이드를 참조하세요.

주제

- 자동 프로비저닝
- 수동 프로비저닝
- SAML 2.0 인증서 관리

자동 프로비저닝

IAM Identity Center는 도메인 간 ID 관리 시스템(SCIM) v2.0 프로토콜을 사용하여 ID 제공업체(idP)의 사용자 및 그룹 정보를 IAM Identity Center로 자동 프로비저닝(동기화)할 수 있도록 지원합니다. SCIM 동기화를 구성할 때 ID 제공업체(idP) 사용자 속성을 IAM Identity Center의 명명된 속성에 매핑합니다. 이로 인해 IAM Identity Center와 IdP 간에 예상 속성이 일치하게 됩니다. IAM Identity Center의 SCIM 엔드포인트와 IAM Identity Center에서 생성한 베어러 토큰을 사용하여 IdP에서 이 연결을 구성합니다.

주제

- 자동 프로비저닝을 사용할 때 고려 사항
- 액세스 토큰 만료를 모니터링하는 방법
- 자동 프로비저닝을 활성화하는 방법
- 자동 프로비저닝을 비활성화하는 방법
- 새 액세스 토큰을 생성하는 방법
- 액세스 토큰 삭제 방법
- 액세스 토큰 교체 방법

자동 프로비저닝을 사용할 때 고려 사항

SCIM 배포를 시작하기 전에 먼저 IAM Identity Center와의 작동 방식에 대한 다음과 같은 중요한 고려 사항을 검토하는 것이 좋습니다. 추가 프로비저닝 고려 사항은 해당 IdP에 시작하기 튜토리얼 해당하는 사항을 참조하십시오.

- 기본 이메일 주소를 프로비저닝하는 경우 이 속성 값은 각 사용자마다 고유해야 합니다. 일부의 IdPs 경우 기본 이메일 주소가 실제 이메일 주소가 아닐 수도 있습니다. 예를 들어 이메일처럼 보이는 범용 사용자 이름(UPN)일 수 있습니다. 여기에는 사용자의 실제 이메일 주소가 포함된 보조 또는 "기타" 이메일 주소가 IdPs 있을 수 있습니다. IdP에서 NULL이 아닌 고유 이메일 주소를 IAM Identity Center 기본 이메일 주소 속성에 매핑하도록 SCIM을 구성해야 합니다. 그리고 NULL이 아닌 사용자의 고유 로그인 속성을 IAM Identity Center 사용자 이름 속성에 매핑해야 합니다. IdP에 로그인 속성과 사용자 이메일 이름을 모두 포함하는 단일 값이 있는지 확인합니다. 그렇다면 해당 IdP 필드를 IAM Identity Center 기본 이메일과 IAM Identity Center 사용자 이름 모두에 매핑할 수 있습니다.
- SCIM 동기화가 작동하려면 모든 사용자에게 이름, 성, 사용자 이름 및 디스플레이 이름 값을 지정해야 합니다. 사용자에게 이러한 값이 하나라도 없으면 해당 사용자는 프로비저닝되지 않습니다.
- 타사 애플리케이션을 사용해야 하는 경우 먼저 아웃바운드 SAML 주체 속성을 사용자 이름 속성에 매핑해야 합니다. 타사 애플리케이션에 라우팅 가능한 이메일 주소가 필요한 경우 IdP에 이메일 속성을 제공해야 합니다.
- SCIM 프로비저닝 및 업데이트 주기는 ID 제공업체가 제어합니다. ID 제공업체의 사용자 및 그룹에 대한 변경 사항은 ID 제공업체가 해당 변경 사항을 IAM Identity Center로 전송한 후에만 IAM Identity Center에 반영됩니다. 사용자 및 그룹 업데이트 빈도에 대한 자세한 내용은 ID 제공업체에 문의하세요.
- 현재 SCIM에는 다중 값 속성(예: 특정 사용자에 대한 여러 이메일 또는 전화번호)이 프로비저닝되지 않습니다. SCIM을 사용하여 다중 값 속성을 IAM Identity Center에 동기화할 수 없습니다. 동기화에 실패하지 않으려면 각 속성에 대해 단일 값만 전달해야 합니다. 다중 값 속성을 가진 사용자가 있는 경우 IAM Identity Center에 연결하기 위해 IdP에서 SCIM의 중복 속성 매핑을 제거하거나 수정합니다.
- IdP의 `externalId` SCIM 매핑이 고유하고 항상 존재하며 사용자에 대해 변경될 가능성이 가장 적은 값에 해당하는지 확인합니다. 예를 들어, IdP는 이름 및 이메일과 같은 사용자 속성의 변경에 영향을 받지 않는 보장된 `objectId` 또는 기타 식별자를 제공할 수 있습니다. 그렇다면 해당 값을 SCIM `externalId` 필드에 매핑할 수 있습니다. 이렇게 하면 이름이나 이메일을 변경해야 하는 경우에도 사용자가 AWS 자격, 할당 또는 권한을 잃지 않을 수 있습니다.
- 아직 애플리케이션에 할당되지 않았거나 IAM Identity Center에 AWS 계정 프로비저닝할 수 없는 사용자 사용자와 그룹을 동기화하려면 IAM Identity Center에 대한 IdP의 연결을 나타내는 애플리케이션 또는 기타 설정에 해당 사용자와 그룹을 할당해야 합니다.
- 사용자 프로비저닝 해제 동작은 ID 공급자가 관리하며 구현에 따라 달라질 수 있습니다. 사용자 프로비저닝에 대한 자세한 내용은 ID 공급자에게 문의하십시오.

IAM Identity Center의 SCIM 구현에 대한 자세한 내용은 IAM Identity Center SCIM 구현 개발자 가이드를 참조하세요.

액세스 토큰 만료를 모니터링하는 방법

SCIM 액세스 토큰의 유효 기간은 1년으로 생성됩니다. SCIM 액세스 토큰이 90일 이내에 만료되도록 설정되면 IAM Identity Center 콘솔과 AWS Health 대시보드를 통해 알림을 AWS 보내 토큰 교체에 도움을 줍니다. SCIM 액세스 토큰이 만료되기 전에 이를 교체하면 사용자 및 그룹 정보의 자동 프로비저닝을 지속적으로 보호할 수 있습니다. SCIM 액세스 토큰이 만료되면 ID 제공업체의 사용자 및 그룹 정보를 IAM Identity Center로 동기화하는 작업이 중지되므로 더 이상 자동 프로비저닝을 통해 정보를 업데이트하거나 생성 및 삭제할 수 없습니다. 자동 프로비저닝이 중단되면 보안 위험이 증가하고 서비스 액세스에 영향을 미칠 수 있습니다.

Identity Center 콘솔은 SCIM 액세스 토큰을 교체하고 사용하지 않거나 만료된 액세스 토큰을 삭제할 때까지 지속적으로 알림을 보냅니다. AWS Health 대시보드 이벤트는 90일에서 60일 사이에 매주, 60일에서 30일까지 주 2회, 30일에서 15일까지 주 3회, SCIM 액세스 토큰이 만료될 때까지 15일에서 매일 갱신됩니다.

자동 프로비저닝을 활성화하는 방법

다음 절차를 따라 SCIM 프로토콜을 사용하여 IdP에서 IAM Identity Center로 사용자 및 그룹을 자동으로 프로비저닝할 수 있습니다.

> **Note**
>
> 이 절차를 시작하기 전에 먼저 IdP에 적용되는 프로비저닝 고려 사항을 검토하는 것이 좋습니다. 자세한 내용은 시작하기 튜토리얼 IdP용 을 참조하십시오.

IAM Identity Center에서 자동 프로비저닝을 활성화하려면

1. 사전 필수 조건을 완료한 후 IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 자동 프로비저닝 정보 상자를 찾은 다음 활성화를 선택합니다. 그러면 IAM Identity Center에서 자동 프로비저닝이 즉시 활성화되고 필요한 SCIM 엔드포인트 및 액세스 토큰 정보가 표시됩니다.
4. 인바운드 자동 프로비저닝 대화 상자에서 다음 옵션의 각 값을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.

   a. SCIM 엔드포인트

   b. 액세스 토큰

5. 닫기를 선택하세요.

이 절차를 완료한 후에는 IdP에서 자동 프로비저닝을 구성해야 합니다. 자세한 내용은 시작하기 튜토리얼 IdP용 을 참조하십시오.

자동 프로비저닝을 비활성화하는 방법

다음 절차에 따라 IAM Identity Center 콘솔에서 자동 프로비저닝을 비활성화합니다.

> **Important**
>
> 이 절차를 시작하기 전에 액세스 토큰을 삭제해야 합니다. 자세한 내용은 액세스 토큰 삭제 방법 단원을 참조하세요.

IAM Identity Center 콘솔에서 자동 프로비저닝을 비활성화하려면

1. IAM Identity Center 콘솔의 왼쪽 탐색 창에서 설정을 선택합니다.
2. 설정 페이지에서 ID 소스 탭을 선택한 다음 작업 > 프로비저닝 관리를 선택합니다.
3. 자동 프로비저닝 페이지에서 비활성화를 선택합니다.
4. 자동 프로비저닝 비활성화 대화 상자에서 정보를 검토하고 비활성화을 입력한 다음 자동 프로비저닝 비활성화를 선택합니다.

새 액세스 토큰을 생성하는 방법

다음 절차를 사용하여 IAM Identity Center 콘솔에서 새 액세스 토큰을 생성합니다.

> **Note**
>
> 이 절차를 수행하려면 이전에 자동 프로비저닝을 활성화한 적이 있어야 합니다. 자세한 내용은 자동 프로비저닝을 활성화하는 방법 단원을 참조하세요.

새 액세스 토큰을 생성하려면

1. IAM Identity Center 콘솔의 왼쪽 탐색 창에서 설정을 선택합니다.
2. 설정 페이지에서 ID 소스 탭을 선택한 다음 작업 > 프로비저닝 관리를 선택합니다.
3. 자동 프로비저닝 페이지의 액세스 토큰에서 토큰 생성을 선택합니다.

4. 새 액세스 토큰 생성 대화 상자에서 새 액세스 토큰을 복사하여 안전한 장소에 저장합니다.
5. 닫기를 선택하세요.

액세스 토큰 삭제 방법

다음 절차를 사용하여 IAM Identity Center 콘솔에서 기존 액세스 토큰을 삭제합니다.

기존 액세스 토큰을 삭제하려면

1. IAM Identity Center 콘솔의 왼쪽 탐색 창에서 설정을 선택합니다.
2. 설정 페이지에서 ID 소스 탭을 선택한 다음 작업 > 프로비저닝 관리를 선택합니다.
3. 자동 프로비저닝 페이지의 액세스 토큰에서 삭제하려는 액세스 토큰을 선택한 다음 삭제를 선택합니다.
4. 액세스 토큰 삭제 대화 상자에서 정보를 검토하고 삭제를 입력한 다음 액세스 토큰 삭제를 선택합니다.

액세스 토큰 교체 방법

IAM Identity Center 디렉터리는 한 번에 최대 2개의 액세스 토큰을 지원합니다. 교체 전에 추가 액세스 토큰을 생성하려면 만료되었거나 사용하지 않은 액세스 토큰을 모두 삭제합니다.

SCIM 액세스 토큰이 곧 만료되는 경우 다음 절차를 사용하여 IAM Identity Center 콘솔에서 기존 액세스 토큰을 교체할 수 있습니다.

액세스 토큰을 교체하려면

1. IAM Identity Center 콘솔의 왼쪽 탐색 창에서 설정을 선택합니다.
2. 설정 페이지에서 ID 소스 탭을 선택한 다음 작업 > 프로비저닝 관리를 선택합니다.
3. 자동 프로비저닝 페이지의 액세스 토큰에서 교체하려는 토큰의 토큰 ID를 기록해 둡니다.
4. 새 액세스 토큰을 생성하는 방법의 단계에 따라 새 토큰을 생성합니다. 이미 최대 개수의 SCIM 액세스 토큰을 생성한 경우 기존 토큰 중 하나를 먼저 삭제해야 합니다.
5. ID 제공업체의 웹 사이트로 이동하여 SCIM 프로비저닝을 위한 새 액세스 토큰을 구성한 다음 새 SCIM 액세스 토큰을 사용하여 IAM Identity Center 연결을 테스트합니다. 새 토큰을 사용하여 프로비저닝이 정상적으로 작동하는 것을 확인했으면 이 절차의 다음 단계를 진행합니다.
6. 액세스 토큰 삭제 방법 단계에 따라 앞서 기록해 둔 이전 액세스 토큰을 삭제합니다. 토큰 생성 날짜를 제거할 토큰에 대한 힌트로 사용할 수도 있습니다.

수동 프로비저닝

일부는 IdPs 도메인 간 ID 관리 시스템 (SCIM) 을 지원하지 않거나 호환되지 않는 SCIM 구현을 갖추고 있습니다. 이러한 경우 IAM Identity Center 콘솔을 통해 사용자를 수동으로 프로비저닝할 수 있습니다. IAM Identity Center에 사용자를 추가할 때는 사용자 이름을 IdP에 있는 사용자 이름과 동일하게 설정해야 합니다. 최소한 고유한 이메일 주소와 사용자 이름이 있어야 합니다. 자세한 내용은 사용자 이름 및 이메일 주소 고유성 단원을 참조하세요.

또한 IAM Identity Center에서 모든 그룹을 수동으로 관리해야 합니다. 이렇게 하려면 그룹을 생성하고 IAM Identity Center 콘솔을 사용하여 추가합니다. 이러한 그룹은 IdP에 있는 그룹과 일치하지 않아도 됩니다. 자세한 내용은 그룹 단원을 참조하세요.

SAML 2.0 인증서 관리

IAM Identity Center와 외부 ID 제공업체(idP) 간에 SAML 신뢰 관계를 설정하기 위해 IAM Identity Center는 인증서를 사용합니다. IAM Identity Center에서 외부 IdP를 추가할 때는 외부 IdP로부터 하나 이상의 퍼블릭 SAML 2.0 X.509 인증서를 받아야 합니다. 일반적으로 이 인증서는 트러스트 생성 과정에서 IdP SAML 메타데이터 교환 중에 자동으로 설치됩니다.

IAM Identity Center 관리자는 이전 IdP 인증서를 새 인증서로 교체해야 하는 경우가 있습니다. 예를 들어, 인증서 만료 날짜가 다가올 경우 IdP 인증서를 교체해야 할 수도 있습니다. 이전 인증서를 새 인증서로 교체하는 프로세스를 인증서 교체라고 합니다.

주제

- SAML 2.0 인증서 교체
- 인증서 만료 상태 표시

SAML 2.0 인증서 교체

ID 제공업체가 발급한 유효하지 않거나 만료된 인증서를 교체하려면 정기적으로 인증서를 가져와야 할 수 있습니다. 이는 인증 중단이나 다운타임을 방지하는 데 도움이 됩니다. 가져온 모든 인증서는 자동으로 활성화됩니다. 인증서는 관련 ID 제공업체에서 더 이상 사용하지 않도록 확인한 후에 삭제해야만 합니다.

또한 일부는 여러 인증서를 지원하지 IdPs 않을 수 있다는 점도 고려해야 합니다. 이 경우 인증서를 인증서로 교체하면 사용자에게 일시적인 서비스 중단이 IdPs 발생할 수 있습니다. 해당 IdP와의 신뢰가 성공적으로 재설정되면 서비스가 복원됩니다. 가능하면 사용량이 적은 시간에 신중하게 이 작업을 계획하세요.

> **Note**
>
> 보안 모범 사례를 위해, 기존 SAML 인증서가 손상되거나 잘못 취급된 흔적이 있는 경우 인증서를 즉시 제거하고 교체해야 합니다.

IAM Identity Center 인증서 교체는 다음을 포함하는 다단계 절차입니다.

- IdP에서 새 인증서 받기
- 새 인증서를 IAM Identity Center로 가져오기
- IdP에서 새 인증서 활성화
- 이전 인증서 삭제

인증 다운타임을 피하면서 인증서 교체 프로세스를 완료하려면 다음 절차를 모두 따릅니다.

1단계: IdP에서 새 인증서 받기

IdP 웹사이트로 이동하여 SAML 2.0 인증서를 다운로드합니다. 인증서 파일이 PEM 인코딩 형식으로 다운로드되었는지 확인합니다. 대부분의 제공업체는 IdP에서 여러 SAML 2.0 인증서를 생성할 수 있도록 허용합니다. 이러한 인증은 비활성화 또는 비활성으로 표시될 수 있습니다.

2단계: 새 인증서를 IAM Identity Center로 가져오기

IAM Identity Center 콘솔을 사용하여 새 인증서를 가져오려면 다음 절차를 따릅니다.

1. IAM Identity Center 콘솔에서 설정을 선택합니다.
2. 설정 페이지에서 ID 소스 탭을 선택한 다음 작업 > 인증 관리를 선택합니다.
3. SAML 2.0 인증서 관리 페이지에서 인증서 가져오기를 선택합니다.
4. SAML 2.0 인증서 가져오기 대화 상자에서 파일 선택을 선택하고 인증서 파일을 찾은 다음 인증서 가져오기를 선택합니다.

이때 IAM Identity Center는 가져온 두 인증서에서 서명된 수신 SAML 메시지를 모두 신뢰합니다.

3단계: IdP에서 새 인증서 활성화

IdP 웹사이트로 돌아가서 이전에 만든 새 인증서를 기본 또는 활성 인증서로 표시합니다. 이때 IdP가 서명한 모든 SAML 메시지는 새 인증서를 사용해야 합니다.

4단계: 이전 인증서 삭제

다음 절차를 사용하여 IdP 인증서 교체 프로세스를 완료합니다. 항상 하나 이상의 유효한 인증서가 나열되어 있어야 하며 이는 제거할 수 없습니다.

> **Note**
>
> 삭제하기 전에 ID 제공업체가 이 인증서를 사용하여 더 이상 SAML 응답에 서명하지 않는지 확인합니다.

1. SAML 2.0 인증서 관리 페이지에서 삭제할 인증서를 선택합니다. 삭제를 선택합니다.
2. SAML 2.0 인증서 삭제 대화 상자에 **DELETE**를 입력한 다음 삭제를 선택합니다.
3. IdP 웹사이트로 돌아가서 필요한 단계를 수행하여 비활성된 이전 인증서를 제거합니다.

인증서 만료 상태 표시

SAML 2.0 인증서 관리 페이지에서 컬러로 나타난 상태 표시기 아이콘을 볼 수 있습니다. 이러한 아이콘은 목록의 각 인증서 옆에 있는 만료 날짜 열에 표시됩니다. 다음은 IAM Identity Center에서 각 인증서에 표시할 아이콘을 결정하는 데 사용하는 기준에 대한 설명입니다.

- 빨간색 - 인증서가 현재 만료되었음을 나타냅니다.
- 노란색 - 인증서가 90일 이내에 만료됨을 나타냅니다.
- 녹색 - 인증서가 현재 유효하며 최소 90일 이상 유효함을 나타냅니다.

인증서 현재 상태를 확인하려면

1. IAM Identity Center 콘솔에서 설정을 선택합니다.
2. 설정 페이지에서 ID 소스 탭을 선택한 다음 작업 > 인증 관리를 선택합니다.
3. SAML 2.0 인증 관리 페이지의 SAML 2.0 인증서 관리에서 만료 날짜 열에 표시된 대로 목록의 인증서 상태를 검토합니다.

AWS 액세스 포털 사용

AWS 액세스 포털은 사용자 (최종 사용자) 에게 Office 365, Concur, Salesforce 등과 같이 가장 일반적으로 사용되는 모든 클라우드 응용 프로그램에 대한 싱글 사인온 액세스를 제공합니다. AWS 계정 포

털에서 AWS 계정 또는 애플리케이션 아이콘을 선택하기만 하면 여러 애플리케이션을 빠르게 시작할 수 있습니다. AWS 액세스 포털에 응용 프로그램 아이콘이 있다는 것은 회사의 관리자가 해당 응용 프로그램 또는 응용 프로그램에 대한 액세스 권한을 부여했음을 의미합니다. AWS 계정 또한 추가 로그인 메시지 없이 액세스 포털에서 이러한 모든 계정이나 애플리케이션에 AWS 액세스할 수 있습니다.

다음과 같은 경우 관리자에게 문의해 추가 액세스 권한을 요청하세요.

- 액세스해야 하는 AWS 계정 OR 애플리케이션은 보이지 않습니다.
- 특정 계정 또는 애플리케이션에 대한 액세스 권한이 예상과 다릅니다.

주제

- IAM Identity Center 가입 초대 수락
- AWS 액세스 포털에 로그인
- IAM Identity Center의 사용자 암호 재설정하기
- AWS CLI 또는 AWS SDK에 대한 IAM Identity Center 사용자 자격 증명 가져오기
- AWS Management Console 목적지 바로가기 링크 만들기
- 디바이스에 MFA 등록
- AWS 액세스 포털 URL 사용자 지정

IAM Identity Center 가입 초대 수락

AWS 액세스 포털에 처음 로그인하는 경우 이메일에서 사용자 자격 증명을 활성화하는 방법에 대한 지침을 확인하세요.

사용자 보안 인증 정보 활성화

1. 회사에서 받은 이메일에 따라 다음 방법 중 하나를 선택하여 사용자 자격 증명을 활성화하면 AWS 액세스 포털 사용을 시작할 수 있습니다.

   a. AWS IAM Identity Center 가입 초대 (Single AWS Sign-On의 후속 기능) 라는 제목의 이메일을 받은 경우 해당 이메일을 열고 초대 수락을 선택합니다. 새 사용자 가입 페이지에서 암호를 입력하고 확인한 다음 새 암호 설정을 선택합니다. 포털에 로그인할 때마다 이 암호를 사용하게 됩니다.

   b. 회사의 IT 지원 부서 또는 IT 관리자로부터 이메일을 받은 경우 제공된 지침에 따라 사용자 보안 인증 정보를 활성화합니다.

2. 새 비밀번호를 제공하여 사용자 자격 증명을 활성화하면 AWS 액세스 포털에서 자동으로 로그인합니다. 이 문제가 해결되지 않으면 다음 섹션에 나와 있는 지침에 따라 AWS 액세스 포털에 수동으로 로그인할 수 있습니다.

AWS 액세스 포털에 로그인

지금쯤이면 관리자가 AWS 액세스 포털에 대한 특정 로그인 URL을 제공했어야 합니다. 이 URL을 통해 포털에 로그인할 수 있습니다. 자세한 내용은 AWS 액세스 포털에 로그인을 참조하십시오.

> **Note**
>
> 로그인한 후 AWS 액세스 포털 세션의 기본 기간은 8시간입니다. 관리자가 이 세션의 기간을 변경할 수 있다는 점에 유의하세요.

신뢰할 수 있는 디바이스

로그인 페이지에서 신뢰할 수 있는 디바이스 옵션을 선택하면, IAM Identity Center는 향후 해당 디바이스를 통한 모든 로그인이 승인된 것으로 간주합니다. 즉, 신뢰할 수 있는 디바이스를 사용하는 동안에는 IAM Identity Center에 MFA 코드를 입력하라는 옵션이 표시되지 않습니다. 하지만 새 브라우저에서 로그인하거나 디바이스에 알 수 없는 IP 주소가 발급된 경우 등 몇 가지 예외가 있습니다.

AWS 액세스 포털을 위한 로그인 팁

다음은 AWS 액세스 포털 환경을 관리하는 데 도움이 되는 몇 가지 팁입니다.

- 경우에 따라 AWS 액세스 포털에서 로그아웃했다가 다시 로그인해야 할 수도 있습니다. 관리자가 최근에 할당한 새 애플리케이션에 액세스하는 데 필요할 수 있습니다. 하지만 모든 새 애플리케이션은 1시간마다 새로 고침을 하기 때문에 반드시 필요한 것은 아닙니다.
- AWS 액세스 포털에 로그인하면 애플리케이션 아이콘을 선택하여 포털에 나열된 애플리케이션을 열 수 있습니다. 애플리케이션 사용을 완료한 후에는 애플리케이션을 닫거나 AWS 액세스 포털에서 로그아웃할 수 있습니다. 애플리케이션을 닫으면 해당 애플리케이션에서만 로그아웃됩니다. AWS 액세스 포털에서 연 다른 모든 애플리케이션은 계속 열려 있고 실행 중입니다.
- 다른 사용자로 로그인하려면 먼저 AWS 액세스 포털에서 로그아웃해야 합니다. 포털에서 로그아웃하면 브라우저 세션에서 보안 인증이 완전히 제거됩니다.
- AWS 액세스 포털에 로그인한 후에는 역할로 전환할 수 있습니다. 역할을 전환하면 기존 사용자 권한이 일시적으로 무효화되고 역할에게 할당된 권한이 부여됩니다. 자세한 내용은 역할(콘솔) 전환을 참조하세요.

AWS 액세스 포털에서 로그아웃

포털에서 로그아웃하면 브라우저 세션에서 보안 인증이 완전히 제거됩니다. 자세한 내용은 AWS 로그인가이드의 AWS 액세스 포털에서 로그아웃을 참조하십시오.

AWS 액세스 포털에서 로그아웃하려면

- AWS 액세스 포털의 탐색 막대에서 로그아웃을 선택합니다.

> **Note**
> 다른 사용자로 로그인하려면 먼저 AWS 액세스 포털에서 로그아웃해야 합니다.

IAM Identity Center의 사용자 암호 재설정하기

AWS 액세스 포털은 IAM Identity Center 사용자에게 웹 포털을 통해 할당된 모든 AWS 계정과 클라우드 애플리케이션에 대한 Single Sign-On 액세스를 제공합니다. AWS 액세스 포털은 리소스 관리를 위한 서비스 콘솔 AWS Management Console모음인 와 다릅니다. AWS

이 절차를 사용하여 액세스 포털의 IAM Identity Center 사용자 비밀번호를 재설정합니다. AWS AWS 로그인 사용 설명서에서 사용자 유형에 대해 자세히 알아보세요.

고려 사항

AWS 액세스 포털의 암호 재설정 기능은 Identity Center 디렉터리를 사용하거나 ID AWS Managed Microsoft AD소스로 사용하는 Identity Center 인스턴스 사용자만 사용할 수 있습니다. 사용자가 외부 ID 공급자 또는 AD Connector에 연결되어 있는 경우 외부 ID 공급자에서 사용자 암호 재설정을 수행하거나 Active Directory 연결해야 합니다.

- ID 소스가 IAM Identity Center 디렉터리인 경우 을 참조하십시오. IAM Identity Center에서 ID를 관리할 때 암호 요구 사항
- ID 소스가 AWS Managed Microsoft ADa인 경우 비밀번호 재설정 시 비밀번호 요구 사항을 참조하십시오. AWS Managed Microsoft AD

AWS 액세스 포털의 비밀번호를 재설정하려면

1. 웹 브라우저를 열고 AWS 액세스 포털의 로그인 페이지로 이동합니다.

AWS 액세스 포털 URL이 없는 경우 이메일을 확인하세요. 액세스 포털로 연결되는 특정 로그인 URL이 포함된 AWS IAM Identity Center 가입 초대장을 이메일로 받으셨을 것입니다. AWS 또는 관리자가 일회용 비밀번호와 액세스 포털 URL을 직접 제공했을 수도 있습니다. AWS 이 정보를 찾을 수 없는 경우 관리자에게 해당 정보를 보내 달라고 요청합니다.

AWS 액세스 포털에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.

2. 사용자 이름을 입력하고 다음을 선택합니다.
3. 암호에서 암호 분실을 선택합니다.

   사용자 ID를 인증하고 제공된 이미지의 문자를 입력하여 로봇이 아님을 확인합니다. 다음을 선택합니다. 문자를 입력할 수 없는 경우 광고 차단 소프트웨어를 비활성화해야 할 수 있습니다.
4. 암호 재설정 이메일이 전송되었음을 확인하는 메시지가 나타납니다. 계속을 선택합니다.
5. `no-reply@signin.aws`로부터 암호 재설정이 요청됨이라는 제목의 이메일이 전송됩니다. 이메일에서 암호 재설정을 선택합니다.
6. 비밀번호 재설정 페이지에서 사용자 이름을 확인하고 AWS 액세스 포털의 새 비밀번호를 지정한 다음 새 비밀번호 설정을 선택합니다.
7. `no-reply@signin.aws`로부터 암호가 업데이트됨이라는 이메일이 전송됩니다.

> **Note**
>
> 관리자는 암호 재설정 지침이 포함된 이메일을 보내거나 일회용 암호를 생성하여 공유함으로써 암호를 재설정할 수 있습니다. 관리자인 경우 IAM Identity Center 최종 사용자 암호 재설정 섹션을 참조하세요.

AWS CLI 또는 AWS SDK에 대한 IAM Identity Center 사용자 자격 증명 가져오기

IAM Identity Center의 사용자 자격 증명과 함께 AWS Command Line Interface 또는 AWS 소프트웨어 개발 키트 (SDK) 를 사용하여 프로그래밍 방식으로 AWS 서비스에 액세스할 수 있습니다. 이 주제에서는 IAM Identity Center에서 사용자의 임시 보안 인증을 얻는 방법을 설명합니다.

AWS 액세스 포털은 IAM Identity Center 사용자에게 자신과 클라우드 애플리케이션에 대한 싱글 사인온 액세스를 제공합니다. AWS 계정 IAM Identity Center 사용자로 AWS 액세스 포털에 로그인한 후 임

시 자격 증명을 받을 수 있습니다. 그런 다음 AWS CLI 또는 AWS SDK에서 IAM Identity Center 사용자 자격 증명이라고도 하는 자격 증명을 사용하여 리소스에 액세스할 수 있습니다. AWS 계정

를 사용하여 프로그래밍 방식으로 AWS 서비스에 액세스하는 경우 이 항목의 절차를 사용하여 에 대한 액세스를 시작할 수 있습니다. AWS CLI AWS CLI에 AWS CLI대한 자세한 내용은 AWS Command Line Interface 사용 설명서를 참조하십시오.

AWS SDK를 사용하여 프로그래밍 방식으로 AWS 서비스에 액세스하는 경우 이 항목의 절차를 따르면 SDK에 대한 인증도 직접 설정됩니다. AWS SDK에 대한 자세한 내용은 AWS SDK 및 도구 참조 안내서를 참조하십시오.AWS

> **Note**
>
> IAM Identity Center의 사용자는 IAM 사용자와 다릅니다. IAM 사용자에게는 리소스에 대한 장기 자격 증명이 부여됩니다. AWS IAM Identity Center의 사용자에게는 임시 보안 인증이 부여됩니다. 임시 자격 증명은 로그인할 때마다 AWS 계정 생성되므로 액세스에 대한 보안 모범 사례로 사용하는 것이 좋습니다.

필수 조건

IAM Identity Center 사용자의 임시보안 인증을 받으려면 다음이 필요합니다.

- IAM Identity Center 사용자 - 이 사용자로 AWS 액세스 포털에 로그인합니다. 귀하 또는 관리자가 이 사용자를 생성할 수 있습니다. IAM Identity Center를 활성화하고 IAM Identity Center 사용자를 생성하는 방법에 대한 자세한 내용은 IAM Identity Center에서 일반 작업 시작을 참조하세요.
- 사용자 액세스 AWS 계정 — IAM Identity Center 사용자에게 임시 자격 증명을 검색할 수 있는 권한을 부여하려면 사용자 또는 관리자가 IAM Identity Center 사용자에게 권한 집합을 할당해야 합니다. 권한 집합은 IAM Identity Center에 저장되며 IAM Identity Center 사용자가 AWS 계정에 액세스할 수 있는 수준을 정의합니다. 관리자가 대신 IAM Identity Center 사용자를 생성한 경우 이 액세스 권한을 추가해 달라고 요청하세요. 자세한 정보는 사용자에게 액세스 권한을 할당하십시오. AWS 계정을 참조하세요.
- AWS CLI 설치됨 - 임시 자격 증명을 사용하려면 를 설치해야 합니다. AWS CLI설치 지침은 AWS CLI 사용 설명서의 AWS CLI의 최신 버전 설치 또는 업데이트를 참조하세요.

고려 사항

IAM Identity Center 사용자의 임시 보안 인증을 얻기 위한 단계를 완료하기 전에 다음 사항을 반드시 고려하세요.

- IAM Identity Center에서 IAM 역할 생성 - IAM Identity Center의 사용자에게 권한 집합을 할당하면 IAM Identity Center가 해당 권한 집합에서 해당 IAM 역할을 생성합니다. 권한 집합으로 생성된 IAM 역할은 다음과 같은 AWS Identity and Access Management 점에서 생성된 IAM 역할과 다릅니다.
  - IAM Identity Center는 권한 집합으로 생성된 역할을 소유하고 보호합니다. IAM Identity Center만 이 역할을 수정할 수 있습니다.
  - IAM Identity Center의 사용자만 할당된 권한 집합에 해당하는 역할을 맡을 수 있습니다. IAM 사용자, IAM 페더레이션 사용자 또는 서비스 계정에는 권한 집합 액세스 권한을 할당할 수 없습니다.
  - 이러한 역할에 대한 역할 신뢰 정책을 수정하여 IAM ID 센터 외부의 주체에 대한 액세스를 허용할 수 없습니다.

  IAM에서 생성한 역할의 임시 보안 인증을 얻는 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 AWS CLI에서 임시 보안 인증 사용을 참조하세요.
- 권한 집합의 세션 기간을 설정할 수 있습니다. AWS 액세스 포털에 로그인하면 IAM Identity Center 사용자에게 할당된 권한 집합이 사용 가능한 역할로 표시됩니다. IAM Identity Center는 이 역할을 위한 별도의 세션을 생성합니다. 이 세션은 권한 집합에 구성된 세션 기간에 따라 1시간에서 12시간까지 가능합니다. 세션은 기본적으로 1시간 동안 지속됩니다. 자세한 정보는 세션 기간 설정을 참조하세요.

임시 보안 인증 가져오기 및 새로 고침

IAM Identity Center 사용자의 임시 보안 인증을 자동 또는 수동으로 가져오고 새로 고칠 수 있습니다.

주제

- 자동 보안 인증 새로 고침 (권장)
- 수동 보안 인증 새로 고침

자동 보안 인증 새로 고침 (권장)

자동 보안 인증 새로 고침에서는 Open ID Connect (OIDC) 디바이스 코드 인증 표준을 사용합니다. 이 방법을 사용하면 AWS CLI에서 `aws configure sso` 명령을 사용하여 직접 액세스할 수 있습니다. 이 명령을 사용하면 할당된 권한 집합과 관련된 모든 역할에 자동으로 액세스할 수 있습니다 AWS 계정.

IAM Identity Center 사용자를 위해 생성된 역할에 액세스하려면 `aws configure sso` 명령을 실행한 다음 브라우저 창에서 권한을 부여하십시오. AWS CLI AWS 액세스 포털 세션이 활성 상태이면 는 자동으로 임시 자격 증명을 검색하고 자격 증명을 AWS CLI 자동으로 새로 고칩니다.

자세한 내용은 AWS Command Line Interface 사용 설명서에서 `aws configure sso wizard`를 사용한 빠른 구성 부분을 참조하세요.

자동으로 새로 고침되는 임시 보안 인증을 가져오는 방법

1. 관리자가 제공한 특정 로그인 URL을 사용하여 AWS 액세스 포털에 로그인합니다. IAM Identity Center 사용자를 생성한 경우 로그인 URL이 포함된 이메일 초대장을 AWS 보냈습니다. 자세한 내용은 로그인 사용 AWS 설명서의 액세스 포털에AWS 로그인을 참조하십시오.
2. 계정 탭에서 자격 증명을 검색하려는 계정을 찾습니다. AWS 계정 계정을 선택하면 해당 계정과 연결된 계정 이름, 계정 ID 및 이메일 주소가 표시됩니다.

   > **Note**
   >
   > 목록에 AWS 계정가 표시되지 않으면 해당 계정에 대한 권한 집합이 아직 할당되지 않았을 가능성이 높습니다. 이 경우 관리자에게 연락하여 이 액세스 권한을 추가해 달라고 요청합니다. 자세한 정보는 사용자에게 액세스 권한을 할당하십시오. AWS 계정을 참조하세요.

3. 계정 이름 아래에는 IAM Identity Center 사용자에게 할당된 권한 집합이 사용 가능한 역할로 표시됩니다. 예를 들어, IAM Identity Center 사용자에게 계정에 대한 PowerUserAccess권한 집합이 할당되면 AWS 액세스 포털에 역할이 로 PowerUserAccess표시됩니다.
4. 역할 이름 옆의 옵션에 따라 액세스 키를 선택하거나 명령줄 또는 프로그래밍 방식 액세스를 선택합니다.
5. 자격 증명 가져오기 대화 상자에서 설치한 운영 체제에 따라 macOS 및 Linux PowerShell, Windows 또는 중 하나를 선택합니다. AWS CLI
6. AWS IAM Identity Center 보안 인증(권장)에 `SSO Start URL`와 `SSO Region`가 표시됩니다. 이 값은 IAM Identity Center 지원 프로파일과 `sso-session`을 AWS CLI에 구성하는 데 필요합니다. 이 구성을 완료하려면 AWS Command Line Interface 사용 설명서의 `aws configure sso wizard`로 프로필 구성 지침을 따릅니다.

자격 증명이 AWS 계정 만료될 때까지 AWS CLI 필요에 따라 를 계속 사용하십시오.

수동 보안 인증 새로 고침

수동 자격 증명 새로 고침 방법을 사용하여 특정 권한 집합과 연결된 역할에 대한 임시 자격 증명을 가져올 수 있습니다. AWS 계정이렇게 하려면 임시 보안 인증에 필요한 명령을 복사하여 붙여 넣습니다. 이 방법을 사용하면 임시 보안 인증을 수동으로 새로 고침해야 합니다.

임시 자격 증명이 만료될 때까지 AWS CLI 명령을 실행할 수 있습니다.

수동으로 새로 고침되는 보안 인증을 가져오는 방법

1. 관리자가 제공한 특정 로그인 URL을 사용하여 AWS 액세스 포털에 로그인합니다. IAM Identity Center 사용자를 생성한 경우 로그인 URL이 포함된 이메일 초대장을 AWS 보냈습니다. 자세한 내용은 로그인 사용 AWS 설명서의 액세스 포털에AWS 로그인을 참조하십시오.
2. 계정 탭에서 액세스 자격 증명을 검색하려는 계정을 찾은 다음 확장하여 IAM 역할 이름 (예: Administrator) 을 표시합니다. AWS 계정 IAM 역할 이름 옆의 옵션에 따라 액세스 키를 선택하거나 명령줄 또는 프로그래밍 방식 액세스를 선택합니다.

   > **Note**
   >
   > 목록에 AWS 계정가 표시되지 않으면 해당 계정에 대한 권한 집합이 아직 할당되지 않았을 가능성이 높습니다. 이 경우 관리자에게 연락하여 이 액세스 권한을 추가해 달라고 요청합니다. 자세한 정보는 사용자에게 액세스 권한을 할당하십시오. AWS 계정을 참조하세요.

3. 자격 증명 가져오기 대화 상자에서 를 설치한 운영 체제에 따라 macOS 및 Linux PowerShell, Windows 또는 를 선택합니다. AWS CLI
4. 다음 옵션 중 하나를 선택합니다.

   - 옵션 1: AWS 환경 변수 설정

     `credentials`파일 및 `config` 파일의 설정을 포함하여 모든 자격 증명 설정을 재정의하려면 이 옵션을 선택합니다. 자세한 내용은 AWS CLI 사용 설명서의 AWS CLI를 구성할 환경 변수를 참조하세요.

     이 옵션을 사용하려면 명령을 클립보드에 복사하고 명령을 AWS CLI 터미널 창에 붙여넣은 다음 Enter 키를 눌러 필요한 환경 변수를 설정합니다.

   - 옵션 2: 자격 증명 파일에 프로필 AWS 추가

     다양한 보안 인증 집합을 사용하여 명령을 실행하려면 이 옵션을 선택합니다.

이 옵션을 사용하려면 명령을 클립보드에 복사한 다음 명령을 공유 AWS `credentials` 파일에 붙여넣어 이름이 지정된 새 프로필을 설정하십시오. 자세한 정보는 AWS SDK 및 도구 참조 설명서의 공유 구성 및 자격 증명 파일을 참조하세요. 이 자격 증명을 사용하려면 명령에 `--profile` 옵션을 지정하십시오. AWS CLI 이는 동일한 보안 인증 파일을 사용하는 모든 환경에 영향을 줍니다.

- 옵션 3: AWS 서비스 클라이언트에서 개별 값 사용

  AWS 서비스 클라이언트에서 AWS 리소스에 액세스하려면 이 옵션을 선택합니다. 자세한 내용은 빌드 기반 도구를 참조하십시오 AWS.

  이 옵션을 사용하려면 값을 클립보드에 복사하고 코드에 붙여 넣은 다음 SDK에 적합한 변수에 할당합니다. 자세한 내용은 해당 SDK API 관련 설명서를 참조하세요.

AWS Management Console 목적지 바로가기 링크 만들기

AWS 액세스 포털에서 생성된 바로가기 링크를 통해 IAM Identity Center 사용자는 특정 권한 설정이 있는 특정 대상 AWS Management Console, 특정 위치로 이동할 수 있습니다. AWS 계정

바로가기 링크를 사용하면 사용자와 공동 작업자의 시간을 절약할 수 있습니다. AWS 액세스 포털을 비롯한 여러 페이지를 통해 AWS Management Console (예: Amazon S3 버킷 인스턴스 페이지) 에서 원하는 대상 URL로 이동하는 대신 바로가기 링크를 사용하여 동일한 목적지로 자동으로 이동할 수 있습니다.

바로가기 링크 대상 옵션

바로가기 링크에는 세 가지 대상 옵션이 있으며, 여기에는 우선순위별로 나열되어 있습니다.

- (선택 사항) 바로가기 링크에 AWS Management Console 지정된 모든 대상 URL. Amazon S3 버킷 인스턴스 페이지를 예로 들 수 있습니다.
- (선택 사항) 해당 권한 집합에 대해 관리자가 구성한 릴레이 상태 URL. 릴레이 상태 설정에 대한 자세한 내용은 을 참조하십시오. 릴레이 상태 설정
- AWS Management Console 홈. 기본 목적지 (지정하지 않은 경우)

> **Note**
>
> 목적지로의 자동 탐색은 IAM Identity Center로 인증되고 AWS 계정 및 대상 URL에 필요한 권한 세트를 할당한 경우에만 성공합니다.

AWS 액세스 포털에는 공유 가능한 바로가기 링크를 생성하는 데 도움이 되는 바로가기 생성 버튼이 있습니다. 대상 URL (이전 목록의 첫 번째 옵션) 을 지정하려는 경우 URL을 클립보드에 복사하여 공유할 수 있습니다.

액세스 포털에서 바로가기 링크를 생성하세요. AWS

1. AWS 액세스 포털에 로그인한 상태에서 계정 탭을 선택한 다음 바로가기 만들기 버튼을 선택합니다.
2. 대화 상자에서:
   a. 계정 ID 또는 계정 이름을 AWS 계정 사용하여 선택합니다. 입력할 때 드롭다운 메뉴에 액세스할 수 있는 일치하는 계정 ID와 이름이 표시됩니다. 액세스 권한이 있는 계정만 선택할 수 있습니다.
   b. 드롭다운 목록에서 IAM 역할을 선택할 수도 있습니다. 선택한 계정에 할당된 권한 집합은 다음과 같습니다. 역할 선택을 생략하면 바로 가기 링크를 사용할 때 선택한 계정에 할당된 역할을 선택하라는 메시지가 표시됩니다.

      > **Note**
      >
      > 바로가기 링크를 사용하여 새 액세스 권한을 부여할 수 없습니다. 바로가기 링크는 사용자에게 이미 할당된 권한 집합에서만 작동합니다. 사용자에게 계정 및 대상 URL에 필요한 권한 집합이 할당되지 않은 경우 액세스가 거부됩니다.

   c. 선택적으로 AWS 액세스 포털 대상 URL을 입력합니다. URL 입력을 생략하면 앞서 언급한 바로가기 링크 대상 옵션에 따라 바로가기 링크를 사용할 때 목적지가 자동으로 결정됩니다.
   d. 입력한 내용에 따라 대화 상자 하단에 바로가기 링크가 생성됩니다. URL 복사 버튼을 선택합니다. 이제 복사한 바로가기 링크로 북마크를 만들거나 동일한 권한 집합이나 충분한 다른 권한 집합으로 동일한 계정에 액세스할 수 있는 공동 작업자와 공유할 수 있습니다.

URL 인코딩으로 안전한 AWS Management Console 바로가기 링크 만들기

계정 ID, 권한 집합 이름, 대상 URL을 비롯한 URL의 모든 매개 변수 값은 URL로 인코딩되어야 합니다.

바로가기 링크는 AWS 액세스 포털 URL을 다음 경로로 확장합니다.

```
/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

클래식 AWS 파티션의 전체 URL은 다음 패턴을 따릅니다.

```
https://[your_subdomain].awsapps.com/start/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

다음은 `S3FullAccess` 권한 설정을 사용하여 사용자를 `123456789012` 계정으로 로그인시키고 S3 콘솔 홈 페이지로 이동하는 단축 링크의 예시입니다.

- `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

디바이스에 MFA 등록

AWS 액세스 포털 내에서 다음 절차를 사용하여 다단계 인증 (MFA) 을 위해 새 디바이스를 등록하십시오.

> **Note**
>
> 이 절차의 단계를 시작하기 전에 먼저 적절한 인증 앱을 디바이스에 다운로드하는 것이 좋습니다. MFA 디바이스에서 사용할 수 있는 앱 목록은 가상 인증 앱을 참조하세요.

MFA를 사용할 디바이스를 등록하는 방법

1. AWS 액세스 포털에 로그인합니다. 자세한 정보는 AWS 액세스 포털에 로그인을 참조하세요.

2. 페이지의 우측 상단 근처에서 MFA 디바이스를 선택합니다.
3. 다중 인증(MFA) 디바이스 페이지에서 디바이스 등록을 선택합니다.

> **Note**
>
> MFA 디바이스 등록 옵션이 회색으로 표시된 경우 관리자에게 문의하여 디바이스 등록에 대한 도움을 받으세요.

4. MFA 디바이스 등록 페이지에서 다음 MFA 디바이스 유형 중 하나를 선택하고 안내를 따릅니다.

- 인증 앱
  1. 인증 앱 설정 페이지에서 QR 코드 그래픽을 포함하여 새 MFA 디바이스의 구성 정보를 확인할 수 있습니다. 그래픽은 QR 코드를 지원하지 않는 장치에서 수동으로 입력할 수 있는 비밀 키를 나타냅니다.
  2. 실물 MFA 디바이스를 사용하여 다음을 수행합니다.
     a. 호환되는 MFA 인증 앱을 엽니다. MFA 디바이스에서 사용할 수 있는 테스트 완료된 앱 목록은 가상 인증 앱을 참조하세요. MFA 앱이 다수의 계정(다수의 MFA 디바이스)을 지원하는 경우 옵션을 선택하여 새로운 계정(새 MFA 디바이스)을 생성합니다.
     b. MFA 앱의 QR 코드 지원 여부를 결정한 후 인증 관리자 앱 설정 페이지에서 다음 중 한 가지를 실행합니다.
        i. QR 코드 표시를 선택한 다음 해당 앱을 사용하여 QR 코드를 스캔합니다. 예를 들어, 카메라 모양의 아이콘을 선택하거나 코드 스캔와 비슷한 옵션을 선택합니다. 그런 다음 디바이스의 카메라를 사용하여 해당 코드를 스캔합니다.
        ii. 비밀 키 표시를 선택한 다음 MFA 앱에 해당 비밀 키를 입력합니다.

> **Important**
>
> IAM Identity Center용 MFA 디바이스를 구성할 때는 QR 코드 또는 보안 키 사본을 안전한 곳에 저장하는 것이 좋습니다. 휴대폰을 분실했거나 MFA 인증 앱을 다시 설치해야 하는 경우에 도움이 될 수 있습니다. 이러한 상황이 발생하면 동일한 MFA 구성을 사용하도록 앱을 빠르게 재구성할 수 있습니다.

  3. 인증 앱 설정 페이지의 인증 코드에서 현재 실물 MFA 디바이스에 표시된 일회용 비밀번호를 입력합니다.

> **Important**
>
> 코드를 생성한 후 즉시 요청을 제출하세요. 코드를 생성한 후 너무 오래 기다렸다 요청을 제출할 경우 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스 동기화가 되지 않을 수 있습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 디바이스를 다시 동기화할 수 있습니다.

4. Assign MFA(MFA 할당)을 선택합니다. 이제 MFA 디바이스에서 일회용 암호 생성을 시작할 수 있으며 이제 에서 사용할 준비가 되었습니다. AWS

- 보안 키 또는 내장된 인증자

  1. 사용자 보안 키 등록 페이지에서 브라우저 또는 플랫폼에 나와 있는 지침을 따릅니다.

> **Note**
>
> 환경은 브라우저 또는 플랫폼에 따라 다릅니다. 디바이스가 성공적으로 등록되면 친숙한 표시 이름을 새로 등록된 디바이스에 연결할 수 있습니다. 이를 변경하려면 이름 바꾸기를 선택하고 새 이름을 입력한 다음 저장을 선택합니다.

AWS 액세스 포털 URL 사용자 지정

기본적으로 다음 `d-xxxxxxxxxx.awsapps.com/start` 형식을 따르는 URL을 사용하여 AWS 액세스 포털에 접근할 수 있습니다. 다음과 같이 URL을 사용자 지정할 수 있습니다: *`your_subdomain`*`.awsapps.com/start`.

> **Important**
>
> AWS 액세스 포털 URL을 변경하면 나중에 수정할 수 없습니다.

URL을 사용자 지정하는 방법

1. https://console.aws.amazon.com/singlesignon/ 에서 AWS IAM Identity Center 콘솔을 엽니다.
2. IAM Identity Center 콘솔의 탐색 창에서 대시보드를 선택하고 설정 요약 섹션을 찾습니다.
3. AWS 액세스 포털 URL 아래에 있는 사용자 지정 버튼을 선택합니다.

> **Note**
>
> 사용자 지정 버튼이 표시되지 않으면 AWS 액세스 포털이 이미 사용자 지정되었음을 의미합니다. AWS 액세스 포털 URL 사용자 지정은 한 번의 작업으로 되돌릴 수 없습니다.

4. 원하는 하위 도메인 이름을 입력하고 저장을 선택합니다.

이제 사용자 지정 URL을 사용하여 AWS 액세스 AWS 포털을 통해 콘솔에 로그인할 수 있습니다.

Identity Center 사용자를 위한 다중 인증

다중 인증(MFA)은 사용자 이름과 비밀번호라는 기본 인증 메커니즘에 보호 계층을 추가할 수 있는 간단하고 안전한 방법입니다.

관리자가 MFA를 활성화하면 사용자는 두 가지 요소를 사용하여 AWS 액세스 포털에 로그인해야 합니다

- 사용자 이름과 암호. 이는 첫 번째 요소이며 사용자가 알고 있는 내용입니다.
- 코드, 보안 키 또는 생체 인식 중 하나를 선택합니다. 이는 두 번째 요소이며 사용자가 소유하고 있거나(소유물) 생체 인식이 가능한(생체 인식) 요소입니다. 두 번째 요소는 모바일 디바이스에서 생성된 인증 코드, 컴퓨터에 연결된 보안 키 또는 사용자의 생체 인식 스캔일 수 있습니다.

이러한 여러 요소를 함께 사용하면 하면 유효한 MFA 시도가 성공적으로 완료되는 경우를 제외하고 AWS 리소스에 대한 무단 액세스를 방지하여 보안을 강화할 수 있습니다.

각 사용자는 모바일 디바이스 또는 태블릿에 설치된 일회성 비밀번호 인증 애플리케이션인 가상 인증 앱을 최대 2개까지 등록할 수 있으며, 내장 인증자 및 보안 키를 포함한 FIDO 인증자를 최대 6개까지 등록하여 총 8개의 MFA 디바이스를 사용할 수 있습니다. IAM Identity Center에서 사용 가능한 MFA 유형 섹션에 대해 자세히 알아봅니다.

> **Important**
>
> 보안 모범 사례로 MFA를 활성화할 것을 강력히 권장합니다.

주제

- IAM Identity Center에서 사용 가능한 MFA 유형
- MFA 구성
- IAM Identity Center에서 MFA 디바이스 관리

IAM Identity Center에서 사용 가능한 MFA 유형

다중 인증(MFA)은 사용자의 보안을 강화하는 간단하고 효과적인 메커니즘입니다. 사용자의 첫 번째 요소인 암호는 기억해야 하는 비밀이며 지식 요소라고도 합니다. 다른 요소로는 보유 요소(보안 키 등 귀하가 보유하는 것) 또는 고유 요소(생체인식 스캔 등 귀하에 대한 것)가 있습니다. 계정 보안을 위한 추가 레이어를 추가하도록 MFA를 설정하는 것이 좋습니다.

IAM Identity Center MFA는 다음과 같은 디바이스 유형을 지원합니다. 브라우저 기반 콘솔 액세스뿐만 아니라 IAM Identity Center와 함께 AWS CLI v2를 사용하는 경우 모든 MFA 유형이 지원됩니다.

- FIDO2 인증자(내장형 인증자와 보안 키가 포함)
- 가상 인증 앱
- AWS Managed Microsoft AD를 통해 연결된 나만의 RADIUS MFA 구현

사용자는 하나의 계정에 최대 2개의 가상 인증 앱과 6개의 FIDO 인증자를 포함하여 최대 8개의 MFA 디바이스를 사용할 수 있습니다. 사용자가 로그인할 때마다 MFA를 요구하거나 로그인할 때마다 MFA가 필요하지 않은 신뢰할 수 있는 디바이스를 활성화하도록 MFA 활성화 설정을 구성할 수도 있습니다. 사용자를 위해 MFA 유형을 설정하는 방법에 대한 자세한 내용은 MFA 유형 선택 및 MFA 디바이스 적용 구성 섹션을 참조하십시오.

FIDO2 인증자

FIDO2는 CTAP2 및 WebAuthn을 포함하는 표준이며, 공개 키 암호화를 기반으로 합니다. FIDO 보안 인증은 AWS와(과) 같이 해당 보안 인증이 생성된 웹사이트에 고유한 것이므로 피싱 방지 기능이 있습니다.

AWS은(는) FIDO 인증자의 가장 일반적인 두 가지 폼 팩터인 내장 인증자와 보안 키를 지원합니다. 가장 일반적인 유형의 FIDO 인증자에 대한 자세한 내용은 아래를 참조하십시오.

주제

- 내장된 인증자
- 보안 키

- 암호 관리자, 패스키 공급자, 기타 FIDO 인증자

내장된 인증자

대부분의 현대적인 컴퓨터와 휴대전화는 MacBook의 TouchID 또는 Windows Hello 호환 카메라와 같이 내장된 인증자가 있습니다. 디바이스에 FIDO 호환 내장된 인증자가 있는 경우 지문, 얼굴 또는 디바이스 핀을 두 번째 요소로 사용할 수 있습니다.

보안 키

보안 키는 구입하여 USB, BLE 또는 NFC를 통해 디바이스에 연결할 수 있는 FIDO 호환 외장형 하드웨어 인증자입니다. MFA를 입력하라는 메시지가 표시되면 키의 센서로 제스처를 취하기만 하면 됩니다. 보안 키의 몇 가지 예로는 YubiKeys 및 Feitian 키가 있으며, 가장 일반적인 보안 키는 디바이스 바인딩 FIDO 보안 인증을 생성합니다. 모든 FIDO 인증 보안 키 목록은 FIDO 인증 제품을 참조하십시오.

암호 관리자, 패스키 공급자, 기타 FIDO 인증자

여러 제3자 공급자는 모바일 애플리케이션에서 암호 관리자, FIDO 모드가 있는 스마트 카드 및 기타 폼 팩터의 기능으로 FIDO 인증을 지원합니다. 이러한 FIDO 호환 디바이스는 IAM Identity Center에서도 작동할 수 있지만, MFA에 이 옵션을 활성화하기 전에 FIDO 인증자를 직접 테스트해 보는 것이 좋습니다.

> **Note**
>
> 일부 FIDO 인증자는 패스키라고 하는 검색 가능한 FIDO 보안 인증을 생성할 수 있습니다. 패스키는 이를 생성한 디바이스에 바인딩되거나, 클라우드에 동기화되거나 백업될 수 있습니다. 예를 들어, 지원되는 Macbook에서 Apple Touch ID를 사용하여 패스키를 등록한 다음, 로그인 시 화면에 표시되는 메시지에 따라 iCloud에 있는 패스키를 사용하여 Google Chrome을 사용하는 Windows 노트북에서 어떠한 사이트에 로그인할 수 있습니다. 동기화 가능한 패스키를 지원하는 디바이스 및 운영 체제와 브라우저 간의 현재 패스키 상호 운용성에 대한 자세한 내용은 FIDO Alliance And World Wide Web Consortium(W3C)에서 관리하는 리소스인 passkeys.dev에서 디바이스 지원을 참조하십시오.

가상 인증 앱

인증 앱은 기본적으로 일회용 암호(OTP) 기반 제3자 인증자입니다. 모바일 디바이스 또는 태블릿에 설치된 인증 애플리케이션을 승인된 MFA 디바이스로 사용할 수 있습니다. 제3자 인증 애플리케이션은 6

자리 인증 코드를 생성할 수 있는 표준 기반 시간 기반 일회용 암호(TOTP) 알고리즘인 RFC 6238과 호환되어야 합니다.

MFA에 대한 메시지가 표시되면 사용자는 제공된 입력 상자에 인증 앱에서 보낸 유효한 코드를 입력해야 합니다. 사용자에게 할당된 각 MFA 디바이스는 고유해야 합니다. 특정 사용자에 대해 두 개의 인증 앱을 등록할 수 있습니다.

테스트를 거친 인증 앱

모든 TOTP 호환 애플리케이션은 IAM Identity Center MFA와 호환됩니다. 다음 표에는 선택할 수 있는 잘 알려진 제3자 인증 앱이 나열되어 있습니다.

운영 체제	테스트를 거친 인증 앱
Android	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

RADIUS MFA

원격 인증 전화 접속 사용자 서비스(RADIUS)는 사용자가 네트워크 서비스에 연결할 수 있도록 인증, 권한 부여 및 계정(AAA) 관리 서비스를 제공하는 업계 표준 클라이언트 서버 프로토콜입니다. AWS Directory Service에는 MFA 솔루션을 구현한 RADIUS 서버에 연결되는 RADIUS 클라이언트가 포함됩니다. 자세한 내용은 AWS Managed Microsoft AD 다중 인증 활성화를 참조하십시오.

사용자 포털에 대한 사용자 로그인에 RADIUS MFA 또는 IAM Identity Center의 MFA 중 하나를 사용할 수 있지만 둘 다 사용할 수는 없습니다. 포털에 액세스하기 위해 AWS 기본 2단계 인증을 원하는 경우, IAM Identity Center의 MFA는 RADIUS MFA의 대안이 될 수 있습니다.

IAM Identity Center에서 MFA를 활성화하면 사용자가 AWS 액세스 포털에 로그인하려면 MFA 디바이스가 필요합니다. 이전에 RADIUS MFA를 사용했다면, IAM Identity Center에서 MFA를 활성화하면 AWS 액세스 포털에 로그인하는 사용자의 RADIUS MFA를 효과적으로 재정의합니다. 하지만 RADIUS MFA는 사용자가 Amazon WorkDocs와 같이 AWS Directory Service와 함께 작동하는 다른 모든 애플리케이션에 로그인할 때 계속해서 문제를 일으킵니다.

IAM Identity Center 콘솔에서 MFA가 비활성화되어 있고 AWS Directory Service로 RADIUS MFA를 구성한 경우 RADIUS MFA는 AWS 액세스 포털 로그인을 관리합니다. 즉, MFA를 비활성화하면 IAM Identity Center는 RADIUS MFA 구성으로 되돌아갑니다.

MFA 구성

다음 주제에서는 IAM Identity Center에서 MFA 디바이스를 구성하는 방법에 대해 설명합니다.

주제

- IAM Identity Center에서 MFA를 활성화하기 전 고려 사항
- IAM Identity Center에서 MFA 활성화
- MFA 유형 선택
- MFA 디바이스 적용 구성
- 사용자가 자신의 MFA 디바이스를 등록하도록 허용

IAM Identity Center에서 MFA를 활성화하기 전 고려 사항

MFA를 활성화하기 전에 다음을 고려하세요.

