



Add a permission의

AWS IAM Identity Center



AWS IAM Identity Center: Add a permission의

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

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

Table of Contents

IAM Identity Center란 무엇인가요?	1
IAM Identity Center를 사용하는 이유는 무엇입니까?	1
IAM Identity Center 이름 변경	3
기존 네임스페이스는 동일하게 유지	3
시작하기	4
IAM Identity Center 전제 조건 및 고려 사항	5
AWS 리전선택	7
애플리케이션에만 IAM Identity Center 사용	13
IAM Identity Center에서 생성한 IAM 역할	13
IAM Identity Center 및 AWS Organizations	14
IAM Identity Center 인스턴스	15
AWS 계정 IAM Identity Center를 활성화할 수 있는 유형	15
IAM Identity Center의 조직 인스턴스 관리	17
IAM Identity Center의 계정 인스턴스	18
IAM Identity Center 인스턴스 삭제	22
IAM Identity Center 활성화	24
IAM Identity Center의 인스턴스 활성화	25
ID 소스 확인	27
방화벽 및 게이트웨이 업데이트	29
도메인 및 URL 엔드포인트 허용 목록에 대한 고려 사항	32
ID 소스 자습서	33
Active Directory	34
CyberArk	36
사전 조건	37
SCIM 고려 사항	37
1단계: IAM Identity Center 프로비저닝 활성화	38
2단계: CyberArk에서 프로비저닝 구성	39
(선택 사항) 3단계: IAM Identity Center에서 액세스 제어(ABAC)에 사용되는 CyberArk 사용자 속성 구성	39
(선택 사항) 액세스 제어에 속성 전달	40
Google Workspace	41
고려 사항	42
1단계: Google Workspace: SAML 애플리케이션 구성	42

2단계: IAM Identity Center 및 Google Workspace: IAM Identity Center ID 소스를 변경하고 Google Workspace를 SAML ID 제공업체로 설정합니다.	43
3단계: Google Workspace: 앱 활성화	44
4단계: IAM Identity Center: IAM Identity Center 자동 프로비저닝 설정	45
5단계: Google Workspace에서 자동 프로비저닝 구성	46
액세스 제어에 속성 전달-선택 사항	47
에 액세스 권한 할당 AWS 계정	48
다음 단계	50
문제 해결	51
JumpCloud	51
사전 조건	52
SCIM 고려 사항	52
1단계: IAM Identity Center 프로비저닝 활성화	53
2단계: JumpCloud에서 프로비저닝 구성	53
(선택 사항) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 JumpCloud 사용자 속성 구성	54
(선택 사항) 액세스 제어에 속성 전달	55
Microsoft Entra ID	56
사전 조건	56
고려 사항	56
1단계: Microsoft 테넌트 준비	58
2단계: AWS 계정 준비	60
3단계: SAML 연결 구성 및 테스트	62
4단계: SCIM 동기화 구성 및 테스트	66
5단계: ABAC 구성-선택 사항	70
에 액세스 권한 할당 AWS 계정	71
Microsoft Entra ID 추가 리전에 액세스하기 위한 구성	73
문제 해결	74
Okta	76
고려 사항	77
1단계: Okta: Okta 계정에서 SAML 메타데이터 획득	78
2단계: Okta를 IAM Identity Center의 ID 소스로 구성	78
3단계: IAM Identity Center 및 Okta: Okta 사용자 프로비저닝	80
4단계: Okta: Okta의 사용자를 IAM Identity Center와 동기화	81
액세스 제어에 속성 전달-선택 사항	82
에 액세스 권한 할당 AWS 계정	83