- 사용자는 활성화된 모든 MFA 유형에 대해 여러 백업 인증자를 등록하는 것이 좋습니다. 이렇게 하면 MFA 디바이스가 고장 나거나 잘못 배치된 경우 액세스 권한이 손실되는 것을 방지할 수 있습니다.
- 사용자가 이메일에 액세스하기 위해 AWS 액세스 포털에 로그인해야 하는 경우 이메일로 전송된 일회용 비밀번호 입력 옵션을 선택하지 마십시오. 예를 들어, 사용자가 AWS 액세스 포털에서 이메일을 읽을 때 Microsoft 365를 사용할 수 있습니다. 이 경우 사용자는 인증 코드를 검색할 수 없으며 AWS 액세스 포털에 로그인할 수 없게 됩니다. 자세한 내용은 MFA 디바이스 적용 구성 섹션을 참조하세요.
- AWS Directory Service로 구성한 RADIUS MFA를 이미 사용하고 있는 경우, IAM Identity Center 내에서 MFA를 활성화할 필요가 없습니다. IAM Identity Center의 MFA는 IAM Identity Center의 Microsoft Active Directory 사용자를 위한 RADIUS MFA의 대안입니다. 자세한 내용은 RADIUS MFA 섹션을 참조하세요.
- ID 소스가 IAM Identity Center의 ID 저장소, AWS Managed Microsoft AD 또는 AD 커넥터로 구성된 경우 IAM Identity Center에서 MFA 기능을 사용할 수 있습니다. 현재 외부 ID 제공업체에 대해서는 IAM Identity Center의 MFA가 지원되지 않습니다.

IAM Identity Center에서 MFA 활성화

AWS 액세스 포털, IAM Identity Center 통합 앱 및 AWS CLI에 대한 보안 액세스를 활성화하고 다중 인증(MFA)을 활성화할 수 있습니다.

주제

- 사용자에게 MFA에 대한 메시지 표시
- IAM Identity Center 디렉터리의 MFA 비활성화

사용자에게 MFA에 대한 메시지 표시

다음 단계에 따라 IAM Identity Center 콘솔에서 MFA를 활성화합니다. 시작하기 전에 먼저 IAM Identity Center에서 사용 가능한 MFA 유형를 이해하는 것이 좋습니다.

> **Note**
>
> 외부 IdP를 사용하는 경우 다중 인증을 사용할 수 없습니다. 외부 IdP가 MFA 설정을 관리하는 것이 아니라 IAM Identity Center에서 관리합니다.

MFA를 활성화하는 방법

1. IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 다중 인증 섹션에서 구성을 선택합니다.
5. 다중 인증 구성 페이지의 사용자에게 MFA에 대한 메시지 표시에서 비즈니스에 필요한 보안 수준에 따라 다음 인증 모드 중 하나를 선택합니다.

   - 로그인 컨텍스트가 변경될 때만 (컨텍스트 인식)

     이 모드(기본값)에서 IAM Identity Center는 로그인하는 동안 사용자에게 디바이스를 신뢰하는지 묻는 옵션을 제공합니다. 사용자가 디바이스를 신뢰한다고 표시하면 IAM Identity Center는 사용자에게 MFA를 요청하는 메시지를 한 번 표시하고 사용자의 후속 로그인을 위해 로그인 컨텍스트(디바이스, 브라우저, 위치 등)를 분석합니다. IAM Identity Center는 후속 로그인 시 사용자가 이전에 신뢰할 수 있는 컨텍스트로 로그인하고 있는지 확인합니다. 사용자의 로그인 컨텍스트가 변경되면 IAM Identity Center는 사용자에게 이메일 주소 및 비밀번호 보안 인증 정보 외에 MFA를 입력하라는 메시지를 표시합니다.

이 모드는 직장에서 자주 로그인하는 사용자가 쉽게 사용할 수 있는 모드로, 로그인할 때마다 MFA 단계를 완료하지 않아도 됩니다. 로그인 컨텍스트가 변경되는 경우에만 MFA를 입력하라는 메시지가 표시됩니다.

- 로그인할 때마다(상시 접속)

  이 모드에서는 등록된 MFA 디바이스가 있는 사용자가 로그인할 때마다 IAMIdentity Center에 메시지가 표시됩니다. 사용자가 AWS 액세스 포털에 로그인할 때마다 MFA를 완료해야 하는 조직 또는 규정 준수 정책이 있는 경우 이 모드를 사용해야 합니다. 예를 들어, PCI DSS는 고위험 결제 거래를 지원하는 애플리케이션에 액세스하기 위해 로그인할 때마다 MFA 사용을 강력히 권장합니다.

- 사용 안 함(비활성화)

  이 모드에서는 모든 사용자가 표준 사용자 이름과 비밀번호로만 로그인합니다. 이 옵션을 선택하면 IAM Identity Center MFA가 비활성화됩니다.

  > **Note**
  >
  > AWS Directory Service로 구성한 RADIUS MFA를 이미 사용하고 있으며, 이를 기본 MFA 유형으로 계속 사용하려는 경우 인증 모드를 비활성화된 상태로 두면 IAM Identity Center에서 MFA 기능을 우회합니다. 비활성화 모드에서 컨텍스트 인식 또는 상시 접속 모드로 변경하면 기존 RADIUS MFA 설정이 재정의됩니다. 자세한 내용은 RADIUS MFA 섹션을 참조하세요.

6. 변경 사항 저장을 선택합니다.

관련 주제

- MFA 유형 선택
- MFA 디바이스 적용 구성
- 사용자가 자신의 MFA 디바이스를 등록하도록 허용

IAM Identity Center 디렉터리의 MFA 비활성화

IAM Identity Center 디렉터리에서 다중 인증(MFA)을 비활성화하면 사용자는 표준 사용자 이름과 비밀번호로만 로그인할 수 있습니다. 사용자의 Identity Center 디렉터리에서 MFA가 비활성화되어 있는 동안에는 해당 사용자의 사용자 세부 정보에서 MFA 디바이스를 관리할 수 없으며, Identity Center 디렉터리 사용자는 AWS 액세스 포털에서 MFA 디바이스를 관리할 수 없습니다.

IAM Identity Center 디렉터리의 MFA를 비활성화하려면

> **Important**
>
> 이 섹션의 지침은 AWS IAM Identity Center에 적용됩니다. AWS Identity and Access Management(IAM)에는 적용되지 않습니다. IAM 사용자, 그룹 및 IAM 사용자 보안 인증은 IAM Identity Center 사용자, 그룹 및 사용자 보안 인증과 다릅니다. IAM 사용자용 MFA를 비활성화하는 방법에 대한 지침을 찾으려면 AWS Identity and Access Management 사용 설명서의 MFA 디바이스 비활성화를 참조하십시오.

1. IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 다중 인증 섹션에서 구성을 선택합니다.
5. 다중 인증 구성 페이지의 사용자에게 MFA에 대한 메시지 표시 섹션에서 사용 안 함(비활성화) 라디오 버튼을 선택합니다.
6. 변경 사항 저장을 선택합니다.

MFA 유형 선택

AWS 액세스 포털에서 MFA를 입력하라는 메시지가 표시되면 다음 절차에 따라 사용자가 인증할 수 있는 디바이스 유형을 선택합니다.

사용자의 MFA 유형을 구성하는 방법

1. IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 다중 인증 섹션에서 구성을 선택합니다.
5. 다중 인증 구성 페이지의 사용자는 다음 MFA 유형으로 인증할 수 있습니다에서 비즈니스 요구 사항에 따라 다음 MFA 유형 중 하나를 선택합니다. 자세한 내용은 IAM Identity Center에서 사용 가능한 MFA 유형 섹션을 참조하세요.

   - 내장형 인증자와 보안 키를 포함한 FIDO2 인증

- 가상 인증 앱

6. 변경 사항 저장을 선택합니다.

MFA 디바이스 적용 구성

다음 절차에 따라 사용자가 AWS 액세스 포털에 로그인할 때 등록된 MFA 디바이스를 가지고 있어야 하는지 확인합니다.

사용자의 MFA 디바이스 적용을 구성하는 방법

1. IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 다중 인증 섹션에서 구성을 선택합니다.
5. 다중 인증 구성 페이지의 사용자에게 아직 등록된 MFA 디바이스가 없는 경우에서 비즈니스 요구 사항에 따라 다음 중 하나를 선택합니다.

   - 로그인 시 MFA 디바이스를 등록하도록 요구

     이는 IAM Identity Center에 대해 MFA를 처음 구성할 때 기본 설정입니다. 아직 등록된 MFA 디바이스가 없는 사용자가 비밀번호 인증에 성공한 후 로그인하는 동안 디바이스를 직접 등록하도록 요구하려면 이 옵션을 사용합니다. 이를 통해 인증 디바이스를 개별적으로 등록하고 사용자에게 배포할 필요 없이 MFA로 조직의 AWS 환경을 보호할 수 있습니다. 셀프 등록을 하는 동안 사용자는 이전에 활성화한 사용 가능한 IAM Identity Center에서 사용 가능한 MFA 유형 중에서 원하는 디바이스를 등록할 수 있습니다. 등록을 완료한 후 사용자는 새로 등록한 MFA 디바이스에 친숙한 이름을 지정할 수 있으며, 그러면 IAM Identity Center는 사용자를 원래 대상으로 리디렉션합니다. 사용자 디바이스를 분실하거나 도난당한 경우 계정에서 해당 디바이스를 제거하기만 하면 됩니다. 그러면 IAM Identity Center에서 다음 로그인 시 새 디바이스를 직접 등록하도록 요구합니다.
   - 로그인 시 이메일로 전송된 일회용 비밀번호 입력 요구

     사용자에게 이메일로 인증 코드를 보내도록 할 때 이 옵션을 사용합니다. 이메일은 특정 디바이스에 바인딩되지 않기 때문에 이 옵션은 업계 표준 다중 인증 기준을 충족하지 못합니다. 하지만 비밀번호만 사용하는 것보다 보안 기능이 향상됩니다. 이메일 인증은 사용자가 MFA 디바이스를 등록하지 않은 경우에만 요청됩니다. 컨텍스트 인식 인증 방법이 활성화된 경우 사용자는 이메일을 수신하는 디바이스를 신뢰할 수 있는 디바이스로 표시할 수 있습니다. 이후에는 해당 디바이스, 브라우저, IP 주소 조합으로 향후 로그인할 때 이메일 코드를 인증할 필요가 없습니다.

> **Note**
>
> Active Directory를 IAM Identity Center 지원 ID 소스로 사용하는 경우 이메일 주소는 항상 Active Directory `email` 속성을 기반으로 합니다. 사용자 지정 Active Directory 속성 매핑은 이 동작을 재정의하지 않습니다.

- 로그인 차단

  모든 사용자가 AWS에 로그인하기 전에 MFA를 사용하도록 강제하려면 로그인 차단 옵션을 사용합니다.

  > **Important**
  >
  > 인증 방법이 컨텍스트 인식으로 설정된 경우 사용자는 로그인 페이지에서 이 디바이스는 신뢰할 수 있는 디바이스입니다 체크박스를 선택할 수 있습니다. 이 경우 로그인 차단 설정이 활성화되어 있더라도 해당 사용자에게 MFA를 입력하라는 메시지가 표시되지 않습니다. 이러한 사용자에게 메시지가 표시되도록 하려면 인증 방법을 상시 접속으로 변경합니다.

- 로그인 허용

  사용자가 AWS 액세스 포털에 로그인하는 데 MFA 디바이스가 필요하지 않다고 표시하고자 할 때 이 옵션을 사용합니다. MFA 디바이스를 등록한 사용자에게는 계속해서 MFA를 입력하라는 메시지가 표시됩니다.

6. 변경 사항 저장을 선택합니다.

사용자가 자신의 MFA 디바이스를 등록하도록 허용

다음 절차에 따라 사용자가 자신의 MFA 디바이스를 직접 등록할 수 있도록 할 수 있습니다.

사용자가 자신의 MFA 디바이스를 등록하도록 허용하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 다중 인증 섹션에서 구성을 선택합니다.

5. 다중 인증 구성 페이지의 MFA 디바이스를 관리할 수 있는 대상에서 사용자가 자신의 MFA 디바이스를 추가하고 관리할 수 있음을 선택합니다.
6. 변경 사항 저장을 선택합니다.

> **Note**
>
> 사용자를 위한 셀프 등록을 설정한 후 사용자에게 디바이스에 MFA 등록 절차에 대한 링크를 보내는 것이 좋습니다. 이 주제에서는 자신의 MFA 디바이스를 설정하는 방법을 자세히 설명합니다.

IAM Identity Center에서 MFA 디바이스 관리

다음 주제에서는 IAM Identity Center에서 MFA 디바이스를 관리하는 방법을 설명합니다.

주제

- MFA 디바이스 등록
- 사용자의 MFA 디바이스 관리

MFA 디바이스 등록

다음 절차에 따라 IAM Identity Center 콘솔에서 특정 사용자가 액세스할 수 있도록 새 MFA 디바이스를 설정합니다. 등록하려면 사용자의 MFA 디바이스에 물리적으로 액세스할 수 있어야 합니다. 예를 들어, 스마트폰에서 MFA 디바이스를 실행하는 사용자에게 MFA를 구성한 경우 등록 절차를 완료하려면 스마트폰에 물리적으로 액세스해야 합니다. 또는 사용자가 자신의 MFA 디바이스를 직접 구성하고 관리하도록 허용할 수 있습니다. 자세한 내용은 사용자가 자신의 MFA 디바이스를 등록하도록 허용 섹션을 참조하세요.

MFA 디바이스를 등록하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자를 선택합니다. 목록에서 사용자를 선택합니다. 이 단계에서는 사용자 옆에 있는 체크박스를 선택하지 마십시오.
3. 사용자 세부 정보 페이지에서 MFA 디바이스 탭을 선택한 다음 MFA 디바이스 등록을 선택합니다.
4. MFA 디바이스 등록 페이지에서 다음 MFA 디바이스 유형 중 하나를 선택하고 안내를 따릅니다.
    - 인증 앱

1. 인증 앱 설정 페이지에서 IAM Identity Center는 QR 코드 그래픽을 포함하여 새 MFA 디바이스에 대한 구성 정보를 표시합니다. 그래픽은 QR 코드를 지원하지 않는 디바이스 상에서 수동 입력할 수 있는 보안 구성 키를 표시한 것입니다.
2. 실물 MFA 디바이스를 사용하여 다음을 수행합니다.
   a. 호환되는 MFA 인증 앱을 엽니다. MFA 디바이스에서 사용할 수 있는 테스트 완료된 앱 목록은 가상 인증 앱을 참조하십시오. MFA 앱이 다수의 계정(다수의 MFA 디바이스)을 지원하는 경우 옵션을 선택하여 새로운 계정(새 MFA 디바이스)을 생성합니다.
   b. MFA 앱의 QR 코드 지원 여부를 결정한 후 인증 관리자 앱 설정 페이지에서 다음 중 한 가지를 실행합니다.
      i. QR 코드 표시를 선택한 다음 해당 앱을 사용하여 QR 코드를 스캔합니다. 예를 들어, 카메라 모양의 아이콘을 선택하거나 코드 스캔과 비슷한 옵션을 선택합니다. 그런 다음 디바이스의 카메라를 사용하여 해당 코드를 스캔합니다.
      ii. 비밀 키 표시를 선택한 다음 MFA 앱에 해당 비밀 키를 입력합니다.

> **Important**
>
> IAM Identity Center용 MFA 디바이스를 구성할 때는 QR 코드 또는 보안 키 사본을 안전한 곳에 저장하는 것이 좋습니다. 이렇게 하면 할당된 사용자가 휴대폰을 분실하거나 MFA 인증 앱을 다시 설치해야 하는 경우에 도움이 될 수 있습니다. 이러한 상황이 발생하면 동일한 MFA 구성을 사용하도록 앱을 빠르게 재구성할 수 있습니다. 그러므로 사용자를 위해 IAM Identity Center에서 새로운 MFA 디바이스를 생성할 필요가 없습니다.

3. 인증 앱 설정 페이지의 인증 코드에서 현재 실물 MFA 디바이스에 표시된 일회용 비밀번호를 입력합니다.

> **Important**
>
> 코드를 생성한 후 즉시 요청을 제출하세요. 코드를 생성하고 너무 오래 시간이 지난 후 요청을 제출하면 MFA 디바이스가 사용자와 연결은 되지만 MFA 디바이스가 동기화되지 않습니다. 이는 시간 기반 일회용 암호(TOTP)가 잠시 후에 만료되기 때문입니다. 이 경우, 디바이스를 재동기화할 수 있습니다.

4. MFA 할당을 선택합니다. 이제 MFA 디바이스에서 일회용 비밀번호 생성을 시작할 수 있으며 AWS와 함께 사용할 준비가 되었습니다.

- 보안 키
  1. 사용자 보안 키 등록 페이지에서 브라우저 또는 플랫폼에 나와 있는 지침을 따릅니다.

> **Note**
>
> 이 환경은 운영 체제 및 브라우저에 따라 달라질 수 있으므로 브라우저 또는 플랫폼에 표시되는 지침을 따르십시오. 사용자의 디바이스가 성공적으로 등록되면 새로 등록한 사용자의 디바이스에 친숙한 표시 이름을 연결할 수 있는 옵션이 제공됩니다. 이를 변경하려면 이름 바꾸기를 선택하고 새 이름을 입력한 다음 저장을 선택합니다. 사용자가 자신의 디바이스를 관리하도록 허용하는 옵션을 활성화한 경우 사용자는 AWS 액세스 포털에서 이 친숙한 이름을 보게 됩니다.

사용자의 MFA 디바이스 관리

사용자의 MFA 디바이스 이름을 변경하거나 삭제해야 하는 경우 다음 절차를 따릅니다.

MFA 디바이스의 이름을 변경하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자를 선택합니다. 목록에서 사용자를 선택합니다. 이 단계에서는 사용자 옆에 있는 체크박스를 선택하지 마십시오.
3. 사용자 세부 정보 페이지에서 MFA 디바이스 탭을 선택한 다음 디바이스를 선택하고 이름 바꾸기를 선택합니다.
4. 메시지가 표시되면 새 이름을 입력한 다음 이름 바꾸기를 선택합니다.

MFA 디바이스 삭제하기

1. IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 사용자를 선택합니다. 목록에서 사용자를 선택합니다.
3. 사용자 세부 정보 페이지에서 MFA 디바이스 탭을 선택한 다음 디바이스를 선택하고 삭제를 선택합니다.
4. 삭제를 입력한 후 삭제를 선택하여 확인합니다.

액세스 관리 AWS 계정

AWS IAM Identity Center 와 AWS Organizations통합되어 있으므로 각 계정을 수동으로 AWS 계정 구성하지 않고도 여러 계정의 권한을 중앙에서 관리할 수 있습니다. 권한을 정의하고 이러한 권한을 직원 사용자에게 할당하여 특정 AWS 계정항목에 대한 액세스를 제어할 수 있습니다.

AWS 계정 유형

핀에는 두 가지 AWS Organizations유형이 AWS 계정 있습니다.

- 관리 계정 - 조직을 만드는 데 사용되는 계정입니다. AWS 계정
- 멤버 계정 - 조직에 AWS 계정 속한 나머지 계정.

AWS 계정 유형에 대한 자세한 내용은 AWS Organizations 사용 설명서의AWS Organizations 용어 및 개념을 참조하십시오.

또한 멤버 계정을 IAM Identity Center의 위임 관리자로 등록하도록 선택할 수 있습니다. 이 계정의 사용자는 대부분의 IAM Identity Center 관리 작업을 수행할 수 있습니다. 자세한 내용은 위임된 관리 단원을 참조하세요.

다음 표에는 각 작업 및 계정 유형에 대해 해당 계정의 사용자가 IAM Identity Center 관리 작업을 수행할 수 있는지 여부가 나와 있습니다.

IAM Identity Center 관리 작업	멤버 계정	위임된 관리자 계정	관리 계정
사용자 또는 그룹 읽기 그룹 자체 및 그룹 구성원 읽기)	 예	 예	 예
사용자 또는 그룹 추가, 편집 또는 삭제	 아니요	 예	 예

IAM Identity Center 관리 작업	멤버 계정	위임된 관리자 계정	관리 계정
사용자 액세스 활성화 또는 비활성화	 아니요	 예	 예
수신 속성을 활성화, 비활성화 또는 관리합니다.	 아니요	 예	 예
ID 소스 변경 또는 관리	 아니요	 예	 예
애플리케이션 생성, 편집 또는 삭제	 아니요	 예	 예
MFA 구성	 아니요	 예	 예
관리 계정에 프로비저닝되지 않은 권한 집합 관리	 아니요	 예	 예
관리 계정에 프로비저닝된 권한 집합 관리	 아니요	 아니요	 예

IAM Identity Center 관리 작업	멤버 계정	위임된 관리자 계정	관리 계정
IAM Identity Center 활성화	 아니요	 아니요	 예
IAM Identity Center 구성 삭제	 아니요	 아니요	 예
관리 계정에서 사용자 액세스를 활성화 또는 비활성화합니다.	 아니요	 아니요	 예
위임된 관리자로 멤버 계정 등록 또는 등록 해지	 아니요	 아니요	 예

액세스 권한 할당 AWS 계정

권한 집합을 사용하면 AWS 계정에 조직의 사용자 및 그룹에 액세스 권한을 할당하는 방법을 단순화할 수 있습니다. 권한 집합은 IAM Identity Center에 저장되며 사용자 및 그룹이 AWS 계정에 대해 보유할 수 있는 액세스 수준을 정의합니다. 단일 권한 집합을 만들어 조직 AWS 계정 내 여러 권한에 할당할 수 있습니다. 동일한 사용자에게 여러 권한 집합을 할당할 수도 있습니다.

권한에 대한 자세한 내용은 권한 세트 생성, 관리 및 삭제 단원을 참조하세요.

> **Note**
>
> 사용자에게 애플리케이션에 대한 Single Sign-On 액세스 권한을 할당할 수도 있습니다. 자세한 내용은 애플리케이션 액세스 관리 단원을 참조하세요.

최종 사용자 경험

AWS 액세스 포털은 IAM Identity Center 사용자에게 웹 포털을 통해 할당된 모든 애플리케이션 AWS 계정 및 애플리케이션에 대한 싱글 사인온 액세스를 제공합니다. AWS 액세스 포털은 리소스 관리를 위한 서비스 콘솔 AWS Management Console모음인 와 다릅니다. AWS

권한 집합을 생성하면 권한 집합에 지정한 이름이 AWS 액세스 포털에서 사용 가능한 역할로 표시됩니다. 사용자는 AWS 액세스 포털에 로그인하고 하나를 선택한 다음 역할을 선택합니다. AWS 계정역할을 선택한 후에는 를 사용하여 AWS 서비스에 AWS Management Console 접근하거나 임시 자격 증명을 검색하여 프로그래밍 방식으로 AWS 서비스에 접근할 수 있습니다.

AWS 프로그래밍 방식으로 액세스하기 위한 임시 자격 증명을 AWS Management Console 열거나 검색하려면 사용자는 다음 단계를 완료하십시오.

1. 사용자는 브라우저 창을 열고 제공된 로그인 URL을 사용하여 AWS 액세스 포털로 이동합니다.
2. 디렉터리 자격 증명을 사용하여 AWS 액세스 포털에 로그인합니다.
3. 인증 후 AWS 액세스 포털 페이지에서 계정 탭을 선택하여 접근 권한이 있는 목록을 AWS 계정 표시합니다.
4. 그러면 사용자는 사용하려는 AWS 계정 것을 선택합니다.
5. 의 AWS 계정이름 아래에는 사용자에게 할당된 모든 권한 집합이 사용 가능한 역할로 표시됩니다. 예를 들어, 사용자에게 `PowerUser` 권한 `john_stiles` 집합을 할당한 경우 역할은 AWS 액세스 포털에 로 표시됩니다`PowerUser/john_stiles`. 여러 권한 집합이 할당된 사용자는 사용할 역할을 선택합니다. 사용자는 자신의 역할을 선택하여 에 접근할 수 AWS Management Console있습니다.
6. 역할 외에도 AWS 액세스 포털 사용자는 접근 키를 선택하여 명령줄 또는 프로그래밍 액세스를 위한 임시 자격 증명을 검색할 수 있습니다.

직원 사용자에게 제공할 수 있는 step-by-step 지침은 AWS 액세스 포털 사용 및 AWS CLI 또는 AWS SDK에 대한 IAM Identity Center 사용자 자격 증명 가져오기 을 참조하십시오.

액세스 적용 및 제한

IAM Identity Center를 활성화하면 IAM Identity Center가 서비스 연결 역할을 생성합니다. 서비스 제어 정책(SCP)도 사용할 수 있습니다.

액세스 위임 및 적용

서비스 연결 역할은 서비스에 직접 연결된 IAM 역할 유형입니다. AWS IAM ID 센터를 활성화한 후 IAM Identity Center는 조직 내 각 조직에 서비스 연결 역할을 생성할 수 있습니다. AWS 계정 이 역할은 사전 정의된 권한을 제공하여 IAM Identity Center에서 조직 내 특정 항목에 대해 SSO (Single Sign-On) 액세스 권한을 가진 사용자를 위임하고 적용할 수 있도록 합니다. AWS 계정 AWS Organizations 이 역할을 사용하려면 계정에 대한 액세스 권한을 가진 한 명 이상의 사용자를 할당해야 합니다. 자세한 내용은 서비스 연결 역할 및 IAM Identity Center 서비스 연결 역할 사용 단원을 참조하세요.

멤버 계정에서 ID 스토어에 액세스하는 것을 제한합니다.

IAM Identity Center에서 사용하는 ID 스토어 서비스의 경우, 멤버 계정에 액세스할 수 있는 사용자는 읽기 권한이 필요한 API 작업을 사용할 수 있습니다. 멤버 계정은 sso-directory 및 identitystore 네임스페이스 모두에서 읽기 작업에 액세스할 수 있습니다. 자세한 내용은 서비스 권한 부여 참조의 AWS IAM Identity Center 디렉터리에 대한 작업, 리소스 및 조건 키와 AWS Identity Store의 작업, 리소스 및 조건 키를 참조하십시오.

멤버 계정의 사용자가 ID 스토어에서 API 작업을 사용하지 못하도록 서비스 제어 정책(SCP)을 연결할 수 있습니다. SCP는 조직의 권한을 관리하는 데 사용할 수 있는 조직 정책 유형입니다. 다음 예시 SCP는 멤버 계정의 사용자가 ID 스토어의 모든 API 작업에 액세스하는 것을 방지합니다.

```
{
    "Sid": "ExplicitlyBlockIdentityStoreAccess",
    "Effect": "Deny",
    "Action": "identitystore:*", "sso-directory:*"],
    "Resource": "*"
}
```

> **Note**
>
> 멤버 계정의 액세스를 제한하면 IAM Identity Center 지원 애플리케이션의 기능이 저하될 수 있습니다.

자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책(SCP)을 참조하세요.

위임된 관리

위임된 관리는 등록된 멤버 계정의 할당된 사용자가 대부분의 IAM Identity Center 관리 작업을 수행할 수 있는 편리한 방법을 제공합니다. IAM ID 센터를 활성화하면 IAM ID 센터 인스턴스가 기본적으로 관리 계정에 생성됩니다. AWS Organizations 이는 원래 IAM Identity Center가 조직의 모든 멤버 계정에서 역할을 프로비저닝, 프로비저닝 해제 및 업데이트할 수 있도록 이러한 방식으로 설계되었습니다. IAM Identity Center 인스턴스가 항상 관리 계정에 있어야 하지만 IAM Identity Center 관리를 의 멤버 계정에 위임하도록 선택하여 관리 계정 외부에서 IAM Identity Center를 관리할 수 있는 기능을 확장할 수 있습니다. AWS Organizations

위임된 관리를 활성화하면 다음과 같은 이점이 있습니다.

- 관리 계정에 액세스해야 하는 사용자 수를 최소화하여 보안 문제를 완화하는 데 도움이 됩니다.
- 일부 관리자가 애플리케이션과 조직의 멤버 계정에 사용자 및 그룹을 할당할 수 있습니다.

IAM Identity Center의 작동 방식에 대한 자세한 내용은 을 참조하십시오. AWS Organizations액세스 관리 AWS 계정 추가 정보를 확인하고 위임 관리를 구성하는 방법을 보여주는 예제 회사 시나리오를 검토하려면 AWS 보안 블로그의 IAM Identity Center 위임 관리 시작하기를 참조하세요.

주제

- 모범 사례
- 필수 조건
- 멤버 계정 등록
- 멤버 계정 해지
- 위임된 관리자로 등록된 멤버 계정을 볼 수 있습니다.

모범 사례

위임된 관리를 구성하기 전에 고려해야 할 몇 가지 모범 사례는 다음과 같습니다.

- 관리 계정에 최소 권한 부여 - 관리 계정은 권한이 높은 계정이며 보안 주체 최소 권한 원칙을 준수하기 위해 관리 계정에 대한 액세스를 가능한 한 적은 사용자만 제한하는 것이 좋습니다. 위임 관리자 기능은 관리 계정에 액세스해야 하는 사용자 수를 최소화하기 위한 것입니다.
- 관리 계정에서만 사용할 권한 집합 생성 - 이렇게 하면 관리 계정에 액세스하는 사용자에 맞게 조정된 권한 집합을 더 쉽게 관리할 수 있으며 위임된 관리자 계정으로 관리되는 권한 집합과 구분할 수 있습니다.

- Active Directory 위치 고려 – Active Directory를 IAM Identity Center ID 소스로 사용할 계획이라면 IAM Identity Center 위임 관리자 기능을 활성화한 멤버 계정의 디렉터리를 찾습니다. IAM Identity Center ID 소스를 다른 소스에서 Active Directory로 변경하거나 Active Directory에서 다른 소스로 변경하려는 경우 해당 디렉터리는 IAM Identity Center에서 위임한 관리자 계정(있는 경우)에 있어야 하고 그렇지 않으면 관리 계정에 있어야 합니다.
- 관리 계정에서만 사용자 할당 생성 - 위임된 관리자는 관리 계정에 제공된 권한 집합을 변경할 수 없습니다. 하지만 위임된 관리자는 그룹 및 그룹 할당을 추가, 편집, 삭제할 수 있습니다.

필수 조건

계정을 위임된 관리자로 등록하려면 먼저 다음 환경을 배포해야 합니다.

- AWS Organizations 기본 관리 계정 외에 적어도 하나의 회원 계정으로 활성화하고 구성해야 합니다.
- ID 소스가 Active Directory로 설정된 경우 IAM Identity Center 구성 가능 AD 동기화 기능을 활성화해야 합니다.

멤버 계정 등록

위임 관리를 구성하려면 먼저 조직의 멤버 계정을 위임 관리자로 등록해야 합니다. 해당 멤버 계정에서 충분한 권한을 가진 사용자는 IAM Identity Center에 대한 관리 액세스 권한을 갖게 됩니다. 멤버 계정이 위임 관리를 위해 성공적으로 등록되면 이를 위임된 관리자 계정이라고 합니다. 위임된 관리자 계정으로 수행할 수 있는 작업에 대한 자세한 내용은 AWS 계정 유형 단원을 참조하세요.

IAM Identity Center는 한 번에 하나의 멤버 계정만 위임된 관리자로 등록할 수 있도록 지원합니다. 관리 계정의 자격 증명으로 로그인한 상태에서만 멤버 계정을 등록할 수 있습니다.

다음 절차에 따라 AWS 조직의 특정 구성원 계정을 위임 관리자로 등록하여 IAM Identity Center에 대한 관리 액세스 권한을 부여하십시오.

> **Important**
>
> 이 작업을 수행하면 이 멤버 계정의 관리자에게 IAM Identity Center 관리 액세스 권한이 위임됩니다. 이 위임된 관리자 계정에 대한 충분한 권한을 가진 모든 사용자는 해당 계정에서 모든 IAM Identity Center 관리 작업을 수행할 수 있습니다. 단, 다음과 같은 경우는 예외입니다.
>
> - IAM Identity Center 활성화

- IAM Identity Center 구성 삭제
- 관리 계정에 프로비저닝된 권한 집합 관리
- 다른 멤버 계정을 위임 관리자로 등록 또는 등록 취소
- 관리 계정에서 사용자 액세스 활성화 또는 비활성화

위임된 관리자는 그룹 멤버십을 편집할 수 있습니다.

멤버 계정을 등록하려면

1. 에서 관리 계정의 자격 증명을 AWS Management Console 사용하여 로그인합니다. AWS OrganizationsRegisterDelegatedAdministratorAPI를 실행하려면 관리 계정 자격 증명이 필요합니다.
2. IAM Identity Center가 활성화된 리전을 선택한 다음 IAM Identity Center 콘솔을 엽니다.
3. 설정을 선택한 다음 관리 탭을 선택합니다.
4. 위임된 관리자 섹션에서 계정 등록을 선택합니다.
5. 위임된 관리자 등록 페이지에서 AWS 계정 등록하려는 관리자를 선택한 다음 계정 등록을 선택합니다.

멤버 계정 해지

관리 계정의 자격 증명으로 로그인한 경우에만 멤버 계정을 등록 취소할 수 있습니다.

다음 절차에 따라 이전에 위임된 관리자로 지정되었던 AWS 조직의 구성원 계정을 등록 취소하여 IAM Identity Center에서 관리 액세스 권한을 제거하십시오.

Important

계정 등록을 취소하면 사실상 모든 관리자가 해당 계정에서 IAM Identity Center를 관리할 수 있는 기능이 제거됩니다. 따라서 이 계정으로는 더 이상 IAM Identity Center ID, 액세스 관리, 인증 또는 애플리케이션 액세스를 관리할 수 없습니다. 이 작업은 IAM Identity Center에 구성된 권한이나 할당에 영향을 주지 않으므로 최종 사용자는 액세스 포털 내에서 앱과 액세스 포털에 계속 액세스할 수 있으므로 영향을 AWS 계정 받지 않습니다. AWS

멤버 계정을 해지하려면

1. 에서 관리 계정의 자격 증명을 AWS Management Console 사용하여 로그인하십시오. AWS OrganizationsDeregisterDelegatedAdministratorAPI를 실행하려면 관리 계정 자격 증명이 필요합니다.
2. IAM Identity Center가 활성화된 리전을 선택한 다음 IAM Identity Center 콘솔을 엽니다.
3. 설정을 선택한 다음 관리 탭을 선택합니다.
4. 위임된 관리자 섹션에서 계정 등록 취소를 선택합니다.
5. 계정 등록 취소 대화 상자에서 보안에 미치는 영향을 검토한 다음 멤버 계정의 이름을 입력하여 이해했는지 확인합니다.
6. 계정 등록 취소를 선택합니다.

위임된 관리자로 등록된 멤버 계정을 볼 수 있습니다.

다음 절차를 사용하여 IAM Identity Center의 위임 관리자로 구성된 구성원 계정을 찾을 수 있습니다. AWS Organizations

등록된 멤버 계정을 보려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 세부 정보 섹션의 위임된 관리자 아래에서 등록된 계정 이름을 찾습니다. 관리 탭을 선택하고 위임된 관리자 섹션에서 확인해도 이 정보를 찾을 수 있습니다.

임시 권한 상승

모든 액세스 AWS 계정 권한에는 일정 수준의 권한이 포함됩니다. 프로덕션 환경과 같이 가치가 높은 리소스의 구성을 변경하는 것과 같은 민감한 작업에는 범위와 잠재적 영향을 고려하여 특별한 처리가 필요합니다. 임시 권한 상승 (just-in-time 액세스라고도 함) 은 지정된 기간 동안 특정 작업을 수행하기 위한 권한 사용을 요청, 승인 및 추적하는 방법입니다. 임시 승격된 액세스는 권한 집합 및 다단계 인증과 같은 다른 형태의 액세스 제어를 보완합니다.

AWS IAM Identity Center 다양한 비즈니스 및 기술 환경에서 임시 승격 액세스 관리를 위한 다음 옵션을 제공합니다.

- 벤더가 관리하고 지원하는 솔루션 — AWS엄선된 파트너 오퍼링의 IAM Identity Center 통합을 검증하고 공통적인 고객 요구 사항을 기준으로 해당 파트너의 기능을 평가했습니다. 시나리오에 가장 적합한 솔루션을 선택하고 제공업체의 지침에 따라 IAM Identity Center에서 기능을 활성화합니다.
- 자체 관리 및 자체 지원 — 이 옵션은 일시적으로 액세스 권한 AWS 상승에만 관심이 있고 기능을 직접 배포, 조정 및 유지 관리할 수 있는 경우 출발점이 됩니다. 자세한 내용은 임시 승격 액세스 관리(TEAM)를 참조하세요.

임시 권한 승격에 대한 검증된 보안 파트너 AWS

AWS 보안 파트너는 다양한 접근 방식을 사용하여 공통적인 일시적 액세스 권한 상승 요구 사항을 해결합니다. 각 파트너 솔루션을 주의 깊게 검토하여 비즈니스, 클라우드 환경의 아키텍처, 예산 등 요구 사항과 선호도에 가장 적합한 솔루션을 선택할 수 있도록 하는 것이 좋습니다.

> **Note**
>
> 재해 복구를 위해서는 중단이 발생하기 AWS Management Console전에 에 대한 긴급 액세스를 설정하는 것이 좋습니다.

AWS Identity는 보안 파트너가 제공하는 다음 just-in-time 서비스에 대한 기능 및 IAM Identity Center와의 통합을 검증했습니다. AWS

- CyberArk Secure Cloud Access— 이 오퍼링의 일부로CyberArk Identity Security Platform, 이 오퍼링은 멀티 클라우드 환경에 대한 온디맨드 고급 액세스를 제공합니다. AWS 승인은 ITSM 또는 툴링과의 통합을 통해 이루어집니다. ChatOps 감사 및 규정 준수를 위해 모든 세션을 기록할 수 있습니다.
- Tenable (previously Ermetic)— Tenable 플랫폼에는 멀티 클라우드 환경 내 관리 작업을 위한 just-in-time 권한 있는 액세스 프로비저닝이 포함됩니다. AWS AWS CloudTrail 액세스 로그를 포함한 모든 클라우드 환경의 세션 로그를 분석 및 감사를 위해 단일 인터페이스에서 사용할 수 있습니다. 이 기능은 Slack 및 Microsoft Teams와 같은 엔터프라이즈 및 개발자 도구와 통합됩니다.
- Okta액세스 요청 — Okta ID 거버넌스의 일부로, IAM Identity Center 외부 ID 공급자 (IdP) 와 IAM ID 센터 권한 집합을 사용하여 just-in-time Okta 액세스 요청 워크플로를 구성할 수 있습니다.

이 목록은 추가 파트너 솔루션의 기능과 이러한 솔루션과 IAM Identity Center의 통합을 AWS 검증하기 위해 업데이트될 예정입니다.

> **Note**
>
> 리소스 기반 정책, Amazon Elastic Kubernetes Service (Amazon EKS AWS Key Management Service) 또는 (리소스 정책, Amazon EKS의 권한 집합 참조 및 AWS KMS)AWS KMS를 사용하는 경우 솔루션을 선택하기 전에 먼저 참조하십시오. just-in-time

파트너 검증을 위해 일시적으로 상승된 액세스 기능을 평가했습니다. AWS

AWS Identity는 CyberArk Secure Cloud AccessTenable, 및 Okta Access Request에서 제공하는 임시 액세스 권한 상승 기능이 다음과 같은 일반적인 고객 요구 사항을 충족하는지 확인했습니다.

- 사용자는 AWS 계정, 권한 집합, 기간 및 이유를 지정하여 사용자가 지정한 기간 동안 권한 집합에 대한 액세스를 요청할 수 있습니다.
- 사용자는 요청에 대한 승인 상태를 받을 수 있습니다.
- 동일한 범위의 승인된 요청이 있고 승인된 기간 중에 세션을 호출하지 않는 한 사용자는 지정된 범위의 세션을 호출할 수 없습니다.
- 요청을 승인할 수 있는 사람을 지정하는 방법이 있습니다.
- 승인자는 자신의 요청을 승인할 수 없습니다.
- 승인자는 보류 중인 요청, 승인된 요청, 거부된 요청의 목록을 가지고 있으며 감사자를 위해 이를 내보낼 수 있습니다.
- 승인자는 보류 중인 요청을 승인하거나 거부할 수 있습니다.
- 승인자는 결정을 설명하는 메모를 추가할 수 있습니다.
- 승인자는 승인된 요청을 취소하여 향후 승격된 액세스를 사용하지 못하게 할 수 있습니다.

> **Note**
>
> 승인된 요청이 취소되었을 때 사용자가 상위 액세스 권한으로 로그인하면 승인이 취소된 후 최대 1시간 동안 세션이 활성 상태로 유지됩니다. 인증 세션에 대한 내용은 인증 단원을 참조하세요.

- 사용자 작업 및 승인은 감사에 사용할 수 있습니다.

싱글 사인온 액세스: AWS 계정

일반적인 직무에 AWS Organizations 따라 연결된 디렉터리의 사용자에게 조직의 관리 계정 또는 구성원 계정 권한을 할당할 수 있습니다. 또는 사용자 지정 권한을 사용하여 특정 보안 요구 사항을 충족할 수 있습니다. 예를 들어 데이터베이스 관리자에게 개발 계정에서는 Amazon RDS에 광범위한 권한을 부여하지만 프로덕션 계정에서는 권한을 제한할 수 있습니다. IAM Identity Center는 AWS 계정 에서 필요한 모든 사용자 권한을 자동으로 구성합니다.

> **Note**
>
> AWS Organizations 관리 계정에서 작업하려면 사용자 또는 그룹에 권한을 부여해야 할 수 있습니다. 권한이 높은 계정이므로 추가 보안 제한을 적용하려면 먼저 IAM FullAccess 정책 또는 이에 상응하는 권한이 있어야 설정할 수 있습니다. 조직의 구성원 AWS 계정에는 이러한 추가 보안 제한이 필요하지 않습니다.

사용자에게 액세스 권한을 할당하십시오. AWS 계정

다음 절차를 사용하여 연결된 디렉터리의 사용자 및 그룹에 Single Sign-On 액세스를 할당하고 권한 집합을 사용하여 액세스 수준을 결정합니다.

기존 사용자 및 그룹 액세스를 확인하려면 을 참조하십시오사용자 및 그룹 할당 보기.

> **Note**
>
> 액세스 권한 관리를 단순화하려면 개별 사용자에게 할당하는 대신 그룹에 직접 액세스 권한을 할당하는 것이 좋습니다. 그룹을 사용하면 개별 사용자에게 권한을 적용할 필요 없이 사용자 그룹에 권한을 부여하거나 거부할 수 있습니다. 사용자가 다른 조직으로 이동할 경우 해당 사용자를 다른 그룹으로 이동하기만 하면 새 조직에 필요한 권한이 해당 사용자에게 자동으로 부여됩니다.

사용자 또는 그룹 액세스 권한을 할당하려면 AWS 계정

1. IAM Identity Center 콘솔을 엽니다.

> **Note**
>
> 다음 단계로 넘어가기 전에 IAM Identity Center 콘솔이 AWS Managed Microsoft AD 디렉터리가 위치한 리전을 사용하고 있는지 확인합니다.

2. 탐색 창의 다중 계정 권한에서 AWS 계정을 선택합니다.
3. AWS 계정 페이지에는 조직의 트리 뷰 목록이 표시됩니다. Single Sign-On 액세스를 할당하려는 하나 이상의 AWS 계정 옆에 있는 확인란을 선택합니다.

> **Note**
>
> 사용자 및 그룹에 Single Sign-On 액세스를 할당할 때 권한 집합당 한 AWS 계정 번에 최대 10개까지 선택할 수 있습니다. 동일한 사용자 및 그룹 AWS 계정 집합에 10명 이상을 할당하려면 추가 계정에 필요한 만큼 이 절차를 반복합니다. 메시지가 표시되면 동일한 사용자, 그룹 및 권한 집합을 선택합니다.

4. 사용자 또는 그룹 할당을 선택합니다.
5. 1단계: 사용자 및 그룹 선택 - "***AWS-account-name***"에 사용자 및 그룹 할당 페이지에서 다음을 수행합니다.

   1. 사용자 탭에서 Single Sign-On 액세스를 허용할 사용자를 한 명 이상 선택합니다.

      결과를 필터링하려면 검색 상자에 원하는 사용자 이름을 순서대로 입력합니다.

   2. 그룹 탭에서 Single Sign-On 액세스를 허용할 하나 이상의 그룹을 선택합니다.

      결과를 필터링하려면 검색 상자에 원하는 그룹 이름을 순서대로 입력합니다.

   3. 선택한 사용자와 그룹을 표시하려면 선택한 사용자 및 그룹 옆에 있는 옆의 삼각형을 선택합니다.
   4. 올바른 사용자와 그룹이 선택되었는지 확인한 후 다음을 선택합니다.

6. 2단계: 권한 집합 선택의 경우 “***AWS-account-name***”에 권한 집합 할당페이지에서 다음 작업을 수행합니다.

   1. 하나 이상의 권한 집합을 선택합니다. 필요한 경우 새 권한 집합을 만들고 선택할 수 있습니다.
      - 기존 사용 권한 집합을 하나 이상 선택하려면 권한 집합에서 이전 단계에서 선택한 사용자 및 그룹에 적용할 사용 권한 집합을 선택합니다.

- 새 사용 권한 집합을 하나 이상 만들려면 사용 권한 집합 만들기를 선택하고 권한 집합을 생성합니다. 단계를 따릅니다. 적용하려는 권한 집합을 생성한 후 IAM Identity Center 콘솔에서 AWS 계정로 돌아가 2단계: 권한 집합 선택에 도달할 때까지 지침을 따릅니다. 이 단계에 도달하면 생성한 새 권한 집합을 선택하고 이 절차의 다음 단계를 진행합니다.

2. 올바른 권한 집합이 선택되었는지 확인한 후 다음을 선택합니다.

7. 3단계: 검토 및 제출의 경우 "***AWS-account-name***"에 대한 할당 검토 및 제출 페이지에서 다음을 수행합니다.

   1. 선택한 사용자, 그룹 및 권한 집합을 검토합니다.
   2. 올바른 사용자, 그룹 및 권한 집합이 선택되었는지 확인한 후 제출을 선택합니다.

> **Important**
>
> 사용자 및 그룹 할당 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 프로세스가 성공적으로 완료될 때까지 이 페이지를 열어둡니다.

> **Note**
>
> AWS Organizations 관리 계정에서 작업하려면 사용자 또는 그룹에 권한을 부여해야 할 수 있습니다. 권한이 높은 계정이므로 추가 보안 제한을 적용하려면 먼저 IAM FullAccess 정책 또는 이에 상응하는 권한이 있어야 설정할 수 있습니다. 조직의 구성원 AWS 계정에는 이러한 추가 보안 제한이 필요하지 않습니다.

사용자 및 그룹 액세스 제거

이 절차를 사용하여 연결된 디렉터리에 있는 한 명 이상의 사용자 및 그룹에 AWS 계정 대한 Single Sign-On 액세스를 제거하십시오.

에 대한 사용자 및 그룹 액세스를 제거하려면 AWS 계정

1. IAM Identity Center 콘솔을 엽니다.
2. 탐색 창의 다중 계정 권한에서 AWS 계정을 선택합니다.
3. AWS 계정 페이지에는 조직의 트리 뷰 목록이 표시됩니다. Single Sign-On 액세스를 제거하려는 사용자 및 그룹이 AWS 계정 포함된 이름을 선택합니다.

4. 에 대한 개요 페이지의 할당된 사용자 및 그룹에서 하나 이상의 사용자 또는 그룹 이름을 선택하고 액세스 제거를 선택합니다. AWS 계정
5. 액세스 제거 대화 상자에서 사용자 또는 그룹 이름이 올바른지 확인하고 액세스 제거를 선택합니다.

권한 집합으로 생성된 활성 IAM 역할 세션 취소

다음은 IAM Identity Center 사용자의 활성 권한 집합 세션을 취소하는 일반적인 절차입니다. 이 절차에서는 자격 증명을 도용한 사용자 또는 시스템에 있는 악의적인 행위자에 대한 모든 액세스 권한을 제거하려는 것으로 가정합니다. 전제 조건은 의 지침을 따랐어야 합니다. 권한 집합으로 생성된 활성 IAM 역할 세션을 취소할 준비를 하십시오. SCP (서비스 제어 정책) 에 모두 거부 정책이 있다고 가정합니다.

> **Note**
>
> AWS 콘솔 전용 작업을 제외한 모든 단계를 처리하도록 자동화를 구축할 것을 권장합니다.

1. 액세스 권한을 취소해야 하는 사람의 사용자 ID를 확보하세요. ID 저장소 API를 사용하여 사용자 이름으로 사용자를 찾을 수 있습니다.
2. 거부 정책을 업데이트하여 SCP (서비스 제어 정책) 1단계의 사용자 ID를 추가하세요. 이 단계를 완료하면 대상 사용자는 액세스 권한을 잃고 정책이 영향을 받는 역할에 대한 조치를 취할 수 없게 됩니다.
3. 사용자에 대한 모든 권한 집합 할당을 제거합니다. 그룹 구성원을 통해 액세스 권한이 할당된 경우 모든 그룹 및 모든 직접 사용 권한 집합 할당에서 사용자를 제거합니다. 이 단계에서는 사용자가 추가 IAM 역할을 맡을 수 없습니다. 활성 AWS 액세스 포털 세션을 갖고 있는 사용자에게 해당 사용자를 비활성화하면 액세스 권한을 제거할 때까지 새 역할을 계속 수임할 수 있습니다.
4. ID 공급자 (IdP) 또는 Microsoft Active Directory를 ID 소스로 사용하는 경우 ID 소스에서 사용자를 비활성화하십시오. 사용자를 비활성화하면 추가 AWS 액세스 포털 세션을 생성할 수 없습니다. IdP 또는 Microsoft Active Directory API 설명서를 사용하여 이 단계를 자동화하는 방법을 알아보십시오. IAM Identity Center 디렉터리를 ID 소스로 사용하는 경우 아직 사용자 액세스를 비활성화하지 마세요. 6단계에서 사용자 액세스를 비활성화합니다.
5. IAM Identity Center 콘솔에서 사용자를 찾아 활성 세션을 삭제합니다.

    a. 사용자를 선택하세요.

    b. 활성 세션을 삭제하려는 사용자를 선택합니다.

c. 사용자 세부 정보 페이지에서 활성 세션 탭을 선택합니다.

d. 삭제하려는 세션 옆의 확인란을 선택하고 세션 삭제를 선택합니다.

이렇게 하면 사용자의 AWS 액세스 포털 세션이 약 60분 이내에 중지됩니다. 세션 시간에 대해 알아보세요.

6. IAM ID 센터 콘솔에서 사용자 액세스를 비활성화합니다.

a. 사용자를 선택하세요.

b. 액세스를 비활성화하려는 사용자를 선택합니다.

c. 사용자의 세부 정보 페이지에서 일반 정보를 확장하고 사용자 액세스 비활성화 버튼을 선택하여 사용자가 더 이상 로그인하지 못하도록 합니다.

7. 거부 정책을 최소 12시간 동안 그대로 두십시오. 그렇지 않으면 활성 IAM 역할 세션을 가진 사용자가 IAM 역할을 사용하여 작업을 복원하게 됩니다. 12시간을 기다리면 활성 세션이 만료되고 사용자는 IAM 역할에 다시 액세스할 수 없게 됩니다.

> **Important**
>
> 사용자 세션을 중지하기 전에 사용자 액세스를 비활성화하면 (5단계를 완료하지 않고 6단계를 완료함), 더 이상 IAM Identity Center 콘솔을 통해 사용자 세션을 중지할 수 없습니다. 사용자 세션을 중지하기 전에 실수로 사용자 액세스를 비활성화한 경우 사용자를 다시 활성화하고 세션을 중지한 다음 액세스를 다시 비활성화할 수 있습니다.

이제 암호가 손상된 경우 사용자의 자격 증명을 변경하고 할당을 복원할 수 있습니다.

관리 계정의 사용자 및 그룹에 Single Sign-On 액세스 권한을 할당할 수 있는 사람을 위임합니다.

IAM Identity Center 콘솔을 사용하여 관리 계정에 Single Sign-on 액세스 권한을 할당하는 것은 권한 있는 작업입니다. 기본적으로 IAMFullAccess AWS 관리형 정책이 연결된 사용자 AWS 계정 루트 사용자 또는 한 명만 관리 계정에 AWSSSOMasterAccountAdministratorSingle Sign-On 액세스 권한을 할당할 수 있습니다. AWSSSOMasterAccountAdministrator및 IAMFullAccess정책은 조직 내 관리 계정에 대한 Single Sign-On 액세스를 관리합니다. AWS Organizations

다음 단계를 사용하여 디렉터리의 사용자 및 그룹에 Single Sign-On 액세스를 관리할 권한을 위임합니다.

디렉터리 내 사용자 및 그룹에 Single Sign-On 액세스를 관리할 수 있는 권한을 부여하려면

1. 관리 계정의 루트 사용자 또는 관리 계정에 대한 관리자 권한이 있는 다른 사용자로 IAM Identity Center 콘솔에 로그인합니다.
2. 권한 집합을 생성합니다. 단계에 따라 권한 집합을 생성한 후 다음을 수행합니다.

    1. 새 권한 집합 만들기 페이지에서 사용자 지정 권한 집합 만들기 확인란을 선택하고 다음: 세부 정보를 선택합니다.
    2. 새 권한 집합 만들기 페이지에서 사용자 지정 권한 집합의 이름과 설명(선택 사항)을 지정합니다. 필요한 경우 세션 기간을 수정하고 릴레이 상태 URL을 지정합니다.

    > **Note**
    >
    > 릴레이 상태 URL의 경우 AWS Management Console에 있는 URL을 지정해야 합니다. 예:
    > **`https://console.aws.amazon.com/ec2/`**
    > 자세한 내용은 릴레이 상태 설정 단원을 참조하세요.

    3. 권한 집합에 포함하려는 정책은 무엇인가요?, AWS 관리형 정책 연결 확인란을 선택합니다.
    4. IAM 정책 목록에서 AWSSSOMasterAccountAdministrator정책과 IAMFullAccess AWS 관리형 정책을 모두 선택합니다. 이러한 정책은 향후 이 권한 집합에 대한 액세스 권한이 할당된 모든 사용자 및 그룹에 권한을 부여합니다.
    5. 다음: 태그를 선택합니다.
    6. 태그 추가(선택 사항)에서 키 및 값(선택 사항)의 값을 지정하고 다음: 검토를 선택합니다. 태그에 대한 자세한 내용은 AWS IAM Identity Center 리소스에 태그 지정 단원을 참조하세요.
    7. 선택 사항을 검토한 후 생성을 선택합니다.
3. 사용자에게 액세스 권한을 할당하십시오. AWS 계정의 단계에 따라 방금 만든 권한 집합에 적절한 사용자와 그룹을 할당합니다.
4. 할당된 사용자에게 다음을 알리십시오. 할당된 사용자는 AWS 액세스 포털에 로그인하고 계정 탭을 선택할 때 방금 위임한 권한으로 인증받을 적절한 역할 이름을 선택해야 합니다.

권한 세트

권한 세트는 하나 이상의 IAM 정책 컬렉션을 정의하는 템플릿으로, 생성 및 유지 관리하는 템플릿입니다. 권한 집합은 기관 내 사용자 및 그룹에 대한 AWS 계정 접근 권한 할당을 단순화합니다. 예를 들어 AWS RDS, DynamoDB 및 Aurora 서비스를 관리하기 위한 정책이 포함된 데이터베이스 관리자 권한

집합을 생성하고 이 단일 권한 집합을 사용하여 데이터베이스 관리자에게 조직 내 AWS 계정 대상 목록에 대한 액세스 권한을 부여할 수 있습니다.AWS

IAM Identity Center는 권한 집합이 있는 하나 이상의 사용자 또는 그룹에 액세스 권한을 할당합니다. AWS 계정 권한 세트를 할당하면 IAM Identity Center가 각 계정에 해당되는 IAM Identity Center 제어 역할을 생성하고 권한 세트에 지정된 정책을 해당 역할에 연결합니다. IAM Identity Center는 역할을 관리하고, IAM Identity Center 사용자 포털 또는 AWS CLI를 사용하여 사용자가 정의한 인증된 사용자가 역할을 수임하도록 허용합니다. 권한 세트를 수정하면 IAM Identity Center에서 해당 IAM 정책 및 역할이 그에 따라 업데이트되도록 합니다.

권한 세트에 AWS 관리형 정책, 고객 관리형 정책, 인라인 정책, 직무 역할에 대한AWS 관리형 정책을 추가할 수 있습니다. AWS 관리형 정책 또는 고객 관리형 정책을 권한 경계로 할당할 수도 있습니다.

권한 세트를 생성하려면 권한 세트 생성, 관리 및 삭제을 참조하세요.

주제

- 사전 정의된 권한
- 사용자 지정 권한
- 권한 세트 생성, 관리 및 삭제
- 권한 집합 속성을 구성합니다.

사전 정의된 권한

관리형 정책을 사용하여 사전 정의된 권한 세트를 생성할 수 있습니다. AWS

사전 정의된 권한으로 사용 권한 집합을 만들 때는 AWS 관리형 정책 목록에서 정책 하나를 선택합니다. 사용 가능한 정책 내에서 일반 권한 정책 및 직무 정책 중에서 선택할 수 있습니다.

일반 권한 정책

전체 AWS 계정리소스에 액세스할 수 있게 해주는 AWS 관리형 정책 목록에서 선택하세요. 다음 정책 중 한 가지를 추가할 수 있습니다.

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

직무 정책

조직 내 업무와 관련이 있을 수 있는 리소스에 액세스할 수 AWS 계정 있는 AWS 관리형 정책 목록에서 선택하세요. 다음 정책 중 한 가지를 추가할 수 있습니다.

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

사용 가능한 일반 권한 정책 및 직무 정책의 목록과 설명은 AWS Identity and Access Management IAM 사용 설명서의 직무 역할에 대한AWS 관리형 정책을 참조하세요.

권한 세트를 생성하는 방법에 대한 지침은 권한 세트 생성, 관리 및 삭제을 참조하세요.

사용자 지정 권한

IAM AWS Identity and Access Management () 에 있는 AWS 관리형 및 고객 관리형 정책을 인라인 정책과 결합하여 사용자 지정 권한으로 권한 집합을 만들 수 있습니다. 또한 권한 경계를 포함하여 다른 정책이 해당 권한 집합의 사용자에게 부여할 수 있는 최대 권한을 설정할 수 있습니다.

권한 세트를 생성하는 방법에 대한 지침은 권한 세트 생성, 관리 및 삭제을 참조하세요.

권한 세트에 연결할 수 있는 정책 유형

주제

- 인라인 정책
- AWS 관리형 정책
- 고객 관리형 정책
- 권한 경계

인라인 정책

권한 세트에 인라인 정책을 연결할 수 있습니다. 인라인 정책은 권한 세트에 직접 추가하는 IAM 정책 형식의 텍스트 블록입니다. 정책을 붙여 넣거나 새 권한 세트를 생성할 때 IAM Identity Center 콘솔의

정책 생성 도구를 사용하여 새 정책을 생성할 수 있습니다. AWS 정책 생성기를 사용하여 IAM 정책을 생성할 수도 있습니다.

인라인 정책을 사용하여 권한 집합을 배포하면 IAM Identity Center는 권한 집합을 할당한 AWS 계정 위치에 IAM 정책을 생성합니다. IAM Identity Center는 계정에 권한 세트를 할당할 때 정책을 생성합니다. 그러면 해당 정책이 사용자가 AWS 계정 위임하는 IAM 역할에 연결됩니다.

인라인 정책을 생성하고 권한 집합을 할당하면 IAM Identity Center에서 정책을 자동으로 구성합니다. AWS 계정 를 사용하여 권한 집합을 구축할 고객 관리형 정책 경우 권한 집합을 할당하기 전에 정책을 AWS 계정 직접 생성해야 합니다.

AWS 관리형 정책

권한 집합에 AWS 관리형 정책을 추가할 수 있습니다. AWS 관리형 정책은 AWS 유지 관리하는 IAM 정책입니다. 반대로 고객 관리형 정책 계정에 IAM 정책을 생성하고 유지 관리하는 정책이 있습니다. AWS 관리형 정책은 사용자의 일반적인 최소 권한 사용 사례를 다룹니다. AWS 계정 IAM Identity Center에서 생성한 역할에 대한 권한으로 AWS 관리형 정책을 할당하거나 권한 경계로 할당할 수 있습니다.

AWS 리소스에 작업별 액세스 권한을 할당하는 직무에 대한AWS 관리형 정책을 유지 관리합니다. AWS 권한 세트와 함께 사전 정의된 권한을 사용하도록 선택한 경우 직무 정책 하나를 추가할 수 있습니다. 사용자 지정 권한을 선택하면 두 개 이상의 직무 정책을 추가할 수 있습니다.

AWS 계정 또한 특정 정책 AWS 서비스 및 조합에 대한 다수의 AWS 관리형 IAM 정책이 포함되어 있습니다. AWS 서비스사용자 지정 권한으로 권한 집합을 생성할 경우 많은 추가 AWS 관리형 정책 중에서 선택하여 권한 집합에 할당할 수 있습니다.

AWS 모든 항목을 AWS 관리형 AWS 계정 정책으로 채웁니다. AWS 관리형 정책이 포함된 권한 집합을 배포하기 위해 먼저 정책을 생성할 필요는 없습니다. AWS 계정로 권한 집합을 구축하는 고객 관리형 정책 경우 권한 집합을 할당하기 전에 정책을 AWS 계정 직접 만들어야 합니다.

AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하십시오.

고객 관리형 정책

권한 세트에 고객 관리형 정책을 추가할 수 있습니다. 고객 관리형 정책은 자신의 계정에서 생성 및 관리하는 IAM 정책입니다. 반대로 계정의 IAM 정책은 유지 AWS 관리형 정책 관리됩니다. AWS IAM Identity Center에서 생성한 역할에 대한 권한으로 고객 관리형 정책을 할당하거나 권한 경계로 할당할 수 있습니다.

고객 관리형 정책을 사용하여 권한 집합을 생성할 때는 IAM Identity Center에서 권한 집합을 AWS 계정 할당하는 각 권한 집합에 동일한 이름과 경로를 사용하여 IAM 정책을 생성해야 합니다. 사용자 지정 경로를 지정하는 경우 각 AWS 계정에 동일한 경로를 지정해야 합니다. 자세한 내용을 알아보려면 IAM 사용 설명서의 표시 이름 및 경로를 참조하세요. IAM Identity Center는 AWS 계정에 IAM 정책을 생성한 IAM 역할에 연결합니다. 가장 좋은 방법은 권한 세트를 할당하는 각 계정의 정책에 동일한 권한을 적용하는 것입니다. 자세한 정보는 권한 집합에서 IAM 정책 사용을 참조하세요.

자세한 내용은 IAM 사용 설명서의 고객 관리형 정책을 참조하세요.

권한 경계

권한 세트에 권한 경계를 추가할 수 있습니다. 권한 경계는 ID 기반 정책이 IAM 보안 주체에 부여할 수 있는 최대 권한을 설정하는 관리형 또는 고객 관리형 IAM 정책입니다. AWS 권한 경계를 적용하면 인라인 정책, 고객 관리형 정책 및 AWS 관리형 정책에게는 권한 경계에서 허용한 권한을 초과하는 권한을 부여할 수 없습니다. 권한 경계는 어떤 권한도 허용하지 않고 대신 IAM이 경계 밖의 모든 권한을 무시하도록 만듭니다.

권한 경계로 고객 관리형 정책을 사용하여 권한 세트를 생성할 때는 IAM Identity Center에서 권한 집합을 할당하는 각 AWS 계정 에 동일한 이름을 사용하여 IAM 정책을 생성해야 합니다. IAM Identity Center는 AWS 계정 에 생성한 IAM 역할에 권한 경계로 IAM 정책을 연결합니다.

자세한 내용은 IAM 사용 설명서의 IAM 개체에 대한 권한 경계를 참조하세요.

권한 세트 생성, 관리 및 삭제

권한 집합은 사용자와 그룹이 AWS 계정에 대해 보유할 수 있는 액세스 수준을 정의합니다. 권한 집합은 IAM Identity Center에 저장되며 하나 이상의 AWS 계정에 프로비저닝할 수 있습니다. 한 사용자에게 두 개 이상의 권한 집합을 할당할 수 있습니다. 권한 집합 및 IAM Identity Center에서 권한 집합을 사용하는 방법에 대한 자세한 내용은 권한 세트 단원을 참조하세요.

권한 세트를 생성할 때 고려할 사항:

- 사전 정의된 권한 세트로 시작

  사전 정의된 권한을 사용하는 사전 정의된 권한 집합을 사용하면 사용 가능한 정책 목록에서 단일 AWS 관리형 정책을 선택할 수 있습니다. 각 정책은 AWS 서비스 및 리소스에 대한 특정 수준의 액세스 권한 또는 공통 직무에 대한 권한을 부여합니다. 각 정책에 대한 자세한 내용은 직무 역할에 대한 AWS 관리형 정책을 참조하세요. 사용 데이터를 수집한 후 권한 세트를 더 제한적으로 조정할 수 있습니다.

- 관리 세션 지속 시간을 합리적인 작업 기간으로 제한

  사용자가 AWS 관리 콘솔 또는AWS CLI (AWS 명령줄 인터페이스) 에 통합하여 사용하는 경우 IAM Identity Center는 권한 세트의 세션 기간 설정을 사용하여 세션 기간을 제어합니다. AWS 계정 사용자 세션이 세션 지속 시간에 도달하면 콘솔에서 로그아웃되고 다시 로그인하라는 메시지가 표시됩니다. 보안 모범 사례로 세션 지속 시간을 역할을 수행하는 데 필요한 길이보다 길게 설정하지 않는 것이 좋습니다. 기본적으로 세션 지속 시간 값은 1시간입니다. 최대 12시간까지 값을 지정할 수 있습니다. 자세한 정보는 세션 기간 설정을 참조하세요.

- 직원 사용자 포털 세션 지속 시간 제한

  직원 사용자는 포털 세션을 사용하여 역할을 선택하고 애플리케이션에 액세스합니다. 직원 사용자가 재인증을 받기 전에 AWS 액세스 포털에 로그인할 수 있는 시간을 결정하는 최대 세션 지속 시간 값은 기본적으로 8시간입니다. 최대 90일까지 값을 지정할 수 있습니다. 자세한 정보는 AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간을 구성합니다.을 참조하세요.

- 최소 권한을 제공하는 역할 사용

  생성하여 사용자에게 할당한 각 권한 집합은 AWS 액세스 포털에서 사용 가능한 역할로 표시됩니다. 해당 사용자로 포털에 로그인할 때는 계정에서 작업을 수행하는 데 사용할 수 있는 가장 제한적인 권한 세트에 해당하는 역할을 대신 `AdministratorAccess`를 선택하세요. 사용자 초대를 보내기 전에 권한 세트를 테스트하여 필요한 액세스 권한을 제공하는지 확인합니다.

> **Note**
>
> 또는 AWS CloudFormation을 사용하여 권한 세트를 생성 및 할당하고 해당 권한 세트에 사용자를 할당할 수 있습니다.

주제

- 권한 집합을 생성합니다.
- 권한 집합 관리 위임
- 권한 집합에서 IAM 정책 사용
- 권한 집합을 삭제합니다.

권한 집합을 생성합니다.

이 절차를 사용하여 단일 AWS 관리형 정책을 사용하는 사전 정의된 권한 집합이나 최대 10개의 AWS 관리형 또는 고객 관리형 정책과 인라인 정책을 사용하는 사용자 지정 권한 집합을 생성할 수 있습니다. IAM용 Service Quotas 콘솔에서 최대 10개 정책에 대한 조정을 요청할 수 있습니다.

IAM Identity Center 콘솔에서 권한 집합을 생성할 수 있습니다.

권한 집합을 생성하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한 아래에서 권한 집합을 선택합니다.
3. 권한 집합 생성을 선택합니다.
4. 권한 집합 유형 선택 페이지의 권한 집합 유형에서 권한 집합 유형을 선택합니다.
5. 권한 집합 유형에 따라 사용 권한 집합에 사용할 정책을 하나 이상 선택합니다.

   - 사전 정의된 권한 집합
     1. 미리 정의된 권한 집합에 대한 정책에서 목록에 있는 IAM Job 기능 정책 또는 일반 권한 정책 중 하나를 선택하고 다음을 선택합니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
     2. 6단계로 이동하여 권한 집합 세부 정보 지정 페이지를 완료하십시오.
   - 사용자 지정 권한 집합
     1. 다음을 선택합니다.
     2. 정책 및 권한 경계 지정 페이지에서 새 권한 집합에 적용할 IAM 정책 유형을 선택합니다. 기본적으로 최대 10개의 AWS 관리형 정책과 고객 관리형 정책을 원하는 대로 조합하여 권한 집합에 추가할 수 있습니다. 이 할당량은 IAM에서 설정합니다. 이를 높이려면 권한 집합을 할당하려는 각 AWS 계정 의 Service Quotas 콘솔에서 IAM 역할에 연결된 IAM 할당량 관리형 정책을 늘려달라고 요청합니다.
        - AWS 관리형 정책을 확장하여 AWS 구축 및 유지 관리하는 IAM의 정책을 추가하세요. 자세한 정보는 AWS 관리형 정책을 참조하세요.
          a. 권한 집합에서 사용자에게 적용할 AWS 관리형 정책을 검색하여 선택합니다.
          b. 다른 유형의 정책을 추가하려면 해당 컨테이너를 선택합니다. 적용하려는 정책을 모두 선택했으면 다음을 선택합니다. 6단계로 이동하여 권한 세트 세부 정보 지정 페이지를 완료하십시오.

- 고객 관리형 정책을 확장하여 구축 및 유지 관리하는 IAM의 정책을 추가합니다. 자세한 내용은 고객 관리형 정책 단원을 참조하세요.

  a. 정책 연결를 선택하고 권한 집합에 추가하려는 정책의 이름을 입력합니다. 권한 집합을 할당하려는 각 계정에서 입력한 이름으로 정책을 생성합니다. 가장 좋은 방법은 각 계정의 정책에 동일한 권한을 할당하는 것입니다.

  b. 다른 정책을 추가하려면 정책 연결을 선택합니다.

  c. 다른 유형의 정책을 추가하려면 해당 컨테이너를 선택합니다. 적용하려는 정책을 모두 선택했으면 다음을 선택합니다. 6단계로 이동하여 권한 집합 세부 정보 지정 페이지를 완료하십시오.

- 인라인 정책을 확장하여 JSON 형식의 사용자 지정 정책 텍스트를 추가합니다. 인라인 정책이 기존 IAM 리소스와 일치하지 않습니다. 인라인 정책을 생성하려면 제공된 양식에 사용자 지정 정책 언어를 입력합니다. IAM Identity Center는 멤버 계정에서 생성하는 IAM 리소스에 정책을 추가합니다. 자세한 정보는 인라인 정책을 참조하세요.

  a. 대화형 편집기 내에서 원하는 작업과 리소스를 인라인 정책에 추가합니다. 새 명령문 추가를 사용하여 추가 설명을 추가할 수 있습니다.

  b. 다른 유형의 정책을 추가하려면 해당 컨테이너를 선택합니다. 적용하려는 정책을 모두 선택했으면 다음을 선택합니다. 6단계로 이동하여 권한 집합 세부 정보 지정 페이지를 완료하십시오.

- 권한 범위를 확장하여 AWS 관리형 또는 고객 관리형 IAM 정책을 권한 집합의 다른 정책이 할당할 수 있는 최대 권한으로 추가합니다. 자세한 정보는 권한 경계을 참조하세요.

  a. 최대 권한을 제어하려면 권한 경계 사용 을 선택합니다.

  b. AWS 관리형 정책을 선택하여 권한 경계로 AWS가 구축 및 유지 관리하는 IAM의 정책을 설정합니다. 사용자 관리형 정책을 선택하여 IAM에서 정책을 설정하고 이를 권한 경계로 구축하고 유지 관리합니다.

  c. 다른 유형의 정책을 추가하려면 해당 컨테이너를 선택합니다. 적용하려는 정책을 모두 선택했으면 다음을 선택합니다. 6단계로 이동하여 권한 집합 세부 정보 지정 페이지를 완료하십시오.

6. 권한 집합 세부정보 지정 페이지에서 다음 작업을 수행합니다.

   1. 권한 집합 이름 아래에 IAM Identity Center의 이 권한 집합을 식별하는 이름을 입력합니다. 이 권한 집합에 지정한 이름은 AWS 액세스 포털에서 사용 가능한 역할로 표시됩니다. 사용자는 AWS 액세스 포털에 로그인하고 원하는 역할을 AWS 계정선택한 다음 역할을 선택합니다.
   2. (선택 사항) 또한 설명을 추가할 수도 있습니다. 설명은 IAM Identity Center 콘솔에만 표시되며 AWS 액세스 포털에는 표시되지 않습니다.

3. (선택 사항) 세션 기간 값을 지정합니다. 이 값은 콘솔이 세션에서 로그아웃하기 전에 사용자가 로그온할 수 있는 시간을 결정합니다. 자세한 내용은 세션 기간 설정 단원을 참조하세요.
4. (선택 사항) 릴레이 상태 값을 지정합니다. 이 값은 페더레이션 프로세스 중 계정 내에서 사용자를 리디렉션하는 데 사용됩니다. 자세한 정보는 릴레이 상태 설정을 참조하세요.

> **Note**
>
> 릴레이 상태 URL은 AWS Management Console범위 내에 있어야 합니다. 예: **`https://console.aws.amazon.com/ec2/`**

5. 태그(선택 사항)를 확장하고 태그 추가를 선택한 다음 키 및 값(선택 사항) 의 값을 지정합니다.

   태그에 대한 자세한 내용은 AWS IAM Identity Center 리소스에 태그 지정 단원을 참조하세요.
6. 다음을 선택합니다.

7. 검토 및 생성 페이지에서 선택한 내용을 검토한 다음 생성을 선택합니다.
8. 기본적으로 권한 집합을 생성할 때 권한 집합은 프로비저닝되지 않습니다 (어느 곳에서나 사용됨). AWS 계정에서 권한 세트를 프로비전하려면 계정의 사용자 및 그룹에 IAM Identity Center 액세스 권한을 할당한 다음 해당 사용자 및 그룹에 권한 세트를 적용해야 합니다. AWS 계정자세한 정보는 싱글 사인온 액세스: AWS 계정을 참조하세요.

권한 집합 관리 위임

IAM Identity Center를 사용하면 IAM Identity Center 리소스의 Amazon 리소스 이름(ARN)을 참조하는 IAM 정책을 생성하여 계정의 권한 집합 및 할당 관리를 위임할 수 있습니다. 예를 들어, 여러 관리자가 특정 태그가 있는 권한 집합에 대해 지정된 계정의 할당을 관리할 수 있도록 정책을 생성할 수 있습니다.

다음 방법 중 하나를 사용하여 이러한 유형의 정책을 생성할 수 있습니다.

- (권장) IAM Identity Center에서 각각 다른 정책을 사용하여 권한 집합을 생성하고 이 권한 집합을 다른 사용자 또는 그룹에 할당합니다. 이렇게 하면 선택한 IAM Identity Center ID 소스를 사용하여 로그인하는 사용자의 관리자 권한을 관리할 수 있습니다.
- IAM에서 사용자 지정 정책을 생성한 다음 이를 관리자가 수임하는 IAM 역할에 연결합니다. 역할에 대한 자세한 내용은 할당된 IAM Identity Center 관리 권한을 얻기 위한 IAM 역할을 참조하세요.

> **Important**
>
> IAM Identity Center 리소스 ARN은 대소문자를 구분합니다.

다음은 IAM Identity Center 권한 집합 및 계정 리소스 유형을 참조하는 적절한 경우를 보여줍니다.

리소스 유형	ARN	컨텍스트 키
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`
계정	`arn:${Partition}:sso:::account/${AccountId}`	해당 사항 없음

권한 집합에서 IAM 정책 사용

권한 집합을 생성합니다.에서는 고객 관리형 정책 및 권한 경계를 비롯한 정책을 권한 집합에 추가하는 방법을 배웠습니다. 고객 관리형 정책 및 권한을 권한 집합에 추가할 때 IAM Identity Center는 어떤 AWS 계정에도 정책을 생성하지 않습니다. 대신 권한 집합을 할당하려는 각 계정에서 이러한 정책을 미리 만들어 권한 집합의 이름 및 경로 사양과 일치시켜야 합니다. 조직 내 사용자에게 권한 세트를 할당하면 IAM Identity AWS 계정 Center에서 AWS Identity and Access Management (IAM) 역할을 생성하고 IAM 정책을 해당 역할에 연결합니다.

> **Note**
>
> IAM 정책을 사용하여 권한 집합을 할당하기 전에 먼저 멤버 계정을 준비해야 합니다. 멤버 계정의 IAM 정책 이름은 관리 계정의 정책 이름과 대소문자를 구분하여 일치해야 합니다. 멤버 계정에 정책이 없는 경우 IAM Identity Center에서 권한 집합을 할당하지 못합니다.
> 정책에서 부여하는 권한이 계정 간에 정확히 일치할 필요는 없습니다.

권한 집합에 IAM 정책을 할당하려면

1. 권한 집합을 할당하려는 각 AWS 계정 위치에 IAM 정책을 생성합니다.

2. IAM 정책에 권한을 할당합니다. 계정마다 다른 권한을 할당할 수 있습니다. 일관된 경험을 위해 각 정책에서 동일한 권한을 구성하고 유지합니다. 예를 들어 자동화 리소스를 사용하여 각 구성원 계정에서 동일한 이름과 권한을 가진 IAM 정책의 사본을 만들 수 있습니다. AWS CloudFormation StackSets 에 대한 CloudFormation StackSets 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation StackSets 작업하기를 참조하십시오.
3. 관리 계정에서 권한 집합을 생성하고 고객 관리형 정책 또는 권한 경계 아래에 IAM 정책을 추가합니다. 권한 집합을 생성하는 방법에 대한 자세한 내용은 권한 집합을 생성합니다.을 참조하세요.
4. 준비한 인라인 정책, AWS 관리형 정책 또는 추가 IAM 정책을 추가합니다.
5. 권한 집합을 생성하고 할당합니다.

권한 집합을 삭제합니다.

활성 권한 집합 세션을 취소하려면 을 참조하십시오. 권한 집합으로 생성된 활성 IAM 역할 세션 취소

IAM Identity Center에서 권한 집합을 삭제하려면 먼저 해당 권한 집합을 사용하는 모든 AWS 계정 에서 권한 집합을 제거해야 합니다. 기존 사용자 및 그룹 액세스를 확인하려면 을 참조하십시오. 사용자 및 그룹 할당 보기

에서 권한 세트를 제거하려면 AWS 계정

1. IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한에서 AWS 계정를 선택합니다.
3. AWS 계정 페이지에는 조직의 트리 뷰 목록이 표시됩니다. 권한 집합을 AWS 계정 제거하려는 권한 집합의 이름을 선택합니다.
4. 의 개요 페이지에서 사용 권한 집합 탭을 선택합니다. AWS 계정
5. 제거할 권한 집합 옆에 있는 확인란을 선택한 다음 제거를 선택합니다.
6. 권한 집합 제거 대화 상자에서 올바른 권한 집합이 선택되었는지 확인하고, **`Delete`**를 입력하여 제거를 확인한 다음, 액세스 제거를 선택합니다.

다음 절차에 따라 조직 AWS 계정 내에서 더 이상 사용할 수 없도록 하나 이상의 권한 집합을 삭제하십시오.

> **Note**
>
> 이 사용 권한 집합을 할당받은 모든 사용자와 그룹은 사용 권한에 관계없이 AWS 계정 더 이상 로그인할 수 없습니다. 기존 사용자 및 그룹 액세스를 확인하려면 을 참조하십시오사용자 및 그룹 할당 보기.

에서 권한 세트를 삭제하려면 AWS 계정

1. IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한 아래에서 권한 집합을 선택합니다.
3. 삭제하려는 권한 집합을 선택하고 삭제를 선택합니다.
4. 권한 집합 삭제 대화 상자에서 권한 집합의 이름을 입력하여 삭제를 확인한 다음 삭제를 선택합니다. 이름은 대/소문자를 구분합니다.

권한 집합 속성을 구성합니다.

IAM Identity Center에서 다음과 같은 권한 집합 속성을 구성하여 사용자 환경을 사용자 지정할 수 있습니다.

주제

- 세션 기간 설정
- 릴레이 상태 설정
- 거부 정책을 사용하여 활성 사용자 권한을 취소할 수 있습니다.

세션 기간 설정

각 권한 집합에 대해 세션 기간을 지정하여 사용자가 AWS 계정에 로그인할 수 있는 시간을 제어할 수 있습니다. 지정된 기간이 경과하면 사용자를 AWS 세션에서 로그아웃합니다.

새 권한 집합을 만들면 기본적으로 세션 지속 시간이 1시간(초)으로 설정됩니다. 최소 세션 지속 시간은 1시간이며 최대 12시간으로 설정할 수 있습니다. IAM Identity Center는 각 권한 집합에 대해 할당된 각 계정에 IAM 역할을 자동으로 생성하고 이러한 역할을 최대 세션 지속 시간이 12시간으로 구성되도록 구성합니다.

사용자가 AWS 계정 콘솔로 페더레이션하거나 AWS Command Line Interface (AWS CLI) 를 사용하는 경우 IAM Identity Center는 권한 세트의 세션 기간 설정을 사용하여 세션 기간을 제어합니다. 기본적으

로 IAM Identity Center에서 권한 집합에 대해 생성한 IAM 역할은 IAM Identity Center 사용자만 맡을 수 있으므로 IAM Identity Center 권한 집합에 지정된 세션 기간이 적용되도록 보장합니다.

> **Important**
>
> 보안 모범 사례로 세션 지속 시간을 역할을 수행하는 데 필요한 길이보다 길게 설정하지 않는 것이 좋습니다.

사용 권한 집합을 만든 후 이를 업데이트하여 새 세션 기간을 적용할 수 있습니다. 다음 절차에 따라 사용 권한 집합의 세션 기간 길이를 수정합니다.

세션 기간을 설정하려면

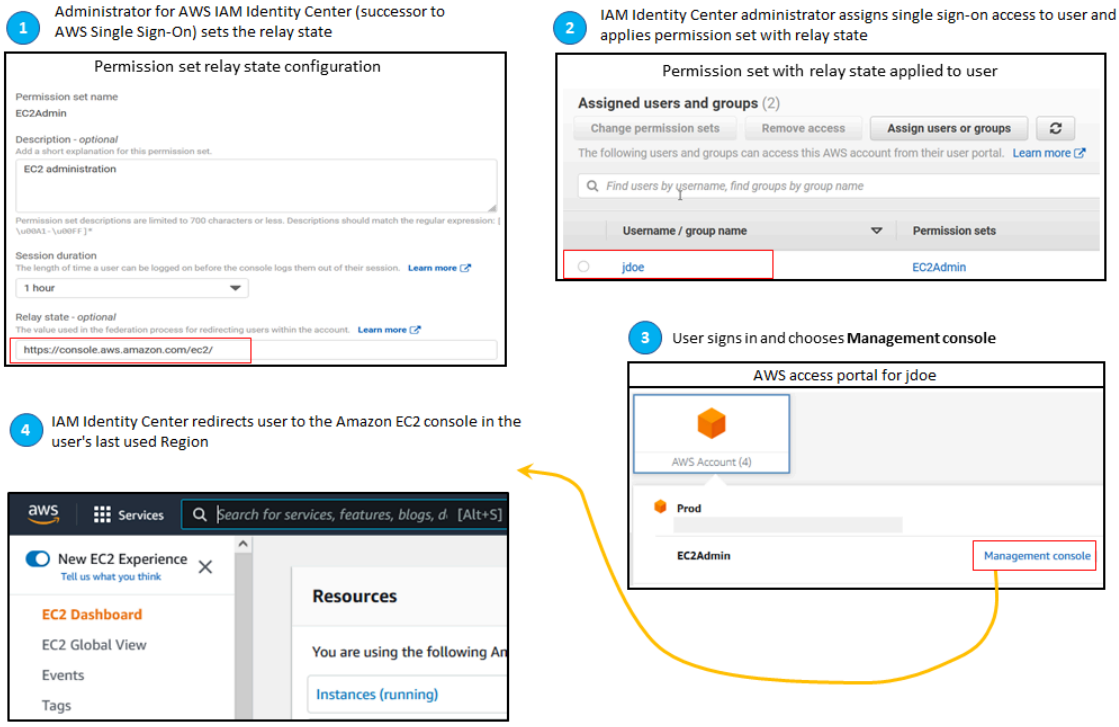
1. IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한 아래에서 권한 집합을 선택합니다.
3. 세션 기간을 변경하려는 사용 권한 집합의 이름을 선택합니다.
4. 권한 집합의 세부 정보 페이지에서 일반 설정 섹션 제목 오른쪽에 있는 편집을 선택합니다.
5. 일반 사용 권한 집합 설정 편집 페이지에서 세션 기간의 새 값을 선택합니다.
6. 권한 집합이 어떤 AWS 계정형태로든 프로비저닝된 경우 계정 이름이 자동으로 재프로비저닝 목록에 표시됩니다.AWS 계정 권한 집합의 세션 기간 값이 업데이트되면 해당 권한 집합을 사용하는 모든 AWS 계정 사용자가 다시 프로비전됩니다. 즉, 이 설정의 새 값은 해당 권한 집합을 사용하는 모든 AWS 계정 사용자에게 적용됩니다.
7. 변경 사항 저장을 선택합니다.
8. AWS 계정 페이지 상단에 알림이 표시됩니다.

    - 권한 집합이 하나 이상 AWS 계정에 프로비전된 경우 해당 AWS 계정 이 성공적으로 재프로비전되었으며 업데이트된 권한 집합이 계정에 적용되었음을 알리는 알림이 표시됩니다.
    - 사용 권한 집합이 에서 제공되지 않은 경우 해당 권한 집합의 설정이 업데이트되었음을 알리는 알림이 표시됩니다. AWS 계정

릴레이 상태 설정

기본적으로 사용자가 AWS 액세스 포털에 로그인하고 계정을 선택한 다음 할당된 권한 집합에서 AWS 생성하는 역할을 선택하면 IAM Identity Center는 사용자의 브라우저를 로 리디렉션합니다. AWS Management Console릴레이 상태를 다른 콘솔 URL로 설정하여 이 동작을 변경할 수 있습니다. 릴레

이 상태를 설정하면 사용자가 자신의 역할에 가장 적합한 콘솔에 빠르게 액세스할 수 있습니다. 예를 들어, 사용자가 Amazon EC2 관리자 역할을 선택할 때 해당 콘솔로 리디렉션하도록 릴레이 상태를 Amazon EC2 콘솔 URL(**`https://console.aws.amazon.com/ec2/`**)로 설정할 수 있습니다. 기본 URL 또는 릴레이 상태 URL로 리디렉션하는 동안 IAM Identity Center는 사용자의 브라우저를 사용자가 마지막으로 사용한 콘솔 엔드포인트로 라우팅합니다. AWS 리전 예를 들어, 사용자가 유럽(스톡홀름) 리전(eu-north-1)에서 마지막 콘솔 세션을 종료한 경우 사용자는 해당 리전의 Amazon EC2 콘솔로 리디렉션됩니다.



사용자를 특정 AWS 리전의 콘솔로 리디렉션하도록 IAM Identity Center를 구성하려면 URL의 일부로 리전 사양을 포함합니다. 예를 들어 사용자를 미국 동부(오하이오) 리전(us-east-2)에서 Amazon EC2 콘솔로 리디렉션하려면 해당 리전(**`https://us-east-2.console.aws.amazon.com/ec2/`**)에서 Amazon EC2 콘솔의 URL을 지정합니다. 미국 서부(오레곤) 리전(us-west-2)에서 IAM Identity Center를 활성화하고 사용자를 해당 리전으로 안내하려는 경우 **`https://us-west-2.console.aws.amazon.com`**을 지정합니다.

다음 절차에 따라 권한 집합에 대한 릴레이 상태 URL을 구성합니다.

릴레이 상태를 구성하려면

1. IAM Identity Center 콘솔을 엽니다.

2. 다중 계정 권한 아래에서 권한 집합을 선택합니다.
3. 새 릴레이 상태 URL을 설정하려는 권한 집합의 이름을 선택합니다.
4. 권한 집합의 세부 정보 페이지에서 일반 설정 섹션 제목 오른쪽에 있는 편집을 선택합니다.
5. 일반 권한 집합 설정 편집 페이지의 릴레이 상태에서 모든 서비스의 콘솔 URL을 입력합니다. AWS 예:

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > 릴레이 상태 URL은 AWS Management Console범위 내에 있어야 합니다.

6. 권한 집합이 어떤 AWS 계정형태로든 프로비전된 경우 계정 이름이 자동으로 다시AWS 계정 프로비전되도록 표시됩니다. 권한 집합의 릴레이 상태 URL이 업데이트되면 해당 권한 집합을 사용하는 모든 AWS 계정 사용자가 다시 프로비전됩니다. 즉, 이 설정의 새 값은 해당 권한 집합을 사용하는 모든 AWS 계정 사용자에게 적용됩니다.
7. 변경 사항 저장를 선택합니다.
8. AWS 조직 페이지 상단에 알림이 표시됩니다.

   - 권한 집합이 하나 이상 AWS 계정에 프로비전된 경우 해당 AWS 계정 이 성공적으로 재프로비전되었으며 업데이트된 권한 집합이 계정에 적용되었음을 알리는 알림이 표시됩니다.
   - 사용 권한 집합이 에서 제공되지 않은 경우 해당 권한 집합의 설정이 업데이트되었음을 알리는 알림이 표시됩니다. AWS 계정

> **Note**
>
> AWS API, AWS SDK 또는 () 를 사용하여 이 프로세스를 자동화할 수 있습니다. AWS Command Line InterfaceAWS CLI자세한 내용은 다음을 참조하세요.
>
> - IAM Identity Center API 참조의 `CreatePermissionSet` 또는 `UpdatePermissionSet` 작업
> - AWS CLI 명령 참조의 sso-admin 섹션의 `create-permission-set` or `update-permission-set` 명령.

거부 정책을 사용하여 활성 사용자 권한을 취소할 수 있습니다.

사용자가 권한 세트를 적극적으로 사용하는 AWS 계정 동안에는 IAM Identity Center 사용자의 액세스를 취소해야 할 수 있습니다. 지정되지 않은 사용자에 대해 미리 거부 정책을 구현하여 활성 IAM 역할 세션을 사용하지 못하게 할 수 있습니다. 그런 다음 필요한 경우 거부 정책을 업데이트하여 액세스를 차단하려는 사용자를 지정할 수 있습니다. 이 항목에서는 거부 정책을 생성하는 방법과 정책을 배포하는 방법에 대한 고려 사항에 대해 설명합니다.

권한 집합으로 생성된 활성 IAM 역할 세션을 취소할 준비를 하십시오.

서비스 제어 정책을 사용하여 특정 사용자에 대해 모두 거부 정책을 적용하여 사용자가 현재 사용 중인 IAM 역할로 작업을 수행하지 못하도록 할 수 있습니다. 또한 암호를 변경할 때까지 사용자가 권한 세트를 사용하지 못하도록 하여 악의적인 공격자가 훔친 자격 증명을 적극적으로 악용하는 것을 방지할 수 있습니다. 액세스를 광범위하게 거부하고 사용자가 권한 집합을 다시 입력하거나 다른 권한 집합에 접근하는 것을 방지해야 하는 경우 모든 사용자 액세스를 제거하고 Active AWS Access Portal 세션을 중지하고 사용자 로그인을 비활성화할 수도 있습니다. 광범위한 액세스 취소를 위한 추가 조치와 함께 거부 정책을 사용하는 방법을 권한 집합으로 생성된 활성 IAM 역할 세션 취소 알아보려면 을 참조하십시오.

거부 정책

IAM Identity Center ID 저장소의 사용자 조건과 일치하는 거부 정책을 사용하여 사용자가 적극적으로 사용하고 있는 IAM 역할의 `UserID` 추가 작업을 방지할 수 있습니다. 이 정책을 사용하면 거부 정책을 배포할 때 동일한 권한 세트를 사용하고 있을 수 있는 다른 사용자에게 미치는 영향을 피할 수 있습니다. 이 정책에서는 플레이스홀더 사용자 ID () 를 사용하므로 액세스를 취소하려는 사용자 ID로 업데이트해야 합니다. *`Add user ID here`*`"identitystore:userId"`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "identitystore:userId": "Add user ID here"
                }
```

```
            }
        }
    ]
}
```

와 같은 "aws:userId" 다른 조건 키를 사용할 수도 있지만 이 키는 한 사람과 관련된 전 세계적으로 고유한 "identitystore:userId" 값이므로 확실합니다. 조건에서 사용하는 "aws:userId" 것은 ID 소스에서 사용자 속성이 동기화되는 방식에 영향을 받을 수 있으며, 사용자의 사용자 이름 또는 이메일 주소가 변경되면 변경될 수 있습니다.

IAM Identity Center 콘솔에서 사용자로 이동하여 이름으로 사용자를 검색하고 일반 정보 섹션을 확장한 다음 사용자 ID를 복사하여 사용자를 찾을 수 있습니다. identitystore:userId 사용자 ID를 검색하는 동안 동일한 섹션에서 사용자의 AWS 액세스 포털 세션을 중지하고 로그인 액세스를 비활성화하는 것도 편리합니다. ID 저장소 API 쿼리를 통해 사용자의 사용자 ID를 얻음으로써 거부 정책을 생성하는 프로세스를 자동화할 수 있습니다.

거부 정책 배포

유효하지 않은 자리 표시자 사용자 ID를 사용할 수 있습니다. 예를 *Add user ID here* 들어, 사용자가 액세스할 수 있는 서비스 제어 정책 (SCP) 을 AWS 계정 통해 거부 정책을 미리 배포할 수 있습니다. 쉽고 빠르게 영향을 미치기 위해 이 방법을 사용하는 것이 좋습니다. 거부 정책을 사용하여 사용자의 액세스를 취소할 때는 정책을 편집하여 자리 표시자 사용자 ID를 액세스를 취소하려는 사람의 사용자 ID로 교체합니다. 이렇게 하면 SCP를 연결한 모든 계정에 설정된 권한으로 사용자가 어떤 행동도 할 수 없습니다. 사용자가 활성 AWS 액세스 포털 세션을 사용하여 다른 계정으로 이동하고 다른 역할을 맡더라도 사용자의 작업을 차단합니다. SCP가 사용자의 접근을 완전히 차단한 경우, 필요한 경우 로그인 기능을 비활성화하고, 할당을 취소하고, AWS 액세스 포털 세션을 중지할 수 있습니다.

SCP를 사용하는 대신 권한 집합의 인라인 정책과 사용자가 액세스할 수 있는 권한 집합에서 사용하는 고객 관리형 정책에 거부 정책을 포함할 수도 있습니다.

두 명 이상의 사용자에 대한 액세스를 취소해야 하는 경우 조건 블록에 다음과 같은 값 목록을 사용할 수 있습니다.

```
        "Condition": {
                "StringEquals": {
                    "identitystore:userId": [" user1 userId", "user2 userId"...]
                    }
    }
```

> **Important**
>
> 어떤 방법을 사용하든 다른 수정 조치를 취하고 해당 사용자의 사용자 ID를 정책에 12시간 이상 보관해야 합니다. 이 시간이 지나면 사용자가 맡은 모든 역할이 만료되므로 거부 정책에서 해당 사용자 ID를 제거할 수 있습니다.

리소스 정책, Amazon EKS의 권한 집합 참조 및 AWS KMS

AWS 계정에 권한 세트를 할당하면 IAM Identity Center는 로 시작하는 이름으로 역할을 생성합니다. `AWSReservedSSO_`

역할에 대한 전체 이름 및 Amazon 리소스 이름(ARN)은 다음 형식을 사용합니다.

명칭	ARN
`AWSReservedSSO_` *`permission-set-name_unique-suffix`*	`arn:aws:iam::` *`aws-account-ID`*`:role/aws-reserved/sso.amazonaws.com/` *`aws-region`* `/AWSReservedSSO_` *`permission-set-name_unique-suffix`*

예를 들어 데이터베이스 관리자에게 AWS 계정 액세스 권한을 부여하는 권한 집합을 생성하면 다음 이름과 ARN을 사용하여 해당 역할이 생성됩니다.

명칭	ARN
`AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`	`arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`

AWS 계정의 이 권한 집합에 대한 모든 할당을 삭제하면 IAM Identity Center에서 생성한 해당 역할도 삭제됩니다. 나중에 같은 권한 집합에 새 할당을 하면 IAM Identity Center에서 권한 집합에 대한 새 역

할을 생성합니다. 새 역할의 이름 및 ARN에는 다른 고유한 접미사가 포함됩니다. 이 예제에서 고유한 접미사는 abcdef0123456789입니다.

명칭	ARN
AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**

역할에 대한 새 이름과 ARN의 접미사가 변경되면 원래 이름과 ARN을 참조하는 정책이 그대로 적용되어 해당 권한 집합을 사용하는 개인의 액세스가 중단됩니다. out-of-date 예를 들어, 다음 구성에서 원래 ARN을 참조하는 경우 역할에 대한 ARN이 변경되면 권한 집합의 사용자 액세스가 중단됩니다.

- Amazon Elastic Kubernetes Service(Amazon EKS)의 aws-auth ConfigMap 파일에서
- () 키에 대한 리소스 기반 정책에서. AWS Key Management Service AWS KMS이 정책을 키 정책이라고도 합니다.

권한 집합에 해당하는 역할의 새 ARN을 참조하도록 대부분의 AWS 서비스에 대한 리소스 기반 정책을 업데이트할 수 있지만, Amazon EKS용 IAM 및 AWS KMS ARN이 변경될 경우에 생성한 백업 역할이 있어야 합니다. Amazon EKS의 경우 백업 IAM 역할이 aws-auth ConfigMap에 있어야 합니다. AWS KMS의 경우, 키 정책에 반드시 존재해야 하기 때문입니다. 두 경우 모두 백업 IAM 역할이 없는 경우 AWS Support에 문의해야 합니다.

액세스 중단 방지를 위한 권장 사항

권한 집합에 해당하는 역할의 ARN 변경으로 인한 액세스 중단을 방지하려면 다음과 같이 하는 것이 좋습니다.

- 하나 이상의 권한 집합 할당을 유지합니다.

  Amazon EKS의 주요 정책 또는 기타 리소스 기반 정책에서 참조하는 역할을 포함하는 AWS 계정에서 AWS KMS이 할당을 유지하십시오. aws-auth ConfigMap AWS 서비스

  예를 들어, EKSAccess 권한 집합을 생성하고 AWS 계정에서 해당 역할 ARN을 참조하는 경우 해당 계정의 111122223333 권한 집합에 관리 그룹을 영구적으로 할당합니다. 할당은 영구적이므로

IAM Identity Center는 해당 역할을 삭제하지 않으므로 이름 변경 위험이 없습니다. 관리자 그룹은 권한 상승 위험 없이 항상 액세스할 수 있습니다.

- Amazon EKS의 경우 AWS KMS: IAM에서 생성한 역할을 포함하십시오.

  `aws-auth ConfigMap`에서 Amazon EKS용 클러스터의 권한 집합이나 AWS KMS 키의 키 정책에서 역할 ARN을 참조하는 경우 IAM에서 생성한 역할을 하나 이상 포함하는 것이 좋습니다. 역할을 통해 Amazon EKS 클러스터에 액세스하거나 AWS KMS 키 정책을 관리할 수 있어야 합니다. 권한 집합이 이 역할을 맡을 수 있어야 합니다. 이렇게 하면 권한 집합의 역할 ARN이 변경될 경우 또는 키 정책에서 ARN에 대한 참조를 업데이트할 수 있습니다. `aws-auth ConfigMap` AWS KMS 다음 섹션에서는 IAM에서 생성된 역할에 대해 신뢰 정책을 생성하는 방법의 예를 제공합니다. `AdministratorAccess` 권한 집합으로만 역할을 수임할 수 있습니다.

사용자 지정 신뢰 정책 예

다음은 IAM에서 생성된 역할에 액세스할 수 있는 `AdministratorAccess` 권한 집합을 제공하는 사용자 지정 신뢰 정책의 예입니다. 다음은 이 정책의 주요 요소입니다.

- 이 신뢰 정책의 기본 요소는 AWS 계정 보안 주체를 지정합니다. 이 정책에서는 `sts:AssumeRole` 권한이 `111122223333` 있는 AWS 계정의 보안 주체가 IAM에서 생성된 역할을 수임할 수 있습니다.
- 이 신뢰 정책의 `Condition element`에는 IAM에서 생성된 역할을 수임할 수 있는 보안 주체에 대한 추가 요구 사항이 명시되어 있습니다. 이 정책에서는 다음 역할 ARN을 가진 권한 집합이 역할을 수임할 수 있습니다.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> `Condition` 요소는 `ArnLike` 조건 연산자를 포함하며, 권한 집합 역할 ARN 끝에 고유한 접미사 대신 와일드카드를 사용합니다. 즉, 정책에서는 권한 집합의 역할 ARN이 변경되더라도 권한 집합이 IAM에서 생성된 역할을 수임하도록 허용합니다.

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

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
        }
      }
    }
  ]
}
```

IAM에서 생성한 역할을 이러한 정책에 포함하면 권한 집합이나 권한 집합에 대한 모든 할당이 실수로 삭제되고 다시 생성되는 경우 Amazon EKS 클러스터 또는 기타 AWS 리소스에 긴급 액세스할 수 있습니다. AWS KMS keys

속성 기반 액세스 제어

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM Identity Center를 사용하면 IAM Identity Center ID 소스에서 가져온 사용자 속성을 AWS 계정 사용하여 여러 AWS 리소스에 대한 액세스를 관리할 수 있습니다. AWS에서는 이러한 속성을 태그라고 합니다. 에서 사용자 속성을 태그로 AWS 사용하면 에서 세분화된 권한을 생성하는 프로세스를 간소화하고 직원이 일치하는 태그가 있는 AWS 리소스에만 액세스할 수 있습니다. AWS

예를 들어 서로 다른 두 팀에 속한 개발자 Bob과 Sally에게 IAM Identity Center에서 설정한 동일한 권한을 할당한 다음 액세스 제어를 위한 팀 이름 속성을 선택할 수 있습니다. Bob과 Sally가 로그인하면 IAM Identity Center가 AWS 세션에서 팀 이름 속성을 전송하므로 Bob과 Sally는 팀 이름 속성이 AWS 프로젝트 리소스의 팀 이름 태그와 일치하는 경우에만 프로젝트 리소스에 액세스할 수 있습니다. AWS 계정 Bob이 나중에 Sally의 팀으로 옮기는 경우 회사 디렉토리에서 팀 이름 속성을 업데이트하기만 하면 Bob의 액세스 권한을 수정할 수 있습니다. Bob은 다음 번에 로그인하면 AWS에서 권한을 업데이트할 필요 없이 새 팀의 프로젝트 리소스에 자동으로 액세스할 수 있게 됩니다.

또한 이 접근 방식은 이제 동일한 권한 집합에 연결된 사용자가 해당 속성에 따라 고유한 권한을 가질 수 있으므로 IAM Identity Center에서 생성하고 관리해야 하는 개별 권한의 수를 줄이는 데도 도움이 됩니다. IAM Identity Center 권한 집합 및 리소스 기반 정책에서 이러한 사용자 속성을 사용하여 AWS 리소스에 ABAC를 구현하고 규모에 맞게 권한 관리를 단순화할 수 있습니다.

이점

다음은 IAM Identity Center에서 ABAC를 사용할 때 얻을 수 있는 추가 이점입니다.

- ABAC는 더 적은 수의 권한 집합 필요 – 각 직무에 대해 서로 다른 정책을 생성할 필요가 없기 때문에 생성해야 하는 권한 집합 수가 더 적습니다. 이렇게 하면 권한 관리의 복잡성이 줄어듭니다.
- ABAC를 사용하면 팀이 빠르게 변화하고 성장할 수 있습니다 – 리소스를 생성할 때 적절한 태그가 지정되면 속성을 기반으로 새 리소스에 대한 권한이 자동으로 부여됩니다.
- ABAC를 사용하여 회사 디렉터리의 직원 속성 사용 – IAM Identity Center에 구성된 모든 ID 소스의 기존 직원 속성을 사용하여 AWS에서 액세스 제어 결정을 내릴 수 있습니다.
- 리소스에 액세스하는 사용자 추적 — 보안 관리자는 에서 AWS CloudTrail 사용자 속성을 검토하여 세션의 사용자 활동을 추적함으로써 세션의 ID를 쉽게 확인할 수 있습니다. AWS

IAM Identity Center 콘솔을 사용하여 ABAC를 구성하는 방법에 대한 자세한 내용은 액세스 제어를 위한 속성 단원을 참조하세요. IAM ID 센터 API를 사용하여 ABAC를 활성화하고 구성하는 방법에 대한 자세한 내용은 IAM ID 센터 API 참조 안내서를 참조하십시오 CreateInstanceAccessControlAttributeConfiguration.

주제

- 체크리스트: IAM ID 센터를 사용하여 ABAC 구성 AWS
- 액세스 제어를 위한 속성

체크리스트: IAM ID 센터를 사용하여 ABAC 구성 AWS

이 체크리스트에는 AWS 리소스를 준비하고 ABAC 액세스를 위한 IAM Identity Center를 설정하는 데 필요한 구성 작업이 포함되어 있습니다. 이 체크리스트의 작업을 순서대로 완료합니다. 참조 링크를 통해 특정 항목으로 이동하면 이 항목으로 돌아가서 이 체크리스트의 나머지 작업을 진행할 수 있습니다.

단계	작업	레퍼런스
1	모든 리소스에 태그를 추가하는 방법을 검토하십시오. AWS IAM Identity Center에서 ABAC를 구현하려면 먼저 ABAC를 구현하려는 모든 AWS 리소스에 태그를 추가해야 합니다.	• 리소스에 태그 지정 AWS

단계	작업	레퍼런스
2	ID 스토어의 관련 사용자 ID 및 속성을 사용하여 IAM Identity Center에서 ID 소스를 구성하는 방법을 검토합니다. IAM ID 센터를 사용하면 지원되는 모든 IAM ID 센터 ID 소스의 사용자 속성을 ABAC에 사용할 수 있습니다. AWS	• ID 소스 관리
3	다음 기준에 따라 액세스 제어 결정을 내리는 데 사용할 속성을 결정하고 이를 IAM Identity AWS Center로 전송하십시오.	• 시작하기
	• 외부 ID 제공업체(IdP)를 사용하는 경우 IdP에서 전달된 속성을 사용할지 아니면 IAM Identity Center 내에서 속성을 선택할지를 결정합니다.	• 외부 ID 제공업체를 ID 소스로 사용할 때의 속성 선택
	• IdP가 속성을 전송하도록 선택한 경우 SAML 어설션에서 속성을 전송하도록 IdP를 구성합니다. 특정 IdP에 대해서는 자습서의 `Optional` 섹션을 참조하십시오.	• 시작하기 튜토리얼
	• ID 소스로 IdP를 사용하고 IAM Identity Center에서 속성을 선택하는 경우, 속성 값이 IdP에서 가져오도록 SCIM을 구성하는 방법을 조사합니다. IdP와 함께 SCIM을 사용할 수 없는 경우 IAM Identity Center 콘솔 사용자 페이지를 사용하여 사용자와 해당 속성을 추가합니다.	• 자동 프로비저닝 • 지원되는 외부 ID 제공업체 속성
	• Active Directory 또는 IAM Identity Center를 ID 소스로 사용하거나 IdP를 사용하고 IAM Identity Center에서 속성을 선택하도록 선택한 경우 구성할 수 있는 사용 가능한 속성을 검토합니다. 그런 다음 바로 4단계로 이동하여 IAM Identity Center 콘솔을 사용하여 ABAC 속성 구성을 시작합니다.	• IAM Identity Center를 ID 소스로 사용할 때의 속성 선택 • ID 소스로 AWS Managed Microsoft AD 을 사용할 때의 속성 선택 • 기본 매핑

단계	작업	레퍼런스
4	IAM Identity Center 콘솔의 액세스 제어용 속성 페이지를 사용하여 ABAC에 사용할 속성을 선택합니다. 이 페이지에서는 2단계에서 구성한 ID 소스에서 액세스 제어를 위한 속성을 선택할 수 있습니다. 자격 증명과 해당 속성을 IAM Identity Center에 저장한 후에는 액세스 제어 결정에 사용할 수 있도록 키-값 쌍 (매핑) 을 생성해야 합니다. AWS 계정	• 액세스 제어를 위한 속성 활성화 및 구성
5	권한 집합 내에 사용자 지정 권한 정책을 생성하고 액세스 제어 속성을 사용하여 사용자가 일치하는 태그가 있는 리소스에만 액세스할 수 있도록 ABAC 규칙을 생성합니다. 4단계에서 구성한 사용자 속성은 AWS 에서 액세스 제어 결정을 위한 태그로 사용됩니다. `aws:PrincipalTag/key` 조건을 사용하여 권한 정책의 액세스 제어 속성을 참조할 수 있습니다.	• IAM Identity Center에서 ABAC에 대한 권한 정책 생성
6	다양한 AWS 계정버전에서는 5단계에서 생성한 권한 집합에 사용자를 할당하십시오. 이렇게 하면 사용자가 자신의 계정으로 페더레이션하여 AWS 리소스에 액세스할 때 일치하는 태그를 기반으로 한 액세스 권한만 얻을 수 있습니다.	• 사용자에게 액세스 권한을 할당하십시오. AWS 계정

이 단계를 완료한 후 SSO (Single Sign-On) AWS 계정 를 사용하여 페더레이션한 사용자는 일치하는 속성에 따라 AWS 리소스에 액세스할 수 있게 됩니다.

액세스 제어를 위한 속성

액세스 제어 속성은 정책에 사용하여 리소스에 대한 액세스를 제어하려는사용자 속성을 선택하는 IAM Identity Center 콘솔의 페이지 이름입니다. 사용자 ID 소스의 기존 속성을 AWS 기반으로 사용자를 워크로드에 할당할 수 있습니다.

예를 들어 부서 이름을 기반으로 S3 버킷에 대한 액세스를 할당하려고 한다고 가정해 보겠습니다. 액세스 제어에 속성 페이지 있는 동안 ABAC(속성 기반 액세스 제어)와 함께 사용할 부서 사용자 속성을 선택합니다. 그런 다음 IAM Identity Center 권한 집합에서 부서 속성이 S3 버킷에 할당한 부서 태그와 일치하는 경우에만 사용자에게 액세스 권한을 부여하는 정책을 작성합니다. IAM Identity Center는 사

용자의 부서 속성을 액세스 중인 계정에 전달합니다. 그런 다음 속성을 사용하여 정책을 기반으로 액세스를 결정합니다. ABAC에 대한 자세한 내용은 속성 기반 액세스 제어 단원을 참조하세요.

시작하기

액세스 제어를 위한 속성 구성을 시작하는 방법은 사용 중인 ID 소스에 따라 달라집니다. 선택한 ID 소스에 관계없이 속성을 선택한 후에는 권한 집합 정책을 만들거나 편집해야 합니다. 이러한 정책은 사용자 ID에 AWS 리소스에 대한 액세스 권한을 부여해야 합니다.

IAM Identity Center를 ID 소스로 사용할 때의 속성 선택

IAM Identity Center를 ID 소스로 구성할 때는 먼저 사용자를 추가하고 속성을 구성합니다. 그런 다음 액세스 제어용 속성 페이지로 이동하여 정책에 사용할 속성을 선택합니다. 마지막으로 AWS 계정 페이지로 이동하여 ABAC의 속성을 사용하기 위한 권한 집합을 생성하거나 편집합니다.

ID 소스로 AWS Managed Microsoft AD 을 사용할 때의 속성 선택

를 ID 소스로 사용하여 IAM ID 센터를 구성할 때는 먼저 Active Directory의 속성 세트를 IAM ID 센터의 사용자 속성에 매핑합니다. AWS Managed Microsoft AD 다음으로 액세스 제어용 속성 페이지로 이동합니다. 그런 다음 Active Directory에서 매핑한 기존 SSO 속성 세트를 기반으로 ABAC 구성에서 사용할 속성을 선택합니다. 마지막으로, 권한 집합의 액세스 제어 속성을 사용하여 사용자 ID에 AWS 리소스에 대한 액세스 권한을 부여하는 ABAC 규칙을 작성합니다. IAM Identity Center의 사용자 속성과 디렉터리의 사용자 속성에 대한 기본 매핑 목록은 을 참조하십시오. AWS Managed Microsoft AD 기본 매핑

외부 ID 제공업체를 ID 소스로 사용할 때의 속성 선택

외부 ID 제공업체(IdP)를 ID 소스로 사용하여 IAM Identity Center를 구성하는 경우 ABAC의 속성을 사용하는 두 가지 방법이 있습니다.

- SAML 어설션을 통해 속성을 전송하도록 IdP를 구성할 수 있습니다. 이 경우 IAM Identity Center는 정책 평가를 위해 IdP의 속성 이름과 값을 전달합니다.

> **Note**
>
> SAML 어설션의 속성은 액세스 제어용 속성 페이지에서 볼 수 없습니다. 정책을 작성할 때 이러한 특성을 미리 알고 액세스 제어 규칙에 추가해야 합니다. 외부 속성을 신뢰하기로 결정한 경우 사용자가 IdPs 페더레이션할 때 이러한 속성은 항상 전달됩니다. AWS 계정동일한 속성이 SAML과 SCIM을 통해 IAM Identity Center로 들어오는 시나리오에서는 액세스 제어 결정에서 SAML 속성 값이 우선합니다.

- IAM Identity Center 콘솔의 액세스 제어용 속성 페이지에서 사용할 속성을 구성할 수 있습니다. 여기서 선택한 속성 값은 어설션을 통해 IdP에서 가져온 모든 일치하는 속성의 값을 대체합니다. SCIM 사용 여부에 따라 다음 사항을 고려합니다.
  - SCIM을 사용하는 경우 IdP는 속성 값을 IAM Identity Center에 자동으로 동기화합니다. 액세스 제어에 필요한 추가 속성은 SCIM 속성 목록에 없을 수 있습니다. 이 경우 IdP의 IT 관리자와 협력하여 필수 `https://aws.amazon.com/SAML/Attributes/AccessControl:` 접두사를 사용하여 SAML 어설션을 통해 IAM Identity Center로 이러한 속성을 전송하는 것을 고려해 보세요. SAML 어설션을 통해 전송하도록 IdP에서 액세스 제어를 위한 사용자 속성을 구성하는 방법에 대한 자세한 내용은 해당 IdP의 을 참조하십시오. 시작하기 튜토리얼
  - SCIM을 사용하지 않는 경우 IAM Identity Center를 ID 소스로 사용하는 것처럼 수동으로 사용자를 추가하고 속성을 설정해야 합니다. 그런 다음 액세스 제어를 위한 속성 페이지로 이동하여 정책에 사용할 속성을 선택합니다.

IAM Identity Center의 사용자 속성과 외부 사용자 속성에 지원되는 속성의 전체 목록은 을 참조하십시오. IdPs 지원되는 외부 ID 제공업체 속성

IAM Identity Center에서 ABAC를 시작하려면 다음 주제를 참조하세요.

주제

- 액세스 제어를 위한 속성 활성화 및 구성
- IAM Identity Center에서 ABAC에 대한 권한 정책 생성

액세스 제어를 위한 속성 활성화 및 구성

모든 경우에 ABAC를 사용하려면 먼저 IAM Identity Center 콘솔 또는 IAM Identity Center API를 사용하여 ABAC를 활성화해야 합니다. IAM Identity Center를 사용하여 속성을 선택하려면 IAM Identity Center 콘솔 또는 IAM Identity Center API의 액세스 제어용 속성 페이지를 사용합니다. 자격 증명 소스로 외부 ID 제공업체(idP)를 사용하고 SAML 어설션을 통해 속성을 보내도록 선택한 경우 속성을 전달하도록 IdP를 구성합니다. SAML 어설션으로 이 속성을 전달하는 경우 IAM Identity Center는 속성 값을 IAM Identity Center ID 스토어의 값으로 바꿉니다. 사용자가 계정에 페더레이션할 때 IAM Identity Center에 구성된 속성만 액세스 제어 결정을 내리기 위해 전송됩니다.

> **Note**
>
> IAM Identity Center 콘솔의 액세스 제어 속성 페이지에서는 외부 IdP가 구성 및 전송한 속성을 볼 수 없습니다. 외부 IdP의 SAML 어설션에 액세스 제어 속성을 전달하는 경우 사용자가 페더

레이션할 때 해당 속성이 AWS 계정 로 직접 전송됩니다. 속성은 IAM Identity Center에서 매핑에 사용할 수 없습니다.

액세스 제어에 속성 활성화

다음 절차에 따라 IAM Identity Center 콘솔을 사용하여 액세스용 속성(ABAC) 제어 기능을 활성화합니다.

> **Note**
>
> 기존 권한 집합이 있고 IAM Identity Center 인스턴스에서 ABAC를 활성화하려는 경우 추가 보안 제한 사항을 적용하려면 먼저 `iam:UpdateAssumeRolePolicy` 정책가 있어야 합니다. 계정에 권한 집합을 생성하지 않은 경우에는 이러한 추가 보안 제한이 필요하지 않습니다.

액세스 제어의 속성을 활성화하려면

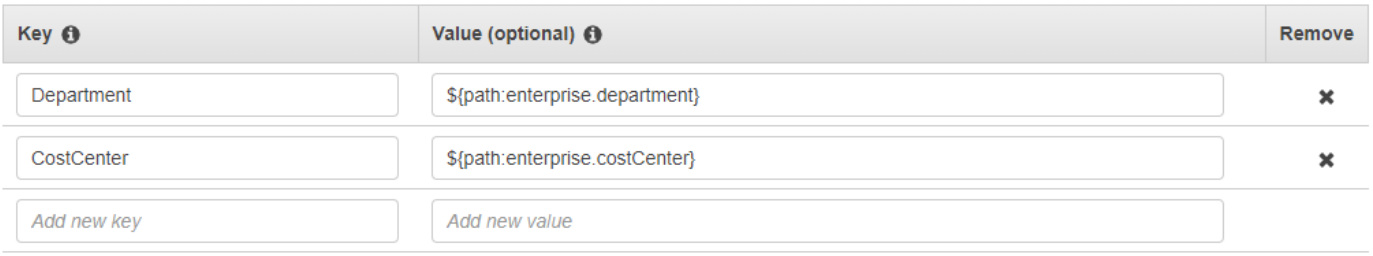
1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 액세스 제어 정보의 속성 정보 상자를 찾은 다음 활성화를 선택합니다. 다음 절차를 계속 진행하여 구성합니다.

속성 선택

다음 절차에 따라 ABAC 구성의 속성을 설정합니다.

IAM Identity Center 콘솔을 사용하여 속성을 선택하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 액세스 제어용 속성 탭을 선택한 다음 속성 관리를 선택합니다.
4. 액세스 제어 속성 페이지에서 속성 추가를 선택하고 키 및 값 세부 정보를 입력합니다. 여기에서 ID에서 가져온 속성을 IAM Identity Center가 세션 태그로 전달하는 속성에 매핑합니다.



키는 정책에 사용하기 위해 속성에 부여하는 이름을 나타냅니다. 이 이름은 임의의 이름일 수 있지만 액세스 제어를 위해 작성하는 정책에 정확한 이름을 지정해야 합니다. 예를 들어 Okta(외부 IdP)를 ID 소스로 사용하고 있으며 조직의 비용 센터 데이터를 세션 태그와 함께 전달해야 한다고 가정해 보겠습니다. 키에는 키 이름과 비슷하게 일치하는 이름을 입력합니다. CostCenter 여기서 어떤 이름을 선택하든 이름은 `aws:PrincipalTag ## #`(즉, `"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"`)에서도 정확하게 같은 이름이어야 한다는 점에 유의해야 합니다.

> **Note**
>
> 키에는 단일 값 속성을 사용합니다(예:)**`Manager`**. IAM Identity Center는 ABAC에 대한 다중 값 속성(예:)**`Manager, IT Systems`**을 지원하지 않습니다.

값은 구성된 ID 소스에서 가져온 속성의 내용을 나타냅니다. 여기에 AWS Managed Microsoft AD 디렉터리의 속성 매핑에 나열된 해당 ID 소스 테이블의 모든 값을 입력할 수 있습니다. 예를 들어, 위에서 언급한 예제에 제공된 컨텍스트를 사용하여 지원되는 IdP 속성 목록을 검토하고 지원되는 속성과 가장 근접하게 일치하는 항목이 **`${path:enterprise.costCenter}`**인지 확인한 다음 값 필드에 입력합니다. 참조는 위에 제공된 스크린샷을 참조하세요. 참고로, SAML 어설션을 통해 속성을 전달하는 옵션을 사용하지 않는 한 ABAC의 경우 이 목록 외부의 외부 IdP 속성 값을 사용할 수 없습니다.

5. 변경 사항 저장를 선택합니다.

이제 액세스 제어 속성 매핑을 구성했으므로 ABAC 구성 프로세스를 완료해야 합니다. 이렇게 하려면 ABAC 규칙을 생성하여 권한 집합 및/또는 리소스 기반 정책에 추가합니다. 이는 사용자 ID에 AWS 리소스에 대한 액세스 권한을 부여하기 위해 필요합니다. 자세한 내용은 IAM Identity Center에서 ABAC에 대한 권한 정책 생성 단원을 참조하세요.