Okta 추가 리전에 액세스하기 위한 구성	85
다음 단계	85
문제 해결	86
OneLogin	88
사전 조건	89
1단계: IAM Identity Center 프로비저닝 활성화	89
2단계: OneLogin에서 프로비저닝 구성	90
(선택 사항) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 OneLogin 사용자 속성 구성	91
(선택 사항) 액세스 제어에 속성 전달	92
문제 해결	92
Ping Identity	93
PingFederate	93
PingOne	100
Identity Center 디렉터리	106
자습서 비디오	111
인력 설정	112
사용자, 그룹 및 프로비저닝	112
사용자 이름 및 이메일 주소 고유성	112
그룹	112
사용자 및 그룹 프로비저닝	113
사용자 및 그룹 프로비저닝	113
ID 소스 관리	113
ID 소스 변경 시 고려 사항	114
ID 소스 변경	119
IAM Identity Center의 사용자 및 그룹 속성	120
외부 ID 제공업체	122
Microsoft AD 디렉터리	138
Identity Center 디렉터리에서 사용자 관리	156
IAM Identity Center에서의 프로비저닝	157
ID 소스 변경	157
사용자 추가	157
그룹 추가	160
그룹에 사용자 추가	161
그룹 삭제	162
사용자 삭제	163

그룹에서 사용자 제거	164
사용자 속성 편집	165
인력 액세스	167
인증 세션 이해	167
인증 세션 유형	168
사용자 세션을 종료하는 방법	169
관리자가 세션을 종료하는 경우 사용자 액세스는 어떻게 되나요?	170
단일 로그아웃	172
세션 관리 모범 사례	172
세션 지속 시간 구성	173
사용자 대화형 세션	173
사용자 백그라운드 세션	174
Kiro에 대한 확장 세션	175
직원 사용자의 활성 세션 종료	176
자격 증명 소스, AWS CLI 및 AWS SDKs에 대한 고려 사항	178
사용자 액세스 비활성화	181
사용자 액세스 거부	182
IAM Identity Center 디렉터리에서 사용자에게 대한 액세스 관리	183
암호 관리	183
MFA	184
사용자 암호 설정	184
다중 인증	187
애플리케이션 액세스	200
AWS 관리형 애플리케이션	200
애플리케이션에 대한 액세스 제어	201
ID 정보 공유	202
AWS 관리형 애플리케이션 사용 제한	203
IAM Identity Center와 함께 사용할 수 있는 애플리케이션	204
AWS 관리형 애플리케이션을 테스트하도록 IAM Identity Center 설정	207
애플리케이션 세부 정보 확인 및 변경	213
AWS 관리형 애플리케이션 비활성화	213
ID 강화 콘솔 세션 활성화	214
고객 관리형 애플리케이션	217
SAML 2.0 및 OAuth 2.0 애플리케이션	218
SAML 2.0 애플리케이션 설정	223
신뢰할 수 있는 ID 전파	226

신뢰할 수 있는 ID 전파의 이점	227
신뢰할 수 있는 ID 전파 활성화	227
신뢰할 수 있는 ID 전파의 작동 방식	227
필수 조건 및 고려 사항	229
사용 사례	230
권한 부여 서비스	255
자체 OAuth 2.0 애플리케이션 설정	265
고객 관리형 애플리케이션 설정	266
신뢰할 수 있는 애플리케이션 지정	269
신뢰할 수 있는 토큰 발급자	270
인증서 교체	284
인증서 교체 전 고려 사항	284
IAM Identity Center 인증서 교체	285
인증서 만료 상태 표시	287
애플리케이션 속성 이해	287
애플리케이션 시작 URL	287
릴레이 상태	288
세션 지속 시간	289
애플리케이션에 사용자 액세스 권한 할당	289
애플리케이션에서 사용자 액세스 제거	291
속성 매핑	291
AWS 계정 액세스	293
AWS 계정 유형	293
AWS 계정 액세스 할당	295
최종 사용자 경험	295
액세스 적용 및 제한	296
액세스 위임 및 적용	296
멤버 계정에서 ID 스토어에 액세스하는 것을 제한합니다.	296
위임된 관리	297
모범 사례	298
사전 조건	302
멤버 계정 등록	302
멤버 계정 해지	303
위임된 관리자 계정 보기	304
임시 권한 상승	305
에 대한 Single Sign-On 액세스 AWS 계정	305