액세스 제어의 속성 비활성화

다음 절차를 사용하여 ABAC 기능을 사용 중지하고 구성된 모든 속성 매핑을 삭제합니다.

액세스 제어의 속성을 비활성화하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 액세스 제어 속성 탭을 선택한 다음 비활성화를 선택합니다.
4. 액세스 제어 속성 비활성화 대화 상자에서 정보를 검토하고 준비가 되면 DELETE를 입력한 다음 확인을 선택합니다.

> **Important**
>
> 이 단계는 구성된 모든 속성을 삭제합니다. 일단 삭제되면 ID 소스에서 받은 모든 속성과 이전에 구성한 사용자 지정 속성은 전달되지 않습니다.

IAM Identity Center에서 ABAC에 대한 권한 정책 생성

구성된 속성 값을 기반으로 AWS 리소스에 액세스할 수 있는 사용자를 결정하는 권한 정책을 생성할 수 있습니다. ABAC를 활성화하고 속성을 지정하면 IAM Identity Center가 정책 평가에 사용할 인증된 사용자의 속성 값을 IAM으로 전달합니다.

aws:PrincipalTag 조건 키

액세스 제어 규칙을 생성하기 위한 `aws:PrincipalTag` 조건 키를 사용하여 권한 집합의 액세스 제어 속성을 사용할 수 있습니다. 예를 들어 다음 신뢰 정책에서는 조직의 모든 리소스에 해당 비용 센터를 태그할 수 있습니다. 개발자에게 비용 센터 리소스에 대한 액세스 권한을 부여하는 단일 권한 집합을 사용할 수도 있습니다. 이제 개발자는 Single Sign-on 및 비용 센터 속성을 사용하여 계정에 페더레이션할 때마다 해당 비용 센터의 리소스에만 액세스할 수 있습니다. 팀이 프로젝트에 더 많은 개발자와 리소스를 추가함에 따라 리소스에 올바른 비용 센터 태그를 지정하기만 하면 됩니다. 그런 다음 개발자가 연합할 때 AWS 세션에 코스트 센터 정보를 전달합니다. AWS 계정따라서 조직에서 새 리소스 및 개발자를 비용 센터에 추가하면 개발자는 권한 업데이트 없이 비용 센터에 맞춰 리소스를 관리할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"
                }
            }
        }
    ]
}
```

자세한 내용은 IAM 사용 설명서의 aws:PrincipalTag 및 EC2: 일치하는 보안 주체 태그와 리소스 태그를 기반으로 인스턴스를 시작하거나 중지 항목을 참조하세요.

정책 조건에 잘못된 속성이 포함된 경우 정책 조건은 실패하고 액세스가 거부됩니다. 자세한 내용은 사용자가 외부 ID 공급업체를 통해 로그인하려고 할 때 “예기치 않은 오류가 발생했습니다” 오류가 표시됩니다. 단원을 참조하세요.

IAM ID 제공업체

SSO (Single Sign-On) 액세스를 추가하면 IAM Identity Center는 각각에 IAM ID 공급자를 생성합니다. AWS 계정 AWS 계정 IAM ID 제공업체를 사용하면 애플리케이션에서 사용자 액세스 키 같은 장기 보안 인증을 배포하거나 포함할 필요가 없으므로 AWS 계정 을 안전하게 보호할 수 있습니다.

IAM ID 제공업체 복구

실수로 ID 제공업체를 삭제하거나 수정한 경우 사용자 및 그룹 할당을 수동으로 다시 적용해야 합니다. 사용자 및 그룹 할당을 다시 적용하면 ID 제공업체가 다시 생성됩니다. 자세한 내용은 다음을 참조하세요.

- 액세스 관리 AWS 계정
- 애플리케이션 액세스 관리

서비스 연결 역할

서비스 연결 역할은 사전 정의된 IAM 권한으로, 이를 통해 IAM Identity Center가 AWS Organizations에서조직의 특정 AWS 계정 에 대한 Single Sign-on 액세스 권한을 가진 사용자를 위임하고 적용할 수 있습니다. 이 서비스는 조직 내 모든 사용자에게 서비스 연결 역할을 제공하여 이 기능을 지원합니다. AWS 계정 그러면 이 서비스를 통해 IAM Identity Center와 같은 다른 AWS 서비스가 이러한 역할을 활용하여 서비스 관련 작업을 수행할 수 있습니다. 자세한 내용은 AWS Organizations 및 서비스 연결 역할 단원을 참조하세요.

IAM Identity Center를 활성화하면 AWS Organizations에서 IAM Identity Center는 조직 내 모든 계정에 서비스 연결 역할을 생성합니다. 또한 IAM Identity Center는 이후에 조직에 추가되는 모든 계정에 동일한 서비스 연결 역할을 생성합니다. 이 역할을 통해 IAM Identity Center는 사용자를 대신하여 각 계정의 리소스에 액세스할 수 있습니다. 자세한 정보는 액세스 관리 AWS 계정을 참조하세요.

각 역할에서 생성되는 서비스 연결 역할의 이름이 지정됩니다. AWS 계정 `AWSServiceRoleForSSO` 자세한 내용은 IAM Identity Center 서비스 연결 역할 사용을(를) 참조하세요.

애플리케이션 액세스 관리

를 사용하면 AWS IAM Identity Center애플리케이션에 대한 Single Sign-On 액세스 권한을 가질 수 있는 사용자를 제어할 수 있습니다. 사용자는 디렉터리 보안 인증 정보를 사용하여 로그인한 후 이러한 애플리케이션에 원활하게 액세스할 수 있습니다.

IAM Identity Center는 IAM Identity Center와 애플리케이션의 서비스 제공업체 간의 신뢰할 수 있는 관계를 통해 이러한 애플리케이션과 안전하게 통신합니다. 이 신뢰는 애플리케이션 유형에 따라 다양한 방식으로 생성될 수 있습니다.

IAM Identity Center는 관리형 애플리케이션과 고객AWS 관리형 애플리케이션이라는 두 가지 애플리케이션 유형을 지원합니다. AWS 관리형 애플리케이션은 관련 애플리케이션 콘솔 내에서 직접 또는 애플리케이션 API를 통해 구성됩니다. 고객 관리형 애플리케이션은 IAM Identity Center 콘솔에 추가되고 IAM Identity Center 및 서비스 공급자 모두에 적합한 메타데이터로 구성되어야 합니다.

IAM Identity Center에서 사용하도록 애플리케이션을 구성한 후에는 애플리케이션에 액세스하는 사용자 또는 그룹을 관리할 수 있습니다. 기본적으로 애플리케이션에는 어떤 사용자도 할당되지 않습니다.

직원에게 조직 내 특정 AWS Management Console 용도에 대한 액세스 권한을 부여할 수도 있습니다 AWS 계정 . 자세한 정보는 액세스 관리 AWS 계정을 참조하세요.

주제

- AWS 관리형 애플리케이션
- 고객 관리형 애플리케이션
- 애플리케이션 간 신뢰할 수 있는 ID 전파
- IAM Identity Center 인증서 관리
- IAM Identity Center 콘솔의 애플리케이션 속성 구성
- IAM Identity Center 콘솔에서 애플리케이션에 사용자 액세스 권한 할당
- IAM Identity Center 콘솔에서 사용자 액세스 제거
- 애플리케이션의 속성을 IAM Identity Center 속성에 매핑

AWS 관리형 애플리케이션

AWS 관리형 애플리케이션은 IAM Identity Center와 통합되며 이를 인증 및 디렉터리 서비스에 사용할 수 있습니다.

AWS 관리형 애플리케이션을 IAM Identity Center와 통합하면 각 애플리케이션에 대해 별도의 페더레이션 또는 사용자 및 그룹 동기화를 설정할 필요 없이 사용자 액세스 권한을 더 쉽게 할당할 수 있습니다. 인증에 사용할 ID 소스를 한 번 연결하면 사용자 및 그룹 할당을 한 눈에 볼 수 있습니다. 신뢰할 수 있는 ID 전파를 지원하는 애플리케이션 관리자는 IAM 역할에 매핑할 필요 없이 사용자 또는 사용자의 그룹 구성원을 기반으로 애플리케이션 리소스에 대한 액세스를 정의하고 감사할 수 있습니다.

AWS 관리형 애플리케이션은 애플리케이션 리소스에 대한 액세스를 관리하는 데 사용할 수 있는 관리 사용자 인터페이스를 제공합니다. 예를 들어 QuickSight 관리자는 그룹 구성원을 기반으로 대시보드에 액세스할 사용자를 할당할 수 있습니다. 대부분의 AWS 관리형 애플리케이션은 애플리케이션에 사용자를 할당할 수 있는 AWS Management Console 환경도 제공합니다. 이러한 애플리케이션의 콘솔 환경은 두 기능을 통합하여 사용자 할당 기능과 애플리케이션 리소스에 대한 액세스 관리 기능을 결합할 수 있습니다.

AWS IAM Identity Center와 통합된 관리형 애플리케이션에는 다음이 포함됩니다.

AWS IAM ID 센터와 통합되는 관리형 애플리케이션

AWS 관리형 애플리케이션	IAM 아이덴티티 센터의 조직 인스턴스와 통합됩니다.	IAM ID 센터의 계정 인스턴스와 통합	IAM ID 센터를 통해 신뢰할 수 있는 ID를 전파할 수 있습니다.
아마존 아테나 SQL	 예	 예	 예
아마존 CodeCatalyst	 예	 예	 아니요
아마존 EMR 노트북	 예	 아니요	 아니요

AWS 관리형 애플리케이션	IAM 아이덴티티 센터의 조직 인스턴스와 통합됩니다.	IAM ID 센터의 계정 인스턴스와 통합	IAM ID 센터를 통해 신뢰할 수 있는 ID를 전파할 수 있습니다.
아마존 EC2 기반 아마존 EMR	 예	 예	 예
Amazon EMR Studio	 예	 예	 예
Amazon Kendra	 예	 아니요	 아니요
Amazon Managed Grafana	 예	 아니요	 아니요
Amazon Monitron	 예	 아니요	 아니요
Amazon Nimble Studio	 예	 아니요	 아니요
Amazon Pinpoint	 예	 아니요	 아니요

AWS 관리형 애플리케이션	IAM 아이덴티티 센터의 조직 인스턴스와 통합됩니다.	IAM ID 센터의 계정 인스턴스와 통합	IAM ID 센터를 통해 신뢰할 수 있는 ID를 전파할 수 있습니다.
Amazon Q 비즈니스용	 예	 예	 아니요
Amazon Q 개발자	 예	 예 *	 아니요
아마존 QuickSight	 예	 예	 예
Amazon Redshift	 예	 예	 예
Amazon S3 액세스 그랜트	 예	 예	 예
아마존 SageMaker 스튜디오	 예	 아니요	 아니요
아마존 WorkSpaces 웹	 예	 아니요	 아니요

AWS 관리형 애플리케이션	IAM 아이덴티티 센터의 조직 인스턴스와 통합됩니다.	IAM ID 센터의 계정 인스턴스와 통합	IAM ID 센터를 통해 신뢰할 수 있는 ID를 전파할 수 있습니다.
AWS CLI	 예	 아니요	 아니요
AWS Deadline Cloud	 예	 예	 아니요
AWS IoT Events	 예	 아니요	 아니요
AWS IoT Fleet Hub	 예	 아니요	 아니요
AWS IoT SiteWise	 예	 아니요	 아니요
AWS Lake Formation	 예	 예	 예

AWS 관리형 애플리케이션	IAM 아이덴티티 센터의 조직 인스턴스와 통합됩니다.	IAM ID 센터의 계정 인스턴스와 통합	IAM ID 센터를 통해 신뢰할 수 있는 ID를 전파할 수 있습니다.
AWS Supply Chain	 예	 아니요	 아니요
AWS Systems Manager	 예	 아니요	 아니요
AWS Verified Access	 예	 아니요	 아니요

* IAM ID 센터의 계정 인스턴스는 사용자가 AWS 콘솔에서 Amazon Q에 액세스하도록 요구하지 않는 한 지원됩니다.

주제

- 액세스 제어
- 관리 작업 조정
- ID 정보를 공유하도록 IAM Identity Center 구성
- ID 정보 공유에 대한 고려 사항 AWS 계정
- ID 인식 콘솔 세션 활성화
- 관리형 애플리케이션 사용 제한 AWS
- AWS 관리형 애플리케이션 관련 세부 정보 보기
- 관리형 AWS 애플리케이션 비활성화

액세스 제어

AWS 관리형 애플리케이션에 대한 액세스는 두 가지 방식으로 제어됩니다.

- 애플리케이션에 대한 초기 입력 - IAM Identity Center가 애플리케이션에 대한 할당을 통해 이를 관리합니다. 기본적으로 AWS 관리되는 애플리케이션에는 할당이 필요합니다.
- 애플리케이션 리소스에 대한 액세스 - 애플리케이션이 제어하는 독립적인 리소스 할당을 통해 이를 관리합니다.

관리 작업 조정

애플리케이션 관리자인 경우 애플리케이션에 할당이 필요한지 여부를 선택할 수 있습니다. 할당이 필요한 경우 사용자가 AWS 액세스 포털에 로그인하면 직접 또는 그룹 과제를 통해 응용 프로그램에 할당된 사용자만 응용 프로그램 타일을 볼 수 있습니다. 또는 할당이 필요하지 않은 경우 모든 IAM Identity Center 사용자가 애플리케이션을 사용하도록 허용할 수 있습니다. 이 경우 애플리케이션은 리소스에 대한 액세스를 관리하며 AWS 액세스 포털을 방문하는 모든 사용자가 애플리케이션 타일을 볼 수 있습니다.

IAM Identity Center 관리자인 경우 IAM Identity Center 콘솔을 사용하여 관리형 애플리케이션에 대한 할당을 제거할 수 있습니다. AWS 할당을 제거하기 전에 애플리케이션 관리자와 협의하는 것이 좋습니다. 할당이 필요한지 여부를 결정하는 설정을 수정하거나 애플리케이션 할당을 자동화하려는 경우에도 애플리케이션 관리자와 협의해야 합니다.

ID 정보를 공유하도록 IAM Identity Center 구성

IAM Identity Center는 로그인 보안 인증 정보를 제외한 사용자 및 그룹 속성이 포함된 ID 저장소를 제공합니다. 다음 방법 중 하나를 사용하여 IAM Identity Center ID 스토어의 사용자 및 그룹을 최신 상태로 유지할 수 있습니다.

- IAM Identity Center ID 스토어를 기본 ID 소스로 사용하세요. 이 방법을 선택하면 IAM Identity Center 콘솔 또는 () 내에서 사용자, 로그인 자격 증명 및 그룹을 관리할 수 있습니다. AWS Command Line Interface AWS CLI자세한 정보는 IAM Identity Center에서 ID 관리을 참조하세요.
- 다음 ID 소스 중 하나에서 들어오는 사용자 및 그룹을 IAM Identity Center ID 저장소에 프로비저닝(동기화)하도록 설정합니다.
  - Active Directory - 자세한 내용은 Microsoft AD 디렉터리에 연결의 내용을 참조하세요.
  - 외부 ID 제공업체 - 자세한 내용은 외부 ID 제공업체에 연결의 내용을 참조하세요.

이 프로비저닝 방법을 선택하면 ID 소스 내에서 사용자와 그룹을 계속 관리할 수 있으며 이러한 변경 사항은 IAM Identity Center ID 스토어에 동기화됩니다.

어떤 ID 소스를 선택하든 IAM Identity Center는 사용자 및 그룹 정보를 관리형 애플리케이션과 공유할 수 있습니다. AWS 이를 통해 ID 소스를 IAM Identity Center에 한 번 연결한 다음 AWS 클라우드의 여러 애플리케이션과 ID 정보를 공유할 수 있습니다. 따라서 각 애플리케이션과 페더레이션 및 ID 프로비저닝을 개별적으로 설정할 필요가 없습니다. 또한 이 공유 기능을 사용하면 사용자에게 서로 다른 AWS 계정의 여러 애플리케이션에 대한 액세스 권한을 쉽게 부여할 수 있습니다.

ID 정보 공유에 대한 고려 사항 AWS 계정

IAM Identity Center는 여러 애플리케이션에서 가장 일반적으로 사용되는 속성을 지원합니다. 이러한 속성에는 이름과 성, 전화번호, 이메일 주소, 주소, 선호 언어 등이 포함됩니다. 이 개인 식별 정보를 사용할 수 있는 애플리케이션과 계정을 신중히 고려하세요.

다음 방법 중 하나로 이 정보에 대한 액세스를 제어할 수 있습니다. AWS Organizations 관리 계정에서만 액세스를 활성화하거나 의 모든 계정에서 액세스를 활성화하도록 선택할 수 AWS Organizations있습니다. 또는 서비스 제어 정책(SCP)을 사용하여 어떤 애플리케이션이 AWS Organizations에 있는 어떤 계정의 정보에 액세스할 수 있는지 제어할 수 있습니다. 예를 들어 AWS Organizations 관리 계정에서만 액세스를 활성화하면 멤버 계정의 애플리케이션은 정보에 액세스할 수 없습니다. 하지만 모든 계정에서 액세스를 활성화하면, SCP를 사용해 허용하려는 애플리케이션을 제외한 모든 애플리케이션의 액세스를 허용하지 않을 수 있습니다.

ID 인식 콘솔 세션 활성화

콘솔용 ID 인식 세션은 사용자 환경을 개인화할 수 있는 추가 사용자 컨텍스트를 제공하여 사용자 AWS 콘솔 세션을 개선합니다. 이 기능은 현재 AWS 콘솔에서 Amazon Q 사용자에게 지원됩니다.

기존 액세스 패턴을 변경하거나 현재 콘솔과의 페더레이션을 변경하지 않고도 ID 인식 AWS 콘솔 세션을 활성화할 수 있습니다. 사용자가 IAM으로 AWS 콘솔에 로그인하는 경우 (예: IAM 사용자로 로그인하거나 IAM을 통한 페더레이션 액세스를 통해 로그인하는 경우) 이러한 방법을 계속 사용할 수 있습니다. 사용자가 AWS 액세스 포털에 로그인하면 IAM Identity Center 사용자 자격 증명을 계속 사용할 수 있습니다.

주제

- 필수 조건 및 고려 사항
- 세션을 활성화하는 방법 identity-aware-console

- ID 인식 콘솔 세션의 작동 방식

필수 조건 및 고려 사항

ID 인식 콘솔 세션을 활성화하기 전에 다음 사전 요구 사항 및 고려 사항을 검토하십시오.

- 콘솔에서 Amazon Q에 액세스해야 하는 사용자를 위해 ID 인식 콘솔 세션을 활성화해야 합니다 AWS .
- ID 인식 콘솔 세션은 현재 콘솔에서 Amazon Q와 함께 사용할 AWS 수만 지원됩니다.
- ID 인식 콘솔 세션에는 IAM Identity Center의 조직 인스턴스가 필요합니다.
- AWS 리전옵트인에서 IAM ID 센터를 활성화하면 Amazon Q와의 통합이 지원되지 않습니다.
- ID 인식 콘솔 세션을 활성화한 후에는 이 기능을 비활성화할 수 없습니다.
- ID 인식 콘솔 세션을 활성화하려면 다음 권한이 있어야 합니다.
  - `sso:CreateApplication`
  - `sso:GetSharedSsoConfiguration`
  - `sso:ListApplications`
  - `sso:PutApplicationAssignmentConfiguration`
  - `sso:PutApplicationAuthenticationMethod`
  - `sso:PutApplicationGrant`
  - `sso:PutApplicationAccessScope`
  - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
  - `signin:ListTrustedIdentityPropagationApplicationForConsole`
  -
- 사용자에게 ID 인식 콘솔 세션을 사용할 수 있게 하려면 ID 기반 정책에서 `sts:setContext` 권한을 부여해야 합니다. 자세한 내용은 사용자에게 ID 인식 콘솔 세션을 사용할 수 있는 권한 부여를 참조하십시오.

세션을 활성화하는 방법 identity-aware-console

Amazon Q 콘솔 또는 IAM ID 센터 콘솔에서 ID 인식 콘솔 세션을 활성화할 수 있습니다.

Amazon Q 콘솔에서 ID 인식 콘솔 세션 활성화

ID 인식 콘솔 세션을 활성화하려면 먼저 ID 소스가 연결된 IAM Identity Center의 조직 인스턴스가 있어야 합니다. IAM ID 센터를 이미 구성한 경우 3단계로 건너뛰십시오.

1. IAM Identity Center 콘솔을 엽니다. 활성화를 선택하고 IAM ID 센터의 조직 인스턴스를 생성합니다. 자세한 내용은 활성화 AWS IAM Identity Center을 참조하세요.
2. 자격 증명 소스를 IAM ID 센터에 연결하고 사용자를 IAM ID 센터에 프로비저닝하십시오. 기본 IAM ID 센터 디렉터리를 ID 소스로 선택하거나 다른 ID 공급자를 사용할 수 있습니다. 자세한 정보는 시작하기 튜토리얼을 참조하세요.
3. IAM ID 센터 설정을 완료한 후 Amazon Q 콘솔을 열고 Amazon Q 개발자 사용 설명서의 구독에 나와 있는 단계를 따르십시오. ID 인식 콘솔 세션을 활성화해야 합니다.

> **Note**
>
> ID 인식 콘솔 세션을 활성화할 충분한 권한이 없는 경우 IAM Identity Center 관리자에게 IAM Identity Center 콘솔에서 이 작업을 수행하도록 요청해야 할 수 있습니다. 자세한 내용은 다음 절차를 참조하세요.

IAM Identity Center 콘솔에서 ID 인식 콘솔 세션을 활성화하십시오.

IAM Identity Center 관리자인 경우 다른 관리자가 IAM Identity Center 콘솔에서 ID 인식 콘솔 세션을 활성화하도록 요청받을 수 있습니다.

1. IAM Identity Center 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. ID 인식 세션 활성화에서 활성화를 선택합니다.
4. 두 번째 메시지에서 [Enable] 을 선택합니다.
5. ID 인식 콘솔 세션 활성화를 완료하면 설정 페이지 상단에 확인 메시지가 나타납니다.
6. 세부 정보 섹션에서 ID 인식 세션의 상태는 활성화로 표시됩니다.

ID 인식 콘솔 세션의 작동 방식

ID 인식 콘솔 세션을 통해 AWS 콘솔의 Amazon Q 사용자는 로그인하고, 웹 사이트 AWS Management Console 또는 다른 AWS 웹 사이트를 열고 AWS, Amazon Q 아이콘을 선택하고, 채팅을 시작하거나

지원되는 다른 기능을 사용할 수 있습니다. 자세한 내용은 Amazon Q Developer 사용 설명서를 참조하세요.

IAM ID 센터는 활성 IAM ID 센터 사용자 ID와 IAM ID 센터 세션 ID를 포함하도록 사용자의 현재 콘솔 세션을 개선합니다.

ID 인식 콘솔 세션에는 다음 세 가지 값이 포함됩니다.

- ID 저장소 사용자 ID (아이덴티티 스토어: UserId) - 이 값은 IAM Identity Center에 연결된 ID 소스에서 사용자를 고유하게 식별하는 데 사용됩니다.
- ID 저장소 디렉터리 ARN (아이덴티티 스토어: IdentityStoreArn) - 이 값은 IAM Identity Center에 연결되어 있고 속성을 조회할 수 있는 ID 저장소의 ARN입니다. `identitystore:UserId`
- IAM ID 센터 세션 ID - 이 값은 사용자의 IAM ID 센터 세션이 여전히 유효한지 여부를 나타냅니다.

값은 동일하지만 사용자가 로그인하는 방식에 따라 다른 방식으로 얻어지며 프로세스의 다른 시점에서 추가됩니다.

- IAM ID 센터 (AWS 액세스 포털): 이 경우 사용자의 ID 저장소 사용자 ID 및 ARN 값은 활성 IAM ID 센터 세션에 이미 제공되어 있습니다. IAM ID 센터는 세션 ID만 추가하여 현재 세션을 개선합니다.
- 기타 로그인 방법: 사용자가 IAM 사용자, IAM 역할 또는 IAM의 연동 사용자로 로그인하는 경우 이러한 값은 제공되지 않습니다. AWS IAM Identity Center는 ID 저장소 사용자 ID, ID 저장소 디렉터리 ARN 및 세션 ID를 추가하여 현재 세션을 개선합니다.

관리형 애플리케이션 사용 제한 AWS

IAM Identity Center를 처음으로 AWS 활성화하면 의 모든 계정에서 AWS 관리형 애플리케이션을 자동으로 사용할 수 있습니다. AWS Organizations애플리케이션을 제한하려면 SCP를 구현해야 합니다. SCP를 사용하여 IAM Identity Center 사용자 및 그룹 정보에 대한 액세스를 차단하고 지정된 계정을 제외하고는 애플리케이션이 시작되지 않도록 할 수 있습니다.

AWS 관리형 애플리케이션 관련 세부 정보 보기

애플리케이션용 콘솔 또는 API를 사용하여 AWS 관리형 애플리케이션을 IAM Identity Center에 연결하면 애플리케이션이 IAM Identity Center에 등록됩니다. 애플리케이션이 IAM Identity Center에 등록된 후에는 IAM Identity Center 콘솔에서 애플리케이션에 관한 세부 정보를 볼 수 있습니다.

IAM Identity Center 콘솔에서 AWS 관리형 애플리케이션에 대한 정보를 보려면

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. AWS 관리형 애플리케이션 탭을 선택합니다.
4. 애플리케이션 목록에서 자세한 정보를 보려는 애플리케이션의 이름을 선택합니다.
5. 애플리케이션에 관한 정보에는 사용자 및 그룹 할당이 필요한지 여부, 해당하는 경우 ID 전파를 위한 할당된 사용자 및 그룹과 신뢰할 수 있는 애플리케이션이 포함됩니다. 신뢰할 수 있는 ID 전파에 관한 자세한 내용은 애플리케이션 간 신뢰할 수 있는 ID 전파의 내용을 참조하세요.

관리형 AWS 애플리케이션 비활성화

사용자가 AWS 관리형 애플리케이션에 인증하지 못하도록 IAM Identity Center 콘솔에서 애플리케이션을 비활성화할 수 있습니다.

> **Warning**
>
> 애플리케이션을 비활성화하면 이 애플리케이션에 대한 모든 사용자 권한이 삭제되고, IAM Identity Center와의 애플리케이션 연결이 끊기며, 애플리케이션에 액세스할 수 없게 됩니다. IAM Identity Center 관리자인 경우 이 작업을 수행하기 전에 애플리케이션 관리자와 협의하는 것이 좋습니다.

관리형 AWS 애플리케이션을 비활성화하려면

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 애플리케이션 페이지의 AWS 관리형 애플리케이션에서 비활성화하려는 애플리케이션을 선택합니다.
4. 애플리케이션을 선택한 상태에서 작업을 선택하고 비활성화를 선택합니다.
5. 애플리케이션 일시 중지 대화 상자에서 일시 중지를 선택합니다.
6. AWS 관리형 애플리케이션 목록에서 애플리케이션 상태는 비활성으로 표시됩니다.

고객 관리형 애플리케이션

IAM Identity Center를 사용하면 인력 사용자를 생성하거나 연결하고 모든 직원 및 애플리케이션에서 직원 액세스를 중앙에서 관리할 수 있습니다 AWS 계정 . IAM Identity Center는 중앙 ID 서비스 역할을 하며 사용자가 인증할 수 있는 다양한 방법을 제공합니다. 이미 ID 제공업체(IdP)를 사용하는 경우 IAM Identity Center를 IdP와 통합하여 사용자 및 그룹을 IAM Identity Center에 프로비저닝하고 IdP를 인증에 사용할 수 있습니다.

SAML 2.0을 지원하는 고객 관리형 애플리케이션을 사용하는 경우 SAML 2.0을 통해 IdP를 IAM Identity Center에 페더레이션하고 IAM Identity Center를 사용하여 해당 애플리케이션에 대한 사용자 액세스를 관리할 수 있습니다. IAM Identity Center는 Salesforce 및 Microsoft 365와 같이 SAML 2.0을 지원하는 일반적으로 사용되는 애플리케이션의 카탈로그를 제공합니다. 이 카탈로그는 IAM ID 센터 콘솔에서 사용할 수 있습니다. 자체 SAML 2.0 애플리케이션을 설정할 수도 있습니다.

> **Note**
>
> OAuth 2.0을 지원하는 고객 관리형 애플리케이션이 있고 사용자가 이러한 애플리케이션에서 AWS 서비스에 액세스해야 하는 경우 신뢰할 수 있는 ID 전파를 사용할 수 있습니다. 신뢰할 수 있는 ID 전파를 통해 사용자는 애플리케이션에 로그인할 수 있으며, 해당 애플리케이션은 서비스의 데이터에 액세스하기 위한 요청에 사용자의 ID를 전달할 수 있습니다. AWS 자세한 정보는 고객 관리형 애플리케이션에서 신뢰할 수 있는 ID 전파 사용을 참조하세요.

주제

- SAML 2.0 및 OAuth 2.0
- 고객 관리형 SAML 2.0 애플리케이션 설정

SAML 2.0 및 OAuth 2.0

IAM Identity Center를 사용하면 사용자에게 SAML 2.0 또는 OAuth 2.0 애플리케이션에 대한 Single Sign-On 액세스를 제공할 수 있습니다. 다음 주제에서는 SAML 2.0 및 OAuth 2.0에 관한 대략적인 개요를 제공합니다.

주제

- SAML 2.0
- OAuth 2.0

SAML 2.0

SAML 2.0은 SAML 기관(ID 제공업체 또는 IdP라고 함)과 SAML 2.0 소비자(서비스 제공업체 또는 SP라고 함) 간에 사용자에 대한 정보를 전달하는 SAML 어설션을 안전하게 교환하는 데 사용되는 업계 표준입니다. IAM Identity Center는 이 정보를 사용하여 액세스 포털 내에서 애플리케이션을 사용할 권한이 있는 사용자에게 페더레이션된 Single Sign-On 액세스를 제공합니다. AWS

OAuth 2.0

OAuth 2.0은 애플리케이션이 암호를 공유하지 않고도 사용자 데이터에 안전하게 액세스하고 공유할 수 있게 해주는 프로토콜입니다. 이 기능은 사용자가 애플리케이션이 리소스에 액세스하도록 허용할 수 있는 안전하고 표준화된 방법을 제공합니다. 액세스는 다양한 OAuth 2.0 승인 플로우를 통해 작동합니다.

IAM Identity Center를 사용하면 퍼블릭 클라이언트에서 실행되는 애플리케이션이 사용자를 대신하여 프로그래밍 방식으로 AWS 계정 액세스하고 서비스하기 위한 임시 자격 증명을 검색할 수 있습니다. 퍼블릭 클라이언트는 일반적으로 애플리케이션을 로컬에서 실행하는 데 사용되는 데스크톱, 랩톱 또는 기타 모바일 디바이스입니다. 공용 클라이언트에서 실행되는 AWS 응용 프로그램의 예로는 AWS Command Line Interface (AWS CLI) AWS Toolkit, AWS 소프트웨어 개발 키트 (SDK) 가 있습니다. 이러한 애플리케이션이 자격 증명을 얻을 수 있도록 IAM Identity Center는 다음 OAuth 2.0 흐름의 일부를 지원합니다.

- 코드 교환을 위한 증명 키 (PKCE) 를 위한 인증 코드 부여 (RFC 6749 및 RFC 7636)
- 디바이스 인증 부여 (RFC 8628)

> **Note**
>
> 이러한 권한 부여 유형은 이 기능을 AWS 서비스 지원하는 경우에만 사용할 수 있습니다. 이러한 서비스는 이 보조금 유형을 전혀 지원하지 않을 수도 AWS 리전있습니다. 지역별 차이에 AWS 서비스 대해서는 관련 설명서를 참조하십시오.

OpenID Connect (OIDC) 는 OAuth 2.0 프레임워크를 기반으로 하는 인증 프로토콜입니다. OIDC는 인증에 OAuth 2.0을 사용하는 방법을 지정합니다. 애플리케이션은 IAM Identity Center OIDC 서비스 API를 통해 OAuth 2.0 클라이언트를 등록하고 이러한 흐름 중 하나를 사용하여 IAM ID 센터 보호 API에 대한 권한을 제공하는 액세스 토큰을 얻습니다. 애플리케이션은 액세스 범위를 지정하여 의도한 API 사용자를 선언합니다. IAM Identity Center 관리자가 ID 소스를 구성한 후에는 애플리케이션 최종 사용자가 로그인 프로세스를 완료해야 합니다 (아직 로그인 프로세스를 완료하지 않았다면). 그러면 최종

사용자는 애플리케이션이 API 호출을 할 수 있도록 동의해야 합니다. 이러한 API 호출은 사용자의 권한을 사용하여 이루어집니다. 이에 대한 응답으로 IAM Identity Center는 사용자가 동의한 액세스 범위가 포함된 액세스 토큰을 애플리케이션에 반환합니다.

OAuth 2.0 승인 흐름 사용

OAuth 2.0 승인 흐름은 흐름을 지원하는 AWS 관리형 애플리케이션을 통해서만 사용할 수 있습니다. OAuth 2.0 흐름을 사용하려면 IAM Identity Center 인스턴스와 사용하는 지원되는 AWS 관리형 애플리케이션을 모두 한 곳에 배포해야 합니다. AWS 리전 AWS 관리형 애플리케이션 및 AWS 서비스 사용하려는 IAM Identity Center 인스턴스의 지역별 가용성을 결정하려면 각 설명서를 참조하십시오.

OAuth 2.0 흐름을 사용하는 애플리케이션을 사용하려면 최종 사용자가 애플리케이션을 연결하고 IAM Identity Center 인스턴스에 등록할 URL을 입력해야 합니다. 애플리케이션에 따라 관리자는 IAM Identity Center 인스턴스의 AWS 액세스 포털 URL 또는 발급자 URL을 사용자에게 제공해야 합니다. 이 두 설정은 IAM ID 센터 콘솔 설정 페이지에서 찾을 수 있습니다. 클라이언트 애플리케이션 구성에 대한 추가 정보는 해당 애플리케이션의 설명서를 참조하십시오.

애플리케이션에 로그인하고 동의를 제공하는 최종 사용자 환경은 애플리케이션이 OR를 사용하는지 여부에 따라 달라집니다장치 인증 부여. PKCE를 통한 권한 부여 코드 허용

PKCE를 통한 권한 부여 코드 허용

이 흐름은 브라우저가 있는 장치에서 실행되는 응용 프로그램에서 사용됩니다.

1. 브라우저 창이 열립니다.
2. 사용자가 인증되지 않은 경우 브라우저는 사용자를 리디렉션하여 사용자 인증을 완료합니다.
3. 인증 후 사용자에게 다음 정보를 표시하는 동의 화면이 표시됩니다.
   - 애플리케이션 이름
   - 애플리케이션이 사용 동의를 요청하는 액세스 범위
4. 사용자는 동의 프로세스를 취소하거나 동의할 수 있으며 애플리케이션은 사용자의 권한에 따라 액세스를 진행합니다.

장치 인증 부여

이 흐름은 브라우저가 있든 없든 디바이스에서 실행되는 애플리케이션에서 사용할 수 있습니다. 응용 프로그램이 흐름을 시작하면 응용 프로그램은 사용자가 흐름의 후반부에 확인해야 하는 URL과 사용자 코드를 제공합니다. 흐름을 시작하는 응용 프로그램이 사용자가 동의한 장치가 아닌 다른 장치에서 실행될 수 있으므로 사용자 코드가 필요합니다. 코드는 사용자가 다른 기기에서 시작한 흐름에 동의하는지 확인합니다.

1. 브라우저가 있는 장치에서 흐름이 시작되면 브라우저 창이 열립니다. 브라우저가 없는 디바이스에서 플로우를 시작하는 경우 사용자는 다른 디바이스에서 브라우저를 열고 애플리케이션이 제공한 URL로 이동해야 합니다.
2. 어느 경우든 사용자가 인증되지 않은 경우 브라우저는 사용자를 리디렉션하여 사용자 인증을 완료합니다.
3. 인증 후 사용자에게 다음 정보를 표시하는 동의 화면이 표시됩니다.
   - 애플리케이션 이름
   - 애플리케이션이 사용 동의를 요청하는 액세스 범위
   - 애플리케이션이 사용자에게 제공한 사용자 코드
4. 사용자는 동의 절차를 취소하거나 동의할 수 있으며 애플리케이션은 사용자의 권한에 따라 액세스를 진행합니다.

액세스 범위

범위는 OAuth 2.0 흐름을 통해 액세스할 수 있는 서비스에 대한 서비스 액세스를 정의합니다. 범위는 리소스 서버라고도 하는 서비스가 작업 및 서비스 리소스와 관련된 권한을 그룹화하는 방법이며 OAuth 2.0 클라이언트가 요청할 수 있는 세분화된 작업을 지정합니다. OAuth 2.0 클라이언트가 IAM Identity Center OIDC 서비스에 등록하면 클라이언트는 의도한 작업을 선언할 범위를 지정하며, 이 경우 사용자는 이에 동의해야 합니다.

OAuth 2.0 클라이언트는 OAuth 2.0 (RFC 6749) 의 섹션 3.3에 정의된 `scope` 값을 사용하여 액세스 토큰에 대해 요청되는 권한을 지정합니다. 클라이언트는 액세스 토큰을 요청할 때 최대 25개의 범위를 지정할 수 있습니다. PKCE 또는 디바이스 권한 부여 절차를 통한 인증 코드 부여 중에 사용자가 동의를 제공하면 IAM Identity Center는 반환되는 액세스 토큰으로 범위를 인코딩합니다.

AWS 지원을 위해 IAM ID 센터에 범위를 추가합니다. AWS 서비스다음 표에는 퍼블릭 클라이언트를 등록할 때 IAM Identity Center OIDC 서비스가 지원하는 범위가 나와 있습니다.

퍼블릭 클라이언트를 등록할 때 IAM Identity Center OIDC 서비스에서 지원하는 액세스 범위는 다음과 같습니다.

범위	설명	지원되는 서비스
`sso:account:access`	IAM Identity Center 관리 계정 및 권한 세트에 액세스합니다.	IAM Identity Center

범위	설명	지원되는 서비스
`codewhisperer:analysis`	Amazon Q 개발자 코드 분석에 액세스할 수 있도록 합니다.	AWS Builder ID 및 IAM 아이덴티티 센터
`codewhisperer:completions`	Amazon Q 인라인 코드 제안에 대한 액세스를 활성화합니다.	AWS Builder ID 그리고 IAM 아이덴티티 센터
`codewhisperer:conversations`	Amazon Q 채팅에 대한 액세스를 활성화합니다.	AWS Builder ID 및 IAM 아이덴티티 센터
`codewhisperer:taskassist`	소프트웨어 개발을 위해 Amazon Q 개발자 에이전트에 액세스할 수 있도록 합니다.	AWS Builder ID 및 IAM 아이덴티티 센터
`codewhisperer:transformations`	코드 변환을 위해 Amazon Q 개발자 에이전트에 액세스할 수 있도록 합니다.	AWS Builder ID 그리고 IAM 아이덴티티 센터
`codecatalyst:read_write`	Amazon CodeCatalyst 리소스를 읽고 쓸 수 있으므로 모든 기존 리소스에 액세스할 수 있습니다.	AWS Builder ID 및 IAM 아이덴티티 센터

고객 관리형 SAML 2.0 애플리케이션 설정

SAML 2.0을 지원하는 고객 관리형 애플리케이션을 사용하는 경우 SAML 2.0을 통해 IdP를 IAM Identity Center에 페더레이션하고 IAM Identity Center를 사용하여 해당 애플리케이션에 대한 사용자 액세스를 관리할 수 있습니다. IAM Identity Center 콘솔의 일반적으로 사용되는 애플리케이션 카탈로그에서 SAML 2.0 애플리케이션을 선택하거나 자체 SAML 2.0 애플리케이션을 설정할 수 있습니다.

> **Note**
>
> OAuth 2.0을 지원하는 고객 관리형 애플리케이션이 있고 사용자가 이러한 애플리케이션에서 AWS 서비스에 액세스해야 하는 경우 신뢰할 수 있는 ID 전파를 사용할 수 있습니다. 신뢰할 수 있는 ID 전파를 통해 사용자는 애플리케이션에 로그인할 수 있으며, 해당 애플리케이션은 서비

스의 데이터에 액세스하기 위한 요청에 사용자의 ID를 전달할 수 있습니다. AWS 자세한 정보는 고객 관리형 애플리케이션에서 신뢰할 수 있는 ID 전파 사용을 참조하세요.

주제

- IAM Identity Center 애플리케이션 카탈로그
- 자체 SAML 2.0 애플리케이션 설정

IAM Identity Center 애플리케이션 카탈로그

IAM Identity Center 콘솔의 애플리케이션 카탈로그를 사용하여 IAM Identity Center에서 일반적으로 사용하는 여러 SAML 2.0 애플리케이션을 추가할 수 있습니다. Salesforce, Box, Microsoft 365를 예로 들 수 있습니다.

대부분의 애플리케이션에는 IAM Identity Center와 애플리케이션 서비스 공급자 간의 신뢰 설정 방법에 대한 자세한 정보가 제공됩니다. 이 정보는 카탈로그에서 애플리케이션을 선택한 후 애플리케이션의 구성 페이지에 제공됩니다. 애플리케이션을 구성한 후 필요에 따라 IAM Identity Center의 사용자 또는 그룹에 액세스 권한을 할당할 수 있습니다.

주제

- 애플리케이션 카탈로그에서 애플리케이션 설정

애플리케이션 카탈로그에서 애플리케이션 설정

IAM Identity Center와 애플리케이션의 서비스 공급자 간에 SAML 2.0 신뢰 관계를 설정해야 하는 경우 이 절차를 사용합니다.

이 절차를 시작하기 전에 보다 효율적으로 신뢰를 설정할 수 있도록 서비스 공급자의 메타데이터 교환 파일이 있는 것이 유용합니다. 이 파일이 없는 경우에도 이 절차를 사용하여 신뢰를 수동으로 구성할 수 있습니다.

애플리케이션 카탈로그에서 애플리케이션 추가 및 구성

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 고객 관리형 탭을 선택합니다.
4. 애플리케이션 추가를 선택합니다.

5. 애플리케이션 유형 선택 페이지의 설정 기본 설정에서 카탈로그에서 애플리케이션을 선택하겠습니다를 선택합니다.
6. 애플리케이션 카탈로그에서 검색 상자에 추가하려는 애플리케이션 이름을 입력하기 시작합니다.
7. 검색 결과에 나타나는 목록에서 애플리케이션 이름을 선택한 후 다음을 선택합니다.
8. 애플리케이션 구성 페이지에서 표시 이름 및 설명 필드에 애플리케이션 관련 세부 정보가 미리 채워집니다. 이 정보를 편집할 수 있습니다.
9. IAM Identity Center 메타데이터에서 다음 작업을 수행합니다.

    a. IAM Identity Center SAML 메타데이터 파일에서 다운로드를 선택하여 ID 제공자 메타데이터를 다운로드합니다.

    b. IAM Identity Center 인증서에서 인증서 다운로드를 선택하여 ID 제공자 인증서를 다운로드합니다.

> **Note**
>
> 이러한 파일은 나중에 서비스 공급자의 웹 사이트에서 애플리케이션을 설정할 때 필요합니다. 해당 제공업체의 지침을 따르세요.

10. (선택 사항) 애플리케이션 속성에서 애플리케이션 시작 URL, 릴레이 상태 및 세션 지속 시간을 지정할 수 있습니다. 자세한 정보는 IAM Identity Center 콘솔의 애플리케이션 속성 구성을 참조하세요.
11. 애플리케이션 메타데이터에서 다음 작업 중 하나를 수행합니다.

    a. 메타데이터 파일이 있는 경우 애플리케이션 SAML 메타데이터 파일 업로드를 선택합니다. 그런 다음 파일 선택에서 메타데이터 파일을 찾아 선택합니다.

    b. 메타데이터 파일이 없는 경우 메타데이터 값 수동 입력을 선택한 다음 애플리케이션 ACS URL 및 애플리케이션 SAML 대상 값을 입력합니다.
12. 제출을 선택합니다. 방금 추가한 애플리케이션의 세부정보 페이지로 이동합니다.

자체 SAML 2.0 애플리케이션 설정

SAML 2.0을 사용하여 ID 페더레이션을 허용하는 자체 애플리케이션을 설정하고 이를 IAM Identity Center에 추가할 수 있습니다. 자체 SAML 2.0 애플리케이션을 설정하는 대부분의 단계는 IAM Identity Center 콘솔의 애플리케이션 카탈로그에서 SAML 2.0 애플리케이션을 설정하는 단계와 동일합니다. 하지만 자체 SAML 2.0 애플리케이션을 위한 추가 SAML 속성 매핑도 제공해야 합니다. 이러한 매핑을

통해 IAM Identity Center에서 애플리케이션에 올바른 SAML 2.0 어설션을 채울 수 있습니다. 애플리케이션을 처음 설정할 때 해당 추가 SAML 속성 매핑을 제공할 수 있습니다. 또한 IAM Identity Center 콘솔의 애플리케이션 세부 정보 페이지에 SAML 2.0 속성 매핑을 제공할 수 있습니다.

IAM Identity Center와 SAML 2.0 애플리케이션의 서비스 공급자 간에 SAML 2.0 신뢰 관계를 설정해야 하는 경우 다음 절차를 사용합니다. 이 절차를 시작하기 전에 신뢰 설정을 완료할 수 있도록 서비스 제공업체의 인증서 및 메타데이터 교환 파일이 있는지 확인하세요.

자체 SAML 2.0 애플리케이션 설정

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 고객 관리형 탭을 선택합니다.
4. 애플리케이션 추가를 선택합니다.
5. 애플리케이션 유형 선택 페이지의 설정 기본 설정에서 설정하고자 하는 애플리케이션이 있습니다를 선택합니다.
6. 애플리케이션 유형에서 SAML 2.0을 선택합니다.
7. 다음을 선택합니다.
8. 애플리케이션 구성 페이지의 애플리케이션 구성에서 **MyApp**와 같이 애플리케이션의 표시 이름을 입력합니다. 그런 다음 설명을 입력합니다.
9. IAM Identity Center 메타데이터에서 다음 작업을 수행합니다.

    a. IAM Identity Center SAML 메타데이터 파일에서 다운로드를 선택하여 ID 제공자 메타데이터를 다운로드합니다.

    b. IAM Identity Center 인증서에서 다운로드를 선택하여 ID 제공업체 인증서를 다운로드합니다.

    > **Note**
    >
    > 이러한 파일은 나중에 서비스 제공자의 웹 사이트에서 사용자 지정 애플리케이션을 설정할 때 필요합니다.

10. (선택 사항) 애플리케이션 속성에서 애플리케이션 시작 URL, 릴레이 상태 및 세션 지속 시간을 지정할 수도 있습니다. 자세한 정보는 IAM Identity Center 콘솔의 애플리케이션 속성 구성을 참조하세요.
11. 애플리케이션 메타데이터에서 메타데이터 값 수동 입력을 선택합니다. 그런 다음 애플리케이션 ACS URL과 애플리케이션 SAML 대상 값을 제공합니다.

12. 제출을 선택합니다. 방금 추가한 애플리케이션의 세부정보 페이지로 이동합니다.

애플리케이션 간 신뢰할 수 있는 ID 전파

신뢰할 수 있는 ID 전파를 통해 AWS 서비스는 다음을 수행할 수 있습니다.

- 사용자의 ID 컨텍스트를 기반으로 AWS 리소스에 대한 액세스를 승인합니다.
- 사용자의 ID 컨텍스트를 다른 AWS 서비스와 안전하게 공유하세요.

이러한 기능을 통해 사용자 액세스를 보다 쉽게 정의, 부여 및 기록할 수 있습니다.

신뢰할 수 있는 ID 전파를 통해 사용자는 애플리케이션에 로그인할 수 있으며, 해당 애플리케이션은 서비스의 데이터에 액세스하기 위한 요청에 사용자의 ID 컨텍스트를 전달할 수 있습니다. AWS 액세스는 사용자 ID를 기반으로 관리되므로 사용자는 데이터 액세스를 위해 데이터베이스 로컬 사용자 보안 인증 정보를 사용하거나 IAM 역할을 맡지 않아도 됩니다.

주제

- 신뢰할 수 있는 ID 전파 개요
- 신뢰할 수 있는 ID 전파 사용 사례
- 신뢰할 수 있는 ID 전파 설정
- 신뢰할 수 있는 토큰 발급자를 사용하여 애플리케이션 사용

신뢰할 수 있는 ID 전파 개요

신뢰할 수 있는 ID 전파를 사용하면 AWS 리소스에 대한 사용자 액세스를 보다 쉽게 정의, 부여 및 기록할 수 있습니다. 신뢰할 수 있는 ID 전파는 OAuth 2.0 권한 부여 프레임워크를 기반으로 하고, 이를 통해 애플리케이션은 암호를 공유하지 않고도 사용자 데이터에 안전하게 액세스하고 이를 공유할 수 있습니다. OAuth 2.0은 애플리케이션 리소스에 대한 보안 위임 액세스를 제공합니다. 액세스가 위임된 이유는 리소스 관리자가 사용자가 로그인한 애플리케이션을 승인하거나 위임하여 다른 애플리케이션에 액세스할 수 있도록 하기 때문입니다.

사용자 암호 공유를 방지하기 위해 신뢰할 수 있는 ID 전파에서는 토큰을 사용합니다. 토큰은 신뢰할 수 있는 애플리케이션이 사용자가 누구인지, 두 애플리케이션 간에 허용되는 요청을 확인할 수 있는 표준 방법을 제공합니다. AWS 신뢰할 수 있는 ID 전파와 통합되는 관리형 애플리케이션은 IAM Identity Center에서 직접 토큰을 얻습니다. 또한 IAM Identity Center는 애플리케이션이 ID 토큰을 교환하고 외부 OAuth 2.0 권한 부여 서버에서 가져온 토큰에 액세스할 수 있는 옵션을 제공합니다. 이를 통해 애플

리케이션은 외부에서 토큰을 인증 및 획득하고 AWS, 토큰을 IAM Identity Center 토큰으로 교환하고, 새 토큰을 사용하여 서비스에 요청할 수 있습니다. AWS 자세한 정보는 신뢰할 수 있는 토큰 발급자를 사용하여 애플리케이션 사용을 참조하세요.

OAuth 2.0 프로세스는 사용자가 애플리케이션에 로그인할 때 시작됩니다. 사용자가 로그인한 애플리케이션은 다른 애플리케이션의 리소스에 대한 액세스 요청을 시작합니다. 시작(요청) 애플리케이션은 권한 부여 서버에서 토큰을 요청하여 사용자 대신 수신 애플리케이션에 액세스할 수 있습니다. 권한 부여 서버가 토큰을 반환하면 시작 애플리케이션이 액세스 요청과 함께 해당 토큰을 수신 애플리케이션에 전달합니다.

신뢰할 수 있는 ID 전파 사용 사례

IAM Identity Center 관리자는 이 기능을 지원하는 다음과 같은 시작 애플리케이션과 연결된 서비스 간에 신뢰할 수 있는 ID 전파를 구성하도록 도와달라는 요청을 받을 수 있습니다. AWS 다음 섹션에서는 신뢰할 수 있는 ID 전파를 시작할 수 있는 애플리케이션이 지원하는 특정 사용 사례에 대한 자세한 정보를 제공합니다.

주제

- Amazon EMR
- 아마존 QuickSight
- Amazon Redshift 쿼리 편집기 v2
- 타사 비즈니스 인텔리전스 애플리케이션
- 사용자 지정 개발 애플리케이션

Amazon EMR

Amazon EMR을 다음과 같은 신뢰할 수 있는 ID 전파 사용 사례의 시작 애플리케이션으로 사용할 수 있습니다.

설명	사용된 기타 서비스 AWS	자세히 알아보기
Amazon EMR 스튜디오를 통해 Amazon EC2 클러스터의 Amazon EMR에서 Apache Spark를 사용하여 대화형 분석을 실행할 수 있습니다. Catalog를 통해	아마존 S3 액세스 그랜트, 아마존 S3를 통해 승인된 AWS Lake Formation아마존 EC2	• Amazon EMR 관리 가이드의 Amazon EMR을 IAM ID 센터와 통합하십시오.

설명	사용된 기타 서비스 AWS	자세히 알아보기
직원 ID 및 관련 속성을 기반으로 액세스 제어를 적용하십시오. AWS Glue AWS Lake Formation	기반 아마존 EMR AWS Service Catalog **Note** • Amazon EMR 스튜디오를 통해 액세스해야 합니다. • 테이블 수준의 액세스 제어만 가능합니다. • 아파치 하이브, 프레스토 SQL/트리노, EMR 서버리스는 지원되지 않습니다.	• Amazon S3 액세스 권한 부여 및 기업 디렉터리 ID는 Amazon 심플 스토리지 서비스 사용 설명서에 나와 있습니다. • 개발자 안내서의 IAM ID 센터에 연결 AWS Lake FormationAWS Lake Formation • 빅 데이터 블로그의 Amazon EMR 및 IAM ID 센터를 통해 기업 ID를 분석에 사용하십시오.AWS

설명	사용된 기타 서비스 AWS	자세히 알아보기
Amazon EMR 스튜디오를 통해 Athena에서 Trino를 사용하여 임시 분석을 실행합니다. Catalog를 통해 직원 ID 및 관련 속성을 기반으로 액세스 제어를 적용하십시오. AWS Glue AWS Lake Formation Amazon S3 액세스 권한을 사용하여 Amazon S3의 Athena 쿼리 결과 버킷 위치에 안전하게 액세스할 수 있습니다.	Athena는 Amazon S3 액세스 AWS Lake Formation그랜트를 통해 인증을 받았습니다. **Note** Amazon EMR 스튜디오를 통해 액세스해야 합니다. Amazon Athena 콘솔에서의 직접 액세스는 지원되지 않습니다.	• Amazon EMR 관리 가이드의 Amazon EMR을 IAM ID 센터와 통합하십시오. • Amazon Athena 사용 설명서에서 IAM ID 센터를 사용하여 Athena 워크그룹을 활성화했습니다. • Amazon S3 액세스 권한 부여 및 기업 디렉터리 ID는 Amazon 심플 스토리지 서비스 사용 설명서에 나와 있습니다. • AWS Lake Formation 개발자 안내서의 IAM ID 센터에 연결 AWS Lake Formation. • Amazon EMR Studio와 Athena의 빅 데이터 블로그에 직원 정체성을 소개하십시오.AWS

아마존 QuickSight

Amazon을 다음과 같은 신뢰할 수 있는 ID 전파 사용 사례의 시작 QuickSight 애플리케이션으로 사용할 수 있습니다.

설명	사용된 기타 서비스 AWS	자세히 알아보기
아마존 QuickSight 사용자는 아마존 Redshift 데이터를 쿼리할 수 있습니다. Amazon Redshift에서는 Amazon Redshift 관리자가 데이터 액세스 권한을 부여합니다.	Amazon Redshift	• Redshift와 IAM ID 센터를 연결하여 Amazon Redshift 관리 가이드에서 사용자에게 싱글 사인온 경험을 제공하십시오. • Amazon Redshift 관리 QuickSight 가이드에서 아마

설명	사용된 기타 서비스 AWS	자세히 알아보기
		존을 통해 Amazon Redshift를 IAM ID 센터와 연결하십시오.
Amazon QuickSight 사용자는 Amazon Redshift Spectrum을 쿼리하여 AWS Lake Formation 관리자의 승인을 받은 액세스 권한을 사용하여 Amazon S3의 정형 데이터를 검색할 수 있습니다.	아마존 Redshift Spectrum, 아마존 S3 정형 데이터 *다음을 통해 승인된 아마존 Redshift Spectrum을 통해 AWS Lake Formation	• Redshift와 IAM ID 센터를 연결하여 Amazon Redshift 관리 가이드에서 사용자에게 싱글 사인온 경험을 제공하십시오. • Amazon Redshift 관리 QuickSight 가이드에서 아마존을 통해 Amazon Redshift를 IAM ID 센터와 연결하십시오. • 개발자 AWS Lake Formation 안내서에서 IAM ID 센터에 연결하기.AWS Lake Formation • Amazon Redshift를 사용하여 액세스 관리를 간소화하고 AWS 빅 데이터 블로그에서 외부 ID 공급자 사용자의 액세스 관리를 간소화하십시오. AWS Lake Formation

설명	사용된 기타 서비스 AWS	자세히 알아보기
Amazon QuickSight 사용자는 관리자가 승인한 액세스 권한으로 Amazon S3의 정형 데이터에 대해 Amazon Redshift 데이터 공유를 쿼리할 수 있습니다. AWS Lake Formation	아마존 Redshift 데이터 셰어, 아마존 S3 정형 데이터 *다음을 통해 승인된 아마존 Redshift를 통해 AWS Lake Formation	• Amazon Redshift 관리 QuickSight 가이드에서 아마존을 통해 Amazon Redshift를 IAM ID 센터와 연결하십시오. • 개발자 AWS Lake Formation 안내서에서 IAM ID 센터에 연결하기.AWS Lake Formation • Amazon Redshift를 사용하여 액세스 관리를 간소화하고 AWS 빅 데이터 블로그에서 외부 ID 공급자 사용자의 액세스 관리를 간소화하십시오. AWS Lake Formation

Amazon Redshift 쿼리 편집기 v2

Amazon Redshift 쿼리 편집기 v2를 다음과 같은 신뢰할 수 있는 ID 전파 사용 사례의 시작 애플리케이션으로 사용할 수 있습니다.

설명	사용된 기타 서비스 AWS	자세히 알아보기
아마존 Redshift 쿼리 에디터 v2 사용자는 아마존 Redshift 데이터를 쿼리할 수 있습니다. Amazon Redshift에서는 Amazon Redshift 관리자가 데이터 액세스 권한을 부여합니다.	Amazon Redshift	• Redshift와 IAM ID 센터를 연결하여 Amazon Redshift 관리 가이드에서 사용자에게 싱글 사인온 경험을 제공하십시오. • Amazon Redshift 관리 가이드에서 Amazon Redshift 데이터베이스에 연결하십시오. • 빅 데이터 블로그에서 원활한 싱글 사인온을 사용하여 AWS IAM Identity Center Amazon

설명	사용된 기타 서비스 AWS	자세히 알아보기
		Redshift 쿼리 편집기 Okta V2와 통합하십시오AWS .
Amazon Redshift 쿼리 에디터 v2 사용자는 Amazon Redshift Spectrum 외부 테이블에서 관리자가 승인한 액세스 권한을 통해 Amazon S3의 정형 데이터를 쿼리할 수 있습니다. AWS Lake Formation	아마존 Redshift Spectrum, 아마존 S3 정형 데이터 *다음을 통해 승인된 아마존 Redshift Spectrum을 통해 AWS Lake Formation	• Redshift와 IAM ID 센터를 연결하여 Amazon Redshift 관리 가이드에서 사용자에게 싱글 사인온 경험을 제공하십시오. • Amazon Redshift 관리 가이드에서 Amazon Redshift 데이터베이스에 연결하십시오. • 개발자 AWS Lake Formation 안내서에서 IAM ID 센터에 연결하기.AWS Lake Formation
Amazon Redshift 쿼리 에디터 v2 사용자는 관리자가 승인한 액세스 권한으로 Amazon Redshift 데이터 공유를 쿼리할 수 있습니다. AWS Lake Formation	아마존 레드시프트 데이터웨어, AWS Lake Formation	• Amazon Redshift 관리 가이드에서 Amazon Redshift 데이터베이스에 연결하십시오. • 개발자 AWS Lake Formation 안내서에서 IAM ID 센터에 연결하기.AWS Lake Formation

타사 비즈니스 인텔리전스 애플리케이션

Tableau와 같은 타사 비즈니스 인텔리전스 애플리케이션을 신뢰할 수 있는 특정 ID 전파 사용 사례의 시작 애플리케이션으로 사용할 수 있습니다. 수정된 타사 비즈니스 인텔리전스 애플리케이션은 OAuth ID 토큰 또는 액세스 토큰을 통해 Amazon Redshift 드라이버에 사용자 ID를 전달하여 Amazon Redshift 관리자가 승인한 액세스 권한이 있는 데이터를 Amazon Redshift에 쿼리할 수 있습니다.

사용자 지정 개발 애플리케이션

자체 개발한 애플리케이션을 다음과 같은 신뢰할 수 있는 ID 전파 사용 사례의 시작 애플리케이션으로 사용할 수 있습니다.

설명	사용된 기타 서비스 AWS	자세히 알아보기
OAuth 권한 부여 서버를 통해 사용자를 인증하는 애플리케이션을 만든 다음, AWS IAM Identity Center 및 IAM을 사용하여 ID 강화 IAM 역할 자격 증명을 얻으십시오. 이 자격 증명은 Amazon S3 Access Grants 관리자가 승인한 액세스 권한과 함께 Amazon S3의 비정형 데이터에 대한 액세스를 요청하는 데 사용됩니다.	AWS IAM Identity Center, 아마존 S3 비정형 데이터 *Amazon S3 액세스 허가를 통해 승인됨	• Amazon S3 액세스 권한 부여 및 기업 디렉터리 ID는 Amazon 심플 스토리지 서비스 사용 설명서에 나와 있습니다. • IAM ID 센터 및 Amazon S3 액세스 권한 부여 (1부) 및 (2부)를 사용하여 사용자 대상 데이터 애플리케이션을 개발하는 방법은AWS 스토리지 블로그에 실려 있습니다.
Amazon Q Business와 상호 작용하여 자체 콘텐츠 및 사용자 권한을 기반으로 사용자 질문에 응답하는 사용자 지정 애플리케이션을 구축하십시오.	IAM 아이덴티티 센터, 아마존 Q 비즈니스	• Amazon Q 비즈니스 사용 설명서에서 IAM ID 센터 인스턴스를 활성화하고 구성하십시오. • IAM Identity Center에서 AWS 관리형 애플리케이션을 사용하는 방법: 보안 블로그에서 기존 IAM 페더레이션 플로우를 마이그레이션하지 않고 Amazon Q를AWS 활성화하십시오.

신뢰할 수 있는 ID 전파 설정

신뢰할 수 있는 ID 전파는 애플리케이션이 사용자 ID를 서비스에 전달할 수 있도록 다양한 인증 방법을 지원합니다. AWS 신뢰할 수 있는 ID 전파 설정은 애플리케이션 유형 및 인증 방법에 따라 달라집니다.

> **Note**
>
> 관리 애플리케이션에 대한 액세스를 요청하지만 AWS API를 사용하여 연결하지 않는 고객 관리형 애플리케이션이 있는 경우 신뢰할 수 AWS 있는 토큰 발급자를 설정해야 합니다.

주제

- 필수 조건 및 고려 사항
- 관리되는 애플리케이션에 신뢰할 수 있는 ID 전파 사용 AWS
- 고객 관리형 애플리케이션에서 신뢰할 수 있는 ID 전파 사용

필수 조건 및 고려 사항

신뢰할 수 있는 ID 전파를 설정하기 전에 다음 사전 조건 및 고려 사항을 검토합니다.

주제

- 필수 조건
- 추가 고려 사항

필수 조건

신뢰할 수 있는 ID 전파를 사용하려면 환경에서 다음 사전 조건이 충족되어야 합니다.

- 사용자 및 그룹이 프로비저닝된 IAM Identity Center 배포

  신뢰할 수 있는 ID 전파를 사용하려면 IAM Identity Center를 활성화하고 사용자 및 그룹을 프로비저닝해야 합니다. 자세한 내용은 IAM Identity Center에서 일반 작업 시작을 참조하세요.

  조직 인스턴스 권장 - Organizations의 관리 계정에서 활성화한 IAM Identity Center의 AWS 조직 인스턴스를 사용하는 것이 좋습니다. 신뢰할 수 있는 ID 전파를 사용하여 사용자가 동일한 조직 AWS 계정 내의 다른 AWS 서비스 및 관련 리소스에 액세스할 수 있도록 하려는 경우 IAM Identity Center 인스턴스 관리를 구성원 계정에 위임할 수 있습니다.

  IAM Identity Center의 단일 계정 인스턴스를 사용하려는 경우 신뢰할 수 있는 ID 전파를 통해 사용자가 액세스하도록 하려는 모든 AWS서비스와 리소스는 IAM Identity Center를 활성화한 조직의 동일한 독립 실행형 AWS 계정또는 동일한 구성원 계정에 있어야 합니다. 자세한 정보는 IAM Identity Center의 계정 인스턴스을 참조하세요.
- AWS 관리형 애플리케이션의 경우, IAM ID 센터에 연결

  신뢰할 수 있는 ID 전파를 사용하려면 AWS 관리형 애플리케이션을 IAM Identity Center와 통합해야 합니다.

추가 고려 사항

신뢰할 수 있는 ID 전파 사용에 관한 추가 고려 사항에 유의하세요.

- 관리형 애플리케이션의 할당 필요 설정을 수정하지 마세요. AWS

  AWS 관리되는 애플리케이션에는 사용자 및 그룹에 할당이 필요한지 여부를 결정하는 기본 설정 구성이 있습니다. 이 설정은 수정하지 않는 것이 좋습니다. 특정 리소스에 대한 사용자 액세스를 허용하는 세분화된 권한을 구성한 경우에도 할당 필요 설정을 수정하면 해당 리소스에 대한 사용자 액세스가 중단되는 등 예기치 않은 동작이 발생할 수 있습니다.

- 다중 계정 권한(권한 세트)은 필요하지 않음

  신뢰할 수 있는 ID 전파에는 다중 계정 권한(권한 세트) 설정이 필요하지 않습니다. IAM Identity Center를 활성화하고 신뢰할 수 있는 ID 전파에만 사용할 수 있습니다.

관리되는 애플리케이션에 신뢰할 수 있는 ID 전파 사용 AWS

신뢰할 수 있는 ID 전파를 통해 AWS 관리형 애플리케이션은 사용자를 대신하여 AWS 서비스의 데이터에 대한 액세스를 요청할 수 있습니다. 데이터 액세스 관리는 사용자 ID를 기반으로 하므로 관리자는 사용자의 기존 사용자 및 그룹 구성원 자격을 기반으로 액세스 권한을 부여할 수 있습니다. 사용자의 ID, 사용자를 대신하여 수행된 작업 및 기타 이벤트는 서비스별 로그 및 이벤트에 기록됩니다. CloudTrail

신뢰할 수 있는 ID 전파는 OAuth 2.0 표준을 기반으로 합니다. 이 기능을 사용하려면 AWS 관리형 애플리케이션을 IAM Identity Center와 통합해야 합니다. AWS 분석 서비스는 호환 가능한 애플리케이션이 신뢰할 수 있는 ID 전파를 사용할 수 있도록 하는 드라이버 기반 인터페이스를 제공할 수 있습니다. 예를 들어, JDBC, ODBC 및 Python 드라이버를 사용하면 호환 쿼리 도구에서 추가 설정 단계를 완료할 필요 없이 신뢰할 수 있는 ID 전파를 사용할 수 있습니다.

주제

- 신뢰할 수 있는 ID 전파를 위한 AWS 관리형 애플리케이션을 설정합니다.
- 관리형 애플리케이션을 위한 신뢰할 수 있는 ID 전파 요청 흐름 AWS
- 애플리케이션에서 토큰을 획득한 후
- ID 강화 IAM 역할 세션
- ID 강화 IAM 역할 세션의 유형
- AWS 관리되는 애플리케이션의 설정 프로세스 및 요청 흐름

신뢰할 수 있는 ID 전파를 위한 AWS 관리형 애플리케이션을 설정합니다.

AWS 신뢰할 수 있는 ID 전파를 지원하는 서비스는 이 기능을 설정하는 데 사용할 수 있는 관리 사용자 인터페이스와 API를 제공합니다. IAM Identity Center 내에서 이러한 서비스를 구성할 필요는 없습니다.

다음은 신뢰할 수 있는 ID 전파를 위한 AWS 서비스를 설정하는 고급 프로세스입니다. 구체적인 단계는 애플리케이션에서 제공하는 관리 인터페이스 및 API에 따라 달라집니다.

1. 애플리케이션 콘솔 또는 API를 사용하여 애플리케이션을 IAM Identity Center 인스턴스에 연결

   AWS 관리형 애플리케이션용 콘솔 또는 애플리케이션 API를 사용하여 애플리케이션을 IAM Identity Center 인스턴스에 연결합니다. 애플리케이션용 콘솔을 사용하는 경우 관리 사용자 인터페이스에 설정 및 연결 프로세스를 간소화하는 위젯이 포함됩니다.
2. 애플리케이션 콘솔 또는 API를 사용하여 애플리케이션 리소스에 대한 사용자 액세스 설정

   이 단계를 완료하여 사용자의 리소스 또는 데이터 액세스 권한을 부여합니다. 액세스는 사용자의 ID 또는 그룹 구성원 자격을 기반으로 합니다. 권한 부여 모델은 애플리케이션에 따라 다릅니다.

> **Important**
>
> 사용자가 AWS 서비스 리소스에 액세스할 수 있도록 하려면 이 단계를 완료해야 합니다. 그렇지 않으면 요청 애플리케이션에 서비스의 액세스 요청 권한이 부여되어도 사용자는 리소스에 액세스할 수 없습니다.

관리형 애플리케이션을 위한 신뢰할 수 있는 ID 전파 요청 흐름 AWS

AWS 관리형 애플리케이션으로의 모든 신뢰할 수 있는 ID 전파 흐름은 IAM Identity Center에서 토큰을 가져오는 애플리케이션에서 시작해야 합니다. 이 토큰은 IAM Identity Center에 알려진 사용자 및 IAM Identity Center에 등록된 애플리케이션에 대한 참조를 포함하므로 필요합니다.

다음 섹션에서는 AWS 관리형 애플리케이션이 IAM Identity Center로부터 토큰을 획득하여 신뢰할 수 있는 ID 전파를 시작하는 방법을 설명합니다.

주제

- 웹 기반, IAM Identity Center 인증
- 콘솔 기반, 사용자 시작 인증 요청

웹 기반, IAM Identity Center 인증

이 흐름의 경우 AWS 관리형 애플리케이션은 인증을 위해 IAM Identity Center를 사용하는 웹 기반 싱글 사인온 환경을 제공합니다.

사용자가 AWS 관리형 애플리케이션을 열면 IAM Identity Center를 사용하는 싱글 사인온 플로우가 트리거됩니다. IAM Identity Center의 사용자에 대한 활성 세션이 없는 경우 지정한 ID 소스를 기반으로 하는 로그인 페이지가 사용자에게 표시되고, IAM Identity Center에서 해당 사용자에 대한 세션을 생성합니다.

IAM Identity Center는 사용자 자격 증명, 대상 목록 (Auds) 및 애플리케이션이 사용하도록 등록된 관련 범위를 포함하는 토큰을 AWS 관리형 애플리케이션에 제공합니다. 그러면 애플리케이션은 토큰을 사용하여 다른 수신 AWS 서비스에 요청을 보낼 수 있습니다.

콘솔 기반, 사용자 시작 인증 요청

이 흐름을 위해 AWS 관리형 애플리케이션은 사용자가 시작하는 콘솔 환경을 제공합니다.

이 경우 AWS 관리 애플리케이션은 역할을 맡은 후 AWS 관리 콘솔에서 입력됩니다. 애플리케이션에서 토큰을 획득하려면 사용자가 애플리케이션을 트리거하여 사용자를 인증하는 프로세스를 시작해야 합니다. 그러면 IAM Identity Center를 사용한 인증이 시작되고, 이 인증은 구성한 ID 소스로 사용자를 리디렉션합니다.

애플리케이션에서 토큰을 획득한 후

요청 애플리케이션이 IAM Identity Center에서 토큰을 획득한 후 애플리케이션은 주기적으로 토큰을 새로 고치고, 이 토큰은 사용자 세션 수명 동안 사용할 수 있습니다. 이 사이 애플리케이션은 다음을 수행할 수 있습니다.

- 토큰에 관한 자세한 정보를 얻어 사용자가 누구인지, 애플리케이션이 다른 수신 AWS 관리형 애플리케이션에서 사용할 수 있는 범위를 결정합니다.
- 토큰을 호출하여 토큰 사용을 지원하는 다른 수신 AWS 관리 애플리케이션에 전달합니다.
- AWS 서명 버전 4를 사용하는 다른 AWS 관리형 애플리케이션에 요청하는 데 사용할 수 있는 ID 강화 IAM 역할 세션을 확보하세요.

  ID 강화 IAM 역할 세션은 IAM Identity Center에서 생성한 토큰에 저장된 사용자의 전파된 ID를 포함하는 IAM 역할 세션입니다.

ID 강화 IAM 역할 세션

AWS Security Token Service 이를 통해 애플리케이션은 ID 강화 IAM 역할 세션을 확보할 수 있습니다. AWS 역할 세션에서 사용자 컨텍스트를 지원하는 관리형 애플리케이션은 ID 정보를 사용하여 역할 세션에 있는 사용자를 기반으로 액세스를 승인할 수 있습니다. 이 새 컨텍스트를 통해 응용 프로그램은 AWS 서명 버전 4 API 요청을 통해 신뢰할 수 있는 ID 전파를 지원하는 AWS 관리되는 응용 프로그램에 요청을 보낼 수 있습니다.

AWS 관리형 애플리케이션이 ID 강화 IAM 역할 세션을 사용하여 리소스에 액세스하는 경우 사용자의 ID (User-ID), 시작 세션 및 수행한 작업을 CloudTrail 기록합니다.

애플리케이션이 ID 강화 IAM 역할 세션을 사용하여 수신 애플리케이션에 요청하면 수신 애플리케이션이 사용자의 ID나 그룹 구성원 자격 또는 IAM 역할을 기반으로 액세스 권한을 부여할 수 있도록 세션에 컨텍스트를 추가합니다. 수신 애플리케이션 또는 요청된 리소스가 사용자의 ID 또는 그룹 구성원 자격을 기반으로 액세스 권한을 부여하도록 구성되지 않은 경우 신뢰할 수 있는 ID 전파를 지원하는 수신 애플리케이션에서 오류를 반환합니다.

이 문제를 방지하려면 다음 중 하나를 수행합니다.

- 수신 애플리케이션이 IAM Identity Center에 연결되어 있는지 확인합니다.
- 수신 애플리케이션용 콘솔 또는 애플리케이션 API를 사용하여 애플리케이션이 사용자의 ID 또는 그룹 구성원 자격을 기반으로 리소스에 대한 액세스 권한을 부여하도록 설정합니다. 이에 대한 설정 요구 사항은 애플리케이션에 따라 다릅니다.

자세한 내용은 수신 AWS 관리형 애플리케이션의 설명서를 참조하세요.

ID 강화 IAM 역할 세션의 유형

애플리케이션은 AWS STS `AssumeRole` API에 요청을 보내고 요청의 파라미터에 컨텍스트 어설션을 전달하여 ID 강화 IAM 역할 세션을 확보합니다. `ProvidedContexts` `AssumeRole` 컨텍스트 어설션은 `SSO OIDC` `CreateTokenWithIAM` 요청의 응답에서 제공되는 `idToken` 클레임에서 가져옵니다.

AWS STS 요청에 제공된 컨텍스트 어설션에 따라 두 가지 유형의 ID 강화 IAM 역할 세션을 생성할 수 있습니다. `AssumeRole`

- 사용자 ID만 기록하는 세션. CloudTrail
- 전파된 사용자 ID를 기반으로 인증을 활성화하고 이를 로그에 기록하는 CloudTrail 세션

CloudTrail 트레일에 등록된 감사 정보만 AWS STS 제공하는 ID 강화 IAM 역할 세션을 얻으려면 요청에 클레임의 가치를 제공하십시오. `sts:audit_context` `AssumeRole` 수신 AWS 서비스가 IAM Identity Center 사용자에게 작업을 수행할 수 있는 권한을 부여할 수 있는 세션을 확보하려면 요청에 클레임 값을 제공하십시오. `sts:identity_context` `AssumeRole` 컨텍스트는 하나만 제공할 수 있습니다.

`sts:audit_context`로 생성된 ID 강화 IAM 역할 세션

로 `sts:audit_context` 생성한 ID 강화 IAM 역할 세션을 사용하여 AWS 서비스를 요청하면 사용자의 IAM Identity `userId` Center가 요소에 로그인됩니다. CloudTrail `OnBehalfOf`

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

> **Note**
>
> 이러한 세션은 Identity Center 사용자 권한 부여에 사용할 수 없습니다. 하지만 IAM 역할 권한을 부여하는 데 사용할 수 있습니다.

에서 AWS STS이러한 유형의 역할 세션을 가져오려면 요청 파라미터의 AssumeRole 요청에 sts:audit_context 필드 값을 제공하십시오. ProvidedContexts arn:aws:iam::aws:contextProvider/IdentityStore를 ProviderArn의 값으로 사용합니다.

sts:identity_context로 생성된 ID 강화 IAM 역할 세션

로 생성된 ID 강화 IAM 역할 세션을 사용하여 사용자가 AWS 서비스에 요청하면 로 sts:identity_context 생성한 세션과 동일한 방식으로 사용자의 IAM Identity userId Center가 onBehalfOf 요소에 로그인됩니다. CloudTrail sts:audit_context

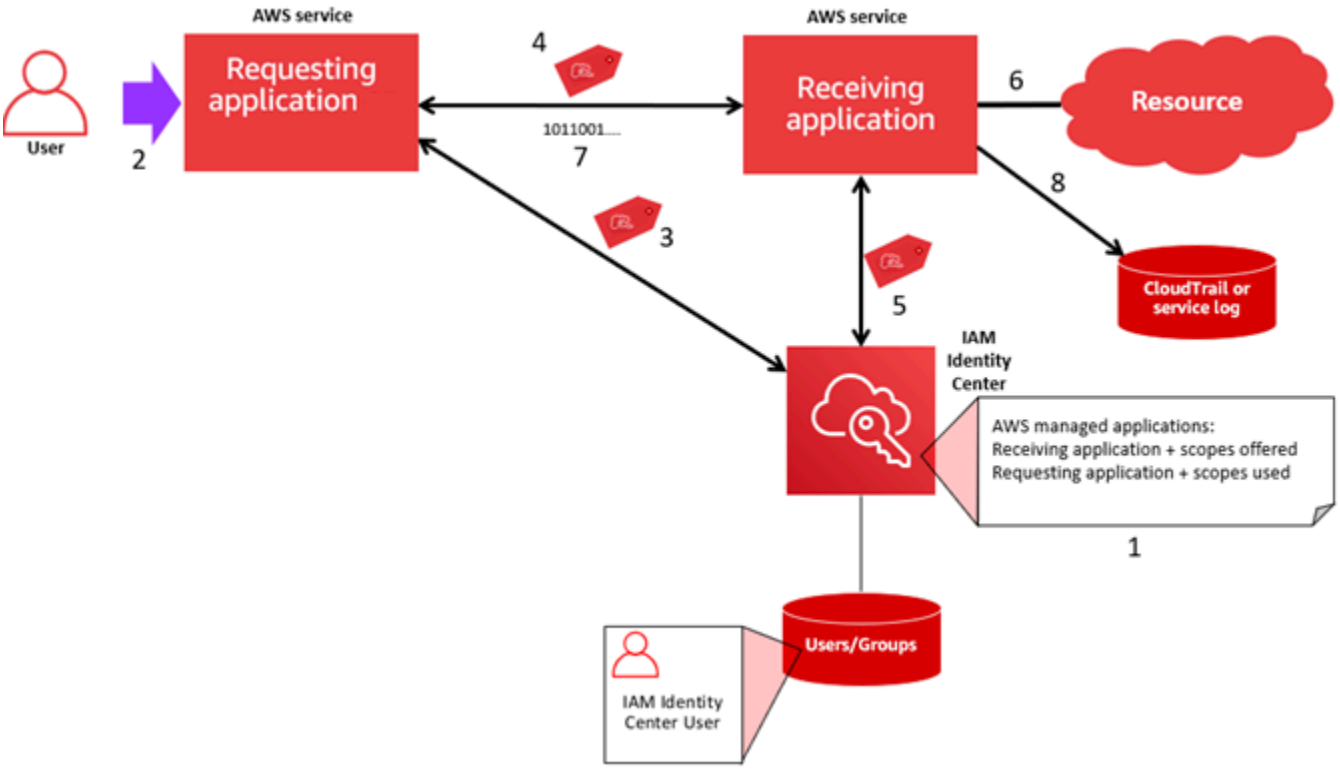
이 유형의 세션은 IAM Identity Center 사용자의 로그인에 userId 로그인하는 CloudTrail 것 외에도 지원되는 API에서 전파된 사용자 ID를 기반으로 작업을 승인하는 데 사용됩니다. 지원되는 API의 IAM 작업 목록은 관리형 정책을 참조하십시오. AWSIAMIdentityCenterAllowListForIdentityContext AWS 이 AWS 관리형 정책은 를 사용하여 ID 강화 IAM 역할 세션을 생성할 때 세션 정책으로 제공됩니다. sts:identity_context 이 정책은 지원되지 않는 서비스에서는 역할 세션을 사용할 수 없도록 합니다. AWS

이 유형의 역할 세션을 AWS STS가져오려면 요청 파라미터의 AssumeRoleProvidedContexts 요청에 sts:identity_context 필드 값을 제공하십시오. arn:aws:iam::aws:contextProvider/IdentityStore를 ProviderArn의 값으로 사용합니다.

AWS 관리되는 애플리케이션의 설정 프로세스 및 요청 흐름

이 섹션에서는 신뢰할 수 있는 ID 전파를 사용하고 웹 기반 Single Sign-On 환경을 제공하는 AWS 관리형 애플리케이션의 설정 프로세스와 요청 흐름을 설명합니다.

다음 다이어그램은 이 프로세스의 개요를 제공합니다.



다음 단계는 이 프로세스에 관한 추가 정보를 제공합니다.

1. AWS 관리 대상 애플리케이션 또는 애플리케이션 API용 콘솔을 사용하여 다음을 수행하십시오.
   a. 애플리케이션을 IAM Identity Center 인스턴스에 연결합니다.
   b. 권한을 설정하여 사용자가 액세스할 수 있는 애플리케이션 리소스에 대한 권한을 부여합니다.
2. 요청 흐름은 사용자가 리소스에 대한 액세스를 요청할 수 있는 AWS 관리형 애플리케이션 (요청 애플리케이션) 을 열 때 시작됩니다.
3. 수신 AWS 관리형 애플리케이션에 액세스할 수 있는 토큰을 얻기 위해 요청하는 AWS 관리형 애플리케이션은 IAM Identity Center에 대한 로그인 요청을 시작합니다.

   사용자가 로그인하지 않은 경우 IAM Identity Center는 지정한 ID 소스에 대한 사용자 인증 흐름을 트리거합니다. 그러면 IAM Identity Center에서 구성한 기간 동안 사용자를 위한 새 AWS 액세스 포털 세션이 생성됩니다. 그런 다음 IAM Identity Center는 세션과 연결된 토큰을 생성하며, 애플리케이션은 사용자 AWS 액세스 포털 세션의 남은 기간 동안 작동할 수 있습니다. 사용자가 애플리케이션에서 로그아웃하거나 세션을 삭제하면 세션은 2시간 이내에 자동으로 종료됩니다.
4. AWS 관리형 애플리케이션은 수신 애플리케이션에 요청을 시작하고 해당 토큰을 제공합니다.
5. 수신 애플리케이션은 IAM Identity Center에 호출하여 사용자 ID와 토큰에 인코딩된 범위를 획득합니다. 수신 애플리케이션은 Identity Center 디렉터리에서 사용자 속성이나 사용자 그룹 구성원 자격을 획득하도록 요청할 수도 있습니다.

6. 수신 애플리케이션은 해당 권한 부여 구성을 사용하여 사용자에게 요청된 애플리케이션 리소스에 액세스할 권한이 부여되어 있는지 확인합니다.
7. 사용자에게 요청된 애플리케이션 리소스에 액세스할 수 있는 권한이 부여된 경우 애플리케이션은 요청에 응답합니다.
8. 사용자의 ID, 사용자를 대신하여 수행한 작업, 수신 애플리케이션 로그 및 AWS CloudTrail 이벤트에 기록된 기타 이벤트. 이 정보가 로깅되는 구체적인 방법은 애플리케이션에 따라 다릅니다.

고객 관리형 애플리케이션에서 신뢰할 수 있는 ID 전파 사용

신뢰할 수 있는 ID 전파를 통해 고객 관리 애플리케이션은 사용자를 대신하여 AWS 서비스의 데이터에 대한 액세스를 요청할 수 있습니다. 데이터 액세스 관리는 사용자 ID를 기반으로 하므로 관리자는 사용자의 기존 사용자 및 그룹 구성원 자격을 기반으로 액세스 권한을 부여할 수 있습니다. 사용자의 ID, 사용자를 대신하여 수행된 작업 및 기타 이벤트는 서비스별 로그 및 이벤트에 기록됩니다. CloudTrail

신뢰할 수 있는 ID 전파를 통해 사용자는 고객 관리형 애플리케이션에 로그인할 수 있으며, 애플리케이션은 서비스의 데이터에 액세스하기 위한 요청에 사용자의 ID를 전달할 수 있습니다. AWS

> **Important**
>
> AWS 서비스에 액세스하려면 고객 관리형 애플리케이션이 IAM Identity Center 외부에 있는 신뢰할 수 있는 토큰 발급자로부터 토큰을 받아야 합니다. 신뢰할 수 있는 토큰 발급자는 서명된 토큰을 생성하는 OAuth 2.0 권한 부여 서버입니다. 이러한 토큰은 AWS 서비스 액세스 요청을 시작하는 애플리케이션 (수신 애플리케이션) 을 승인합니다. 자세한 정보는 신뢰할 수 있는 토큰 발급자를 사용하여 애플리케이션 사용을 참조하세요.

주제

- 신뢰할 수 있는 ID 전파에 대해 고객 관리형 OAuth 2.0 애플리케이션 설정
- 신뢰할 수 있는 애플리케이션 지정

신뢰할 수 있는 ID 전파에 대해 고객 관리형 OAuth 2.0 애플리케이션 설정

신뢰할 수 있는 ID 전파에 대해 고객 관리형 OAuth 2.0 애플리케이션을 설정하려면 먼저 IAM Identity Center에 추가해야 합니다. 다음 절차를 사용하여 애플리케이션을 IAM Identity Center에 연결합니다.

주제

- 1단계: 애플리케이션 유형 선택
- 2단계: 애플리케이션 세부 정보 지정
- 3단계: 인증 설정 지정
- 4단계: 애플리케이션 보안 인증 정보 지정
- 5단계: 검토 및 구성

1단계: 애플리케이션 유형 선택

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 고객 관리형 탭을 선택합니다.
4. 애플리케이션 추가를 선택합니다.
5. 애플리케이션 유형 선택 페이지의 설정 기본 설정에서 설정하고자 하는 애플리케이션이 있습니다를 선택합니다.
6. 애플리케이션 유형에서 OAuth 2.0을 선택합니다.
7. 다음을 선택하여 다음 페이지(2단계: 애플리케이션 세부 정보 지정)로 이동합니다.

2단계: 애플리케이션 세부 정보 지정

1. 애플리케이션 세부 정보 지정 페이지의 애플리케이션 이름 및 설명에서 **MyApp**과 같이 애플리케이션의 표시 이름을 입력합니다. 그런 다음 설명을 입력합니다.
2. 사용자 및 그룹 할당 방법에서 다음 옵션 중 하나를 선택합니다.

   - 할당 필요 - 이 애플리케이션에 할당된 IAM Identity Center 사용자 및 그룹만 애플리케이션에 액세스할 수 있도록 허용합니다.

     응용 프로그램 타일 표시 여부 - AWS 액세스 포털의 응용 프로그램 가시성이 표시로 설정된 경우 응용 프로그램에 직접 또는 그룹 과제를 통해 할당된 사용자만 Access Portal에서 AWS 응용 프로그램 타일을 볼 수 있습니다.
   - 할당 불필요 - 모든 권한 부여된 IAM Identity Center 사용자 및 그룹이 이 애플리케이션에 액세스할 수 있도록 허용합니다.

     애플리케이션 타일 가시성 - AWS 액세스 포털의 애플리케이션 가시성이 표시되지 않음으로 설정되지 않는 한 AWS 액세스 포털에 로그인하는 모든 사용자가 애플리케이션 타일을 볼 수 있습니다.

3. AWS 액세스 포털에서 사용자가 애플리케이션에 액세스할 수 있는 URL을 입력하고 AWS 액세스 포털에서 애플리케이션 타일을 표시할지 여부를 지정합니다. 표시되지 않음을 선택하면 할당된 사용자도 애플리케이션 타일을 볼 수 없습니다.
4. 태그(선택 사항)에서 새 태그 추가를 선택한 다음 키 및 값(선택 사항) 의 값을 지정합니다.

   태그에 대한 자세한 내용은 AWS IAM Identity Center 리소스에 태그 지정 단원을 참조하세요.
5. 다음을 선택하고, 다음 페이지(3단계: 인증 설정 지정)로 이동합니다.

3단계: 인증 설정 지정

OAuth 2.0을 지원하는 고객 관리형 애플리케이션을 IAM Identity Center에 추가하려면 신뢰할 수 있는 토큰 발급자를 지정해야 합니다. 신뢰할 수 있는 토큰 발급자는 서명된 토큰을 생성하는 OAuth 2.0 권한 부여 서버입니다. 이러한 토큰은 AWS 관리되는 응용 프로그램 (수신 응용 프로그램) 에 대한 액세스 요청 (응용 프로그램 요청) 을 시작하는 응용 프로그램을 승인합니다.

1. 인증 설정 지정 페이지의 신뢰할 수 있는 토큰 발급자에서 다음 중 하나를 수행합니다.
   - 기존의 신뢰할 수 있는 토큰 발급자 사용:

     사용할 신뢰할 수 있는 토큰 발급자의 이름 옆에 있는 확인란을 선택합니다.
   - 새 신뢰할 수 있는 토큰 발급자 추가:
     1. 신뢰할 수 있는 토큰 발급자 생성을 선택합니다.
     2. 새 브라우저 탭이 열립니다. IAM Identity Center 콘솔에 신뢰할 수 있는 토큰 발급자를 추가하는 방법에서 5~8단계를 따릅니다.
     3. 이 단계를 완료한 후 애플리케이션 설정에 사용 중인 브라우저 창으로 돌아가서 방금 추가한 신뢰할 수 있는 토큰 발급자를 선택합니다.
     4. 신뢰할 수 있는 토큰 발급자 목록에서 방금 추가한 신뢰할 수 있는 토큰 발급자 이름 옆에 있는 확인란을 선택합니다.

        신뢰할 수 있는 토큰 발급자를 선택하면 선택한 신뢰할 수 있는 토큰 발급자 구성 섹션이 표시됩니다.
2. 선택한 신뢰할 수 있는 토큰 발급자 구성에서 Aud claim을 입력합니다. Aud claim은 신뢰할 수 있는 토큰 발급자가 생성한 토큰의 대상(수신자)을 식별합니다. 자세한 정보는 aud 클레임을 참조하세요.

3. 사용자가 이 애플리케이션을 사용할 때 재인증하지 않아도 되도록 하려면 활성 애플리케이션 세션에 대한 사용자 인증 자동 새로 고침을 선택합니다. 이 옵션을 선택하면 세션이 만료되거나 사용자가 세션을 종료할 때까지 60분마다 세션의 액세스 토큰이 새로 고쳐집니다.
4. 다음을 선택하고, 다음 페이지(4단계: 애플리케이션 보안 인증 정보 지정)로 이동합니다.

4단계: 애플리케이션 보안 인증 정보 지정

이 절차의 단계를 완료하여 애플리케이션이 신뢰할 수 있는 애플리케이션과의 토큰 교환 작업을 수행하는 데 사용하는 보안 인증 정보를 지정합니다. 이러한 보안 인증 정보는 리소스 기반 정책에서 사용됩니다. 정책을 사용하려면 정책에 지정된 작업을 수행할 권한이 있는 보안 주체를 지정해야 합니다. 신뢰할 수 있는 애플리케이션이 동일한 AWS 계정에 있더라도 보안 주체를 지정해야 합니다.

> **Note**
>
> 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.

이 정책에는 `sso-oauth:CreateTokenWithIAM` 작업이 필요합니다.

1. 애플리케이션 보안 인증 정보 지정 페이지에서 다음 중 하나를 수행합니다.
   - 하나 이상의 IAM 역할을 빠르게 지정:
     1. 하나 이상의 IAM 역할 입력을 선택합니다.
     2. IAM 역할 입력에서 기존 IAM 역할의 Amazon 리소스 이름(ARN)을 지정합니다. ARN을 지정하려면 다음 구문을 사용합니다. IAM 리소스가 글로벌이기 때문에 ARN의 리전 부분은 공백입니다.

        ```
        arn:aws:iam::account:role/role-name-with-path
        ```

        자세한 내용은 AWS Identity and Access Management 사용 설명서의 리소스 기반 정책을 사용한 크로스 계정 액세스 및 IAM ARN을 참조하세요.
   - 정책을 수동으로 편집하려면 (AWS 비자격 증명을 지정하는 경우 필수):
     1. 애플리케이션 정책 편집을 선택합니다.
     2. JSON 텍스트 상자에 입력하거나 붙여 넣어 정책을 수정합니다.

3. 정책 검증 동안 생성된 모든 보안 경고, 오류 또는 일반 경고를 해결합니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 IAM 정책 검증을 참조하세요.

2. 다음을 선택하고, 다음 페이지(5단계: 검토 및 구성)로 이동합니다.

5단계: 검토 및 구성

1. 검토 및 구성 페이지에서 선택한 항목을 검토합니다. 변경하려면 원하는 구성 섹션을 선택하고 편집을 선택한 다음 필요한 사항을 변경합니다.
2. 완료되면 애플리케이션 추가를 선택합니다.
3. 추가한 애플리케이션이 고객 관리형 애플리케이션 목록에 표시됩니다.
4. IAM Identity Center에서 고객 관리형 애플리케이션을 설정한 후에는 ID 전파를 위해 하나 이상의 AWS 서비스 또는 신뢰할 수 있는 애플리케이션을 지정해야 합니다. 이를 통해 사용자는 고객 관리형 애플리케이션에 로그인하고 신뢰할 수 있는 애플리케이션의 데이터에 액세스할 수 있습니다.

   자세한 정보는 신뢰할 수 있는 애플리케이션 지정 을 참조하세요.

신뢰할 수 있는 애플리케이션 지정

고객 관리형 애플리케이션을 설정한 후에는 ID 전파에 사용할 신뢰할 수 있는 AWS 서비스 또는 신뢰할 수 있는 애플리케이션을 하나 이상 지정해야 합니다. 고객 관리 애플리케이션 사용자가 액세스해야 하는 데이터가 포함된 AWS 서비스를 지정하십시오. 사용자가 고객 관리형 애플리케이션에 로그인하면 해당 애플리케이션이 사용자 ID를 신뢰할 수 있는 애플리케이션에 전달합니다.

다음 절차에 따라 서비스를 선택하고, 해당 서비스에 대해 신뢰할 수 있는 개별 애플리케이션을 지정합니다.

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 고객 관리형 탭을 선택합니다.
4. 고객 관리형 애플리케이션 목록에서 액세스 요청을 시작하려는 OAuth 2.0 애플리케이션을 선택합니다. 이 애플리케이션은 사용자가 로그인하는 애플리케이션입니다.
5. 세부 정보 페이지의 ID 전파에 신뢰할 수 있는 애플리케이션에서 신뢰할 수 있는 애플리케이션 지정을 선택합니다.
6. 설정 유형에서 개별 애플리케이션 및 액세스 지정을 선택하고, 다음을 선택합니다.

7. 서비스 선택 페이지에서 고객 관리형 애플리케이션이 ID 전파에 신뢰할 수 있는 애플리케이션을 보유한 AWS 서비스를 선택하고 다음을 선택합니다.

   선택한 서비스에 따라 신뢰할 수 있는 애플리케이션이 정의됩니다. 다음 단계에서 애플리케이션을 선택합니다.

8. 애플리케이션 선택 페이지에서 개별 애플리케이션을 선택하고, 액세스 요청을 수신할 수 있는 각 애플리케이션의 확인란을 선택한 후 다음을 선택합니다.

9. 액세스 구성 페이지의 구성 방법에서 다음 중 하나를 수행합니다.

   - 애플리케이션별 액세스 선택 - 이 옵션을 선택하여 각 애플리케이션에 대해 다른 액세스 수준을 구성합니다. 액세스 수준을 구성하려는 애플리케이션을 선택하고, 액세스 편집을 선택합니다. 적용할 액세스 수준에서 필요한 정도로 액세스 수준을 변경한 다음 변경 사항 저장을 선택합니다.
   - 모든 애플리케이션에 동일한 수준의 액세스 적용 - 애플리케이션별로 액세스 수준을 구성할 필요가 없는 경우 이 옵션을 선택합니다.

10. 다음을 선택합니다.

11. 구성 검토 페이지에서 선택한 항목을 검토합니다. 변경하려면 원하는 구성 섹션을 선택하고 액세스 편집을 선택한 다음 필요한 사항을 변경합니다.

12. 완료되면 애플리케이션 신뢰를 선택합니다.

신뢰할 수 있는 토큰 발급자를 사용하여 애플리케이션 사용

신뢰할 수 있는 토큰 발급자를 사용하면 외부에서 인증하는 애플리케이션에 신뢰할 수 있는 ID 전파를 사용할 수 있습니다. AWS신뢰할 수 있는 토큰 발급자를 사용하면 이러한 애플리케이션이 사용자를 대신하여 AWS 관리형 애플리케이션에 대한 액세스를 요청할 권한을 부여할 수 있습니다.

다음 주제에서는 신뢰할 수 있는 토큰 발급자의 작동 방식을 설명하고 설정 지침을 제공합니다.

주제

- 신뢰할 수 있는 토큰 발급자 개요
- 신뢰할 수 있는 토큰 발급자의 사전 조건 및 고려 사항
- JTI 클레임 세부 정보
- 신뢰할 수 있는 토큰 발급자 구성 설정
- 신뢰할 수 있는 토큰 발급자 설정

신뢰할 수 있는 토큰 발급자 개요

신뢰할 수 있는 ID 전파는 외부에서 인증하는 애플리케이션이 신뢰할 수 있는 토큰 발급자를 사용하여 사용자를 AWS 대신하여 요청할 수 있는 메커니즘을 제공합니다. 신뢰할 수 있는 토큰 발급자는 서명된 토큰을 생성하는 OAuth 2.0 권한 부여 서버입니다. 이러한 토큰은 AWS 서비스 액세스 요청 (애플리케이션 요청) 을 시작하는 애플리케이션 (수신 애플리케이션) 을 승인합니다. 요청 애플리케이션은 신뢰할 수 있는 토큰 발급자가 인증한 사용자 대신 액세스 요청을 시작합니다. 사용자는 신뢰할 수 있는 토큰 발급자와 IAM Identity Center 모두에 알려져 있습니다.

AWS 요청을 받는 서비스는 Identity Center 디렉터리에 표시된 사용자 및 그룹 구성원을 기반으로 리소스에 대한 세분화된 권한 부여를 관리합니다. AWS 서비스는 외부 토큰 발급자의 토큰을 직접 사용할 수 없습니다.

이 문제를 해결하기 위해 IAM Identity Center는 요청 애플리케이션 또는 요청 애플리케이션에서 사용하는 AWS 드라이버가 신뢰할 수 있는 토큰 발급자가 발행한 토큰을 IAM Identity Center에서 생성한 토큰으로 교환하는 방법을 제공합니다. IAM Identity Center에서 생성된 토큰은 해당 IAM Identity Center 사용자를 참조합니다. 요청 애플리케이션 또는 드라이버는 새 토큰을 사용하여 수신 애플리케이션에 대한 요청을 시작합니다. 새 토큰은 IAM Identity Center의 해당 사용자를 참조하므로 수신 애플리케이션은 IAM Identity Center에 표시된 사용자 또는 그룹 구성원 자격을 기반으로 요청된 액세스 권한을 부여할 수 있습니다.

> **Important**
>
> 신뢰할 수 있는 토큰 발급자로 추가할 OAuth 2.0 권한 부여 서버를 선택하는 것은 신중한 고려가 필요한 보안 결정입니다. 신뢰할 수 있는 토큰 발급자만 선택하여 다음 작업을 수행하세요.
>
> - 토큰에 지정된 사용자를 인증합니다.
> - 수신 애플리케이션에 대한 해당 사용자의 액세스 권한을 부여합니다.
> - IAM Identity Center에서 IAM Identity Center 생성 토큰으로 교환할 수 있는 토큰을 생성합니다.

신뢰할 수 있는 토큰 발급자의 사전 조건 및 고려 사항

신뢰할 수 있는 토큰 발급자를 설정하기 전에 다음 사전 조건 및 고려 사항을 검토합니다.

- 신뢰할 수 있는 토큰 발급자 구성

OAuth 2.0 인증 서버 (신뢰할 수 있는 토큰 발급자) 를 구성해야 합니다. 일반적으로 신뢰할 수 있는 토큰 발급자가 IAM Identity Center의 ID 소스로 사용하는 ID 공급자이지만 반드시 그럴 필요는 없습니다. 신뢰할 수 있는 토큰 발급자를 설정하는 방법에 대한 자세한 내용은 관련 ID 제공자의 설명서를 참조하십시오.

> **Note**
>
> 신뢰할 수 있는 토큰 발급자의 각 사용자 ID를 IAM Identity Center의 해당 사용자에 매핑하는 한 IAM Identity Center에서 사용할 신뢰할 수 있는 토큰 발급자를 최대 10개까지 구성할 수 있습니다.

- 토큰을 생성하는 OAuth 2.0 권한 부여 서버(신뢰할 수 있는 토큰 발급자)에는 IAM Identity Center에서 토큰 서명을 확인하기 위한 퍼블릭 키를 획득하는 데 사용할 수 있는 OpenID Connect(OIDC) 검색 엔드포인트가 있어야 합니다. 자세한 정보는 OIDC 검색 엔드포인트 URL (발급자 URL)을 참조하세요.
- 신뢰할 수 있는 토큰 발급자가 발행한 토큰

  신뢰할 수 있는 토큰 발행자의 토큰은 다음 요구 사항을 충족해야 합니다.

  - 토큰은 RS256 알고리즘을 사용하여 JWT (JSON 웹 토큰) 형식으로 서명되어야 합니다.
  - 토큰에는 다음과 같은 클레임이 포함되어야 합니다.
    - 발행자 (iss) — 토큰을 발행한 주체. 이 값은 신뢰할 수 있는 토큰 발급자의 OIDC 검색 엔드포인트 (발급자 URL) 에 구성된 값과 일치해야 합니다.
    - 제목 (sub) — 인증된 사용자입니다.
    - 대상 (aud) — 토큰의 의도된 수신자. IAM Identity Center에서 토큰을 토큰으로 교환한 후 액세스할 수 있는 AWS 서비스입니다. 자세한 정보는 aud 클레임을 참조하세요.
    - 만료 시간 (exp) — 토큰이 만료되기까지의 시간입니다.
    -
  - 토큰은 ID 토큰 또는 액세스 토큰일 수 있습니다.
  - 토큰에는 IAM Identity Center 사용자 한 명에게 고유하게 매핑될 수 있는 속성이 있어야 합니다.
- 선택적 클레임

  IAM Identity Center는 RFC 7523에 정의된 모든 선택적 클레임을 지원합니다. 자세한 내용은 이 RFC의 섹션 3: JWT 형식 및 처리 요구 사항을 참조하세요.

예를 들어 토큰에는 JTI(JWT ID) 클레임이 포함될 수 있습니다. 이 클레임이 있는 경우 동일한 JTI를 가진 토큰을 토큰 교환에 재사용할 수 없게 됩니다. JTI 클레임에 관한 자세한 내용은 JTI 클레임 세부 정보의 내용을 참조하세요.

- 신뢰할 수 있는 토큰 발급자에서 사용하도록 IAM Identity Center 구성

  또한 IAM Identity Center를 활성화하고, IAM Identity Center의 ID 소스를 구성하고, 신뢰할 수 있는 토큰 발급자 디렉터리의 사용자에 해당하는 사용자를 프로비저닝해야 합니다.

  이렇게 하려면 다음을 수행해야 합니다.

  - SCIM(System for Cross-domain Identity Management) 2.0 프로토콜을 사용하여 IAM Identity Center와 사용자를 동기화합니다.
  - IAM Identity Center에서 직접 사용자를 생성합니다.

> **Note**
>
> Active Directory 도메인 서비스를 ID 소스로 사용하는 경우 신뢰할 수 있는 토큰 발급자는 지원되지 않습니다.

JTI 클레임 세부 정보

IAM Identity Center가 IAM Identity Center에서 이미 교환한 토큰을 교환하는 요청을 받으면 요청은 실패합니다. 토큰 교환을 위한 토큰 재사용을 감지하고 방지하려면 JTI 클레임을 포함시킬 수 있습니다. IAM Identity Center는 토큰의 클레임을 기반으로 토큰의 재사용을 방지합니다.

모든 OAuth 2.0 권한 부여 서버가 토큰에 JTI 클레임을 추가하는 것은 아닙니다. 일부 OAuth 2.0 권한 부여 서버는 JTI를 사용자 지정 클레임으로 추가하는 것을 허용하지 않을 수 있습니다. JTI 클레임 사용을 지원하는 OAuth 2.0 권한 부여 서버는 이 클레임을 ID 토큰에만 추가하거나 액세스 토큰에만 추가하거나 둘 모두에 추가할 수 있습니다. 자세한 내용은 OAuth 2.0 권한 부여 서버 설명서를 참조하세요.

토큰을 교환하는 애플리케이션을 빌드하는 방법에 대한 자세한 내용은 IAM Identity Center API 설명서를 참조하세요. 올바른 토큰을 획득하고 교환하도록 고객 관리형 애플리케이션을 구성하는 방법에 대한 자세한 내용은 애플리케이션 설명서를 참조하세요.

신뢰할 수 있는 토큰 발급자 구성 설정

다음 섹션에서는 신뢰할 수 있는 토큰 발급자를 설정하고 사용하는 데 필요한 설정을 설명합니다.

주제

- OIDC 검색 엔드포인트 URL (발급자 URL)
- 속성 매핑
- aud 클레임

OIDC 검색 엔드포인트 URL (발급자 URL)

IAM Identity Center 콘솔에 신뢰할 수 있는 토큰 발급자를 추가하는 경우 OIDC 검색 엔드포인트 URL을 지정해야 합니다. 이 URL은 일반적으로 상대 URL(`/.well-known/openid-configuration`)로 참조됩니다. IAM Identity Center 콘솔에서는 이 URL을 발급자 URL이라고 합니다.

> **Note**
>
> 검색 엔드포인트의 URL을 붙여넣거나 붙여넣지 않으면 붙여넣어야 합니다. `.well-known/openid-configuration` `.well-known/openid-configuration`가 URL에 포함된 경우 신뢰할 수 있는 토큰 발급자 구성이 작동하지 않습니다. IAM Identity Center는 이 URL을 검증하지 않기 때문에 URL이 올바르게 구성되지 않으면 신뢰할 수 있는 토큰 발급자 설정이 알림 없이 실패합니다.

IAM Identity Center는 이 URL을 사용하여 신뢰할 수 있는 토큰 발급자에 관한 추가 정보를 획득합니다. 예를 들어 IAM Identity Center는 이 URL을 사용하여 신뢰할 수 있는 토큰 발급자가 생성하는 토큰을 확인하는 데 필요한 정보를 획득합니다. IAM Identity Center에 신뢰할 수 있는 토큰 발급자를 추가하는 경우 이 URL을 지정해야 합니다. URL을 찾으려면 애플리케이션용 토큰을 생성하는 데 사용하는 OAuth 2.0 권한 부여 서버 공급자의 설명서를 참조하거나 공급자에게 직접 문의하여 지원을 요청하세요.

속성 매핑

속성 매핑을 통해 IAM Identity Center는 신뢰할 수 있는 토큰 발급자가 발급한 토큰으로 표시되는 사용자와 IAM Identity Center의 단일 사용자를 매칭할 수 있습니다. IAM Identity Center에 신뢰할 수 있는 토큰 발급자를 추가하는 경우 이 속성 매핑을 지정해야 합니다. 이 속성 매핑은 신뢰할 수 있는 토큰 발급자가 생성한 토큰의 클레임에 사용됩니다. 클레임의 값은 IAM Identity Center를 검색하는 데 사용됩니다. 검색에서는 지정된 속성을 사용하여 IAM Identity Center의 단일 사용자를 검색하고, 이 사용자는 AWS내에서 사용자로 사용됩니다. 선택한 클레임을 IAM Identity Center ID 저장소의 사용 가능한 고정 속성 목록에 있는 하나의 속성에 매핑해야 합니다. IAM Identity Center ID 저장소 속성(사용자 이름, 이메일 및 외부 ID) 중 하나를 선택할 수 있습니다. IAM Identity Center에서 지정한 속성 값은 각 사용자마다 고유해야 합니다.

aud 클레임

aud 클레임은 토큰의 대상(수신자)을 식별합니다. 액세스를 요청하는 애플리케이션이 IAM Identity Center와 페더레이션되지 않은 ID 제공업체를 통해 인증하는 경우 해당 ID 제공업체를 신뢰할 수 있는 토큰 발급자로 설정해야 합니다. 액세스 요청을 수신하는 애플리케이션(수신 애플리케이션)은 신뢰할 수 있는 토큰 발급자가 생성한 토큰을 IAM Identity Center에서 생성한 토큰으로 교환해야 합니다.

신뢰할 수 있는 토큰 발급자에 등록된 수신 애플리케이션의 aud 클레임 값을 획득하는 방법에 대한 자세한 내용은 신뢰할 수 있는 토큰 발급자의 설명서를 참조하거나 신뢰할 수 있는 토큰 발급자 관리자에게 문의하여 지원을 요청하세요.

신뢰할 수 있는 토큰 발급자 설정

IAM Identity Center 외부에서 인증하는 애플리케이션에 신뢰할 수 있는 ID 전파를 활성화하려면 한 명 이상의 관리자가 신뢰할 수 있는 토큰 발급자를 설정해야 합니다. 신뢰할 수 있는 토큰 발급자는 요청을 시작하는 애플리케이션(요청 애플리케이션)에 토큰을 발급하는 OAuth 2.0 권한 부여 서버입니다. 토큰은 이러한 애플리케이션이 사용자를 대신하여 수신 애플리케이션 (서비스) 에 대한 요청을 시작할 수 있는 권한을 부여합니다. AWS

주제

- 관리 역할 및 책임 협력
- 신뢰할 수 있는 토큰 발급자 설정 작업
- IAM Identity Center 콘솔에 신뢰할 수 있는 토큰 발급자를 추가하는 방법
- IAM Identity Center 콘솔에서 신뢰할 수 있는 토큰 발급자 설정을 보거나 편집하는 방법
- 신뢰할 수 있는 토큰 발급자를 사용하는 애플리케이션의 설정 프로세스 및 요청 흐름

관리 역할 및 책임 협력

경우에 따라 단일 관리자가 신뢰할 수 있는 토큰 발급자를 설정하는 데 필요한 모든 작업을 수행할 수도 있습니다. 여러 관리자가 이러한 작업을 수행하는 경우 긴밀한 협력이 필요합니다. 다음 표에서는 여러 관리자가 협력하여 신뢰할 수 있는 토큰 발급자를 설정하고 이를 사용하도록 AWS 서비스를 구성하는 방법을 설명합니다.

> **Note**
>
> 애플리케이션은 IAM Identity Center와 통합되고 신뢰할 수 있는 ID 전파를 지원하는 모든 AWS 서비스가 될 수 있습니다.

자세한 정보는 신뢰할 수 있는 토큰 발급자 설정 작업을 참조하세요.

역할	다음 작업 수행	협력 당사자
IAM Identity Center 관리자	외부 IdP를 신뢰할 수 있는 토큰 발급자로 IAM Identity Center 콘솔에 추가합니다. IAM Identity Center와 외부 IdP 간에 올바른 속성 매핑을 설정하는 데 도움을 줍니다. 신뢰할 수 있는 토큰 발급자가 IAM Identity Center 콘솔에 추가되면 AWS 서비스 관리자에게 알립니다.	외부 IdP(신뢰할 수 있는 토큰 발급자) 관리자 AWS 서비스 관리자
외부 IdP(신뢰할 수 있는 토큰 발급자) 관리자	토큰을 발급하도록 외부 IdP를 구성합니다. IAM Identity Center와 외부 IdP 간에 올바른 속성 매핑을 설정하는 데 도움을 줍니다. AWS 서비스 관리자에게 대상 이름(Aud 클레임)을 제공합니다.	IAM Identity Center 관리자 AWS 서비스 관리자
AWS 서비스 관리자	AWS 서비스 콘솔에서 신뢰할 수 있는 토큰 발급자를 확인합니다. IAM Identity Center 관리자가 IAM Identity Center 콘솔에 추가한 후 신뢰할 수 있는 토큰 발급자는 AWS 서비스 콘솔에 표시됩니다. 신뢰할 수 있는 토큰 발급자를 사용하도록 AWS 서비스를 구성합니다.	IAM Identity Center 관리자 외부 IdP(신뢰할 수 있는 토큰 발급자) 관리자

신뢰할 수 있는 토큰 발급자 설정 작업

신뢰할 수 있는 토큰 발급자를 설정하려면 IAM Identity Center 관리자, 외부 IdP(신뢰할 수 있는 토큰 발급자) 관리자 및 애플리케이션 관리자가 다음 작업을 완료해야 합니다.

> **Note**
>
> 애플리케이션은 IAM Identity Center와 통합되고 신뢰할 수 있는 ID 전파를 지원하는 모든 AWS 서비스가 될 수 있습니다.

1. IAM Identity Center에 신뢰할 수 있는 토큰 발급자 추가 - IAM Identity Center 관리자가 IAM Identity Center 콘솔 또는 API를 사용하여 신뢰할 수 있는 토큰 발급자를 추가합니다. 이 구성에서는 다음을 지정해야 합니다.

   - 신뢰할 수 있는 토큰 발급자 이름
   - OIDC 검색 엔드포인트 URL(IAM Identity Center 콘솔에서 이 URL은 발급자 URL이라고 함).
   - 사용자 조회를 위한 속성 매핑. 이 속성 매핑은 신뢰할 수 있는 토큰 발급자가 생성한 토큰의 클레임에 사용됩니다. 클레임의 값은 IAM Identity Center를 검색하는 데 사용됩니다. 검색에서는 지정된 속성을 사용하여 IAM Identity Center의 단일 사용자를 검색합니다.
2. AWS 서비스를 IAM Identity Center에 연결 - AWS 서비스 관리자는 애플리케이션용 콘솔이나 애플리케이션 API를 사용하여 애플리케이션을 IAM Identity Center에 연결해야 합니다.

   신뢰할 수 있는 토큰 발급자가 IAM Identity Center 콘솔에 추가된 후에는 서비스 콘솔에서도 볼 수 있으며 AWS 서비스 관리자가 선택할 수 있습니다. AWS
3. 토큰 교환 사용 구성 - AWS 서비스 콘솔에서 AWS 서비스 관리자는 신뢰할 수 있는 토큰 발급자가 발행한 토큰을 수락하도록 AWS 서비스를 구성합니다. 이러한 토큰은 IAM Identity Center에서 생성한 토큰으로 교환됩니다. 이를 위해서는 1단계의 신뢰할 수 있는 토큰 발급자 이름과 해당 서비스에 해당하는 Aud 클레임 값을 지정해야 합니다. AWS

   신뢰할 수 있는 토큰 발급자는 발급한 토큰에 Aud 클레임 값을 입력하여 이 토큰이 AWS 서비스의 사용 대상임을 나타냅니다. 이 값을 구하려면 신뢰할 수 있는 토큰 발급자의 관리자에게 문의하세요.

IAM Identity Center 콘솔에 신뢰할 수 있는 토큰 발급자를 추가하는 방법

관리자가 여럿인 조직에서는 IAM Identity Center 관리자가 이 작업을 수행합니다. IAM Identity Center 관리자인 경우 신뢰할 수 있는 토큰 발급자로 사용할 외부 IdP를 선택해야 합니다.

IAM Identity Center 콘솔에 신뢰할 수 있는 토큰 발급자 추가

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 신뢰할 수 있는 토큰 발급자에서 신뢰할 수 있는 토큰 발급자 선택을 선택합니다.
5. 신뢰할 수 있는 토큰을 발급하도록 외부 IdP 설정 페이지의 신뢰할 수 있는 토큰 발급자 세부 정보에서 다음을 수행합니다.

   - 발급자 URL의 경우 신뢰할 수 있는 ID 전파를 위한 토큰을 발행할 외부 IdP의 OIDC 검색 URL을 지정합니다. 검색 엔드포인트의 URL을 이전까지와 사용하지 않을 때까지의 URL을 지정해야 합니다. `.well-known/openid-configuration` 외부 IdP 관리자가 이 URL을 제공할 수 있습니다.

     > **Note**
     >
     > 참고 이 URL은 신뢰할 수 있는 ID 전파를 위해 발급된 토큰의 Issuer (iss) 클레임의 URL과 일치해야 합니다.

   - 신뢰할 수 있는 토큰 발급자 이름의 경우 IAM Identity Center와 애플리케이션 콘솔에서 신뢰할 수 있는 토큰 발급자로 식별할 이름을 입력합니다.
6. 속성 매핑에서 다음을 수행합니다.

   - ID 제공업체 속성의 경우 목록에서 속성을 선택하여 IAM Identity Center ID 저장소의 속성에 매핑합니다.
   - IAM Identity Center 속성의 경우 속성 매핑에 사용할 속성을 선택합니다.
7. 태그(선택 사항)에서 새 태그 추가를 선택하고, 키 및 값(선택 사항)의 값을 지정합니다.

   태그에 대한 자세한 내용은 AWS IAM Identity Center 리소스에 태그 지정 단원을 참조하세요.
8. 신뢰할 수 있는 토큰 발급자 생성을 선택합니다.
9. 신뢰할 수 있는 토큰 발급자 생성을 완료한 후에는 애플리케이션 관리자에게 문의하여 신뢰할 수 있는 토큰 발급자의 이름을 알리면 신뢰할 수 있는 토큰 발급자가 해당 콘솔에 표시되는지 확인할 수 있습니다.
10. 신뢰할 수 있는 ID 전파에 대해 구성된 애플리케이션에서 사용자가 애플리케이션에 액세스할 수 있도록 애플리케이션 관리자가 해당 콘솔에서 이 신뢰할 수 있는 토큰 발급자를 선택해야 합니다.

IAM Identity Center 콘솔에서 신뢰할 수 있는 토큰 발급자 설정을 보거나 편집하는 방법

IAM Identity Center 콘솔에 신뢰할 수 있는 토큰 발급자를 추가한 후에는 관련 설정을 보고 편집할 수 있습니다.

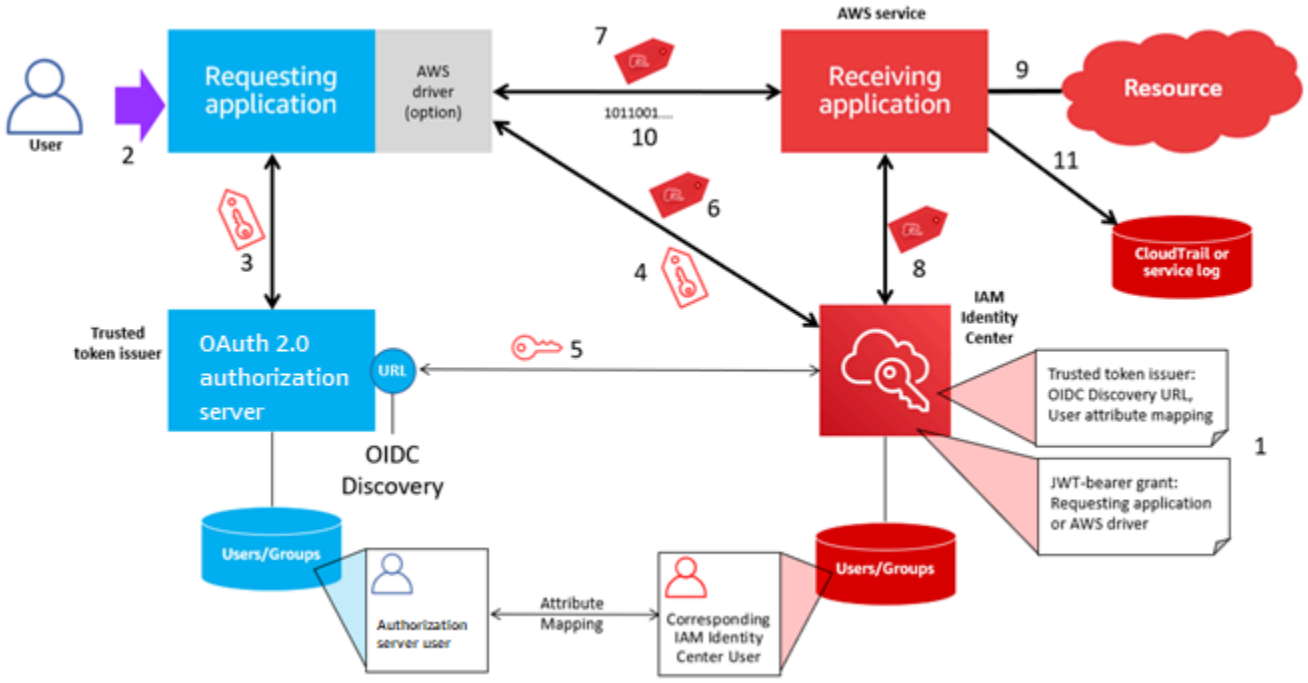
신뢰할 수 있는 토큰 발급자 설정을 편집하려는 경우 이로 인해 사용자가 신뢰할 수 있는 토큰 발급자를 사용하도록 구성된 애플리케이션에 대한 액세스 권한을 상실할 수 있다는 점을 명심해야 합니다. 사용자 액세스가 중단되지 않도록 설정 편집 전에 신뢰할 수 있는 토큰 발급자를 사용하도록 구성된 모든 애플리케이션의 관리자와 협력하는 것이 좋습니다.

IAM Identity Center 콘솔에서 신뢰할 수 있는 토큰 발급자 설정 보기 또는 편집

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 신뢰할 수 있는 토큰 발급자에서 보거나 편집하려는 신뢰할 수 있는 토큰 발급자를 선택합니다.
5. 작업을 선택한 후 편집을 선택합니다.
6. 신뢰할 수 있는 토큰 발급자 편집 페이지에서 필요한 설정을 보거나 편집합니다. 신뢰할 수 있는 토큰 발급자 이름, 속성 매핑 및 태그를 편집할 수 있습니다.
7. 변경 사항 저장를 선택합니다.
8. 신뢰할 수 있는 토큰 발급자 편집 대화 상자에서 변경을 확인하는 메시지가 표시됩니다. 확인을 선택합니다.

신뢰할 수 있는 토큰 발급자를 사용하는 애플리케이션의 설정 프로세스 및 요청 흐름

이 섹션에서는 신뢰할 수 있는 ID 전파에 신뢰할 수 있는 토큰 발급자를 사용하는 애플리케이션의 설정 프로세스와 요청 흐름을 설명합니다. 다음 다이어그램은 이 프로세스의 개요를 제공합니다.



다음 단계는 이 프로세스에 관한 추가 정보를 제공합니다.

1. IAM Identity Center 및 수신 AWS 관리형 애플리케이션이 신뢰할 수 있는 토큰 발급자를 사용하도록 설정하십시오. 자세한 내용은 신뢰할 수 있는 토큰 발급자 설정 작업을 참조하세요.
2. 요청 흐름은 사용자가 요청 애플리케이션을 열 때 시작됩니다.
3. 요청 애플리케이션은 신뢰할 수 있는 토큰 발급자에게 토큰을 요청하여 수신 관리 애플리케이션에 대한 요청을 시작합니다. AWS 사용자가 아직 인증하지 않은 경우 이 프로세스가 인증 흐름을 트리거합니다. 토큰에는 다음 정보가 포함되어 있습니다.
   - 사용자의 주체(Sub).
   - IAM Identity Center가 IAM Identity Center에서 해당 사용자를 조회하는 데 사용하는 속성.
   - 신뢰할 수 있는 토큰 발급자가 수신 AWS 관리형 애플리케이션과 연결한 값을 포함한 대상(Aud) 클레임. 다른 클레임이 있는 경우 IAM Identity Center에서는 이를 사용하지 않습니다.
4. 요청하는 애플리케이션 또는 애플리케이션이 사용하는 AWS 드라이버는 토큰을 IAM Identity Center로 전달하고 토큰을 IAM Identity Center에서 생성한 토큰으로 교환하도록 요청합니다. AWS 드라이버를 사용하는 경우 이 사용 사례에 맞게 드라이버를 구성해야 할 수 있습니다. 자세한 내용은 관련 AWS 관리 애플리케이션의 설명서를 참조하십시오.
5. IAM Identity Center는 OIDC 검색 엔드포인트를 사용하여 토큰의 진본성을 확인하는 데 사용할 수 있는 퍼블릭 키를 획득합니다. 그러면 IAM Identity Center는 다음을 수행합니다.
   - 토큰을 확인합니다.

- Identity Center 디렉터리를 검색합니다. 이를 위해 IAM Identity Center는 토큰에 지정된 매핑된 속성을 사용합니다.
- 사용자에게 수신 애플리케이션 액세스 권한이 부여되어 있는지 확인합니다. 사용자 및 그룹에 대한 할당을 요구하도록 AWS 관리 대상 응용 프로그램을 구성한 경우 사용자는 응용 프로그램에 직접 또는 그룹 기반 할당을 해야 합니다. 그렇지 않으면 요청이 거부됩니다. AWS 관리형 애플리케이션이 사용자 및 그룹 할당을 요구하지 않도록 구성된 경우 처리가 계속 진행됩니다.

> **Note**
>
> AWS 서비스에는 사용자 및 그룹에 할당이 필요한지 여부를 결정하는 기본 설정 구성이 있습니다. 신뢰할 수 있는 ID 전파에 사용하려는 경우 이러한 애플리케이션의 할당 필요 설정을 수정하지 않는 것이 좋습니다. 특정 애플리케이션 리소스에 대한 사용자 액세스를 허용하는 세분화된 권한을 구성한 경우에도 할당 필요 설정을 수정하면 해당 리소스에 대한 사용자 액세스가 중단되는 등 예기치 않은 동작이 발생할 수 있습니다.

- 요청 응용 프로그램이 받는 AWS 관리 응용 프로그램에 유효한 범위를 사용하도록 구성되어 있는지 확인합니다.

6. 이전 확인 단계가 성공적이면 IAM Identity Center에서 새 토큰을 생성합니다. 새 토큰은 IAM Identity Center의 해당 사용자 ID, 수신 관리 대상 애플리케이션의 대상 (Aud), 요청 애플리케이션이 수신 AWS 관리 애플리케이션에 요청할 때 사용할 수 있는 범위를 포함하는 불투명 (암호화된) 토큰입니다. AWS
7. 요청 애플리케이션 또는 요청 애플리케이션에서 사용하는 드라이버는 수신 애플리케이션에 대한 리소스 요청을 시작하고 IAM Identity Center에서 생성한 토큰을 수신 애플리케이션에 전달합니다.
8. 수신 애플리케이션은 IAM Identity Center에 호출하여 사용자 ID와 토큰에 인코딩된 범위를 획득합니다. Identity Center 디렉터리에서 사용자 속성이나 사용자 그룹 구성원 자격을 획득하도록 요청할 수도 있습니다.
9. 수신 애플리케이션은 해당 권한 부여 구성을 사용하여 사용자에게 요청된 애플리케이션 리소스에 액세스할 권한이 부여되어 있는지 확인합니다.
10. 사용자에게 요청된 애플리케이션 리소스에 액세스할 수 있는 권한이 부여된 경우 애플리케이션은 요청에 응답합니다.
11. 사용자의 ID, 사용자를 대신하여 수행된 작업, 수신 애플리케이션 로그 및 이벤트에 기록된 기타 이벤트. CloudTrail 이 정보가 로깅되는 구체적인 방법은 애플리케이션에 따라 다릅니다.

IAM Identity Center 인증서 관리

IAM Identity Center와 애플리케이션의 서비스 공급자 간에 SAML 신뢰 관계를 설정해야 하기 위해 IAM Identity Center는 인증서를 사용합니다. IAM Identity Center에서 애플리케이션을 추가하면 설정 프로세스 중에 해당 애플리케이션과 함께 사용할 수 있는 IAM Identity Center 인증서가 자동으로 생성됩니다. 기본적으로 자동 생성된 해당 IAM Identity Center 인증서는 5년 동안 유효합니다.

IAM Identity Center 관리자는 특정 애플리케이션에서 이전 인증서를 새 인증서로 교체해야 하는 경우가 있습니다. 예를 들어, 인증서 만료 날짜가 다가올 경우 인증서를 교체해야 할 수도 있습니다. 이전 인증서를 새 인증서로 교체하는 프로세스를 인증서 교체라고 합니다.

주제

- 인증서 교체 전 고려 사항
- IAM Identity Center 인증서 교체
- 인증서 만료 상태 표시

인증서 교체 전 고려 사항

IAM Identity Center에서 인증서 교체 프로세스를 시작하기 전에 다음 사항을 고려하세요.

- 인증서 교체 프로세스를 진행하려면 IAM Identity Center와 서비스 공급자 간의 신뢰를 재구축해야 합니다. 신뢰를 다시 구축하려면 IAM Identity Center 인증서 교체에 제공된 절차를 사용하세요.
- 서비스 제공업체를 통해 인증서를 업데이트하면 신뢰가 다시 설정될 때까지 사용자의 서비스가 일시적으로 중단될 수 있습니다. 가능하면 사용량이 적은 시간에 신중하게 이 작업을 계획하세요.

IAM Identity Center 인증서 교체

IAM Identity Center 인증서 교체는 다음을 포함하는 다단계 절차입니다.

- 새 인증서 생성
- 서비스 제공업체의 웹 사이트에 새 인증서 추가
- 새 인증서를 활성으로 설정
- 비활성 인증서 삭제

지정된 애플리케이션에 대한 인증서 교체 프로세스를 완료하려면 다음 절차를 다음 순서대로 모두 따르세요.

1단계: 새 인증서를 생성합니다.

생성한 새 IAM Identity Center 인증서는 다음 속성을 사용하도록 구성할 수 있습니다.

- 유효 기간 - 새 IAM Identity Center 인증서가 만료되기 전에 할당된 시간(개월)을 지정합니다.
- 키 크기 - 키가 암호화 알고리즘과 함께 사용해야 하는 비트 수를 결정합니다. 이 값은 1024비트 RSA 또는 2048비트 RSA로 설정할 수 있습니다. 암호화에서 키 크기가 작동하는 방식에 대한 일반적인 정보는 키 크기를 참조하세요.
- 알고리즘 - SAML 어설션/응답에 서명할 때 IAM Identity Center에서 사용하는 알고리즘을 지정합니다. 이 값을 SHA-1 또는 SHA-256 중 하나로 설정할 수 있습니다. AWS 서비스 공급업체가 SHA-1 요구하지 않는 한 가능하면 SHA-256 사용을 권장합니다. 암호화 알고리즘의 작동 방식에 대한 일반 정보는 공개 키 암호화를 참조하세요.

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 애플리케이션 목록에서 새 인증서를 생성하려는 애플리케이션을 선택합니다.
4. 애플리케이션 세부 정보 페이지에서 구성 탭을 선택합니다. IAM Identity Center 메타데이터에서 인증서 관리를 선택합니다. 구성 탭이 없거나 구성 설정을 사용할 수 없는 경우 이 애플리케이션의 인증서를 교체할 필요가 없습니다.
5. IAM Identity Center 인증서 페이지에서 새 인증서 생성을 선택합니다.
6. 새 IAM Identity Center 인증서 생성 대화 상자에서 유효 기간, 알고리즘 및 키 크기에 적절한 값을 지정합니다. 그리고 생성을 선택합니다.

2단계: 서비스 제공업체의 웹 사이트를 업데이트합니다.

다음 절차를 사용하여 애플리케이션의 서비스 제공업체와의 신뢰를 다시 구축하세요.

> **Important**
>
> 새 인증서를 서비스 제공업체에 업로드할 때 사용자가 인증을 받지 못할 수 있습니다. 이 문제를 해결하려면 다음 단계의 설명에 따라 새 인증서를 활성 인증서로 설정합니다.

1. IAM Identity Center 콘솔에서 방금 새 인증서를 생성한 애플리케이션을 선택합니다.
2. 애플리케이션 세부 정보 페이지에서 구성 편집을 선택합니다.

3. 지침 보기를 선택한 다음, 특정 애플리케이션 서비스 제공업체 웹사이트의 지침에 따라 새로 생성된 인증서를 추가합니다.

3단계: 새 인증서를 활성으로 설정합니다.

애플리케이션에는 인증서를 최대 2개까지 할당할 수 있습니다. IAM Identity Center에서는 활성으로 설정된 인증서를 사용하여 모든 SAML 어설션을 서명합니다.

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 애플리케이션 목록에서 애플리케이션을 선택합니다.
4. 애플리케이션 세부 정보 페이지에서 구성 탭을 선택합니다. IAM Identity Center 메타데이터에서 인증서 관리를 선택합니다.
5. IAM Identity Center 인증서 페이지에서 활성으로 설정하려는 인증서를 선택하고 작업을 선택한 다음 활성으로 설정을 선택합니다.
6. 선택한 인증서를 활성으로 설정 대화 상자에서 인증서를 활성으로 설정하려면 신뢰를 다시 설정해야 할 수도 있다는 점을 이해했는지 확인한 다음 활성화를 선택합니다.

4단계: 이전 인증서를 삭제합니다.

다음 절차를 사용하여 애플리케이션의 인증서 교체 프로세스를 완료합니다. 비활성 상태인 인증서만 삭제할 수 있습니다.

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 애플리케이션 목록에서 애플리케이션을 선택합니다.
4. 애플리케이션 세부 정보 페이지에서 구성 탭을 선택합니다. IAM Identity Center 메타데이터에서 인증서 관리를 선택합니다.
5. IAM Identity Center 인증서 페이지에서 삭제하려는 인증서를 선택합니다. Actions를 선택하고 삭제를 선택합니다.
6. 인증서 삭제 대화 상자에서 삭제를 선택합니다.

인증서 만료 상태 표시

애플리케이션 속성의 애플리케이션 페이지에 있는 동안 컬러 상태 표시 아이콘이 표시될 수 있습니다. 이러한 아이콘은 목록의 각 인증서 옆에 있는 만료 날짜 열에 표시됩니다. 다음은 IAM Identity Center에서 각 인증서에 표시할 아이콘을 결정하는 데 사용하는 기준에 대한 설명입니다.

- 빨간색 - 인증서가 현재 만료되었음을 나타냅니다.
- 노란색 - 인증서가 90일 이내에 만료됨을 나타냅니다.
- 녹색 - 인증서가 현재 유효하며 최소 90일 이상 유효함을 나타냅니다.

인증서 현재 상태를 확인하려면

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 애플리케이션 목록에서 만료 날짜 열에 표시된 대로 목록에 있는 인증서 상태를 검토하세요.

IAM Identity Center 콘솔의 애플리케이션 속성 구성

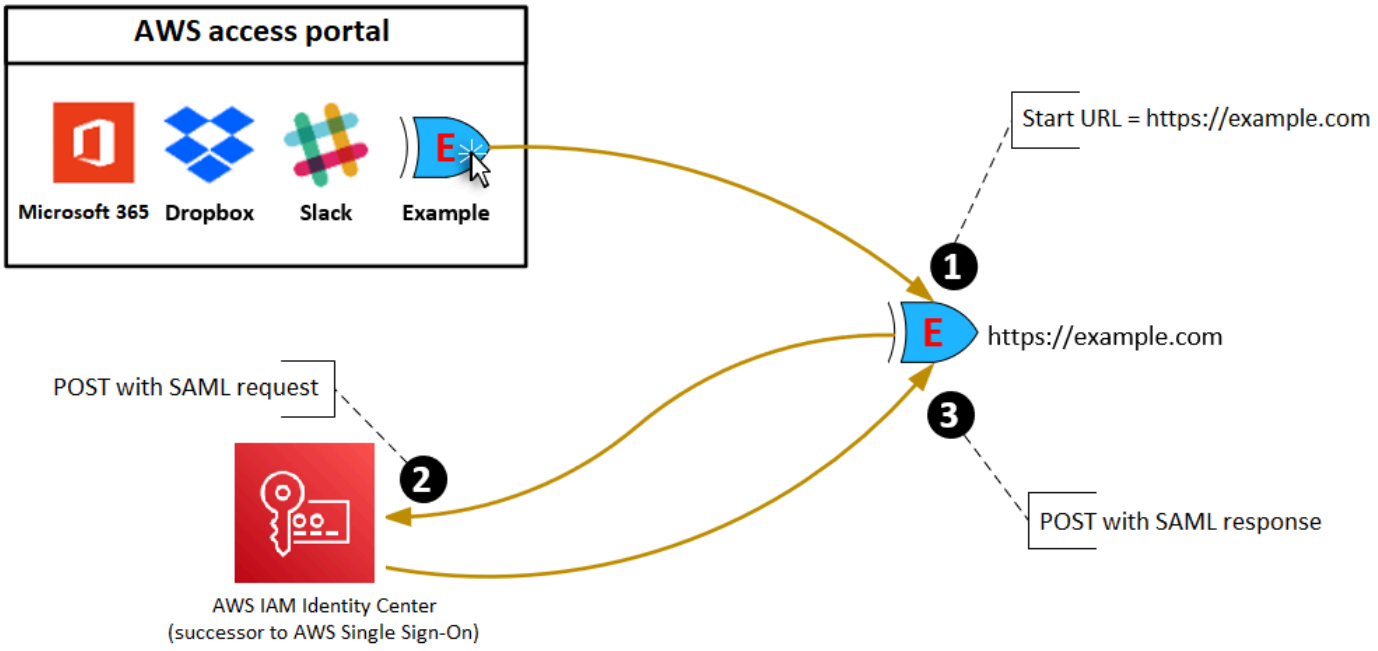
IAM Identity Center에서 애플리케이션 시작 URL, 릴레이 상태 및 세션 기간을 구성하여 사용자 경험을 최적화할 수 있습니다.

애플리케이션 시작 URL

애플리케이션 시작 URL을 사용하여 애플리케이션과의 페더레이션 프로세스를 시작합니다. 일반적으로 SP(서비스 제공업체) 초기 바인딩만 지원하는 애플리케이션에 사용됩니다.

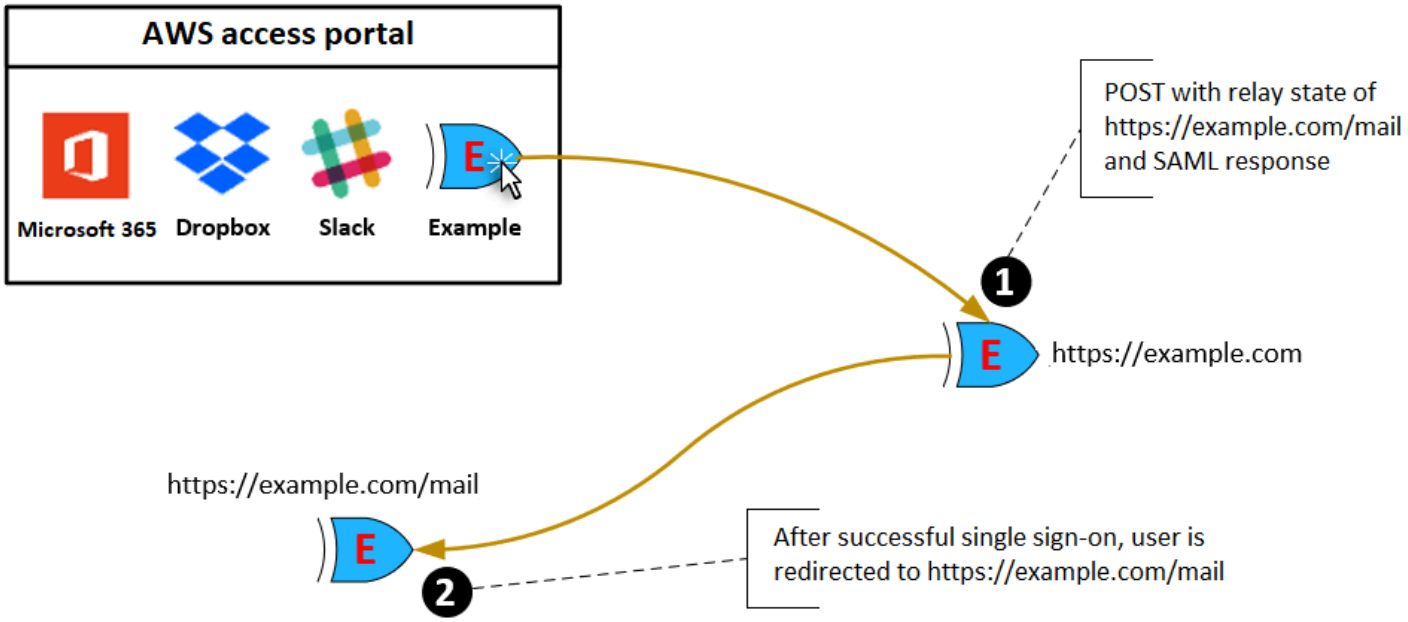
다음 단계와 다이어그램은 사용자가 AWS 액세스 포털에서 애플리케이션을 선택할 때의 애플리케이션 시작 URL 인증 워크플로를 보여줍니다.

1. 사용자 브라우저는 애플리케이션 시작 URL(이 경우 https://example.com)의 값을 사용하여 인증 요청을 리디렉션합니다.
2. 애플리케이션은 `SAMLRequest`와 함께 IAM Identity Center로 `HTML POST`를 전송합니다.
3. 그런 다음 IAM Identity Center는 `SAMLResponse`와 함께 애플리케이션으로 `HTML POST`를 다시 전송합니다.



릴레이 상태

페더레이션 인증 프로세스 중에 릴레이 상태는 애플리케이션 내에서 사용자를 리디렉션합니다. SAML 2.0의 경우 이 값은 수정되지 않고 애플리케이션에 전달됩니다. 애플리케이션 속성을 구성한 후 IAM Identity Center는 SAML 응답과 함께 릴레이 상태 값을 애플리케이션에 전송합니다.



세션 지속 시간

세션 지속 시간은 애플리케이션 사용자 세션이 유효한 시간입니다. SAML 2.0의 경우 이는 SAML 어설션의 요소 `saml2:AuthNStatement`의 `SessionNotOnOrAfter` 날짜 설정에 사용됩니다.

애플리케이션은 다음 방법 중 하나를 사용하여 세션 지속 시간을 해석할 수 있습니다.

- 애플리케이션은 이를 사용하여 사용자 세션에 허용되는 최대 시간을 결정할 수 있습니다. 애플리케이션은 지속 시간이 더 짧은 사용자 세션을 생성할 수 있습니다. 이는 애플리케이션이 구성된 세션 길이보다 짧은 지속 시간의 사용자 세션만 지원하는 경우 발생할 수 있습니다.
- 애플리케이션은 이 기간을 정확한 기간으로 사용할 수 있으며 관리자가 값을 구성하도록 허용하지 않을 수도 있습니다. 이러한 문제는 애플리케이션이 특정한 세션 길이만 지원하는 경우 발생할 수 있습니다.

세션 지속 시간 사용 방법에 대한 자세한 내용은 해당 애플리케이션의 설명서를 참조하세요.

IAM Identity Center 콘솔에서 애플리케이션에 사용자 액세스 권한 할당

사용자에게 애플리케이션 카탈로그의 SAML 2.0 애플리케이션 또는 사용자 지정 SAML 2.0 애플리케이션에 대한 Single Sign-On 액세스 권한을 할당할 수 있습니다.

그룹 할당 고려 사항:

- 그룹에 액세스 권한을 직접 할당하세요. 액세스 권한 관리를 단순화하려면 개별 사용자에게 액세스를 할당하는 대신 그룹에 액세스를 직접 할당하는 것이 좋습니다. 그룹을 사용하면 각 개인에게 권한을 적용하는 대신 사용자 그룹에 권한을 부여하거나 거부할 수 있습니다. 사용자가 다른 조직으로 이동하면 해당 사용자를 다른 그룹으로 이동하기만 하면 됩니다. 그러면 사용자는 새 조직에 필요한 권한을 자동으로 받게 됩니다.
- 중첩된 그룹은 지원되지 않습니다. 애플리케이션에 대한 사용자 액세스 권한을 할당할 때 IAM Identity Center는 사용자가 중첩된 그룹에 추가되는 것을 지원하지 않습니다. 사용자를 중첩된 그룹에 추가하면 로그인하는 동안 “애플리케이션이 없습니다.”라는 메시지가 표시될 수 있습니다. 사용자가 구성원으로 속해 있는 직속 그룹을 대상으로 할당해야 합니다.

애플리케이션에 사용자 또는 액세스 할당

> **Important**
>
> AWS 관리되는 애플리케이션의 경우 관련 애플리케이션 콘솔 내에서 직접 또는 API를 통해 사용자를 추가해야 합니다.

1. IAM Identity Center 콘솔을 엽니다.

   > **Note**
   >
   > 에서 사용자를 관리하는 경우 다음 AWS Managed Microsoft AD단계를 수행하기 전에 IAM Identity Center 콘솔이 AWS Managed Microsoft AD 디렉터리가 위치한 AWS 지역을 사용하고 있는지 확인하십시오.

2. [Applications]를 선택합니다.
3. 애플리케이션 목록에서 액세스 권한을 할당하려는 애플리케이션 이름을 선택합니다.
4. 애플리케이션 세부 정보 페이지의 할당된 사용자 섹션에서 사용자 할당을 선택합니다.
5. 사용자 할당 대화 상자에 사용자 또는 그룹 이름을 입력합니다. 사용자 및 그룹을 검색할 수도 있습니다. 검색 결과에 나타나는 해당 계정을 선택하여 여러 사용자 또는 그룹을 지정할 수 있습니다.
6. 사용자 배정를 선택합니다.

IAM Identity Center 콘솔에서 사용자 액세스 제거

이 절차를 사용하여 애플리케이션 카탈로그의 SAML 2.0 애플리케이션 또는 사용자 지정 SAML 2.0 애플리케이션에 대한 사용자 액세스를 제거합니다.

애플리케이션에서 사용자 액세스 제거

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 애플리케이션 목록에서 사용자 액세스를 제거하려는 애플리케이션을 선택합니다.
4. 애플리케이션 세부 정보 페이지의 할당된 사용자 섹션에서 제거하려는 사용자 또는 그룹을 선택한 다음 액세스 제거 버튼을 선택합니다.

5. 액세스 제거 대화 상자에서 사용자 또는 그룹 이름을 확인합니다. 그런 다음 액세스 제거를 선택합니다.

애플리케이션의 속성을 IAM Identity Center 속성에 매핑

일부 서비스 제공업체는 사용자 로그인에 대한 추가 데이터를 전달하기 위해 사용자 지정 SAML 어설션을 요구합니다. 이 경우 다음 절차를 사용하여 애플리케이션 사용자 속성을 IAM Identity Center의 해당 속성에 매핑하는 방법을 지정하세요.

애플리케이션의 속성을 IAM Identity Center 속성에 매핑하려면

1. IAM Identity Center 콘솔을 엽니다.
2. [Applications]를 선택합니다.
3. 애플리케이션 목록에서 속성을 매핑하려는 애플리케이션을 선택합니다.
4. 애플리케이션 세부 정보 페이지에서 작업을 선택한 다음 속성 매핑 편집을 선택합니다.
5. 새 속성 매핑 추가를 선택합니다.
6. 첫 번째 텍스트 상자에 애플리케이션 속성을 입력합니다.
7. 두 번째 텍스트 상자에 애플리케이션 속성에 매핑하려는 IAM Identity Center의 속성을 입력합니다. 예를 들어 애플리케이션 속성 **`Username`**을 IAM Identity Center 사용자 속성 **`email`**에 매핑하고 싶을 수 있습니다. IAM Identity Center에서 허용된 사용자 속성 목록을 보려면 AWS Managed Microsoft AD 디렉터리의 속성 매핑의 표를 참조하세요.
8. 표의 세 번째 열에 있는 메뉴에서 속성에 적합한 형식을 선택합니다.
9. 변경 사항 저장를 선택합니다.

복원력 설계 및 리전 동작

IAM Identity Center 서비스는 완전 관리형이며 Amazon S3 및 Amazon EC2와 같은 고가용성 및 내구성이 뛰어난 AWS 서비스를 사용합니다. 가용성 영역이 중단되는 경우 가용성을 보장하기 위해 IAM Identity Center는 여러 가용성 영역에서 작동합니다. IAM Identity Center의 가용성 설계 목표에 대한 자세한 내용은 신뢰성 요소 가이드의 부록 A: 일부 AWS 서비스의 가용성을 고려한 설계를 참조하세요.

AWS Organizations 관리 계정에서 IAM Identity Center를 활성화합니다. 이는 IAM Identity Center가 모든 AWS 계정에서 역할을 프로비저닝, 프로비저닝 해제 및 업데이트하기 위해 필요합니다. IAM Identity Center를 활성화하면 현재 선택된 AWS 리전에 배포됩니다. 특정 AWS 리전에 배포하려면 IAM Identity Center를 활성화하기 전에 리전 선택을 변경해야 합니다.

> **Note**
>
> IAM Identity Center는 기본 리전에서만 해당 권한 세트 및 애플리케이션에 대한 액세스를 제어합니다. IAM Identity Center가 단일 리전에서 작동하는 경우 액세스 제어와 관련된 위험을 고려하는 것이 좋습니다.

IAM Identity Center는 서비스를 활성화한 리전의 액세스를 결정하지만, AWS 계정는 전역에 걸쳐 있습니다. 즉, 사용자가 IAM Identity Center에 로그인한 후 IAM Identity Center를 통해 AWS 계정에 액세스하면 어느 리전에서나 작동할 수 있습니다. 그러나 SageMaker Amazon과 같은 대부분의 AWS 관리형 애플리케이션은 사용자가 이러한 애플리케이션을 인증하고 액세스 권한을 할당하려면 IAM Identity Center와 동일한 지역에 설치해야 합니다. IAM Identity Center와 함께 애플리케이션을 사용할 때 발생하는 리전별 제약에 대한 자세한 내용은 애플리케이션 설명서를 참조하십시오.

또한 IAM Identity Center를 사용하면 애플리케이션이 구축된 플랫폼이나 클라우드에 관계없이 공개 URL을 통해 연결할 수 있는 SAML 기반 애플리케이션에 대한 액세스를 인증하고 권한을 부여할 수 있습니다.

조직 인스턴스에 연결되지 않은 두 번째 격리된 제어 지점이 생성되므로 복원력을 구현하기 위한 수단으로 IAM Identity Center의 계정 인스턴스 사용은 권장되지 않습니다.

AWS Management Console에 대한 비상 액세스를 설정합니다.

IAM Identity Center는 고가용성 AWS 인프라로 구축되었으며 가용 영역 아키텍처를 사용하여 단일 장애 지점을 제거합니다. 예상치 못한 IAM ID 센터 또는 AWS 리전 장애 발생 시 추가 보호 계층을 확보

하려면 IAM Identity Center에 대한 임시 액세스를 제공하는 데 사용할 수 있는 구성을 설정하는 것이 좋습니다. AWS Management Console

내용

- 개요
- 비상 액세스 구성 요약
- 중요 운영 역할을 설계하는 방법
- 액세스 모델을 계획하는 방법
- 비상 역할, 계정 및 그룹 매핑을 설계하는 방법
- 비상 액세스 구성을 만드는 방법
- 비상 상황 대비 작업
- 비상 장애 조치 프로세스
- 정상 작동 상태로 복귀합니다.
- Okta에서 직접 IAM 페더레이션 애플리케이션을 한 번만 설정하면 됩니다.

개요

AWS를 통해 다음을 수행할 수 있습니다.

- 타사 IdP를 IAM Identity Center에 연결합니다.
- SAML 2.0 기반 페더레이션을 사용하여 타사 IdP를 개별 AWS 계정에 연결합니다.

IAM Identity Center를 사용하면 이러한 기능을 사용하여 다음 섹션에 설명된 비상 액세스 구성을 생성할 수 있습니다. 이 구성을 통해 AWS 계정 액세스를 위한 메커니즘으로 IAM Identity Center를 사용할 수 있습니다. IAM Identity Center가 중단되는 경우 비상 가동 사용자는 계정에 액세스할 때 사용하는 것과 동일한 보안 인증 정보 사용하여 직접 페더레이션을 통해 AWS Management Console에 로그인할 수 있습니다. 이 구성은 IAM Identity Center를 사용할 수 없지만 IAM 데이터 영역과 외부 ID 제공업체(idP)를 사용할 수 있는 경우에 작동합니다.

> **Important**
>
> 필요한 IAM 역할을 생성하기 위한 액세스 권한도 중단되면 구성을 생성할 수 없으므로 중단이 발생하기 전에 이 구성을 배포하는 것이 좋습니다. 또한, IAM Identity Center가 중단될 경우 팀에서 어떤 조치를 취해야 하는지 파악할 수 있도록 이 구성을 주기적으로 테스트합니다.

비상 액세스 구성 요약

긴급 액세스를 구성하려면 다음 작업을 완료해야 합니다.

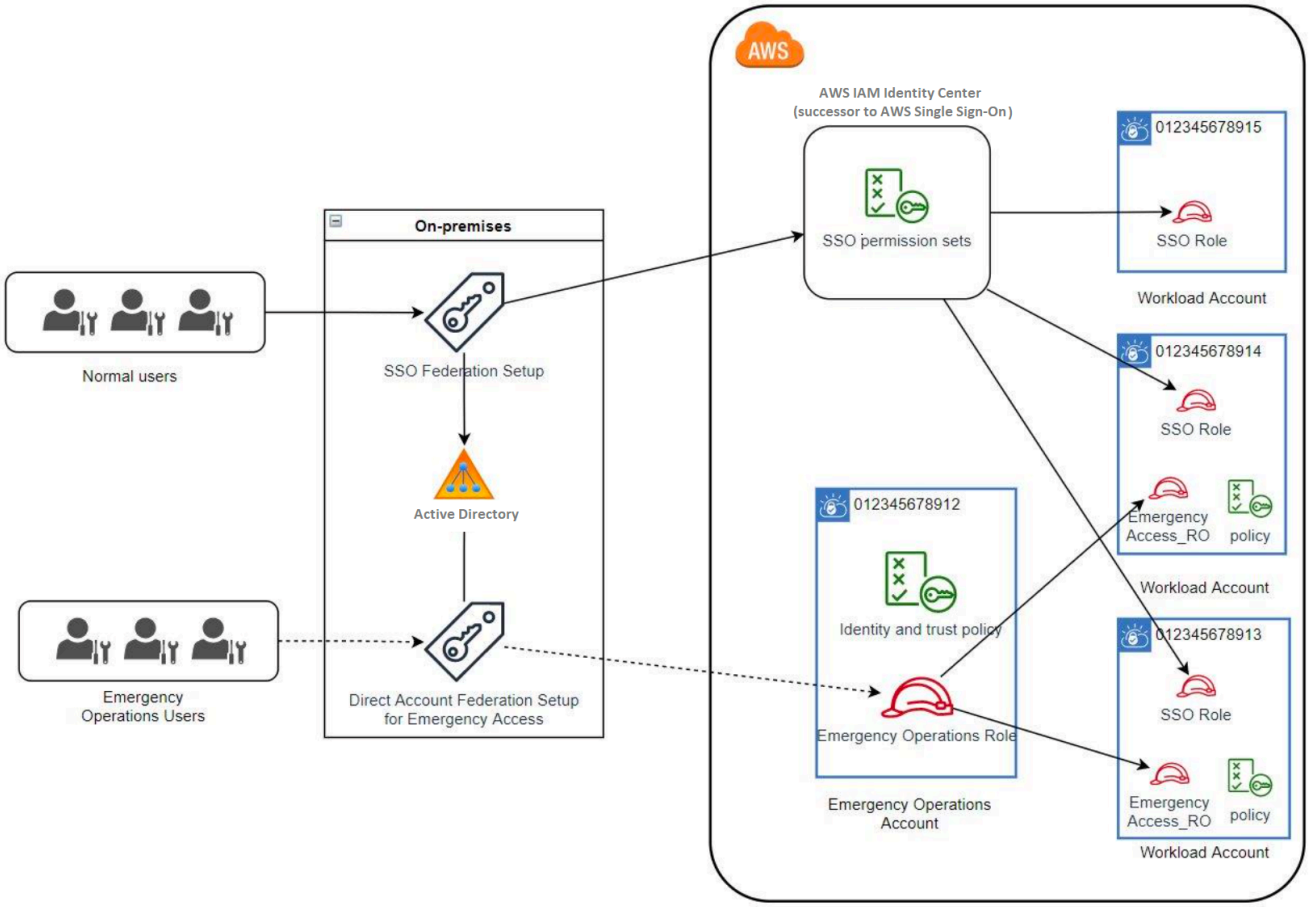
1. AWS Organizations에서 조직의 비상 운영 계정을 계정을 만듭니다.
2. SAML 2.0 기반 페더레이션을 사용하여 IdP를 IdP를 비상 운영 계정에 연결합니다.
3. 비상 운영 계정에서 제3자 ID 제공업체 페더레이션에 필요한 역할을 생성합니다. 또한 필요한 권한을 사용하여 각 워크로드 계정에서 비상 운영 역할을 생성합니다.
4. 비상 운영 계정에서 생성한 IAM 역할의 워크로드 계정에 대한 액세스 권한을 위임합니다. 비상 운영 계정에 대한 액세스 권한을 부여하려면 IdP에서 구성원이 없이 비상 운영 그룹을 만듭니다.
5. IdP에 AWS Management Console에 대한 SSAML 2.0 페더레이션 액세스를 활성화하는 규칙을 생성하여 IdP의 비상 운영 그룹이 비상 운영 역할을 사용하도록 설정합니다.

정상 운영 중에는 IdP의 비상 운영 그룹에 구성원이 없으므로 아무도 비상 운영 계정에 액세스할 수 없습니다. IAM Identity Center가 중단되는 경우 IdP를 사용하여 신뢰할 수 있는 사용자를 IdP의 비상 운영 그룹에 추가합니다. 그러면 해당 사용자는 IdP에 로그인하여 AWS Management Console로 이동한 다음 비상 운영 계정에서 비상 운영 역할을 맡을 수 있습니다. 여기에서 해당 사용자는 비상 운영을 수행해야 하는 워크로드 계정에서 비상 액세스 역할로 역할을 전환할 수 있습니다.

중요 운영 역할을 설계하는 방법

이 설계를 사용하면 IAM을 통해 페더레이션하는 단일 AWS 계정를 구성하여 사용자가 중요 운영 역할을 맡을 수 있습니다. 중요 운영 역할에는 사용자가 워크로드 계정에서 해당 역할을 맡을 수 있도록 하는 신뢰 정책이 있습니다. 워크로드 계정의 역할은 사용자가 필수 작업을 수행하는 데 필요한 권한을 제공합니다.

다음 다이어그램은 디자인 개요를 보여줍니다.



액세스 모델을 계획하는 방법

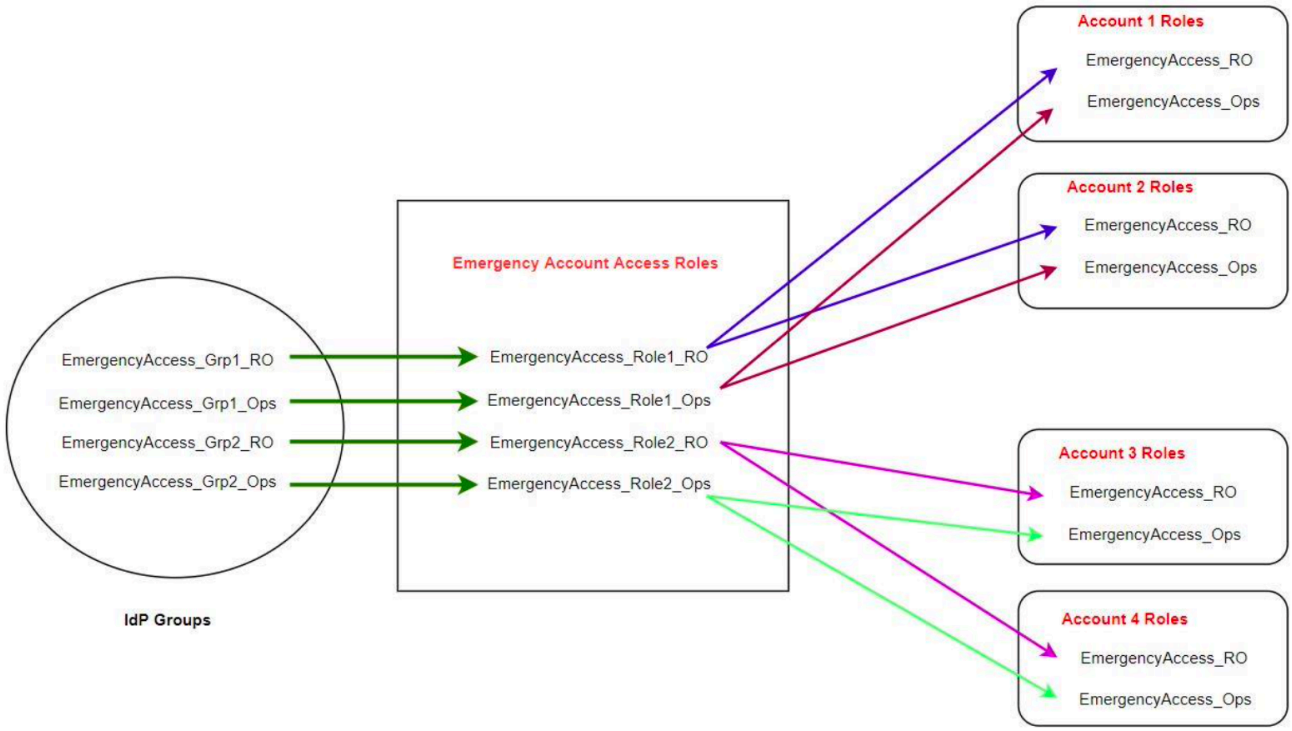
비상 액세스를 구성하기 전에 액세스 모델 작동 방식에 대한 계획을 세웁니다. 다음 프로세스를 사용하여 이 계획을 생성합니다.

1. IAM Identity Center가 중단되는 경우 비상 운영자 액세스가 필요한 AWS 계정 를 파악합니다. 예를 들어 프로덕션 계정은 필수적이지만 개발 및 테스트 계정은 그렇지 않을 수 있습니다.
2. 해당 계정 모음에서 계정에 필요한 중요 역할을 파악합니다. 이러한 계정에서 각 역할이 수행할 수 있는 작업을 일관성 있게 정의합니다. 이렇게 하면 교차 계정 역할을 생성하는 비상 액세스 계정에서의 작업이 간소화됩니다. 이러한 계정에서는 읽기 전용(RO)과 운영(Ops) 이렇게 두 가지 역할로 시작하는 것이 좋습니다. 필요한 경우 더 많은 역할을 생성하고 이러한 역할을 설정에서 더 많은 비상 액세스 사용자 그룹에 매핑할 수 있습니다.
3. IdP에서 비상 액세스 그룹을 식별하고 생성합니다. 그룹 구성원은 비상 액세스 역할에 대한 액세스 권한을 위임하는 사용자입니다.

4. 비상 액세스 계정에서 이러한 그룹이 맡을 수 있는 역할을 정의합니다. 이렇게 하려면 그룹이 액세스할 수 있는 역할을 표시하는 클레임을 생성하는 규칙을 IdP에서 정의합니다. 그러면 이러한 그룹이 비상 액세스 계정에서 읽기 전용 또는 운영 역할을 맡을 수 있습니다. 이러한 역할을 통해 워크로드 계정에서 해당 역할을 맡을 수 있습니다.

비상 역할, 계정 및 그룹 매핑을 설계하는 방법

다음 다이어그램은 비상 액세스 그룹을 비상 액세스 계정의 역할에 매핑하는 방법입니다. 이 다이어그램에는 비상 액세스 계정 역할이 워크로드 계정의 해당 역할에 액세스할 수 있도록 하는 계정 간 역할 신뢰 관계도 나와 있습니다. 비상 계획 설계 시 이러한 매핑을 출발점으로 삼는 것이 좋습니다



비상 액세스 구성을 만드는 방법

다음 매핑 표를 사용하여 비상 액세스 구성을 만듭니다. 이 표에는 워크로드 계정에서 읽기 전용(RO) 및 운영(Ops) 이렇게 두 가지 역할과 해당 신뢰 정책 및 권한 정책이 명시된 계획이 나와 있습니다. 신뢰 정책을 사용하면 비상 액세스 계정 역할이 개별 워크로드 계정 역할에 액세스할 수 있습니다. 개별 워크로드 계정 역할에는 해당 역할이 계정에서 수행할 수 있는 작업에 대한 권한 정책도 포함되어 있습니다. 권한 정책은 AWS 관리형 정책 또는 고객 관리형 정책일 수 있습니다.

계정	역할 생성	신뢰 정책	권한 정책
계정 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
계정 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
계정 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:AWS:iam: :aws:policy/ReadOnlyAccess
계정 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
비상 액세스 계정	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	AssumeRole 계정 내 역할 리소스의 경우

이 매핑 계획에서 비상 액세스 계정에는 읽기 전용 역할 2개와 운영 역할 2개가 포함되어 있습니다. 이러한 역할은 IdP를 신뢰하여 어설션에 역할의 이름을 전달함으로써 선택한 그룹이 역할에 액세스할 수 있도록 인증하고 권한을 부여합니다. 워크로드 계정 1과 계정 2에는 해당하는 읽기 전용 및 운영 역할이 있습니다. 워크로드 계정 1의 경우 `EmergencyAccess_RO` 역할은 비상 액세스 계정에 있는 `EmergencyAccess_Role1_RO` 역할을 신뢰합니다. 이 표에는 워크로드 계정 읽기 전용 및 운영 역할과 해당 비상 액세스 역할 간 유사한 신뢰 패턴이 나와 있습니다.

비상 상황 대비 작업

비상 액세스 구성을 준비하려면 비상 상황이 발생하기 전에 다음 작업을 수행하는 것이 좋습니다.

1. IdP에서 직접 IAM 페더레이션 애플리케이션을 설정합니다. 자세한 설명은 Okta에서 직접 IAM 페더레이션 애플리케이션을 한 번만 설정하면 됩니다. 섹션을 참조하세요.
2. 이벤트 중에 액세스할 수 있는 비상 액세스 계정에서 IdP 연결을 만듭니다.
3. 위의 매핑 표에 설명된 대로 비상 액세스 계정에 비상 액세스 역할을 만듭니다.
4. 각 워크로드 계정에서 신뢰 및 권한 정책을 사용하여 임시 운영 역할을 만듭니다.
5. IdP에서 임시 운영 그룹을 생성합니다. 그룹 이름은 임시 운영 역할의 이름에 따라 달라집니다.
6. 직접 IAM 페더레이션을 테스트합니다.
7. 정기적인 사용을 방지하기 위해 IdP에서 IdP 페더레이션 애플리케이션을 비활성화합니다.

비상 장애 조치 프로세스

IAM Identity Center 인스턴스를 사용할 수 없고 AWS 관리 콘솔에 대한 비상 액세스를 제공해야 하는 경우, 다음과 같은 장애 조치 프로세스를 권장합니다.

1. IdP 관리자는 IdP에서 직접 IAM 페더레이션 애플리케이션을 활성화합니다.
2. 사용자는 이메일 요청, Slack 채널 또는 기타 통신 형식과 같은 기존 메커니즘을 통해 임시 운영 그룹에 대한 액세스를 요청합니다.
3. 비상 액세스 그룹에 추가한 사용자는 IdP에 로그인하고, 비상 액세스 계정을 선택하고, 사용자는 비상 액세스 계정에서 사용할 역할을 선택합니다. 이러한 역할 중에서 비상 계정 역할과 계정 간 신뢰를 갖는 해당 워크로드 계정의 역할을 맡을 수 있습니다.

정상 작동 상태로 복귀합니다.

AWS 상태 대시보드를 확인하여 IAM Identity Center 서비스의 상태가 복원되었는지 확인합니다. 정상 작동으로 돌아가려면 다음 단계를 수행합니다.

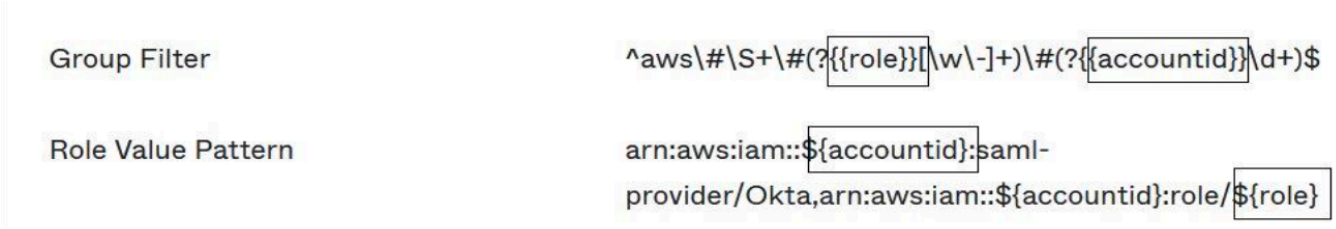
1. IAM Identity Center 서비스의 상태 아이콘이 서비스가 정상이라고 표시되면 IAM Identity Center에 로그인합니다.
2. IAM Identity Center에 성공적으로 로그인할 수 있으면 비상 액세스 사용자에게 IAM Identity Center를 사용할 수 있다고 전달합니다. 이러한 사용자에게 로그아웃하고 AWS 액세스 포털을 사용하여 IAM Identity Center에 다시 로그인하도록 지시합니다.

3. 모든 비상 액세스 사용자가 로그아웃한 후 IdP에서 IdP 페더레이션 애플리케이션을 비활성화합니다. 근무 시간 이후에 이 작업을 수행하는 것이 좋습니다.
4. IdP의 비상 액세스 그룹에서 모든 사용자를 제거합니다.

비상 액세스 역할 인프라는 백업 액세스 계획으로 유지되지만 이제 비활성화됩니다.

Okta에서 직접 IAM 페더레이션 애플리케이션을 한 번만 설정하면 됩니다.

1. 관리 권한을 가진 사용자인 Okta 계정에 로그인합니다.
2. Okta 관리 콘솔의 애플리케이션에서 애플리케이션을 선택합니다.
3. 앱 카탈로그 찾아보기를 선택합니다. AWS 계정 페더레이션을 검색하여 선택합니다. 통합 추가를 선택합니다.
4. AWS 계정 페더레이션을 위한 SAML 2.0 구성 방법의 단계에 따라 AWS와 직접 IAM 페더레이션을 설정합니다.
5. 로그인 옵션 탭에서 SAML 2.0을 선택하고 그룹 필터 및 역할 값 패턴 설정을 입력합니다. 사용자 디렉터리의 그룹 이름은 구성한 필터에 따라 달라집니다.



위 그림에서 `role` 변수는 비상 액세스 계정의 비상 운영 역할에 대한 변수입니다. 예를 들어, 매핑 표에 설명된 대로 AWS 계정 `123456789012`에 `EmergencyAccess_Role1_RO` 역할을 생성하고 그룹 필터 설정이 위 그림과 같이 구성되어 있는 경우 그룹 이름은 `aws#EmergencyAccess_Role1_RO#123456789012`가 되어야 합니다.

6. 디렉터리(예: Active Directory의 디렉터리)에서 비상 액세스 그룹을 만들고 디렉터리 이름(예: `aws#EmergencyAccess_Role1_RO#123456789012`)을 지정합니다. 기존 프로비저닝 메커니즘을 사용하여 사용자를 이 그룹에 할당합니다.
7. 비상 액세스 계정에서 장애 발생 시 비상 액세스 역할을 맡는 데 필요한 권한을 제공하는 사용자 지정 신뢰 정책을 구성합니다. 다음은 `EmergencyAccess_Role1_RO` 역할에 연결된 사용자 지정 신뢰 정책에 대한 예제 설명입니다. 설명을 보려면 비상 역할, 계정 및 그룹 매핑을 설계하는 방법 아래의 다이어그램에서 긴급 계정을 참조하십시오.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:SetSourceIdentity",
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
               "SAML:aud":"https:~/~/signin.aws.amazon.com/saml"
            }
         }
      }
   ]
}
```