에 사용자 또는 그룹 액세스 할당 AWS 계정	306
에 대한 사용자 및 그룹 액세스 제거 AWS 계정	309
활성 권한 세트 세션 취소	309
Single Sign-On 액세스를 할당할 수 있는 대리인	311
권한 세트	312
최소 권한을 적용하는 권한 세트 생성	313
사전 정의된 권한	315
사용자 지정 권한	315
권한 세트 생성, 관리 및 삭제	318
권한 집합 속성을 구성합니다.	329
권한 세트 참조	335
액세스 중단 방지를 위한 권장 사항	337
사용자 지정 신뢰 정책 예	338
속성 기반 액세스 제어	339
이점	339
체크리스트: IAM Identity Center AWS 를 사용하여에서 ABAC 구성	340
액세스 제어를 위한 속성	342
서비스 연결 역할	348
AWS 액세스 포털	350
AWS 액세스 포털 시작하기	350
AWS 액세스 포털 구성	351
구성할 수 있는 항목	351
AWS 액세스 포털 활성화	351
AWS 액세스 포털 URL 사용자 지정	352
사용자가 AWS 액세스 포털에 로그인할 수 있는지 확인	353
AWS 액세스 포털 사용	354
AWS 액세스 포털 사용 방법	354
AWS 액세스 포털에 로그인	355
사용자 암호 재설정	357
AWS CLI 및 AWS SDK 액세스	358
바로가기 링크 생성	363
MFA를 위한 디바이스 등록	366
활성 세션 종료	368
여러에서 IAM Identity Center 사용 AWS 리전	369
다중 리전 지원의 이점	369
필수 조건 및 고려 사항	369

추가 리전 선택	370
IAM Identity Center를 추가 리전에 복제	371
1단계: 복제본 키 생성	371
2단계: 리전 추가	371
3단계: 외부 IdP 설정 업데이트	372
4단계: 방화벽 및 게이트웨이 허용 목록 확인	373
5단계: 사용자에게 정보 제공	373
첫 번째 리전 추가 이후 리전 변경	373
복제되는 데이터는 무엇입니까?	373
추가 리전을 통한 인력 액세스	375
여러의 사용자 세션 AWS 리전	375
AWS 기본 및 추가의 포털 엔드포인트에 액세스 AWS 리전	375
기본 및 추가의 ACS 엔드포인트 AWS 리전	377
여러 ACS URLs 없이 AWS 관리형 애플리케이션 사용	378
AWS 계정 액세스를 위해 추가 리전으로 장애 조치	379
AWS 계정 여러 ACS URLs 없이 복원력에 액세스	379
여러에 애플리케이션 배포 및 관리 AWS 리전	380
여러에 관리형 AWS 애플리케이션 배포 및 관리 AWS 리전	380
여러 AWS 리전에 걸쳐 고객 관리형 애플리케이션 배포 및 관리	382
IAM Identity Center에서 리전 제거	382
1단계: 외부 IdP 구성 업데이트	382
2단계: 리전 제거	382
3단계: 복제본 키 삭제	384
추가에서 지원되는 서비스 APIs AWS 리전	384
기본 및 추가 리전의 CloudTrail 이벤트	384
기본 및 추가 리전의 IAM Identity Center 사용 사례	385
복원력 설계 및 리전 동작	387
가용성을 위한 설계	388
에 대한 긴급 액세스 설정 AWS Management Console	388
비상 액세스 구성 요약	389
중요 운영 역할을 설계하는 방법	390
액세스 모델을 계획하는 방법	391
비상 역할, 계정 및 그룹 매핑을 설계하는 방법	391
비상 액세스 구성을 만드는 방법	392
비상 상황 대비 작업	393
비상 장애 조치 프로세스	394