8. 다음은 EmergencyAccess_Role1_RO 역할에 연결된 사용자 지정 권한 정책에 대한 예제 설명입니다. 설명을 보려면 비상 역할, 계정 및 그룹 매핑을 설계하는 방법 아래의 다이어그램에서 긴급 계정을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Action":"sts:AssumeRole",
         "Resource":[
            "arn:aws:iam::<account 1>:role/EmergencyAccess_RO",
            "arn:aws:iam::<account 2>:role/EmergencyAccess_RO"
         ]
      }
   ]
}
```

9. 워크로드 계정에서 사용자 지정 신뢰 정책을 구성합니다. 다음은 EmergencyAccess_RO 역할에 연결된 사용자 지정 신뢰 정책에 대한 예제 설명입니다. 이 예에서 계정 123456789012는 비상 액세스 계정입니다. 설명을 보려면 비상 역할, 계정 및 그룹 매핑을 설계하는 방법 아래의 다이어그램에서 워크로드 계정을 참조하십시오.

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> 대부분의 IdPs 경우 필요할 때까지 애플리케이션 통합을 비활성화된 상태로 유지할 수 있습니다. 비상 액세스가 필요할 때까지 IdP에서 직접 IAM 페더레이션 애플리케이션을 비활성화 상태로 유지하는 것이 좋습니다.

보안: AWS IAM Identity Center

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

보안은 기업과 기업 간의 AWS 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스를 참조하십시오. AWS IAM Identity Center
- 클라우드에서의 보안 - 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 IAM Identity Center 사용 시 책임 분담 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목적에 맞게 IAM Identity Center를 구성하는 방법을 보여줍니다. 또한 IAM Identity Center 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- IAM Identity Center ID 및 액세스 관리
- IAM Identity Center 콘솔 및 API 인증
- AWS STS IAM ID 센터의 조건 컨텍스트 키
- IAM Identity Center 로깅 및 모니터링
- IAM Identity Center에 대한 규정 준수 확인
- IAM Identity Center 복원성
- IAM Identity Center의 인프라 보안

IAM Identity Center ID 및 액세스 관리

IAM Identity Center에 액세스하려면 요청을 인증하는 데 사용할 AWS 수 있는 자격 증명이 필요합니다. 이러한 자격 증명에는 AWS 관리형 애플리케이션과 같은 AWS 리소스에 액세스할 수 있는 권한이 있어야 합니다.

AWS 액세스 포털에 대한 인증은 IAM Identity Center에 연결된 디렉터리에 의해 제어됩니다. 하지만 AWS 액세스 포털 내에서 사용자가 사용할 수 AWS 계정 있는 권한 부여는 다음 두 가지 요소에 의해 결정됩니다.

1. IAM Identity Center AWS 계정 콘솔에 있는 사용자에게 액세스 권한을 할당받은 사람 자세한 정보는 싱글 사인온 액세스: AWS 계정을 참조하세요.
2. IAM Identity Center 콘솔의 사용자가 AWS 계정에 대한 적절한 액세스를 갖도록 허용된 권한 수준. 자세한 정보는 권한 세트 생성, 관리 및 삭제을 참조하세요.

다음 섹션에서는 관리자가 IAM Identity Center 콘솔에 대한 액세스를 제어하거나 IAM Identity Center 콘솔에서 day-to-day 작업에 대한 관리 액세스를 위임하는 방법을 설명합니다.

- 인증
- 액세스 제어

인증

IAM ID를 AWS 사용하여 액세스하는 방법을 알아보십시오.

액세스 제어

요청을 인증하는 데 유효한 보안 인증이 있더라도 권한이 없다면 IAM Identity Center 리소스를 생성하거나 액세스할 수 없습니다. 예를 들어 IAM Identity Center에 연결된 디렉터리를 생성할 권한이 있어야 합니다.

다음 단원에서는 IAM Identity Center에 대한 권한을 관리하는 방법을 설명합니다. 먼저 개요를 읽어 보면 도움이 됩니다.

- IAM Identity Center 리소스에 대한 액세스 권한 관리 개요
- IAM Identity Center에 대한 자격 증명 기반 정책 예시
- IAM Identity Center 서비스 연결 역할 사용

IAM Identity Center 리소스에 대한 액세스 권한 관리 개요

모든 AWS 리소스는 가 AWS 계정소유하며 리소스를 생성하거나 액세스할 수 있는 권한은 권한 정책에 따라 관리됩니다. 액세스를 제공하기 위해 계정 관리자는 IAM 자격 증명(사용자, 그룹 및 역할)에 권한을 추가할 수 있습니다. AWS Lambda같은 일부 서비스에서도 권한을 리소스에 추가할 수 있습니다.

> **Note**
>
> 계정 관리자 또는 관리자 사용자는 관리자 권한이 있는 사용자입니다. 자세한 내용은 IAM 사용 설명서의 IAM 모범 사례를 참조하십시오.

주제

- IAM Identity Center 리소스 및 작업
- 리소스 소유권 이해
- 리소스 액세스 관리
- 정책 요소 지정: 작업, 효과, 리소스, 보안 주체
- 정책에서 조건 지정

IAM Identity Center 리소스 및 작업

IAM Identity Center의 기본 리소스는 애플리케이션 인스턴스, 프로필, 권한 세트입니다.

리소스 소유권 이해

리소스를 만든 사람은 리소스 소유자입니다. AWS 계정 즉, 리소스 소유자는 리소스를 생성하는 요청을 인증하는 주체 (계정, 사용자 또는 IAM 역할) 의 소유자입니다. AWS 계정 다음 예에서는 이러한 작동 방식을 설명합니다.

- 에서 애플리케이션 인스턴스 또는 권한 집합과 같은 IAM Identity Center 리소스를 AWS 계정 루트 사용자 생성하는 경우 해당 리소스의 소유자는 사용자가 AWS 계정 됩니다.
- AWS 계정에서 사용자를 생성하고 해당 사용자에게 IAM Identity Center 리소스를 생성할 권한을 부여하면 사용자는 IAM Identity Center 리소스를 생성할 수 있습니다. 하지만 사용자가 속한 AWS 계정이 리소스를 소유합니다.
- IAM Identity Center 리소스를 생성할 권한이 있는 IAM 역할을 AWS 계정에 생성하는 경우, 역할을 수임할 수 있는 사람은 누구나 IAM Identity Center 리소스를 생성할 수 있습니다. 이 경우 역할이 속한 AWS 계정이 IAM Identity Center 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 IAM Identity Center의 맥락에서 IAM을 사용하는 방법에 대해 설명합니다. IAM 서비스에 대한 자세한 정보는 다루지 않습니다. IAM 설명서 전체 내용은 IAM 사용 설명서의 IAM이란 무엇인가요? 단원을 참조하세요. IAM 정책 구문 및 설명에 대한 자세한 내용은 IAM 사용 설명서의 AWS IAM 정책 참조 단원을 참조하세요.

IAM ID에 연결된 정책을 ID 기반 정책(IAM 정책)이라고 합니다. 리소스에 연결된 정책을 리소스 기반 정책이라고 합니다. IAM Identity Center는 자격 증명 기반 정책(IAM 정책)만 지원합니다.

주제

- 자격 증명 기반 정책(IAM 정책)
- 리소스 기반 정책

자격 증명 기반 정책(IAM 정책)

IAM Identity Identity에 권한을 추가할 수 있습니다. 예를 들어 다음을 수행할 수 있습니다.

- 사용자 또는 내 그룹에 권한 정책 연결 AWS 계정— 계정 관리자는 특정 사용자와 관련된 권한 정책을 사용하여 해당 사용자에게 새 애플리케이션과 같은 IAM Identity Center 리소스를 추가할 수 있는 권한을 부여할 수 있습니다.
- 역할에 권한 정책 연결(교차 계정 권한 부여) – ID 기반 권한 정책을 IAM 역할에 연결하여 교차 계정 권한을 부여할 수 있습니다.

  IAM을 사용하여 권한을 위임하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 액세스 관리 단원을 참조하십시오.

다음 권한 정책은 사용자에게 `List`로 시작하는 모든 작업을 실행할 수 있는 권한을 부여합니다. 이러한 작업은 IAM Identity Center 리소스에 대한 정보(예: 애플리케이션 인스턴스 또는 권한 세트)를 보여줍니다. `Resource` 요소에 와일드카드 문자(*)가 있으면 계정이 소유한 모든 IAM Identity Center 리소스에 대해 작업이 허용됩니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"sso:List*",
         "Resource":"*"
      }
   ]
}
```

IAM Identity Center에서 자격 증명 기반 정책을 사용하는 방법에 대한 자세한 내용은 IAM Identity Center에 대한 자격 증명 기반 정책 예시을 참조하세요. 사용자, 그룹, 역할 및 권한에 대한 자세한 내용은 IAM User Guide의 Identities (users, groups, and roles)를 참조하세요.

리소스 기반 정책

Amazon S3과 같은 다른 서비스도 리소스 기반 권한 정책을 지원합니다. 예를 들어, 정책을 S3 버킷에 연결하여 해당 버킷에 대한 액세스 권한을 관리할 수 있습니다. IAM Identity Center는 리소스 기반 정책을 지원하지 않습니다.

정책 요소 지정: 작업, 효과, 리소스, 보안 주체

각 IAM Identity Center 리소스(IAM Identity Center 리소스 및 작업 참조)에서 이 서비스는 API 작업을 정의합니다. 이러한 API 작업에 대한 권한을 부여하기 위해 IAM Identity Center는 정책에서 지정할 수 있는 작업을 정의합니다. API 작업을 수행하려면 둘 이상의 작업에 대한 권한이 필요할 수 있습니다.

다음은 기본 정책 요소입니다.

- 리소스 – 정책에서 Amazon 리소스 이름(ARN)을 사용하여 정책을 적용할 리소스를 식별합니다.
- 조치 – 조치 키워드를 사용하여 허용 또는 거부할 리소스 작업을 식별합니다. 예를 들어, `sso:DescribePermissionsPolicies` 권한은 사용자에게 IAM Identity Center `DescribePermissionsPolicies` 작업 수행 권한을 허용합니다.
- 결과 – 사용자가 특정 작업을 요청하는 경우의 결과를 지정합니다. 이는 허용 또는 거부 중에 하나가 될 수 있습니다. 명시적으로 리소스에 대한 액세스 권한을 부여(허용)하지 않는 경우, 액세스는 묵시적으로 거부됩니다. 다른 정책에서 액세스 권한을 부여하는 경우라도 사용자가 해당 리소스에 액세스할 수 없도록 하기 위해 리소스에 대한 권한을 명시적으로 거부할 수도 있습니다.
- 보안 주체 – ID 기반 정책(IAM 정책)에서 정책이 연결되는 사용자는 암시적인 보안 주체입니다. 리소스 기반 정책의 경우, 사용자, 계정, 서비스 또는 권한의 수신자인 기타 개체를 지정합니다(리소스 기반 정책에만 해당). IAM Identity Center는 리소스 기반 정책을 지원하지 않습니다.

IAM 정책 구문과 설명에 대한 자세한 내용은 IAM User Guide의 AWS IAM policy reference를 참조하세요.

정책에서 조건 지정

권한을 부여할 때 액세스 정책 언어를 사용하여 정책을 시행하기 위해 필요한 조건을 지정할 수 있습니다. 예를 들어, 특정 날짜 이후에만 정책을 적용할 수 있습니다. 정책 언어에서의 조건 지정에 관한 자세한 설명은 IAM 사용자 가이드의 조건을 참조하십시오.

조건을 표시하려면 미리 정의된 조건 키를 사용합니다. IAM Identity Center에만 해당되는 특정한 조건 키는 없습니다. 하지만 필요에 따라 사용할 수 있는 AWS 조건 키가 있습니다. 전체 AWS 키 목록은 IAM 사용 설명서의 사용 가능한 글로벌 조건 키를 참조하십시오.

IAM Identity Center에 대한 자격 증명 기반 정책 예시

이 주제에서는 사용자와 역할에 IAM Identity Center를 관리할 권한을 부여하기 위해 생성할 수 있는 IAM 정책의 예를 제공합니다.

> **Important**
>
> IAM Identity Center 리소스에 대한 액세스 관리를 위해 제공되는 기본 개념과 옵션 설명이 나온 소개 주제 부분을 먼저 읽는 것이 좋습니다. 자세한 정보는 IAM Identity Center 리소스에 대한 액세스 권한 관리 개요을 참조하세요.

이 주제의 섹션에서는 다음 내용을 학습합니다.

- 사용자 지정 정책 예
- IAM Identity Center 콘솔을 사용하는 데 필요한 권한

사용자 지정 정책 예

이 섹션에서는 사용자 지정 IAM 정책이 필요한 일반적인 사용 사례를 제공합니다. 이러한 예제 정책은 주요 요소를 지정하지 않는 자격 증명 기반 정책입니다. 자격 증명 기반 정책에서는 권한을 가질 보안 주체를 지정하지 않기 때문입니다. 대신 정책을 보안 주체에 연결합니다. IAM 역할에 자격 증명 기반 권한 정책을 연결할 경우 역할의 신뢰 정책에 식별된 보안 주체는 권한을 가집니다. IAM에서 자격 증명 기반 정책을 생성하여 사용자, 그룹 및/또는 역할에 연결할 수 있습니다. 또한 IAM IAM Identity Center에서 권한 세트를 생성할 때 IAM Identity Center 사용자에게 이러한 정책을 적용할 수 있습니다.

> **Note**
>
> 환경에 맞는 정책을 만들 때 이러한 예를 사용하고 프로덕션 환경에 정책을 배포하기 전에 긍정적("액세스 허용") 및 부정적("액세스 거부") 테스트 사례를 모두 테스트해야 합니다. IAM 정책 테스트에 대한 자세한 내용은 IAM 사용 설명서의 IAM 정책 시뮬레이터로 IAM 정책 테스트를 참조하세요.

주제

- 예 1: 사용자가 IAM Identity Center를 볼 수 있도록 허용
- 예 2: 사용자가 IAM ID 센터에서 권한을 관리하도록 AWS 계정 허용
- 예 3: 사용자가 IAM Identity Center에서 애플리케이션을 관리하도록 허용
- 예 4: 사용자가 Identity Center 디렉터리의 사용자 및 그룹을 관리하도록 허용

예 1: 사용자가 IAM Identity Center를 볼 수 있도록 허용

다음 권한 정책은 IAM Identity Center에 구성된 모든 설정과 디렉터리 정보를 볼 수 있도록 사용자에게 읽기 전용 권한을 부여합니다.

> **Note**
>
> 이 정책은 예시용으로만 제공됩니다. 프로덕션 환경에서는 IAM Identity Center의 `ViewOnlyAccess` AWS 관리형 정책을 사용하는 것이 좋습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
```

```
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListOrganizationalUnitsForParent",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetInlinePolicyForPermissionSet",
                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

예 2: 사용자가 IAM ID 센터에서 권한을 관리하도록 AWS 계정 허용

다음 권한 정책은 사용자가 AWS 계정의 권한 세트를 생성, 관리 및 배포하도록 허용하는 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeleteInlinePolicyFromPermissionSet",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso:UpdatePermissionSet"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "IAMListPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AccessToSSOProvisionedRoles",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
        }
    ]
}
```

Note

`"Sid": "IAMListPermissions"`, 및 `"Sid": "AccessToSSOProvisiondRoles"` 섹션에 나열된 추가 권한은 사용자가 AWS Organizations 관리 계정에서 할당을 생성할 수 있도록

하는 데에만 필요합니다. 경우에 따라 이 섹션에 `iam:UpdateSAMLProvider`을 추가해야 할 수도 있습니다.

예 3: 사용자가 IAM Identity Center에서 애플리케이션을 관리하도록 허용

다음 권한 정책은 사용자가 IAM Identity Center 카탈로그 내에서 사전 통합된 SaaS 애플리케이션을 포함하여 IAM Identity Center의 애플리케이션을 보고 구성할 수 있는 권한을 부여합니다.

> **Note**
>
> 다음 정책 예제에서 사용되는 `sso:AssociateProfile` 작업은 애플리케이션에 대한 사용자 및 그룹 할당을 관리하는 데 필요합니다. 또한 사용자는 기존 권한 집합을 AWS 계정 사용하여 사용자와 그룹을 할당할 수 있습니다. 사용자가 IAM Identity Center 내에서 AWS 계정 액세스를 관리해야 하고 권한 집합을 관리하는 데 필요한 권한이 필요한 경우 를 참조하십시오예 2: 사용자가 IAM ID 센터에서 권한을 관리하도록 AWS 계정 허용.

2020년 10월 기준, 이러한 작업 중 상당수는 AWS 콘솔을 통해서만 사용할 수 있습니다. 이 예제 정책에는 이러한 경우에 대해 콘솔의 오류 없는 작동과 관련된 목록, 가져오기, 검색과 같은 “읽기” 작업이 포함되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:ImportApplicationInstanceServiceProviderMetadata",
                "sso:DeleteApplicationInstance",
                "sso:DeleteProfile",
                "sso:DisassociateProfile",
                "sso:GetApplicationTemplate",
                "sso:UpdateApplicationInstanceServiceProviderConfiguration",
                "sso:UpdateApplicationInstanceDisplayData",
                "sso:DeleteManagedApplicationInstance",
                "sso:UpdateApplicationInstanceStatus",
                "sso:GetManagedApplicationInstance",
                "sso:UpdateManagedApplicationInstanceStatus",
```

```
                "sso:CreateManagedApplicationInstance",
                "sso:UpdateApplicationInstanceSecurityConfiguration",
                "sso:UpdateApplicationInstanceResponseConfiguration",
                "sso:GetApplicationInstance",
                "sso:CreateApplicationInstanceCertificate",
                "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
                "sso:UpdateApplicationInstanceActiveCertificate",
                "sso:DeleteApplicationInstanceCertificate",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationTemplates",
                "sso:ListApplications",
                "sso:ListApplicationInstances",
                "sso:ListDirectoryAssociations",
                "sso:ListProfiles",
                "sso:ListProfileAssociations",
                "sso:ListInstances",
                "sso:GetProfile",
                "sso:GetSSOStatus",
                "sso:GetSsoConfiguration",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeUsers",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

예 4: 사용자가 Identity Center 디렉터리의 사용자 및 그룹을 관리하도록 허용

다음 권한 정책은 사용자가 IAM Identity Center에서 사용자 및 그룹을 생성, 확인, 수정 및 삭제할 수 있도록 허용하는 권한을 부여합니다.

IAM Identity Center의 사용자 및 그룹에 대한 직접 수정이 제한되는 경우도 있습니다. Active Directory 또는 Automatic Provisioning이 활성화된 외부 ID 제공업체를 ID 소스로 선택한 경우를 예로 들 수 있습니다.

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

```
            "Effect": "Allow",
            "Action": [
                "sso-directory:ListGroupsForUser",
                "sso-directory:DisableUser",
                "sso-directory:EnableUser",
                "sso-directory:SearchGroups",
                "sso-directory:DeleteGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:DescribeDirectory",
                "sso-directory:UpdateUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:SearchUsers",
                "sso:ListDirectoryAssociations",
                "sso-directory:RemoveMemberFromGroup",
                "sso-directory:DeleteUser",
                "sso-directory:DescribeUsers",
                "sso-directory:UpdateGroup",
                "sso-directory:CreateGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM Identity Center 콘솔을 사용하는 데 필요한 권한

사용자가 IAM Identity Center 콘솔을 오류 없이 사용하려면 추가 권한이 필요합니다. IAM 정책이 최소 필수 권한보다 더 제한적인 정책을 만들면 콘솔에서는 해당 정책에 연결된 사용자에 의도대로 작동하지 않습니다. 다음 예제는 IAM Identity Center 콘솔 내에서 오류 없이 운영하기 위해 필요할 수 있는 권한 세트를 나열합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
```

```
                "sso:DescribePermissionsPolicies",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "sso:GetPermissionsPolicy",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:ListAccountAssignmentCreationStatus",
                "sso:ListAccountAssignmentDeletionStatus",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationInstances",
                "sso:ListApplications",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetProvisioningStatus",
                "sso:ListPermissionSets",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:ListTagsForResource",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeUsers",
                "sso-directory:ListGroupsForUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS IAM ID 센터의 관리형 정책

팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. AWS 관리형 정책을 사용하면 빠르게 시작할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 정보는 IAM 사용 설명서에서 AWS 관리형 정책을 참조하세요.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 타입의 업데이트는 정책이 연결된 모든 보안 인증(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 여러 서비스에 걸친 작업 기능에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면 새 작업 및 리소스에 대한 읽기 전용 권한이 AWS 추가됩니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

사용자 세션을 나열하고 삭제할 수 있는 새 작업은 새 네임스페이스 `identitystore-auth`에서 사용할 수 있습니다. 해당 네임스페이스의 작업에 대한 추가 권한은 이 페이지에서 업데이트됩니다. 사용자 지정 IAM 정책을 생성할 때는 `identitystore-auth` 뒤에 `*`를 사용하지 않는 것이 좋습니다. 이는 현재 또는 미래에 네임스페이스에 있는 모든 작업에 적용되기 때문입니다.

AWS 관리형 정책: AWSSSOMasterAccountAdministrator

이 `AWSSSOMasterAccountAdministrator` 정책은 보안 주체에게 필요한 관리 조치를 제공합니다. 이 정책은 관리자 역할을 수행하는 주도자를 대상으로 합니다. AWS IAM Identity Center 제공된 작업 목록은 시간이 지나면 IAM Identity Center의 기존 기능 및 관리자에게 필요한 작업에 맞게 업데이트됩니다.

`AWSSSOMasterAccountAdministrator` 정책을 IAM 보안 인증에 연결할 수 있습니다. `AWSSSOMasterAccountAdministrator`정책을 ID에 연결하면 관리자 권한이 AWS IAM Identity Center 부여됩니다. 이 정책의 보안 주체는 AWS Organizations 관리 계정 및 모든 멤버 계정 내에서 IAM Identity Center에 액세스할 수 있습니다. 이 주체는 IAM Identity Center 인스턴스, 사용자, 권한 세트 및 할당을 생성하는 기능을 포함하여 모든 IAM Identity Center 작업을 완벽하게 관리할 수 있습니다. 또한 보안 AWS 주체는 조직 구성원 계정 전체에서 이러한 할당을 인스턴스화하고 AWS Directory Service 관리형 디렉터리와 IAM Identity Center 간에 연결을 설정할 수 있습니다. 새 관리 기능이 출시되면 계정 관리자에게 이러한 권한이 자동으로 부여됩니다.

권한 그룹화

이 정책은 제공된 권한에 따라 명령문으로 그룹화됩니다.

- `AWSSSOMasterAccountAdministrator`— IAM Identity Center가 `AWSServiceRoleforSSO`로 지정된 서비스 역할을 IAM Identity Center에 전달하여 이후에 역할을 맡고 대신 작업을 수행할 수 있도록 합니다. 이는 개인이나 애플리케이션이 IAM Identity Center를 활성화하려고 할 때 필요합니다. 자세한 정보는 액세스 관리 AWS 계정을 참조하세요.
- `AWSSSOMemberAccountAdministrator`— IAM Identity Center가 다중 계정 환경에서 계정 관리자 작업을 수행할 수 있도록 합니다. AWS 자세한 정보는 AWS 관리형 정책: AWSSSOMemberAccountAdministrator을 참조하세요.
- `AWSSSOManageDelegatedAdministrator`— IAM Identity Center에서 조직의 위임된 관리자를 등록 및 등록 취소할 수 있습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 AWSSSOMasterAccountAdministrator참조를 참조하십시오.

이 정책에 대한 추가 정보입니다.

IAM Identity Center를 처음 활성화하면 IAM Identity Center 서비스가 AWS Organizations 관리 계정(이전의 마스터 계정) 에 서비스 연결 역할을 생성하여 IAM Identity Center가 계정의 리소스를 관리할 수 있도록 합니다. 필요한 작업은 다음 코드 조각에 나와 있는 `iam:CreateServiceLinkedRole` 및 `iam:PassRole`입니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSSSOCreateSLR",
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
      },
      {
```

```
            "Sid":"AWSSSOMasterAccountAdministrator",
            "Effect":"Allow",
            "Action":"iam:PassRole",
            "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
            "Condition":{
                "StringLike":{
                  "iam:PassedToService":"sso.amazonaws.com"
                }
            }
        },
    ]
}
```

AWS 관리형 정책: AWSSSOMemberAccountAdministrator

이 AWSSSOMemberAccountAdministrator 정책은 보안 주체에게 필요한 관리 조치를 제공합니다. 이 정책은 IAM Identity Center 관리자 역할을 수행하는 주체를 대상으로 합니다. 제공된 작업 목록은 시간이 지나면 IAM Identity Center의 기존 기능 및 관리자에게 필요한 작업에 맞게 업데이트됩니다.

AWSSSOMemberAccountAdministrator 정책을 IAM 보안 인증에 연결할 수 있습니다. AWSSSOMemberAccountAdministrator정책을 ID에 연결하면 관리자 AWS IAM Identity Center 권한이 부여됩니다. 이 정책의 보안 주체는 AWS Organizations 관리 계정 및 모든 멤버 계정 내에서 IAM Identity Center에 액세스할 수 있습니다. 이 주체는 사용자, 권한 세트 및 할당을 생성하는 기능을 포함하여 모든 IAM Identity Center 작업을 완벽하게 관리할 수 있습니다. 또한 보안 AWS 주체는 조직 구성원 계정 전체에서 이러한 할당을 인스턴스화하고 AWS Directory Service 관리형 디렉터리와 IAM Identity Center 간에 연결을 설정할 수 있습니다. 새 관리 기능이 출시되면 계정 관리자에게 이러한 권한이 자동으로 부여됩니다.

이 정책에 대한 권한을 보려면 관리형 정책 참조를 참조하십시오 AWSSSOMemberAccountAdministrator.AWS

이 정책에 대한 추가 정보입니다.

IAM Identity Center 관리자는 Identity Center 디렉터리 저장소(sso-directory)에서 사용자, 그룹 및 암호를 관리합니다. 계정 관리자 역할에는 다음 작업에 대한 권한이 포함되어 있습니다.

- "sso:*"
- "sso-directory:*"

IAM Identity Center 관리자가 일상적인 작업을 수행하려면 다음 AWS Directory Service 작업에 대한 제한된 권한이 필요합니다.

- "ds:DescribeTrusts"
- "ds:UnauthorizeApplication"
- "ds:DescribeDirectories"
- "ds:AuthorizeApplication"
- “ds:CreateAlias”

이러한 권한을 통해 IAM Identity Center 관리자는 기존 디렉터리를 식별하고 애플리케이션을 관리하여 IAM Identity Center와 함께 사용하도록 구성할 수 있습니다. 각 작업에 대한 자세한 내용을 알아보려면 AWS Directory Service API 권한: 작업, 리소스 및 조건 참조를 참조하세요.

IAM Identity Center는 IAM 정책을 사용하여 IAM Identity Center 사용자에게 권한을 부여합니다. IAM Identity Center 관리자는 권한 세트를 생성하고 여기에 정책을 연결합니다. IAM Identity Center 관리자는 생성 또는 업데이트 중인 권한 세트와 함께 사용할 정책을 선택할 수 있도록 기존 정책을 나열할 권한이 있어야 합니다. 안전하고 기능적인 권한을 설정하려면 IAM Identity Center 관리자에게 IAM Access Analyzer 정책 검증을 실행할 수 있는 권한이 있어야 합니다.

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

IAM Identity Center 관리자가 일상적인 AWS Organizations 작업을 수행하려면 다음 작업에 대한 제한된 액세스 권한이 필요합니다.

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"
- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"

- `"organizations:ListDelegatedAdministrators"`
- `"organizations:RegisterDelegatedAdministrator"`
- `"organizations:DeregisterDelegatedAdministrator"`

이러한 권한을 통해 IAM Identity Center 관리자는 조직 리소스(계정)를 사용하여 다음과 같은 기본적인 IAM Identity Center 관리 작업을 수행할 수 있습니다.

- 조직에 속한 관리 계정 식별
- 조직에 속한 구성원 계정 식별
- 계정에 대한 AWS 서비스 액세스 활성화
- 위임된 관리자 설정 및 관리

IAM Identity Center에서 위임된 관리자를 사용하는 방법에 대한 자세한 내용을 알아보려면 위임된 관리를 참조하세요. 이러한 권한을 사용하는 방법에 대한 자세한 내용은 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하십시오. AWS Organizations

AWS 관리형 정책: AWSSSODirectoryAdministrator

`AWSSSODirectoryAdministrator` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 IAM Identity Center 사용자 및 그룹에 대한 관리 권한을 부여합니다. 이 정책이 연결된 보안 주체는 IAM Identity Center 사용자 및 그룹을 업데이트할 수 있습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSSSODirectoryAdministrator.

AWS 관리형 정책: AWSSSOReadOnly

`AWSSSOReadOnly` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 IAM Identity Center의 정보를 볼 수 있는 읽기 전용 권한을 사용자에게 부여합니다. 이 정책이 연결된 보안 주체는 IAM Identity Center 사용자 및 그룹을 직접 볼 수 없습니다. 이 정책이 연결된 보안 주체는 IAM Identity Center에서 어떤 업데이트도 수행할 수 없습니다. 예를 들어 이러한 권한이 있는 보안 주체는 IAM Identity Center 설정을 볼 수 있지만 설정 값은 변경할 수 없습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSSSOReadOnly.

AWS 관리형 정책: AWSSSODirectoryReadOnly

`AWSSSODirectoryReadOnly` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 IAM Identity Center의 사용자 및 그룹을 볼 수 있는 읽기 전용 권한을 사용자에게 부여합니다. 이 정책이 연결된 보안 주체는 IAM Identity Center 할당, 권한 세트, 애플리케이션 또는 설정을 볼 수 없습니다. 이 정책이 연결된 보안 주체는 IAM Identity Center에서 어떤 업데이트도 수행할 수 없습니다. 예를 들어 이러한 권한을 가진 보안 주체는 IAM Identity Center 사용자를 볼 수 있지만 사용자 속성을 변경하거나 MFA 디바이스를 할당할 수는 없습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSSSODirectoryReadOnly.

AWS 관리형 정책: AWSIdentitySyncFullAccess

`AWSIdentitySyncFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책이 연결된 보안 주체는 동기화 프로필을 생성 및 삭제하고, 동기화 프로필을 동기화 대상과 연결 또는 업데이트하고, 동기화 필터를 생성, 나열 및 삭제하고, 동기화를 시작 또는 중지할 수 있는 전체 액세스 권한을 가집니다.

권한 세부 정보

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSIdentitySyncFullAccess.

AWS 관리형 정책: AWSIdentitySyncReadOnlyAccess

`AWSIdentitySyncReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 사용자가 ID 동기화 프로필, 필터 및 대상 설정에 대한 정보를 볼 수 있는 읽기 전용 권한을 부여합니다. 이 정책이 연결된 보안 주체는 동기화 설정을 업데이트할 수 없습니다. 예를 들어 이러한 권한이 있는 보안 주체는 프로필 동기화 설정을 볼 수 있지만 프로필 또는 필터 값은 변경할 수 없습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSIdentitySyncReadOnlyAccess.

AWS 관리형 정책: AWSSSOServiceRolePolicy

`AWSSSOServiceRolePolicy` 정책을 IAM 자격 증명에 연결할 수 없습니다.

이 정책은 IAM Identity Center에서 특정 정보에 대한 Single Sign-On 액세스 권한을 가진 사용자를 위임하고 적용할 수 있는 서비스 연결 역할에 연결됩니다. AWS 계정 AWS Organizations IAM을 활성화

하면 조직 내 모든 영역에 서비스 연결 역할이 생성됩니다. AWS 계정 또한 IAM Identity Center는 이후에 조직에 추가되는 모든 계정에 동일한 서비스 연결 역할을 생성합니다. 이 역할을 통해 IAM Identity Center는 사용자를 대신하여 각 계정의 리소스에 액세스할 수 있습니다. 각 역할에서 생성되는 서비스 연결 역할의 이름이 지정됩니다. AWS 계정 `AWSServiceRoleForSSO` 자세한 정보는 IAM Identity Center 서비스 연결 역할 사용을 참조하세요.

AWS 관리형 정책: AWSIAMIdentityCenterAllowListForIdentityContext

IAM Identity Center 자격 증명 컨텍스트에서 역할을 수임하는 경우 AWS Security Token Service (AWS STS) 는 `AWSIAMIdentityCenterAllowListForIdentityContext` 정책을 역할에 자동으로 연결합니다.

이 정책은 IAM Identity Center ID 컨텍스트를 사용하여 수임한 역할에서 신뢰할 수 있는 ID 전파를 사용할 때 허용되는 작업 목록을 제공합니다. 이 컨텍스트로 호출되는 다른 모든 작업은 차단됩니다. ID 컨텍스트는 `ProvidedContext`로 전달됩니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AWSIAMIdentityCenterAllowListForIdentityContext.

IAM ID 센터가 AWS 관리형 정책을 업데이트합니다.

다음 표에는 이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 IAM Identity Center의 AWS 관리형 정책이 업데이트된 내용이 설명되어 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 IAM Identity Center 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWSIAMIdentityCenterAllowListForIdentityContext	이제 이 정책에는 Amazon EMR에서의 신뢰할 수 있는 ID 전파를 지원하는 `elasticmapreduce:AddJobFlowSteps` `elasticmapreduce:DescribeCluster` `elasticmapreduce:CancelSteps` `elasticmapreduce:DescribeStep` ,,, 및 `elasticma`	2024년 5월 17일

변경 사항	설명	날짜
	preduce:ListSteps 조치가 포함됩니다.	

변경 사항	설명	날짜
AWSIAMIdentityCenterAllowListForIdentityContext	이제 이 정책에는 이러한 세션을 지원하는 AWS 관리형 응용 프로그램의 ID 인식 콘솔 세션을 지원하는 qapps:CreateQApp qapps:PredictProblemStatementFromConversation qapps:PredictQAppFromProblemStatement qapps:CopyQApp qapps:GetQApp qapps:ListQApps qapps:UpdateQApp qapps:DeleteQApp qapps:AssociateQAppWithUser qapps:DisassociateQAppFromUser qapps:ImportDocumentToQApp qapps:ImportDocumentToQAppSession ,qapps:CreateLibraryItem ,qapps:GetLibraryItem ,,qapps:UpdateLibraryItem ,qapps:CreateLibraryItemReview ,qapps:ListLibraryItems ,qapps:CreateSubscriptionToken ,qapps:StartQAppSession ,,,,,,,,,, 및 qapps:Sto	2024년 4월 30일

변경 사항	설명	날짜
	pQAppSession 조치가 포함됩니다.	
AWSSSOMasterAccountAdministrator	이제 이 정책에는 이러한 세션을 지원하는 AWS 관리 응용 프로그램의 ID 인식 콘솔 세션을 지원하기 위한 signin:CreateTrustedIdentityPropagationApplicationForConsole 및 signin:ListTrustedIdentityPropagationApplicationsForConsole 조치가 포함됩니다.	2024년 4월 26일
AWSSSOMemberAccountAdministrator	이제 이 정책에는 이러한 세션을 지원하는 AWS 관리 응용 프로그램의 ID 인식 콘솔 세션을 지원하기 위한 signin:CreateTrustedIdentityPropagationApplicationForConsole 및 signin:ListTrustedIdentityPropagationApplicationsForConsole 조치가 포함됩니다.	2024년 4월 26일
AWSSSOReadOnly	이제 이 정책에는 이러한 세션을 지원하는 AWS 관리 응용 프로그램에 대한 ID 인식 콘솔 세션을 지원하는 signin:ListTrustedIdentityPropagationApplicationsForConsole 조치가 포함됩니다.	2024년 4월 26일

변경 사항	설명	날짜
AWSIAMIdentityCenterAllowListForIdentityContext	이제 이 정책에는 이러한 세션을 지원하는 AWS 관리 응용 프로그램에 대한 ID 인식 콘솔 세션을 지원하는 `qbusiness:PutFeedback` 작업이 포함됩니다.	2024년 4월 26일
AWSIAMIdentityCenterAllowListForIdentityContext	이제 이 정책에는 이러한 세션을 지원하는 AWS 관리 응용 프로그램의 ID 인식 콘솔 세션을 지원하는 `q:StartConversation` `q:SendMessage` `q:ListConversations` `q:GetConversation` `q:StartTroubleshootingAnalysis` `q:GetTroubleshootingResults` `q:StartTroubleshootingResolutionExplanation` ,,,,,, 및 `q:UpdateTroubleshootingCommandResult` 작업이 포함됩니다.	2024년 4월 24일
AWSIAMIdentityCenterAllowListForIdentityContext	이제 이 정책에는 이러한 세션을 지원하는 AWS 관리 응용 프로그램에 대한 ID 인식 콘솔 세션을 지원하는 `sts:SetContext` 작업이 포함됩니다.	2024년 4월 19일

변경 사항	설명	날짜
AWSIAMIdentityCenterAllowListForIdentityContext	이제 이 정책에는 이러한 세션을 지원하는 AWS 관리 응용 프로그램의 ID 인식 콘솔 세션을 지원하는 `qbusiness:Chat` `qbusiness:ChatSync` `qbusiness:ListConversations` `qbusiness:ListMessages` ,,, 및 `qbusiness:DeleteConversation` 조치가 포함됩니다.	2024년 4월 11일
AWSIAMIdentityCenterAllowListForIdentityContext	이 정책에는 이제 `s3:GetAccessGrantsInstanceForPrefix` 및 `s3:GetDataAccess` 작업이 포함됩니다.	2023년 11월 26일
AWSIAMIdentityCenterAllowListForIdentityContext	이 정책은 IAM Identity Center ID 컨텍스트를 사용하여 수임한 역할에서 신뢰할 수 있는 ID 전파를 사용할 때 허용되는 작업 목록을 제공합니다.	2023년 11월 15일
AWSSSODirectoryReadOnly	이제 이 정책에는 사용자가 세션을 나열하고 가져올 수 있는 새로운 권한이 있는 새 네임스페이스 `identitystore-auth` 가 포함됩니다.	2023년 2월 21일
AWSSSOServiceRolePolicy	이제 이 정책을 통해 관리 계정에서 `UpdateSAMLProvider` 작업을 할 수 있습니다.	2022년 10월 20일

변경 사항	설명	날짜
AWSSSOMasterAccountAdministrator	이제 이 정책에는 관리자가 세션을 나열하고 사용자의 세션을 삭제할 수 있는 새로운 권한이 있는 새 네임스페이스 `identitystore-auth` 가 포함됩니다.	2022년 10월 20일
AWSSSOMemberAccountAdministrator	이제 이 정책에는 관리자가 세션을 나열하고 사용자의 세션을 삭제할 수 있는 새로운 권한이 있는 새 네임스페이스 `identitystore-auth` 가 포함됩니다.	2022년 10월 20일
AWSSSODirectoryAdministrator	이제 이 정책에는 관리자가 세션을 나열하고 사용자의 세션을 삭제할 수 있는 새로운 권한이 있는 새 네임스페이스 `identitystore-auth` 가 포함됩니다.	2022년 10월 20일
AWSSSOMasterAccountAdministrator	이제 이 정책에는 `ListDelegatedAdministrators` 콜인을 위한 새로운 권한이 포함됩니다. AWS Organizations또한 이 정책에는 이제 `RegisterDelegatedAdministrator` 및 `DeregisterDelegatedAdministrator` 를 호출할 수 있는 권한 `AWSSSOManageDelegatedAdministrator` 이 포함된 일부 권한도 포함됩니다.	2022년 8월 16일

변경 사항	설명	날짜
AWSSSOMemberAccountAdministrator	이제 이 ListDelegatedAdministrators 정책에는 콜인을 위한 새 권한이 포함됩니다 AWS Organizations. 또한 이 정책에는 이제 RegisterDelegatedAdministrator 및 DeregisterDelegatedAdministrator 를 호출할 수 있는 권한 AWSSSOManageDelegatedAdministrator 이 포함된 일부 권한도 포함됩니다.	2022년 8월 16일
AWSSSOReadOnly	이제 이 ListDelegatedAdministrators 정책에는 콜인을 위한 새 권한이 포함됩니다 AWS Organizations.	2022년 8월 11일
AWSSSOServiceRolePolicy	이제 이 정책에는 DeleteRolePermissionsBoundary 및 PutRolePermisionsBoundary 를 호출하는 새로운 권한이 포함됩니다.	2022년 7월 14일
AWSSSOServiceRolePolicy	이제 이 정책에는 AWS Organizations에서 ListAWSServiceAccessForOrganization and ListDelegatedAdministrators 를 호출할 수 있는 새로운 권한이 포함됩니다.	2022년 5월 11일

변경 사항	설명	날짜
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	보안 주체가 검증을 위해 정책 확인을 사용하도록 허용하는 IAM Access Analyzer 권한을 추가합니다.	2022년 4월 28일
AWSSSOMasterAccountAdministrator	이 정책은 이제 모든 IAM ID 센터 ID 스토어 서비스 작업을 허용합니다. IAM Identity Center Identity 스토어 서비스에서 가능한 작업에 대한 자세한 내용을 알아보려면 IAM Identity Center 아이덴티티 스토어 API 참조를 참조하세요.	2022년 3월 29일
AWSSSOMemberAccountAdministrator	이 정책은 이제 모든 IAM ID 센터 ID 스토어 서비스 작업을 허용합니다.	2022년 3월 29일
AWSSSODirectoryAdministrator	이 정책은 이제 모든 IAM ID 센터 ID 스토어 서비스 작업을 허용합니다.	2022년 3월 29일
AWSSSODirectoryReadOnly	이 정책은 이제 IAM Identity Center ID 스토어 서비스 읽기 작업에 대한 액세스 권한을 부여합니다. 이 액세스는 IAM Identity Center ID 스토어 서비스에서 사용자 및 그룹 정보를 검색하는 데 필요합니다.	2022년 3월 29일

변경 사항	설명	날짜
AWSIdentitySyncFullAccess	이 정책은 Identity Sync 권한에 대한 모든 액세스를 허용합니다.	2022년 3월 3일
AWSIdentitySyncReadOnlyAccess	이 정책은 보안 주체가 ID 동기화 설정을 볼 수 있도록 허용하는 읽기 전용 권한을 부여합니다.	2022년 3월 3일
AWSSSOReadOnly	이 정책은 보안 주체가 IAM Identity Center 구성 설정을 볼 수 있도록 허용하는 읽기 전용 권한을 부여합니다.	2021년 8월 4일
IAM Identity Center 변경 내용 추적 시작	IAM Identity Center는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 8월 4일

IAM Identity Center 서비스 연결 역할 사용

AWS IAM Identity Center AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 IAM Identity Center에 직접 연결된 고유한 유형의 IAM 역할입니다. IAM Identity Center에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. 자세한 정보는 서비스 연결 역할을 참조하세요.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할은 IAM Identity Center을 더 쉽게 설정할 수 있습니다. IAM Identity Center가 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, IAM Identity Center만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조해 서비스 연결 역할 열이 예인 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

IAM Identity Center에 대한 서비스 연결 역할 권한

IAM Identity Center는 이름이 지정된 AWSServiceRoleForSSO서비스 연결 역할을 사용하여 IAM ID 센터에 IAM 역할, 정책, SAML IdP를 비롯한 AWS 리소스를 관리할 수 있는 권한을 부여합니다.

AWSServiceRoleForSSO 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

- `IAM Identity Center`

AWSServiceRoleForSSO 서비스 연결 역할 권한 정책에 따라 IAM Identity Center는 “/aws-reserved/sso.amazonaws.com/” 경로의 역할에 대해 이름 접두사가 “_”인 역할에 대해 다음을 수행할 수 있습니다. AWSReservedSSO

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`
- `iam:DeleteRolePermissionsBoundary`
- `iam:DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

AWSServiceRoleForSSO 서비스 연결 역할 권한 정책에 따라 IAM Identity Center는 이름 접두사가 “_”인 SAML 공급자에 대해 다음을 완료할 수 있습니다. AWSSSO

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam:DeleteSAMLProvider`

AWSServiceRoleForSSO 서비스 연결 역할 권한 정책을 통해 IAM Identity Center는 모든 조직에서 다음을 완료할 수 있습니다.

- organizations:DescribeAccount
- organizations:DescribeOrganization
- organizations:ListAccounts
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListDelegatedAdministrators

AWSServiceRoleForSSO 서비스 연결 역할 권한 정책에 따라 IAM Identity Center는 모든 IAM 역할 (*)에 대해 다음을 완료할 수 있습니다.

- iam:listRoles

AWSServiceRoleForSSO 서비스 연결 역할 권한 정책에 따라 IAM ID 센터는 “arn:aws:iam: :*:role/ / sso.amazonaws.com/”에서 다음을 완료할 수 있습니다. aws-service-role AWSServiceRoleForSSO

- iam:GetServiceLinkedRoleDeletionStatus
- iam:DeleteServiceLinkedRole

역할 권한 정책은 IAM Identity Center가 리소스에서 다음 작업을 완료하도록 허용합니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"IAMRoleProvisioningActions",
         "Effect":"Allow",
         "Action":[
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:DeleteRolePermissionsBoundary",
            "iam:PutRolePermissionsBoundary",
            "iam:PutRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription",
            "iam:UpdateAssumeRolePolicy"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ],
```

```
         "Condition":{
            "StringNotEquals":{
               "aws:PrincipalOrgMasterAccountId":"${aws:PrincipalAccount}"
            }
         }
      },
      {
         "Sid":"IAMRoleReadActions",
         "Effect":"Allow",
         "Action":[
            "iam:GetRole",
            "iam:ListRoles"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"IAMRoleCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:ListRolePolicies",
            "iam:ListAttachedRolePolicies"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ]
      },
      {
         "Sid":"IAMSLRCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:DeleteRole",
            "iam:GetRole"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
         ]
```

```
    },
    {
      "Sid": "IAMSAMLProviderCreationAction",
      "Effect": "Allow",
      "Action": [
        "iam:CreateSAMLProvider"
    ],
    "Resource": [
       "arn:aws:iam::*:saml-provider/AWSSSO_*"
     ],
    "Condition": {
       "StringNotEquals": {
          "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "IAMSAMLProviderUpdateAction",
      "Effect": "Allow",
      "Action": [
        "iam:UpdateSAMLProvider"
      ],
      "Resource": [
         "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
       "Sid":"IAMSAMLProviderCleanupActions",
       "Effect":"Allow",
       "Action":[
          "iam:DeleteSAMLProvider",
          "iam:GetSAMLProvider"
       ],
       "Resource":[
          "arn:aws:iam::*:saml-provider/AWSSSO_*"
       ]
    },
    {
       "Effect":"Allow",
       "Action":[
          "organizations:DescribeAccount",
          "organizations:DescribeOrganization",
          "organizations:ListAccounts",
          "organizations:ListAWSServiceAccessForOrganization",
```

```
            "organizations:ListDelegatedAdministrators"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowUnauthAppForDirectory",
         "Effect":"Allow",
         "Action":[
            "ds:UnauthorizeApplication"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowDescribeForDirectory",
         "Effect":"Allow",
         "Action":[
            "ds:DescribeDirectories",
            "ds:DescribeTrusts"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowDescribeAndListOperationsOnIdentitySource",
         "Effect":"Allow",
         "Action":[
            "identitystore:DescribeUser",
            "identitystore:DescribeGroup",
            "identitystore:ListGroups",
            "identitystore:ListUsers"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

IAM Identity Center에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 활성화되면 IAM Identity Center는 Organizations의 조직 내 모든 계정에 서비스 연결 역할을 생성합니다. AWS 또한 IAM Identity Center는 이후에 조직에 추가되는 모든 계정에 동일한 서비스 연결 역할을 생성합니다. 이 역할을 통해 IAM Identity Center는 사용자를 대신하여 각 계정의 리소스에 액세스할 수 있습니다.

참고

- 관리 계정에 로그인한 경우, AWS Organizations 관리 계정에는 서비스 연결 역할이 아닌 현재 로그인한 역할이 사용됩니다. 이렇게 하면 권한이 에스컬레이션되는 것을 방지할 수 있습니다.
- IAM Identity Center가 AWS Organizations 관리 계정에서 IAM 작업을 수행하는 경우 모든 작업은 IAM 보안 주체의 자격 증명을 사용하여 수행됩니다. 이렇게 하면 CloudTrail 로그인을 통해 누가 관리 계정에서 모든 권한을 변경했는지 확인할 수 있습니다.

Important

서비스 연결 역할을 지원하기 시작한 2017년 12월 7일 이전에 IAM Identity Center 서비스를 사용하고 있었다면 IAM Identity Center가 사용자 계정에 역할을 생성한 것입니다. AWSServiceRoleForSSO 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다.

IAM Identity Center에 대한 서비스 연결 역할 편집

IAM ID 센터에서는 서비스 연결 역할을 편집할 수 없습니다. AWSServiceRoleForSSO 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

IAM Identity Center에 대한 서비스 연결 역할 삭제

역할을 수동으로 삭제할 필요는 없습니다. AWSServiceRoleForSSO AWS 조직에서 AWS 계정 가 제거되면 IAM Identity Center는 자동으로 리소스를 정리하고 해당 리소스에서 서비스 연결 역할을 삭제합니다. AWS 계정

또한 IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 서비스 연결 역할을 수동으로 삭제할 수 있습니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려 할 때 IAM Identity Center 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

에서 사용하는 IAM ID 센터 리소스를 삭제하려면 AWSServiceRoleForSSO

1. AWS 계정에 액세스할 수 있는 모든 사용자 및 그룹용 사용자 및 그룹 액세스 제거.
2. AWS 계정와 연결한 권한 집합을 삭제합니다..

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 서비스 연결 역할을 삭제합니다. AWSServiceRoleForSSO 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

IAM Identity Center 콘솔 및 API 인증

기존 IAM Identity Center 콘솔 API는 이중 권한 부여를 지원하므로 새 API가 제공되더라도 기존 API 작업을 계속 사용할 수 있습니다. 2023년 11월 15일과 2020년 10월 15일 이전에 생성된 기존 IAM Identity Center 인스턴스가 있는 경우, 다음 표를 사용하여 해당 날짜 이후에 출시된 최신 API 작업에 매핑되는 API 작업을 확인할 수 있습니다.

주제

- 2023년 11월 이후의 API 작업
- 2020년 10월 이후의 API 작업

2023년 11월 이후의 API 작업

2023년 11월 15일 이전에 생성된 IAM Identity Center 인스턴스는 해당 작업에 대한 명시적인 거부가 없는 한 기존 API 작업과 새 API 작업을 모두 적용합니다. 2023년 11월 15일 이후에 생성된 인스턴스는 IAM ID 센터 콘솔에서 권한 부여를 위해 최신 API 작업을 사용합니다.

2023년 11월 15일 이전에 사용된 콘솔 작업 이름	2023년 11월 15일 이후에 사용된 API 작업
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

2020년 10월 이후의 API 작업

2020년 10월 15일 이전에 생성된 IAM Identity Center 인스턴스는 해당 작업에 대한 명시적인 거부가 없는 한 기존 API 작업과 새 API 작업을 모두 적용합니다. 2020년 10월 15일 이후에 생성된 인스턴스는 IAM ID 센터 콘솔에서 권한 부여를 위해 최신 API 작업을 사용합니다.

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS IAM ID 센터의 조건 컨텍스트 키

보안 주체가 요청을 보내면 요청 정보를 요청 컨텍스트로 AWS 수집하여 요청을 평가하고 승인하는 데 사용합니다. AWS JSON 정책의 `Condition` 요소를 사용하여 요청 컨텍스트의 키를 정책에서 지정한 키 값과 비교할 수 있습니다. 요청 정보는 요청을 하는 주체, 리소스, 요청 대상, 요청 자체에 대한 메타데이터 등 다양한 소스에서 제공됩니다. 서비스별 조건 키는 개별 AWS 서비스에 사용할 수 있도록 정의됩니다.

IAM Identity Center에는 AWS 관리형 애플리케이션 및 타사 애플리케이션이 IAM Identity Center에서 정의한 조건 키에 값을 추가할 수 있도록 하는 AWS STS 컨텍스트 공급자가 포함되어 있습니다. 이러한 키는 IAM 역할에 포함됩니다. 키 값은 애플리케이션이 토큰을 전달할 때 설정됩니다. AWS STS애플리케이션은 다음 방법 중 하나로 전달되는 토큰을 AWS STS 획득합니다.

- IAM ID 센터를 통한 인증 시.
- 신뢰할 수 있는 ID 전파를 위해 신뢰할 수 있는 토큰 발급자와 토큰을 교환한 후 이 경우 애플리케이션은 신뢰할 수 있는 토큰 발급자로부터 토큰을 획득하고 해당 토큰을 IAM Identity Center의 토큰으로 교환합니다.

이러한 키는 일반적으로 신뢰할 수 있는 ID 전파와 통합되는 애플리케이션에서 사용됩니다. 경우에 따라 키 값이 있는 경우 생성한 IAM 정책에서 이러한 키를 사용하여 권한을 허용하거나 거부할 수 있습니다.

예를 들어, 의 값에 따라 리소스에 조건부 액세스를 제공하고 싶을 수 있습니다. `UserId` 이 값은 해당 역할을 사용하는 IAM Identity Center 사용자를 나타냅니다. 이 예제는 를 사용하는 `SourceId` 것과 비슷합니다. 하지만 과 `SourceId` 달리 의 값은 ID 저장소에서 인증된 특정 사용자를 `UserId` 나타냅니다. 이 값은 애플리케이션이 가져와서 전달하는 토큰에 AWS STS있습니다. 임의의 값을 포함할 수 있는 범용 문자열이 아닙니다.

주제

- 아이덴티티 스토어: UserId
- 아이덴티티 스토어: IdentityStoreArn
- ID 센터: ApplicationArn
- ID 센터: CredentialId
- 아이덴티티 센터: InstanceArn

아이덴티티 스토어: UserId

이 컨텍스트 키는 IAM ID 센터에서 발행한 컨텍스트 어설션의 대상인 IAM ID 센터 사용자의 것입니다. `UserId` 컨텍스트 어설션이 전달됩니다. AWS STS이 키를 사용하여 요청을 대신 요청한 IAM Identity Center 사용자의 ID를 정책에 지정된 사용자의 식별자와 비교할 수 있습니다. `UserId`

- 가용성 — 이 키는 IAM Identity Center에서 실행한 컨텍스트 어설션이 설정된 후 요청 컨텍스트에 포함됩니다. 이때 또는 API 작업에서 AWS STS `assume-role` 명령을 사용하여 역할을 위임할 때 이 키가 요청 컨텍스트에 포함됩니다. AWS CLI AWS STS `AssumeRole`

- 데이터 유형-문자열
- 값 유형-단일 값

아이덴티티 스토어: IdentityStoreArn

이 컨텍스트 키는 컨텍스트 어설션을 발행한 IAM Identity Center 인스턴스에 연결된 ID 저장소의 ARN입니다. 속성을 조회할 수 있는 ID 저장소이기도 합니다. `identitystore:UserID` 정책에서 이 키를 사용하여 예상 ID 저장소 ARN에서 `identitystore:UserID` 왔는지 여부를 확인할 수 있습니다.

- 가용성 — 이 키는 IAM Identity Center에서 실행한 컨텍스트 어설션이 설정된 후 또는 API 작업에서 AWS STS `assume-role` 명령을 사용하여 역할을 위임할 때 요청 컨텍스트에 포함됩니다. AWS CLI AWS STS `AssumeRole`
- 데이터 유형 — Arn, String
- 값 유형-단일 값

ID 센터: ApplicationArn

이 컨텍스트 키는 IAM Identity Center가 컨텍스트 어설션을 발행한 애플리케이션의 ARN입니다. 정책에서 이 키를 사용하여 예상 애플리케이션에서 `identitycenter:ApplicationArn` 가져온 것인지 여부를 결정할 수 있습니다. 이 키를 사용하면 예상치 못한 애플리케이션이 IAM 역할에 액세스하는 것을 방지할 수 있습니다.

- 가용성 — 이 키는 AWS STS `AssumeRole` API 작업의 요청 컨텍스트에 포함됩니다. 요청 컨텍스트에는 IAM Identity Center에서 발행한 컨텍스트 어설션이 포함됩니다.
- 데이터 유형 — Arn, 문자열
- 값 유형-단일 값

ID 센터: CredentialId

이 컨텍스트 키는 ID 강화 역할 자격 증명의 임의 ID이며 로깅에만 사용됩니다. 이 키 값은 예측할 수 없으므로 정책의 컨텍스트 어설션에는 사용하지 않는 것이 좋습니다.

- 가용성 — 이 키는 API 작업의 요청 컨텍스트에 포함됩니다. AWS STS `AssumeRole` 요청 컨텍스트에는 IAM Identity Center에서 발행한 컨텍스트 어설션이 포함됩니다.
- 데이터 유형-문자열

- 값 유형-단일 값

아이덴티티 센터: InstanceArn

이 컨텍스트 키는 에 대한 컨텍스트 어설션을 발행한 IAM Identity Center 인스턴스의 ARN입니다. `identitystore:UserID` 이 키를 사용하여 `identitystore:UserID` 및 컨텍스트 어설션이 예상 IAM Identity Center 인스턴스 ARN에서 왔는지 여부를 확인할 수 있습니다.

- 가용성 - 이 키는 API 작업의 요청 컨텍스트에 포함됩니다. AWS STS `AssumeRole` 요청 컨텍스트에는 IAM Identity Center에서 발행한 컨텍스트 어설션이 포함됩니다.
- 데이터 유형 — Arn, 문자열
- 값 유형-단일 값

IAM Identity Center 로깅 및 모니터링

조직에서 변경 사항이 기록되고 있는지 모니터링하는 것이 좋습니다. 이렇게 하면 예상치 못한 변경 사항을 조사하고 원치 않는 변경 사항을 롤백할 수 있습니다. AWS IAM Identity Center 현재는 조직과 조직 내에서 발생하는 활동을 모니터링하는 데 도움이 되는 두 가지 AWS 서비스를 지원합니다.

주제

- IAM ID 센터 API 호출을 다음과 같이 로깅합니다. AWS CloudTrail
- 아마존 EventBridge
- AD 동기화 및 구성 가능한 AD 동기화 오류 로깅

IAM ID 센터 API 호출을 다음과 같이 로깅합니다. AWS CloudTrail

AWS IAM Identity Center IAM Identity Center에서 사용자, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합됩니다. AWS CloudTrail CloudTrail IAM ID 센터에 대한 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 IAM Identity Center 콘솔로부터의 호출과 IAM Identity Center API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 IAM ID 센터에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷에 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 IAM Identity Center에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

주제

- IAM ID 센터 정보: CloudTrail
- IAM Identity Center 로그 파일 항목 이해
- IAM Identity Center 로그인 이벤트 이해

IAM ID 센터 정보: CloudTrail

CloudTrail 계정을 생성할 AWS 계정 때 활성화됩니다. IAM Identity Center에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다. AWS 계정자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

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

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

에서 CloudTrail 로깅이 활성화되면 IAM Identity Center 작업에 대한 API 호출이 로그 파일에서 추적됩니다. AWS 계정 IAM ID 센터 레코드는 다른 AWS 서비스 레코드와 함께 로그 파일에 기록됩니다. CloudTrail 기간과 파일 크기를 기반으로 새 파일을 생성하고 새 파일에 기록할 시기를 결정합니다.

지원되는 IAM ID 센터 CloudTrail 작업은 다음과 같습니다.

콘솔 API 작업	퍼블릭 API 작업
`AssociateDirectory`	`AttachManagedPolicyToPermissionSet`
`AssociateProfile`	`CreateAccountAssignment`

콘솔 API 작업	퍼블릭 API 작업
BatchDeleteSession	CreateInstanceAccessControlAttributeConfiguration
BatchGetSession	CreatePermissionSet
CreateApplicationInstance	DeleteAccountAssignment
CreateApplicationInstanceCertificate	DeleteInlinePolicyFromPermissionSet
CreatePermissionSet	DeleteInstanceAccessControlAttributeConfiguration
CreateProfile	DeletePermissionSet
DeleteApplicationInstance	DescribeAccountAssignmentCreationStatus
DeleteApplicationInstanceCertificate	DescribeAccountAssignmentDeletionStatus
DeletePermissionsPolicy	DescribeInstanceAccessControlAttributeConfiguration
DeletePermissionSet	DescribePermissionSet
DeleteProfile	DescribePermissionSetProvisioningStatus
DescribePermissionsPolicies	DetachManagedPolicyFromPermissionSet
DisassociateDirectory	GetInlinePolicyForPermissionSet
DisassociateProfile	ListAccountAssignmentCreationStatus

콘솔 API 작업	퍼블릭 API 작업
GetApplicationInstance	ListAccountAssignmentDeletionStatus
GetApplicationTemplate	ListAccountAssignments
GetMfaDeviceManagementForDirectory	ListAccountsForProvisionedPermissionSet
GetPermissionSet	ListInstances
GetSSOStatus	ListManagedPoliciesInPermissionSet
ImportApplicationInstanceServiceProviderMetadata	ListPermissionSetProvisioningStatus
ListApplicationInstances	ListPermissionSets
ListApplicationInstanceCertificates	ListPermissionSetsProvisionedToAccount
ListApplicationTemplates	ListTagsForResource
ListDirectoryAssociations	ProvisionPermissionSet
ListPermissionSets	PutInlinePolicyToPermissionSet
ListProfileAssociations	TagResource
ListProfiles	UntagResource
ListSessions	UpdateInstanceAccessControlAttributeConfiguration
PutMfaDeviceManagementForDirectory	UpdatePermissionSet
PutPermissionsPolicy	

콘솔 API 작업	퍼블릭 API 작업
StartSSO	
UpdateApplicationInstanceActiveCertificate	
UpdateApplicationInstanceDisplayData	
UpdateApplicationInstanceServiceProviderConfiguration	
UpdateApplicationInstanceStatus	
UpdateApplicationInstanceResponseConfiguration	
UpdateApplicationInstanceResponseSchemaConfiguration	
UpdateApplicationInstanceSecurityConfiguration	
UpdateDirectoryAssociation	
UpdateProfile	

IAM Identity Center의 퍼블릭 API 작업에 대한 자세한 내용을 알아보려면 IAM Identity Center 참조 설명서를 확인하세요.

지원되는 IAM ID 센터 ID 스토어 CloudTrail 작업은 다음과 같습니다.

- AddMemberToGroup
- CompleteVirtualMfaDeviceRegistration
- CompleteWebAuthnDeviceRegistration
- CreateAlias
- CreateExternalIdPConfigurationForDirectory

- CreateGroup
- CreateUser
- DeleteExternalIdPConfigurationForDirectory
- DeleteGroup
- DeleteMfaDeviceForUser
- DeleteUser
- DescribeDirectory
- DescribeGroups
- DescribeUsers
- DisableExternalIdPConfigurationForDirectory
- DisableUser
- EnableExternalIdPConfigurationForDirectory
- EnableUser
- GetAWSSPConfigurationForDirectory
- ListExternalIdPConfigurationsForDirectory
- ListGroupsForUser
- ListMembersInGroup
- ListMfaDevicesForUser
- PutMfaDeviceManagementForDirectory
- RemoveMemberFromGroup
- SearchGroups
- SearchUsers
- StartVirtualMfaDeviceRegistration
- StartWebAuthnDeviceRegistration
- UpdateExternalIdPConfigurationForDirectory
- UpdateGroup
- UpdateMfaDeviceForUser
- UpdatePassword
- UpdateUser

- `VerifyEmail`

다음과 같은 IAM ID 센터 OIDC 작업이 지원됩니다 CloudTrail .

- `CreateToken`
- `RegisterClient`
- `StartDeviceAuthorization`

다음과 같은 IAM ID 센터 포털 CloudTrail 작업이 지원됩니다.

- `Authenticate`
- `Federate`
- `ListApplications`
- `ListProfilesForApplication`
- `ListAccounts`
- `ListAccountRoles`
- `GetRoleCredentials`
- `Logout`

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

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

자세한 내용은 CloudTrail UserIdentity 요소를 참조하십시오.

IAM Identity Center 로그 파일 항목 이해

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

다음 예는 IAM ID 센터 콘솔에서 발생한 관리자 (samadams@example.com) 의 CloudTrail 로그 항목을 보여줍니다.


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"08966example",
            "accessKeyId":"AKIAIIJM2K4example",
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[

         ],
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```


다음 예는 액세스 포털에서 발생한 최종 사용자 (bobsmith@example.com) 작업에 대한 CloudTrail 로그 항목을 보여줍니다. AWS


```
{
   "Records":[
```

```
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"Unknown",
            "principalId":"example.com//
S-1-5-21-1122334455-3652759393-4233131409-1126",
            "accountId":"08966example",
            "userName":"bobsmith@example.com"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"ListApplications",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":null,
         "responseElements":null,
         "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
         "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

다음 예는 IAM ID 센터 OIDC에서 발생한 최종 사용자 (bobsmith@example.com) 작업에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "Unknown",
        "principalId": "example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
        "accountId": "08966example",
        "userName": "bobsmith@example.com"
      },
      "eventTime": "2020-06-16T01:31:15Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "CreateToken",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
```

```
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "clientId": "clientid1234example",
        "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "grantType": "urn:ietf:params:oauth:grant-type:device_code",
        "deviceCode": "devicecode1234example"
      },
      "responseElements": {
        "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "tokenType": "Bearer",
        "expiresIn": 28800,
        "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
      "readOnly": false,
      "resources": [
        {
          "accountId": "08966example",
          "type": "IdentityStoreId",
          "ARN": "d-1234example"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "08966example"
}
```


IAM Identity Center 로그인 이벤트 이해

AWS CloudTrail 모든 ID 소스의 로그인 성공 및 실패 이벤트를 기록합니다. AWS IAM Identity Center 기본 SSO 및 Active Directory (AD Connector 및 AWS Managed Microsoft AD) 소스 ID에는 사용자에게 특정 자격 증명 문제 또는 요인을 해결하라는 메시지가 표시될 때마다 캡처되는 추가 로그인 이벤트와 해당 특정 자격 증명 확인 요청의 상태가 포함됩니다. 사용자는 필요한 보안 인증 과정을 모두 완료한 후에만 로그인되며, 이 경우 `UserAuthentication` 이벤트가 기록됩니다.

다음 표에는 각 IAM Identity Center 로그인 CloudTrail 이벤트 이름, 목적 및 다양한 ID 소스에 대한 적용 가능성이 정리되어 있습니다.

이벤트 이름	이벤트 목적	ID 소스 적용 가능성
`CredentialChallenge`	IAM Identity Center가 사용자에게 특정 보안 인증 문제를 해결하도록 요청했으며 필요한 사항(예: PASSWORD 또는 TOTP) `CredentialType` 을 지정했음을 알리는 데 사용됩니다.	기본 IAM ID 센터 사용자, AD Connector 및 AWS Managed Microsoft AD
`CredentialVerification`	사용자가 특정 `CredentialChallenge` 요청을 해결하려고 시도했음을 알리고 해당 보안 인증의 성공 또는 실패 여부를 지정하는 데 사용됩니다.	기본 IAM ID 센터 사용자, AD Connector 및 AWS Managed Microsoft AD
`UserAuthentication`	사용자에게 문제가 발생한 모든 인증 요구 사항이 성공적으로 완료되었으며 사용자가 성공적으로 로그인했음을 알리는 데 사용됩니다. 사용자가 필수 보안 인증 과정을 성공적으로 완료하지 못하면 *`UserAuthentication`* 이벤트가 기록되지 않습니다.	모든 ID 소스

다음 표에는 특정 로그인 CloudTrail 이벤트에 포함된 유용한 추가 이벤트 데이터 필드가 나와 있습니다.

이벤트 이름	이벤트 목적	로그인 이벤트 적용 가능성	예제 값
`AuthWorkflowID`	전체 로그인 시퀀스에서 발생하는 모든 이벤트의 상관관계를 파악	`CredentialChallenge` , `Credentia`	“AuthWorkflowID”: “9de74b32-8362-4a01-a524-de21df59fd83"

이벤트 이름	이벤트 목적	로그인 이벤트 적용 가능성	예제 값
	하는 데 사용됩니다. IAM Identity Center는 각 사용자 로그인마다 여러 이벤트를 발생시킬 수 있습니다.	`lVerification` , `UserAuthentication`	
`CredentialType`	문제가 발생한 보안 인증 정보 또는 요소를 지정하는 데 사용됩니다. `UserAuthentication` 이벤트에는 사용자의 로그인 시퀀스에서 성공적으로 확인된 모든 `CredentialType` 값이 포함됩니다.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType“: “비밀번호” 또는 "“: “비밀번호, TOTP” (가능한 값에는 비밀번호, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP 등이 포함됩니다. CredentialType
`DeviceEnrollmentRequired`	사용자가 로그인할 때 MFA 디바이스를 등록해야 하고 해당 요청을 성공적으로 완료했음을 지정하는 데 사용됩니다.	`UserAuthentication`	““: “참” DeviceEnrollmentRequired
`LoginTo`	성공적인 로그인 순서에 따라 리디렉션 위치를 지정하는 데 사용됩니다.	`UserAuthentication`	“LoginTo“:” https://mydirectory.awsapps.com/start/...”

IAM Identity Center 로그인 시나리오의 예제 이벤트

다음 예는 다양한 로그인 시나리오에서 예상되는 CloudTrail 이벤트 순서를 보여줍니다.

주제

- 암호만 사용하여 인증한 경우의 로그인 성공

- 외부 ID 제공업체를 통해 인증한 경우의 로그인 성공
- 암호 및 TOTP 인증 앱으로 인증한 경우의 로그인 성공
- 암호 및 MFA 등록 필수 인증을 통한 로그인 성공
- 암호만 사용하여 인증한 경우의 로그인 실패

암호만 사용하여 인증한 경우의 로그인 성공

다음 이벤트 시퀀스는 성공적인 암호 전용 로그인의 예제입니다.

CredentialChallenge (비밀번호)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:33:58Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
```

```
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

성공 CredentialVerification (비밀번호)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

성공 UserAuthentication (비밀번호만 해당)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

외부 ID 제공업체를 통해 인증한 경우의 로그인 성공

다음 이벤트 시퀀스는 외부 ID 제공업체를 사용하여 SAML 프로토콜을 통해 인증했을 때 성공한 로그인의 예제입니다.

성공 UserAuthentication (외부 ID 제공업체)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":""
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"EXTERNAL_IDP"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
```

```
}
```

암호 및 TOTP 인증 앱으로 인증한 경우의 로그인 성공

다음 이벤트 시퀀스는 로그인 시 다단계 인증이 필요하고 사용자가 암호와 TOTP 인증 앱을 사용하여 성공적으로 로그인한 예제입니다.

CredentialChallenge (비밀번호)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:13Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
   "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

성공 CredentialVerification (비밀번호)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


CredentialChallenge (전체)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
```

```
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


성공 CredentialVerification (TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
```

```
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


성공 UserAuthentication (비밀번호 + TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
```

```
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFfO01O8qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD,TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


암호 및 MFA 등록 필수 인증을 통한 로그인 성공

다음 이벤트 순서는 성공적인 암호 로그인의 예를 보여 주지만, 사용자는 로그인을 완료하기 전에 MFA 디바이스 등록을 완료해야 했습니다.

CredentialChallenge (비밀번호)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
```

```
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:02Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
   "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


성공 CredentialVerification (비밀번호)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
```

```
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
   "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


성공 UserAuthentication (비밀번호+MFA 등록 필요)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:14Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
```

```
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HLlN2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY EgU3fhOL3QWvWiquYnDPMyPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi5OYI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD",
      "DeviceEnrollmentRequired":"true"
   },
   "requestID":"74d24604-a365-4237-8c4a-350795494b92",
   "eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


암호만 사용하여 인증한 경우의 로그인 실패

다음 이벤트 시퀀스는 암호 전용 로그인의 실패 예제입니다.

CredentialChallenge (비밀번호)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:15Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
```

```
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
   "eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


실패 CredentialVerification (비밀번호)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:21Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
```

```
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
   "eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Failure"
   }
}
```


아마존 EventBridge

IAM Identity Center는 EventBridge Amazon과 협력하여 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. 이러한 작업을 찾는 EventBridge 규칙을 구성한 다음 생성된 이벤트를 관리자가 정의한 대상으로 전송할 수 있습니다. 대상은 해당 구독자에게 이메일 또는 문자 메시지를 보내는 Amazon SNS 주제가 될 수 있습니다. 나중에 검토할 수 있도록 작업의 세부 정보를 기록하는 AWS Lambda 함수를 만들 수도 있습니다.

구성 및 활성화 방법을 EventBridge 포함하여 자세한 내용은 Amazon 사용 EventBridge 설명서를 참조하십시오.

AD 동기화 및 구성 가능한 AD 동기화 오류 로깅

Active Directory (AD) 동기화 및 구성 가능한 AD 동기화 구성에서 로깅을 활성화하여 동기화 프로세스 중에 발생할 수 있는 오류에 대한 정보가 포함된 로그를 받을 수 있습니다. 이러한 로그를 사용하여 AD 동기화 및 구성 가능한 AD 동기화에 문제가 있는지 모니터링하고 해당하는 경우 조치를 취할 수 있습니다. Amazon 로그 로그 그룹, Amazon Simple Storage Service (Amazon S3) 버킷 또는 Amazon Data Firehose로 CloudWatch 로그를 보낼 수 있으며, Amazon S3 버킷과 Firehose에 계정 간 전송이 지원됩니다.

제한, 권한 및 판매 로그에 대한 자세한 내용은 로깅 활성화를 참조하십시오. AWS 서비스

> **Note**
>
> 로깅에는 요금이 부과됩니다. 자세한 내용은 Amazon CloudWatch 가격 책정 페이지의 벤드 로그를 참조하십시오.

AD 동기화 및 구성 가능한 AD 동기화 오류 로그를 활성화하려면

1. IAM ID 센터 콘솔에 로그인합니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 로그 관리를 선택합니다.
4. 로그 전송 추가 및 다음 대상 유형 중 하나를 선택합니다.
   a. Amazon CloudWatch Logs를 선택하십시오. 그런 다음 대상 로그 그룹을 선택하거나 입력합니다.
   b. Amazon S3를 선택하세요. 그런 다음 대상 버킷을 선택하거나 입력합니다.
   c. To To Firehose를 선택하세요. 그런 다음 대상 전송 스트림을 선택하거나 입력합니다.
5. 제출을 선택합니다.

AD 동기화 및 구성 가능한 AD 동기화 오류 로그를 비활성화하려면

1. IAM ID 센터 콘솔에 로그인합니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 로그 관리를 선택합니다.
4. 제거하려는 대상에 대해 제거를 선택합니다.
5. 제출을 선택합니다.

AD 동기화 및 구성 가능한 AD 동기화 오류 로그 필드

가능한 오류 로그 필드는 다음 목록을 참조하십시오.

`sync_profile_name`

동기화 프로필의 이름.

`error_code`

발생한 오류 유형을 나타내는 오류 코드입니다.

`error_message`

발생한 오류에 대한 세부 정보가 포함된 메시지입니다.

`sync_source`

동기화 소스는 엔티티가 동기화되는 위치입니다. IAM ID 센터의 경우 이 센터는 에서 관리하는 액티브 디렉터리 (AD) 입니다. AWS Directory Service동기화 소스에는 영향을 받은 디렉토리의 도메인과 ARN이 포함됩니다.

`sync_target`

동기화 대상은 엔티티가 저장되는 대상입니다. IAM ID 센터의 경우 이는 ID 저장소입니다. 동기화 대상에는 영향을 받은 ID 저장소 ARN이 포함되어 있습니다.

`source_entity_id`

오류를 일으키는 엔티티의 고유 식별자입니다. IAM ID 센터의 경우 이는 엔티티의 SID입니다.

`source_entity_type`

오류를 일으킨 개체의 유형. `USER` 또는 `GROUP` 값을 가질 수 있습니다.

`eventTimestamp`

오류가 발생한 시점의 타임스탬프.

AD 동기화 및 구성 가능한 AD 동기화 오류 로그 예제

예 1: AD 디렉터리의 만료된 암호에 대한 오류 로그

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "InvalidDirectoryCredentials",
        "error_message": "The password for your AD directory has expired. Please reset
 the password to allow Identity Sync to access the directory."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
```

```
        "domain": "EXAMPLE.com"
    },
    "eventTimestamp": "1683355579981"
}
```

예 2: 고유하지 않은 사용자 이름을 가진 사용자의 오류 로그

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "ConflictError",
        "error_message": "The source entity has a username conflict with the sync
 target. Please verify that the source identity has a unique username in the target."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "sync_target": {
        "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
    },
    "source_entity_id": "SID-1234",
    "source_entity_type": "USER",
    "eventTimestamp": "1683355579981"
}
```

IAM Identity Center에 대한 규정 준수 확인

제3자 감사자가 여러 규정 AWS 준수 프로그램의 AWS 서비스 AWS IAM Identity Center 일환으로 보안 및 규정 준수를 평가합니다.

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의 범위별, 규정 준수AWS 서비스 프로그램별 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

지원되는 규정 준수 표준

IAM Identity Center는 다음 표준에 대한 감사를 거쳤으며 규정 준수 인증을 획득해야 하는 솔루션의 일부로 사용할 수 있습니다.

AWS 건강 보험 양도 및 책임에 관한 법률 (HIPAA) 규정 준수 프로그램을 확장하여 IAM 아이덴티티 센터를 HIPAA 적격 서비스로 포함시켰습니다.

AWS 의료 정보를 처리하고 저장하는 데 사용할 수 있는 방법에 대해 자세히 알아보려는 고객을 위해 HIPAA에 초점을 맞춘 백서를 제공합니다. AWS 서비스 자세한 내용은 HIPAA 규정 준수를 참조하세요.

IRAP(Information Security Registered Assessors Program)를 통해 호주 정부 고객은 적절한 규정 준수 제어가 이루어지는지 검증하고 호주 사이버 보안 센터(ACSC)에서 제작한 호주 정부 ISM(Information Security Manual)의 요구 사항을 해결하기 위한 적절한 책임 모델을 결정할 수 있습니다. 자세한 내용은 IRAP 리소스를 참조하세요.

IAM Identity Center는 서비스 공급자 레벨 1에서 PCI DSS(지불 결제 산업 데이터 보안 표준) 버전 3.2의 규정 준수 증명을 보유하고 있습니다.

AWS 제품 및 서비스를 사용하여 카드 소지자 데이터를 저장, 처리 또는 전송하는 고객은 IAM Identity Center의 다음 ID 소스를 사용하여 자체 PCI DSS 규정 준수 인증을 관리할 수 있습니다.

- Active Directory
- 외부 ID 제공업체

IAM Identity Center ID 소스는 현재 PCI DSS와 호환되지 않습니다.

PCI AWS 컴플라이언스 패키지의 사본을 요청하는 방법을 포함하여 PCI DSS에 대한 자세한 내용은 PCI DSS 레벨 1을 참조하십시오.

시스템 및 조직 제어(SOC) 보고서는 IAM Identity Center가 주요 규정 준수 제어 기능을 어떻게 확보하고 목표를 어떻게 달성하고 있는지 입증하는 독립적 제3자 검사 기관의 심사 보고서입니다. 이러한 보고서는 고객과 고객의 감사자가 운영 및 규정 준수를 지원하는 제어 항목을 이해하는 데 도움을 주고자 작성되었습니다. SOC 보고서에는 다음 세 가지 유형이 있습니다.

- AWS SOC 1 보고서 - Artifact와 함께 AWS 다운로드
- AWS SOC 2: 보안, 가용성 및 기밀성 보고서 - Artifact와 함께 다운로드 AWS
- AWS SOC 3: 보안, 가용성 및 기밀성 보고서

IAM ID 센터는 AWS SOC 1, SOC 2 및 SOC 3 보고서의 범위에 포함됩니다. 자세한 내용은 SOC 규정 준수를 참조하세요.

IAM Identity Center 복원성

AWS 글로벌 인프라는 AWS 지역 및 가용 영역을 중심으로 구축됩니다. AWS 지역은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이러한 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 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 지역 및 가용 영역에 대한 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

AWS IAM Identity Center 복원력에 대한 자세한 내용은 을 참조하십시오복원력 설계 및 리전 동작.

IAM Identity Center의 인프라 보안

관리형 서비스로서 AWS 글로벌 네트워크 보안으로 AWS IAM Identity Center 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 IAM Identity Center에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(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.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

AWS IAM Identity Center 리소스에 태그 지정

태그는 리소스를 좀 더 쉽게 식별하고 구성하고 검색하기 위해 AWS 리소스에 추가하는 사용자 지정 속성 레이블입니다. 각 태그에는 다음 두 가지 부분이 있습니다.

- 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.

태그를 사용하면 AWS 리소스를 식별하고 구성하는 데 도움이 됩니다. 많은 AWS 서비스가 태그 지정을 지원하므로 다른 서비스의 리소스에 동일한 태그를 할당하여 해당 리소스의 관련 여부를 나타낼 수 있습니다. 예를 들어 IAM Identity Center 인스턴스의 특정 권한 세트에 동일한 태그를 할당할 수 있습니다. 태깅 전략에 대한 자세한 내용은 AWS 일반 참조 설명서의 리소스 AWS 태깅 및 태깅 모범 사례를 참조하십시오.

태그로 AWS 리소스를 식별, 구성 및 추적하는 것 외에도 IAM 정책의 태그를 사용하여 리소스를 보고 상호 작용할 수 있는 사용자를 제어할 수 있습니다. 태그를 사용하여 액세스를 제어하는 자세한 내용은 IAM 사용 설명서의 태그를 사용해 AWS 리소스 액세스 제어를 참조하세요. 예를 들어 IAM Identity Center 권한 세트에 값이 사용자를 업데이트하도록 허용할 수 있지만, 이는 IAM Identity Center 권한 세트에 해당 사용자의 이름 값이 `owner` 태그와 같이 있을 경우에만 가능합니다.

현재는 사용 권한 세트에만 태그를 적용할 수 있습니다. AWS 계정에서 IAM Identity Center가 생성하는 해당 역할에는 태그를 적용할 수 없습니다. IAM Identity Center 콘솔, AWS CLI 또는 IAM Identity Center API를 사용하여 권한 세트의 태그를 추가, 편집 또는 삭제할 수 있습니다.

다음 섹션에서는 IAM Identity Center의 태그에 대한 추가 정보를 제공합니다.

태그 제한

IAM Identity Center 리소스의 태그에 다음과 같은 기본 제한이 적용됩니다.

- 리소스에 할당할 수 있는 최대 태그 수는 50개입니다.
- 최대 키 길이는 유니코드 문자 128자입니다.
- 최대 값 길이는 유니코드 문자 256자입니다.

- 태그 키와 값에 사용할 수 있는 문자는 다음과 같습니다.

  a-z, A-Z, 0-9, 공백 및 특수 문자 _ . : / = + - 및 @
- 키와 값은 대/소문자를 구분합니다.
- 키 접두사로 `aws:`를 사용하지 마세요. AWS 전용입니다.

IAM Identity Center 콘솔을 사용하여 태그 관리

IAM Identity Center 콘솔을 사용하여 인스턴스 또는 권한 세트와 연결된 태그를 추가, 편집 및 제거할 수 있습니다.

IAM Identity Center 콘솔의 권한 세트 태그 관리

1. IAM Identity Center 콘솔을 엽니다.
2. 권한 세트를 선택합니다.
3. 관리할 태그가 있는 권한 세트의 이름을 선택합니다.
4. 권한 탭의 태그에서 다음 중 하나를 수행한 후 다음 단계로 진행하십시오.

   a. 이 권한 세트에 태그가 이미 할당되어 있는 경우 태그 편집을 선택합니다.

   b. 이 권한 세트에 할당된 태그가 없는 경우 태그 추가를 선택합니다.
5. 각각의 새 태그에 대해 키 및 값(선택 사항) 열에 값을 입력합니다. 작업을 마쳤으면 변경 사항 저장을 선택합니다.

태그를 제거하려면 제거할 태그 옆에 있는 제거 열에서 X를 선택합니다.

IAM Identity Center 인스턴스의 태그 관리

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 태그 탭을 선택합니다.
4. 각각의 태그에 대해 키 및 값(선택 사항) 필드에 값을 입력합니다. 완료되면 새 태그 추가 버튼을 선택합니다.

태그를 제거하려면 제거하려는 태그 옆에 있는 제거 버튼을 선택합니다.

AWS CLI 예제

AWS CLI에서는 사용 권한 세트에 할당하는 태그를 관리하는 데 사용할 수 있는 명령을 제공합니다.

태그 할당

다음 명령을 사용하여 권한 세트에 태그를 할당합니다.

Example 권한 세트에 대한 **`tag-resource`** 명령

`sso` 명령 세트에서 `tag-resource`를 사용하여 권한 세트에 태그를 할당합니다.

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

이 명령에는 다음 파라미터가 포함되어 있습니다.

- `instance-arn`— 작업이 실행될 IAM Identity Center 인스턴스의 Amazon 리소스 이름(ARN)입니다.
- `resource-arn`— 나열할 태그가 있는 리소스의 ARN입니다.
- `tags` - 태그의 키-값 페어입니다.

여러 태그를 한 번에 할당하려면 쉼표로 구분된 목록으로 지정합니다.

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

태그 보기

다음 명령을 사용하여 권한 세트에 할당된 태그를 확인합니다.

Example 권한 세트에 대한 **`list-tags-for-resource`** 명령

`sso` 명령 세트에서 `list-tags-for-resource`를 사용하여 권한 세트에 할당한 태그를 확인합니다.

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

태그 제거

다음 명령을 사용하여 권한 세트에 태그를 제거합니다.

Example 권한 세트에 대한 **untag-resource** 명령

sso 명령 세트에서 untag-resource를 사용하여 권한 세트에서 태그를 제거합니다.

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

--tag-keys 파라미터에는 태그 키를 하나 이상 지정하고 태그 값은 포함하지 않습니다.

권한 세트를 생성할 때 태그 적용

다음 명령을 사용하여 권한 세트를 생성할 때 태그를 할당합니다.

Example 태그가 있는 **create-permission-set** 명령

create-permission-set 명령을 사용하여 권한 세트를 생성할 때 --tags 파라미터로 태그를 지정할 수 있습니다.

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

IAM Identity Center API를 사용하여 태그 관리

IAM Identity Center API에서 다음 작업을 사용하여 권한 세트에 대한 태그를 관리할 수 있습니다.

IAM Identity Center 인스턴스 태그에 대한 API 작업

다음 API 작업을 사용하여 IAM Identity Center의 권한 세트 또는 인스턴스에 대한 태그를 할당하고 보고 제거합니다.

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

AWS CLI와 IAM Identity Center 통합

AWS 명령줄 인터페이스(CLI) 버전 2와 IAM Identity Center를 통합하면 로그인 절차가 간소화됩니다. 개발자는 일반적으로 IAM Identity Center에 로그인할 때 사용하는 것과 동일한 Active Directory 또는 IAM Identity Center 보안 인증 정보를 사용하여 AWS CLI에 직접 로그인하고 할당된 계정 및 역할에 액세스할 수 있습니다. 예를 들어, 관리자가 인증에 Active Directory를 사용하도록 IAM Identity Center를 구성하면 개발자는 자신의 Active Directory 보안 인증 정보를 사용하여 AWS CLI에 직접 로그인할 수 있습니다.

AWS CLI와 IAM Identity Center를 통합하면 다음과 같은 이점이 있습니다.

- 기업은 AWS Directory Service를 사용하여 IAM Identity Center를 Active Directory에 연결하여 개발자가 IAM Identity Center 또는 Active Directory의 보안 인증 정보를 사용하여 로그인할 수 있도록 할 수 있습니다.
- 개발자는 CLI에서 로그인하여 더 빠르게 액세스할 수 있습니다.
- 개발자는 액세스 권한이 할당된 계정과 역할을 나열하고 해당 계정과 역할 간에 전환할 수 있습니다.
- 개발자는 명명된 역할 프로필을 생성하여 CLI 구성에 자동으로 저장하고, CLI에서 이를 참조하여 원하는 계정과 역할에서 명령을 실행할 수 있습니다.
- CLI는 단기 보안 인증을 자동으로 관리하므로 개발자는 중단 없이 안전하게 CLI를 시작하고 유지하며 장기 실행 스크립트를 실행할 수 있습니다.

AWS CLI와 IAM Identity Center 통합 방법

AWS CLI와 IAM Identity Center의 통합을 사용하려면 AWS Command Line Interface 버전 2를 다운로드, 설치 및 구성해야 합니다. AWS CLI를 다운로드하여 IAM Identity Center와 통합하는 방법에 대한 자세한 단계는 AWS Command Line Interface 사용 설명서의 IAM Identity Center를 사용하도록 AWS CLI 구성하기를 참조하십시오.

AWS IAM Identity Center 지역 이용 가능 여부

IAM ID 센터는 일반적으로 사용되는 AWS 리전여러 가지로 제공됩니다. 이러한 가용성을 통해 여러 AWS 계정 비즈니스 애플리케이션에 대한 사용자 액세스를 더 쉽게 구성할 수 있습니다. 사용자는 AWS 액세스 포털에 로그인하면 권한이 있는 AWS 계정 대상을 선택한 다음 액세스할 수 AWS Management Console있습니다. IAM ID 센터에서 지원하는 전체 목록은 IAM ID 센터 엔드포인트 및 할당량을 참조하십시오. AWS 리전

IAM Identity Center 리전 데이터

IAM Identity Center를 처음 활성화하면 IAM Identity Center에서 구성하는 모든 데이터가 해당 센터를 구성한 리전에 저장됩니다. 이 데이터에는 디렉터리 구성, 권한 집합, 애플리케이션 인스턴스, 애플리케이션에 대한 사용자 할당이 포함됩니다. AWS 계정 IAM Identity Center ID 스토어를 사용하는 경우, IAM Identity Center에서 생성하는 모든 사용자와 그룹도 같은 리전에 저장됩니다. 비활성화해야 할 리전이 아닌 사용자가 계속 사용할 수 있도록 하려는 리전에 IAM Identity Center를 설치하는 것이 좋습니다.

AWS Organizations 한 AWS 리전 번에 하나만 지원합니다. IAM Identity Center를 다른 리전에서 활성화하려면 먼저 현재 IAM Identity Center 구성을 삭제해야 합니다. 다른 지역으로 전환하면 AWS 액세스 포털의 URL도 변경되므로 모든 권한 집합과 할당을 재구성해야 합니다.

크로스 리전 호출

IAM ID 센터는 최종 사용자가 일회용 암호(OTP)를 두 번째 인증 요소로 사용하여 로그인을 시도할 때 Amazon Simple Email Service(Amazon SES)를 사용하여 이메일을 보냅니다. 또한 이러한 이메일은 사용자에게 초기 암호를 설정하고, 이메일 주소를 확인하고, 암호를 재설정하라는 초대를 받는 경우와 같은 특정 ID 및 보안 인증 관리 이벤트를 위해 전송됩니다. Amazon SES는 IAM 자격 증명 센터가 AWS 리전 지원하는 하위 집합으로 제공됩니다.

IAM Identity Center는 Amazon SES를 AWS 리전의 로컬에서 사용할 수 있을 때 Amazon SES 로컬 엔드포인트를 호출합니다. Amazon SES를 로컬에서 사용할 수 없는 경우, IAM Identity Center는 다음 표에 나와 있는 것처럼 다른 AWS 리전에서 Amazon SES 엔드포인트를 호출합니다.

Amazon SES 리전 코드는 다음 표에 나열되어 있습니다.

IAM Identity Center 리전 코드	IAM Identity Center 리전 이름	Amazon SES 리전 코드	Amazon SES 리전 이름
us-gov-east-1	AWS GovCloud (미국 동부)	us-gov-west-1	AWS GovCloud (미국 서부)
ap-east-1	아시아 태평양(홍콩)	ap-northeast-2	아시아 태평양(서울)
ap-southeast-4	아시아 태평양(멜버른)	ap-southeast-2	아시아 태평양(시드니)
ap-south-2	아시아 태평양(하이데라바드)	ap-south-1	아시아 태평양(뭄바이)
eu-central-2	유럽(취리히)	eu-central-1	유럽(프랑크푸르트)
eu-south-2	유럽(스페인)	eu-west-3	유럽(파리)
me-central-1	중동(UAE)	eu-central-1	유럽(프랑크푸르트)

이러한 리전 간 호출에서 IAM Identity Center는 다음과 같은 사용자 속성을 전송할 수 있습니다.

- 이메일 주소
- 이름
- 성
- 계정 입력 AWS Organizations
- AWS 액세스 포털 URL
- 사용자 이름
- 디렉터리 ID
- 사용자 ID

옵트인 지역 (기본적으로 비활성화된 지역) 에서 IAM ID 센터 관리

AWS 리전 대부분은 기본적으로 모든 AWS 서비스에서 운영할 수 있도록 활성화되어 있습니다. 이러한 리전은 IAM Identity Center와 함께 자동으로 사용이 활성화됩니다. 옵트인 지역은 AWS 리전 다음과 같으며 반드시 활성화해야 합니다.

- 아프리카(케이프타운)
- 아시아 태평양(홍콩)
- 아시아 태평양(자카르타)
- 아시아 태평양(멜버른)
- 아시아 태평양(하이데라바드)
- 유럽(밀라노)
- 유럽(취리히)
- 유럽(스페인)
- 이스라엘(텔아비브)
- 중동(바레인)
- 중동(UAE)

AWS 리전옵트인에서 관리 계정에 대해 IAM Identity Center를 활성화하면 모든 회원 계정에 대한 다음 IAM Identity Center 메타데이터가 지역에 저장됩니다.

- 계정 ID
- 계정 이름
- 계정 이메일
- IAM Identity Center가 구성원 계정에 생성하는 IAM 역할의 Amazon 리소스 이름(ARN)

IAM Identity Center가 설치된 리전을 비활성화하면 IAM Identity Center도 비활성화됩니다. 지역에서 IAM Identity Center가 비활성화되면 해당 지역의 사용자는 애플리케이션에 대한 Single Sign-On 액세스 권한을 가질 수 없습니다. AWS 계정 AWS IAM ID 센터 구성의 데이터를 최소 10일 동안 보존합니다. 이 기간 내에 IAM Identity Center를 다시 활성화해도 IAM Identity Center 구성 데이터는 해당 리전에서 계속 사용할 수 있습니다.

AWS 리전옵트인에서 IAM Identity Center를 다시 활성화하려면 지역을 다시 활성화해야 합니다. IAM Identity Center는 일시 중지된 모든 이벤트를 다시 처리해야 하므로 IAM Identity Center를 다시 활성화하는 데 시간이 걸릴 수 있습니다.

> **Note**
>
> IAM Identity Center는 에서 사용할 수 있도록 설정된 서비스에 대한 액세스만 관리할 수 있습니다. AWS 계정 AWS 리전조직의 모든 계정에 대한 액세스를 관리하려면 IAM Identity Center

와 함께 사용하도록 자동으로 AWS 리전 활성화되는 관리 계정의 IAM Identity Center를 활성화하십시오.

활성화 및 AWS 리전비활성화에 대한 자세한 내용은 일반 AWS 리전참조의 AWS 관리를 참조하십시오.

IAM Identity Center 구성 삭제

IAM Identity Center 구성이 삭제되면 해당 구성의 모든 데이터가 삭제되며 복구할 수 없습니다. 다음 표에는 IAM Identity Center에 현재 구성되어 있는 디렉터리 유형에 따라 삭제되는 데이터가 설명되어 있습니다.

삭제되는 데이터	연결된 디렉터리 (AWS Managed Microsoft AD 또는 AD 커넥터)	IAM Identity Center ID 스토어
구성한 모든 권한 집합 AWS 계정	✓	✓
IAM Identity Center에서 구성한 모든 애플리케이션	✓	✓
구성한 모든 사용자 할당 AWS 계정 및 애플리케이션	✓	✓
디렉터리 또는 스토어의 모든 사용자 및 그룹	해당 사항 없음	✓

현재 IAM Identity Center 구성을 삭제해야 하는 경우 다음 절차를 사용합니다.

IAM Identity Center 구성을 삭제하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 관리를 선택합니다.

4. IAM Identity Center 구성 삭제 섹션에서 삭제를 선택합니다.
5. IAM Identity Center 구성 삭제 대화 상자에서 각 확인란을 선택하여 삭제될 데이터를 인지했음을 확인합니다. 텍스트 상자에 IAM Identity Center 인스턴스를 입력한 다음 확인을 선택합니다.

AWS IAM Identity Center 할당량

다음 표에서는 IAM Identity Center의 할당량에 대해 설명합니다. 할당량 증가 요청은 관리 또는 위임된 관리자 계정에서 이루어져야 합니다. 할당량을 늘리려면 할당량 증가 요청을 참조하세요.

> **Note**
>
> 사용자 50,000명, 그룹 10,000개 또는 권한 집합이 500개 이상인 경우 AWS CLI와 API를 사용하는 것이 좋습니다. CLI에 대한 자세한 내용은 AWS CLI와 IAM Identity Center 통합 단원을 참조하세요. API에 대한 자세한 내용은 IAM Identity Center API 참조 소개를 참조하세요.

애플리케이션 할당량

Resource	기본 할당량	높일 수 있음
서비스 제공업체 SAML 인증서의 파일 크기(PEM 형식)	2KB	아니요
SAML 어설션 제한	50,000자	아니요
IAM ID 센터에 업로드된 IdP 인증서의 파일 크기 제한	2500자(UTF-8)	아니요
애플리케이션별 액세스 범위	25	아니요

AWS 계정 할당량

Resource	기본 할당량	높일 수 있음
IAM Identity Center에서 허용되는 권한 세트 수	2000	예
1개당 허용된 프로비저닝된 권한 집합 수 AWS 계정	250	예

Resource	기본 할당량	높일 수 있음
권한 세트당 인라인 정책 수	1	아니요
권한 집합당 AWS 관리형 및 고객 관리형 정책 수	20 [1]	아니요
권한 세트당 인라인 정책의 최대 크기	32,768바이트. 권한 세트당 인라인 정책에서 공백이 아닌 문자의 최대 크기는 10,240바이트입니다.	아니요
한 번에 업데이트할 수 AWS 계정 있는 의 IAM 역할 (권한 집합) 수	1	아니요

[1]AWS Identity and Access Management (IAM) 은 역할당 관리형 정책 10개로 할당량을 설정합니다. 이 할당량을 활용하려면 권한 세트를 배포하려는 AWS 계정 각 위치에 대해 Service Quotas 콘솔에서 IAM 역할에 연결된 IAM 할당량 관리형 정책을 늘려달라고 요청하십시오.

> **Note**
>
> 권한 세트IAM AWS 계정 역할로 프로비저닝되거나 에서 기존 IAM 역할을 사용하므로 IAM 할당량을 따릅니다. AWS 계정IAM 역할과 관련된 할당량에 대한 자세한 내용은 IAM 및 STS 할당량을 참조하세요.

Active Directory 할당량

Resource	기본 할당량	높일 수 있음
한 번에 사용할 수 있는 연결된 디렉터리 수	1	아니요

IAM Identity Center ID 스토어 할당량

Resource	기본 할당량	높일 수 있음
IAM Identity Center에서 지원되는 사용자 수	100000	예
IAM Identity Center에서 지원되는 그룹 수	100000	아니요
사용자 권한을 평가하는 데 사용할 수 있는 고유 그룹 수	1000	아니요

IAM Identity Center 스로틀 제한

Resource	기본 할당량
IAM Identity Center API	IAM Identity Center API에는 최대 20TPS(초당 트랜잭션)의 총 스로틀이 있습니다. 미해결 비동기 호출 비율은 최대 CreateAccountAssignment10개입니다. 이러한 할당량은 변경할 수 없습니다.

추가 할당량

Resource	기본 할당량	높일 수 있음
구성할 수 있는 전체 AWS 계정 또는 애플리케이션 수*	3000	예
계정당 IAM Identity Center의 총 계정 인스턴스 수	1	아니요
총 신뢰할 수 있는 토큰 발급자 수	10	아니요

* 최대 3000개 AWS 계정 이상의 애플리케이션 (총 합산) 이 지원됩니다. 예를 들어 2750개의 계정과 250개의 애플리케이션을 구성하여 총 3000개의 계정 및 애플리케이션을 생성할 수 있습니다.

IAM Identity Center 문제 해결

다음은 IAM Identity Center 콘솔을 설정하거나 사용하는 동안 발생할 수 있는 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

IAM Identity Center의 계정 인스턴스 생성 문제

IAM Identity Center의 계정 인스턴스를 생성할 때는 몇 가지 제한이 적용될 수 있습니다. IAM Identity Center 콘솔 또는 지원되는 AWS 관리형 애플리케이션의 설치 환경을 통해 계정 인스턴스를 생성할 수 없는 경우 다음 사용 사례를 확인하십시오.

- 계정 AWS 리전 인스턴스를 생성하려는 다른 계정을 확인하십시오. AWS 계정 AWS 계정당 IAM Identity Center 인스턴스는 1개로 제한됩니다. 애플리케이션을 활성화하려면 IAM Identity Center 인스턴스가 AWS 리전 있는 로 전환하거나 IAM Identity Center 인스턴스가 없는 계정으로 전환하십시오.
- 2023년 9월 14일 이전에 조직에서 IAM Identity Center를 활성화한 경우 관리자가 계정 인스턴스 생성에 동의해야 할 수 있습니다. 관리자와 협력하여 관리 계정의 IAM Identity Center 콘솔에서 계정 인스턴스 생성을 활성화합니다.
- 관리자가 IAM Identity Center의 계정 인스턴스 생성을 제한하는 서비스 제어 정책을 만들었을 수 있습니다. 관리자와 상의하여 허용 목록에 계정을 추가하세요.

IAM Identity Center에서 사용하도록 사전 구성된 클라우드 애플리케이션 목록을 보려고 하면 오류가 발생합니다.

다음 오류는 `sso:ListApplications`를 허용하지만 다른 IAM Identity Center API는 허용하지 않는 정책이 있을 때 발생합니다. 정책을 업데이트하여 이 오류를 해결하세요.

`ListApplications` 권한은 여러 API를 승인합니다.

- `ListApplications` API.
- IAM Identity Center 콘솔에서 사용되는 `ListApplicationProviders` API와 유사한 내부 API입니다.

중복 해결에 도움이 되도록 내부 API에서 이제 `ListApplicationProviders` 작업 사용을 승인합니다. 퍼블릭 `ListApplications` API를 허용하지만 내부 API를 거부하려면 정책에 `ListApplicationProviders` 작업을 거부하는 문을 포함해야 합니다.

```
      "Statement": [
    {
         "Effect": "Deny",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

내부 API를 허용하지만 `ListApplications`를 거부하려면 정책에서 `ListApplicationProviders`만 허용해야 합니다. 명시적으로 허용되지 않는 경우 `ListApplications` API가 거부됩니다.

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    }
]
```

정책이 업데이트되면 연락하여 이 사전 조치를 AWS Support 제거하도록 요청하세요.

IAM Identity Center에서 생성된 SAML 어설션 콘텐츠 관련 문제

IAM Identity Center는 액세스 포털에서 SAML 애플리케이션에 액세스하거나 SAML 애플리케이션에 액세스할 때 이러한 어설션 내의 속성을 포함하여 IAM Identity Center에서 생성 및 전송한 SAML 어설션에 대한 웹 기반 디버그 환경을 제공합니다. AWS 계정 AWS IAM Identity Center에서 생성하는 SAML 어설션의 세부 정보를 보려면 다음 단계를 사용하세요.

1. 액세스 포털에 로그인합니다. AWS
2. 포털에 로그인한 후 Shift 키를 누른 상태에서 애플리케이션 타일을 선택한 다음 Shift 키를 놓습니다.
3. 이제 관리자 모드에 있습니다라는 제목의 페이지에 있는 정보를 확인합니다. 나중에 참조할 수 있도록 이 정보를 보관하려면 XML 복사를 선택하고 내용을 다른 곳에 붙여 넣습니다.
4. 계속하려면 <애플리케이션>으로 보내기를 선택합니다. 이 옵션은 서비스 제공업체에 어설션을 전송합니다.

> **Note**
>
> 일부 브라우저 구성 및 운영 체제는 이 절차를 지원하지 않을 수 있습니다. 이 절차는 Windows 10에서 Firefox, Chrome, Edge 브라우저를 사용하여 테스트되었습니다.

특정 사용자가 외부 SCIM 공급자로부터 IAM Identity Center로 동기화하지 못함

IAM Identity Center에 프로비저닝하기 위해 IdP에 구성된 일부 사용자는 SCIM 동기화가 되지만, 다른 사용자는 동기화가 되지 않으면 ID 제공업체의 `'Request is unparsable, syntactically incorrect, or violates schema'`와 유사한 오류가 발생할 수 있습니다. 에서 자세한 프로비저닝 실패 메시지를 볼 수도 있습니다 AWS CloudTrail.

이 문제는 종종 IdP의 사용자가 IAM Identity Center가 지원하지 않는 방식으로 구성되어 있는 경우에 발생합니다. 사용자 객체에 대한 필수, 선택, 금지된 파라미터 및 작업 사양을 포함하여 IAM Identity Center SCIM 구현에 대한 자세한 내용은 IAM Identity Center SCIM 구현 개발자 안내서에서 확인할 수 있습니다. SCIM 개발자 안내서는 SCIM 요구 사항에 대한 신뢰할 수 있는 정보를 제공하는 자료입니다. 하지만 이러한 오류가 발생하는 몇 가지 일반적인 이유는 다음과 같습니다.

1. IdP의 사용자 객체에 이름, 성 및/또는 표시 이름이 없습니다.
   - 해결 방법: 사용자 객체의 이름, 성, 표시 이름을 추가합니다. 또한 IdP의 사용자 객체에 대한 SCIM 프로비저닝 매핑이 이러한 모든 속성에 대해 비어 있지 않은 값을 전송하도록 구성되어 있는지 확인합니다.
2. 단일 속성에 대해 둘 이상의 값이 사용자에게 전송됩니다(“다중 값 속성”이라고도 함). 예를 들어 사용자가 IdP에 직장 전화번호와 집 전화번호를 모두 지정하거나 이메일 또는 실제 주소가 여러

개이거나 IdP가 해당 속성에 대해 여러 값 또는 모든 값을 동기화하도록 구성되어 있을 수 있습니다.

- 가능한 해결 방법:

  i. 지정된 속성에 대해 단일 값만 전송하도록 IdP의 사용자 객체에 대한 SCIM 프로비저닝 매핑을 업데이트합니다. 예를 들어, 각 사용자의 직장 전화번호만 전송하도록 매핑을 구성합니다.

  ii. IdP의 사용자 체에서 추가 속성을 안전하게 제거할 수 있는 경우 추가 값을 제거하여 사용자의 해당 속성에 대해 설정된 값을 하나 또는 0으로 남겨 둘 수 있습니다.

  iii. 의 작업에 속성이 필요하지 않은 경우 IdP의 사용자 개체에 대한 SCIM 프로비저닝 매핑에서 해당 속성에 대한 매핑을 제거하십시오. AWS

3. IdP가 여러 속성을 기반으로 대상(이 경우 IAM Identity Center)의 사용자를 매칭하려고 시도합니다. 사용자 이름은 지정된 IAM Identity Center 인스턴스 내에서 고유성이 보장되므로 매칭에 사용되는 속성으로 `username`만 지정하면 됩니다.

   - 해결 방법: IIdP의 SCIM 구성이 IAM Identity Center의 사용자를 매칭하기 위해 단일 속성만 사용하고 있는지 확인합니다. 예를 들어, IAM Identity Center에 프로비저닝하기 위해 IdP의 `username` 또는 `userPrincipalName`를 SCIM의 `userName` 속성에 매핑하면 대부분의 구현에서 정확하고 충분합니다.

사용자 이름이 UPN 형식인 경우 사용자는 로그인할 수 없습니다.

로그인 페이지에서 사용자 이름을 입력할 때 사용하는 형식에 따라 사용자는 AWS 액세스 포털에 로그인하지 못할 수 있습니다. 대부분의 경우 사용자는 일반 사용자 이름, 하위 수준 로그온 이름 (DOMAIN\UserName) 또는 UPN 로그온 이름 () 을 사용하여 사용자 포털에 로그인할 수 있습니다. `UserName@Corp.Example.com` 단, IAM Identity Center가 MFA를 통해 활성화된 연결된 디렉터리를 사용하고 있고 검증 모드가 Context-aware 또는 Always-on으로 설정된 경우는 예외입니다. 이 시나리오에서 사용자는 하위 수준의 로그온 이름 (DOMAIN\) 으로 로그인해야 합니다. UserName 자세한 정보는 Identity Center 사용자를 위한 다중 인증을 참조하세요. Active Directory에 로그인하는 데 사용되는 사용자 이름 형식에 대한 일반적인 정보는 Microsoft 설명서 웹 사이트의 사용자 이름 형식을 참조하세요.

IAM 역할을 수정할 때 '보호된 역할에서 작업을 수행할 수 없습니다' 오류가 발생합니다.

계정의 IAM 역할을 검토할 때 역할 이름이 '_'로 시작하는 것을 볼 수 있습니다. AWSReservedSSO 이러한 역할은 IAM Identity Center 서비스가 계정에 생성한 역할로, 계정에 권한 세트를 할당하여 만들어졌습니다. IAM 콘솔 내에서 이러한 역할을 수정하려고 하면 다음 오류가 발생합니다.

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by AWS'
```

이러한 역할은 의 관리 계정에 있는 IAM Identity Center 관리자 콘솔에서만 수정할 수 있습니다. AWS Organizations수정한 후에는 당 변경 사항이 할당된 AWS 계정으로 푸시할 수 있습니다.

디렉터리 사용자는 비밀번호를 재설정할 수 없습니다.

디렉터리 사용자가 비밀번호 분실을 사용하여 비밀번호를 재설정하는 경우? AWS 액세스 포털 로그인 시 옵션을 사용하려면 새 비밀번호가 에 설명된 기본 비밀번호 정책을 준수해야 합니다. IAM Identity Center에서 ID를 관리할 때 암호 요구 사항

사용자가 정책을 준수하는 비밀번호를 입력한 후 오류가 발생하는 `We couldn't update your password` 경우 오류가 AWS CloudTrail 기록되었는지 확인하십시오. 이벤트 기록 콘솔에서 검색하거나 다음 필터를 CloudTrail 사용하여 이 작업을 수행할 수 있습니다.

```
"UpdatePassword"
```

다음과 같은 메시지가 표시되면 지원팀에 문의해야 할 수 있습니다.

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

이 문제의 또 다른 가능한 원인은 사용자 이름 값에 적용된 명명 규칙일 수 있습니다. 명명 규칙은 'surname.givenName'과 같은 특정 패턴을 따라야 합니다. 하지만 일부 사용자 이름은 상당히 길거나 특수 문자를 포함할 수 있으며, 이로 인해 API 직접 호출에서 문자가 누락되어 오류가 발생할 수 있습니다. 동일한 방식으로 테스트 사용자에게 비밀번호 재설정을 시도하여 이 경우가 맞는지 확인할 수 있습니다.

문제가 지속된다면 AWS 지원 센터에 문의하세요.

내 사용자는 권한 집합에서 참조할 수 있지만 할당된 계정이나 애플리케이션에 액세스할 수 없습니다.

이 문제는 외부 ID 제공업체를 통해 자동 프로비저닝을 위해 SCIM(System for Cross-domain Identity Management)을 사용하는 경우 발생할 수 있습니다. 특히, 사용자 또는 사용자가 구성원으로 속했던 그룹을 삭제한 후 ID 공급업체에서 동일한 사용자 이름(사용자의 경우) 또는 이름(그룹)을 사용하여 다시 생성하면 IAM Identity Center에서 새 사용자 또는 그룹에 대한 새 고유 내부 식별자가 만들어집니다. 하지만 IAM Identity Center의 권한 데이터베이스에는 여전히 이전 식별자에 대한 참조가 있기 때문에 사용자 또는 그룹의 이름은 UI에 계속 표시되지만 액세스는 실패합니다. UI가 참조하는 기본 사용자 또는 그룹 ID가 더 이상 존재하지 않기 때문입니다.

이 경우 AWS 계정 액세스를 복원하려면 원래 할당된 위치에서 이전 사용자 또는 그룹의 액세스 권한을 제거한 다음 해당 사용자 또는 그룹에 다시 액세스 권한을 할당하면 됩니다. AWS 계정그러면 새 사용자 또는 그룹의 올바른 식별자로 권한 집합이 업데이트됩니다. 마찬가지로 애플리케이션 액세스를 복원하려면 해당 애플리케이션에 할당된 사용자 목록에서 사용자 또는 그룹의 액세스 권한을 제거한 다음 사용자 또는 그룹을 다시 추가하면 됩니다.

CloudTrail 로그에서 해당 사용자 또는 그룹의 이름을 참조하는 SCIM 동기화 이벤트를 검색하여 오류가 AWS CloudTrail 기록되었는지 확인할 수도 있습니다.

애플리케이션 카탈로그에서 애플리케이션을 올바르게 구성할 수 없음

IAM Identity Center의 애플리케이션 카탈로그에서 애플리케이션을 추가한 경우, 각 서비스 공급자가 자체적으로 상세한 설명서를 제공합니다. 이 정보는 IAM Identity Center 콘솔에서 해당 애플리케이션의 구성 탭에서 확인할 수 있습니다.

서비스 공급업체의 애플리케이션과 IAM Identity Center 간 신뢰 설정과 관련된 문제인 경우, 사용 설명서에서 문제 해결 단계를 참조하세요.

사용자가 외부 ID 공급업체를 통해 로그인하려고 할 때 “예기치 않은 오류가 발생했습니다” 오류가 표시됩니다.

이 오류는 여러 가지 이유로 발생할 수 있지만 일반적인 원인 중 하나는 SAML 요청에 포함된 사용자 정보와 IAM Identity Center의 사용자 정보가 일치하지 않기 때문입니다.

외부 IdP를 ID 소스로 사용할 때 IAM Identity Center 사용자가 성공적으로 로그인하려면 다음 조건을 충족해야 합니다.

- SAML nameID 형식(ID 제공업체에서 구성)은 '이메일'이어야 합니다.
- nameID 값은 올바른 (RFC2822) 형식의 문자열(user@domain.com)이어야 합니다.
- nameID 값은 IAM Identity Center에 있는 기존 사용자의 사용자 이름과 정확히 일치해야 합니다(IAM Identity Center의 이메일 주소가 일치하는지 여부는 중요하지 않으며, 인바운드 일치는 사용자 이름을 기반으로 함).
- SAML 2.0 페더레이션의 IAM Identity Center 구현에서는 ID 제공업체와 IAM Identity Center 간 SAML 응답에서 단 하나의 어설션만 지원합니다. 암호화된 SAML 어설션은 지원하지 않습니다.
- 다음 설명은 IAM Identity Center 계정에서 액세스 제어를 위한 속성가 활성화된 경우에 적용됩니다.
  - SAML 요청에 매핑된 속성 개수는 50개 이하여야 합니다.
  - SAML 요청에는 다중 값 속성이 포함되어서는 안 됩니다.
  - SAML 요청에는 동일한 이름의 속성이 여러 개 포함되어서는 안 됩니다.
  - 이 속성에는 구조화된 XML이 값으로 포함되어서는 안 됩니다.
  - 이름 형식은 일반 형식이 아닌 SAML 지정 형식이어야 합니다.

> **Note**
>
> IAM Identity Center는 SAML 페더레이션을 통해 새 사용자 또는 그룹에 대한 사용자 또는 그룹을 “적시에” 생성하지 않습니다. 즉, IAM Identity Center에 로그인하려면 수동 또는 자동 프로비저닝을 통해 IAM Identity Center에서 사용자를 미리 생성해야 합니다.

이 오류는 ID 제공업체에 구성된 Assertion Consumer Service(ACS) 엔드포인트가 IAM Identity Center 인스턴스에서 제공한 ACS URL과 일치하지 않을 때 발생할 수도 있습니다. 이 두 값이 정확히 일치하는지 확인합니다.

또한 이벤트 이름 P로 AWS CloudTrail 이동하여 필터링하여 외부 ID 제공자 로그인 실패 문제를 추가로 해결할 수 있습니다. ExternalId DirectoryLogin

'액세스 제어 속성을 활성화하지 못했습니다' 오류

이 오류는 ABAC를 활성화하는 사용자에게 액세스 제어를 위한 속성를 활성화하는 데 필요한 `iam:UpdateAssumeRolePolicy` 권한이 없는 경우 발생할 수 있습니다.

MFA에 디바이스를 등록하려고 할 때 '브라우저가 지원되지 않습니다' 메시지가 표시됩니다.

WebAuthn 현재 구글 크롬, 모질라 파이어폭스, 마이크로소프트 엣지, 애플 사파리 웹 브라우저, 윈도우 10 및 안드로이드 플랫폼에서 지원됩니다. macOS 및 iOS 브라우저에서의 플랫폼 인증 WebAuthn 지원 등 일부 지원 구성 요소는 다양할 수 있습니다. 사용자가 지원되지 않는 브라우저 또는 플랫폼에서 WebAuthn 장치를 등록하려고 하면 지원되지 않는 특정 옵션이 회색으로 표시되거나 지원되는 모든 방법이 지원되지 않는다는 오류 메시지가 표시됩니다. 이러한 경우 브라우저/플랫폼 지원에 대한 자세한 내용은 FIDO2: 웹 인증 (WebAuthn) 을 참조하십시오. IAM ID 센터에 대한 자세한 내용은 WebAuthn 을 참조하십시오. FIDO2 인증자

Active Directory “도메인 사용자” 그룹이 IAM Identity Center에 제대로 동기화되지 않습니다.

Active Directory 도메인 사용자 그룹은 AD 사용자 객체의 기본 "기본 그룹"입니다. IAM Identity Center에서는 Active Directory 기본 그룹과 해당 구성원 자격을 읽을 수 없습니다. IAM Identity Center 리소스 또는 애플리케이션에 대한 액세스 권한을 할당할 때는 그룹 구성원 자격이 IAM Identity Center ID 저장소에 제대로 반영되도록 도메인 사용자 그룹 이외의 그룹(또는 기본 그룹으로 할당된 다른 그룹)을 사용합니다.

잘못된 MFA 보안 인증 오류

이 오류는 사용자가 SCIM 프로토콜을 사용하여 계정이 IAM Identity Center에 완전히 프로비저닝되기 전에 외부 ID 제공업체(예: Okta 또는Microsoft Entra ID)의 계정을 사용하여 IAM Identity Center에 로그인을 시도할 때 발생할 수 있습니다. 사용자 계정을 IAM Identity Center에 프로비저닝한 후에는 이 문제를 해결해야 합니다. 계정이 IAM Identity Center에 프로비저닝되었는지 확인합니다. 그렇지 않은 경우 외부 ID 제공업체의 프로비저닝 로그를 확인합니다.

인증 앱으로 등록하거나 로그인하려고 시도하면 '예상치 못한 오류가 발생했습니다'라는 메시지가 나타납니다.

IAM Identity Center가 코드 기반 인증 앱과 함께 사용하는 것과 같은 시간 기반 일회용 암호(TOTP) 시스템은 클라이언트와 서버 간의 시간 동기화에 의존합니다. 인증 앱이 설치된 디바이스가 신뢰할 수 있는 시간 출처와 올바르게 동기화되었는지 확인하거나, NIST(https://www.time.gov/) 또는 기타 지역/리전별 등가물과 같은 신뢰할 수 있는 출처와 일치하도록 디바이스의 시간을 수동으로 설정하세요.

IAM ID 센터에 로그인하려고 하면 '당신이 아니에요, 우리예요. '라는 오류 메시지가 나타납니다.

이 오류는 IAM ID 센터의 인스턴스 또는 IAM ID 센터가 ID 소스로 사용하는 외부 ID 공급자 (IdP) 의 인스턴스에 설정 문제가 있음을 나타냅니다. 다음 사항을 확인하는 것이 좋습니다.

- 로그인하는 데 사용하는 장치의 날짜 및 시간 설정을 확인합니다. 날짜와 시간이 자동으로 설정되도록 설정하는 것이 좋습니다. 이를 사용할 수 없는 경우 알려진 네트워크 시간 프로토콜 (NTP) 서버에 날짜 및 시간을 동기화하는 것이 좋습니다.
- IAM ID 센터에 업로드한 IdP 인증서가 IdP에서 제공한 것과 동일한지 확인하십시오. 설정으로 이동하여 IAM ID 센터 콘솔에서 인증서를 확인할 수 있습니다. ID 소스 탭에서 작업을 선택한 다음 인증 관리를 선택합니다. IdP와 IAM ID 센터 인증서가 일치하지 않는 경우 새 인증서를 IAM ID 센터로 가져오십시오.
- ID 제공자의 메타데이터 파일에 있는 NameID 형식이 다음과 같은지 확인하십시오.
  - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- ID AWS Directory Service 공급자로 AD Connector를 사용하는 경우 서비스 계정의 자격 증명이 정확하고 만료되지 않았는지 확인하십시오. 자세한 AWS Directory Service내용은 에서 AD Connector 서비스 계정 자격 증명 업데이트를 참조하십시오.

내 사용자가 IAM Identity Center로부터 이메일을 받지 못하고 있습니다.

IAM Identity Center 서비스에서 보내는 모든 이메일은 주소 `no-reply@signin.aws` 또는 `no-reply@login.awsapps.com` 에서 발송됩니다. 메일 시스템은 이러한 발신자 이메일 주소에서 오는 이메일을 수락하고 정크 또는 스팸으로 처리하지 않도록 구성해야 합니다.

오류: 관리 계정에 프로비저닝된 권한 집합에 대한 액세스 권한을 삭제/수정/제거/할당할 수 없습니다.

이 메시지는 해당 위임된 관리 기능이 활성화되었으며 관리 계정 권한이 있는 사람만 이전에 시도한 작업을 성공적으로 수행할 수 있음을 나타냅니다. AWS Organizations이 문제를 해결하려면 이러한 권한이 있는 사용자로 로그인하여 작업을 다시 수행하거나 올바른 권한을 가진 사람에게 이 작업을 할당하십시오. 자세한 정보는 멤버 계정 등록을 참조하세요.

오류: 세션 토큰을 찾을 수 없거나 유효하지 않습니다.

이 오류는 웹 브라우저 AWS Toolkit AWS CLI, 또는 같은 클라이언트가 서버 측에서 취소되거나 무효화된 세션을 사용하려고 할 때 발생할 수 있습니다. 이 문제를 해결하려면 클라이언트 응용 프로그램이나 웹 사이트로 돌아가서 다시 시도하십시오. 이때 메시지가 표시되면 다시 로그인하십시오. 이로 인해 IDE AWS Toolkit 내에서 보류 중인 연결 시도와 같이 보류 중인 요청도 취소해야 할 수도 있습니다.

문서 이력

다음 표에서는 설명서에 추가된 중요한 내용을 설명합니다. AWS IAM Identity Center 사용자로부터 받은 의견을 수렴하기 위해 설명서가 자주 업데이트됩니다.

- 최종 주요 설명서 업데이트: 2022년 9월 23일

변경 사항	설명	날짜
AWS 관리형 정책 업데이트	`AWSIAMIdentityCenterAllowListForIdentityContext` AWS 관리형 정책의 권한이 업데이트되었습니다.	2024년 5월 17일
AWS 관리형 정책 업데이트	`AWSIAMIdentityCenterAllowListForIdentityContext` AWS 관리형 정책의 권한이 업데이트되었습니다.	2024년 4월 30일
AWS 관리형 정책 업데이트	`AWSSSOMasterAccountAdministrator` AWS 관리형 정책의 권한이 업데이트되었습니다.	2024년 4월 26일
AWS 관리형 정책 업데이트	`AWSSSOMemberAccountAdministrator` AWS 관리형 정책의 권한이 업데이트되었습니다.	2024년 4월 26일
AWS 관리형 정책 업데이트	`AWSSSOReadOnly` AWS 관리형 정책의 권한이 업데이트되었습니다.	2024년 4월 26일
AWS 관리형 정책 업데이트	`AWSIAMIdentityCenterAllowListForIden`	2024년 4월 26일

	tityContext AWS 관리형 정책의 권한이 업데이트되었습니다.	
AWS 관리형 정책 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책의 권한이 업데이트되었습니다.	2024년 4월 24일
AWS 관리형 정책 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책의 권한이 업데이트되었습니다.	2024년 4월 19일
AWS 관리형 정책 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책의 권한이 업데이트되었습니다.	2024년 4월 11일
AWS 관리형 정책 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책의 권한이 업데이트되었습니다.	2023년 11월 26일
새 AWS 관리형 정책 주제	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 세부 정보가 추가되었습니다.	2023년 11월 15일
IAM Identity Center 시작하기에 대한 지침 개선	IAM Identity Center 시작 및 관리 사용자 생성에 대한 새로운 내용이 추가되었습니다.	2022년 9월 23일

Identity Center API 참조의 사용자 및 그룹이 업데이트됨	이 업데이트에는 Identity Center API 참조 가이드의 새로운 생성, 업데이트 및 API 삭제에 대한 참고 사항이 포함되어 있습니다.	2022년 8월 31일
AWS 싱글 사인온 (AWS SSO)이 IAM ID 센터로 이름이 변경되었습니다. AWS	AWS 소개. AWS IAM Identity Center IAM Identity Center는 AWS Identity and Access Management (IAM) 의 기능을 확장하여 직원 사용자의 계정 및 애플리케이션 액세스를 중앙에서 관리할 수 있도록 지원합니다. IAM Identity Center 기능에는 애플리케이션 할당, 다중 계정 권한 및 AWS 액세스 포털이 포함됩니다.	2022년 7월 26일
권한 세트의 권한 경계 및 고객 관리형 정책 지원	권한 집합과 함께 AWS 관리형 및 고객 관리형 AWS Identity and Access Management (IAM) 정책을 사용하기 위한 콘텐츠가 추가되었습니다.	2022년 7월 14일
수동 활성화 AWS 지역 지원	수동으로 활성화된 리전에서 IAM Identity Center 사용에 대한 내용이 추가되었습니다.	2022년 6월 15일
AWS 관리형 정책 업데이트	`AWSSSOServiceRolePolicy` AWS 관리형 정책의 권한이 업데이트되었습니다.	2022년 5월 11일
위임된 관리 지원	위임된 관리 기능에 대한 내용이 추가되었습니다.	2022년 5월 11일

AWS 관리형 정책 업데이트	`AWSSSOMasterAccountAdministrator` `AWSSSOMemberAccountAdministrator` , 및 `AWSSSOReadOnly` AWS 관리형 정책에 대한 권한이 업데이트되었습니다.	2022년 4월 28일
구성 가능한 AD 동기화 지원	구성 가능한 AD 동기화 기능에 대한 내용이 추가되었습니다.	2022년 4월 14일
새 AWS 관리형 정책 주제	`AWSSSOMasterAccountAdministrator` AWS 관리형 정책에 대한 세부 정보가 추가되었습니다.	2021년 8월 4일
할당량 업데이트	할당량 테이블 조정.	2020년 12월 21일
새로운 예시 정책	새로운 고객 관리형 정책 예시를 추가하고 권한 필요 섹션을 업데이트했습니다.	2020년 12월 21일
ABAC(속성 기반 액세스 제어) 지원	ABAC 기능에 대한 내용이 추가되었습니다.	2020년 11월 24일
MFA 강제 등록 지원	사용자가 로그인할 때 MFA 장치 등록을 요구하도록 업데이트되었습니다.	2020년 11월 23일
에 대한 지원 WebAuthn	새 WebAuthn 기능에 대한 내용이 추가되었습니다.	2020년 11월 20일
Ping Identity 지원	지원되는 외부 ID 제공업체로 Ping Identity 제품과 통합에 대한 내용이 추가되었습니다.	2020년 10월 26일

에 대한 지원 OneLogin	지원되는 외부 ID 제공업체로 OneLogin과 통합에 대한 내용이 추가되었습니다.	2020년 7월 31일
Okta 지원	지원되는 외부 ID 제공업체로 Okta과 통합에 대한 내용이 추가되었습니다.	2020년 5월 28일
외부 ID 제공업체 지원	디렉토리에서 ID 소스로 참조를 변경하고 외부 ID 제공업체 지원에 대한 내용이 추가되었습니다.	2019년 11월 26일
새 MFA 설정	2단계 인증 항목을 제거하고 그 자리에 새 MFA 항목을 추가했습니다.	2019년 10월 24일
2단계 인증을 추가하기 위한 새로운 설정	사용자를 위한 2단계 인증을 활성화하는 방법에 대한 내용이 추가되었습니다.	2019년 1월 16일
AWS 계정 세션 지속 시간 지원	AWS 계정의 세션 기간을 설정하는 방법에 대한 내용이 추가되었습니다.	2018년 10월 30일
Identity Center 디렉터리를 사용할 수 있는 새 옵션	Identity Center 디렉터리를 선택하거나 Active Directory의 기존 디렉터리에 연결하는 데 대한 내용이 추가되었습니다.	2018년 10월 17일
애플리케이션의 릴레이 상태 및 세션 기간 지원	애플리케이션의 릴레이 상태 및 세션 기간에 대한 내용이 추가되었습니다.	2018년 10월 10일

새 애플리케이션에 대한 추가 지원	4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvaInSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, 및 UserEcho가 애플리케이션 카탈로그에 추가되었습니다.	2018년 8월 3일
관리 계정에 대한 다중 계정 액세스 지원	관리 계정의 사용자에게 다중 계정 액세스를 위임하는 방법에 대한 내용이 추가되었습니다.	2018년 7월 9일
새 애플리케이션 지원	DocuSign, Keeper Security, 및 SugarCRM가 애플리케이션 카탈로그에 추가되었습니다.	2018년 3월 16일
CLI 액세스를 위한 임시 보안 인증 정보 가져오기	AWS CLI 명령을 실행하기 위한 임시 자격 증명을 가져오는 방법에 대한 정보가 추가되었습니다.	2018년 2월 22일
새 안내서	이 설명서는 IAM Identity Center 사용 설명서의 첫 번째 릴리스입니다.	2017년 12월 7일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 AWS 용어집을 참조하세요.

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