정상 작동 상태로 복귀합니다.	394
Okta에서 직접 IAM 페더레이션 애플리케이션을 한 번만 설정하면 됩니다.	394
를 사용하여 직접 IAM 페더레이션 애플리케이션의 일회성 설정 ADFS	398
보안	404
IAM Identity Center ID 및 액세스 관리	405
Authentication	405
액세스 관리	405
액세스 관리 개요	406
ID 기반 정책 예시	410
리소스 기반 정책 예시	418
AWS 관리형 정책	420
서비스 연결 역할 사용	438
IAM Identity Center 콘솔 및 API 인증	445
2023년 11월 이후의 API 작업	445
2020년 10월 이후의 API 작업	446
AWS STS IAM Identity Center에 사용되는 조건 키	448
UserId	449
IdentityStoreArn	450
ApplicationArn	450
자격 증명Id	450
InstanceArn	451
로그 및 모니터링	451
를 사용하여 IAM Identity Center API 호출 로깅 AWS CloudTrail	451
AWS CloudTrail을 사용하여 IAM Identity Center SCIM 로깅	489
Amazon EventBridge	496
구성 가능한 AD 동기화 오류 로깅	496
규정 준수 확인	499
지원되는 규정 준수 표준	500
복원력	501
인프라 보안	502
데이터 보호	503
전송 중 암호화	503
데이터 개인정보보호	503
데이터 보존	504
저장 시 암호화	504
IAM Identity Center 암호화 컨텍스트	505

암호화 컨텍스트를 사용하여 고객 관리형 키에 대한 액세스 제어	506
IAM Identity Center에 대한 암호화 키 모니터링	506
AWS 관리형 애플리케이션의 IAM Identity Center ID 속성 스토리지, 암호화 및 삭제	507
고객 관리형 KMS 키 구현	507
기본 KMS 키 및 IAM 정책 설명	516
고급 KMS 키 정책 설명	537
리소스에 태그 지정	546
태그 제한 사항	547
콘솔을 통한 태그 관리	547
AWS CLI 예제	548
태그 할당	548
태그 보기	549
태그 제거	549
권한 세트를 생성할 때 태그 적용	549
API 작업	550
AWS CLI와 IAM Identity Center 통합	551
AWS CLI를 IAM Identity Center와 통합하는 방법	551
프라이빗 액세스 고려 사항	552
할당량	553
애플리케이션 할당량	553
AWS 계정 할당량	553
Active Directory 할당량	554
IAM Identity Center ID 스토어 할당량	555
IAM Identity Center 스토어 제한	555
OIDC 서비스 요청 할당량	556
추가 할당량	557
문제 해결	559
IAM Identity Center의 계정 인스턴스 생성 문제	559
IAM Identity Center에서 사용하도록 사전 구성된 클라우드 애플리케이션 목록을 보려고 하면 오류가 발생합니다.	559
IAM Identity Center에서 생성된 SAML 어설션 콘텐츠 관련 문제	560
특정 사용자가 외부 SCIM 공급자로부터 IAM Identity Center로 동기화하지 못함	561
외부 ID 제공업체에서 사용자 또는 그룹을 프로비저닝할 때의 중복 사용자 또는 그룹 오류	562
사용자 이름이 UPN 형식인 경우 사용자는 로그인할 수 없습니다.	563
IAM 역할을 수정할 때 '보호된 역할에서 작업을 수행할 수 없습니다' 오류가 발생합니다.	564
디렉터리 사용자는 비밀번호를 재설정할 수 없습니다.	564

내 사용자는 권한 집합에서 참조할 수 있지만 할당된 계정이나 애플리케이션에 액세스할 수 없습니다.	565
애플리케이션 카탈로그에서 애플리케이션을 올바르게 구성할 수 없습니다.	565
사용자가 외부 ID 공급업체를 통해 로그인하려고 할 때 “예기치 않은 오류가 발생했습니다” 오류가 표시됩니다.	565
'액세스 제어 속성을 활성화하지 못했습니다' 오류	566
MFA에 디바이스를 등록하려고 할 때 '브라우저가 지원되지 않습니다' 메시지가 표시됩니다.	567
Active Directory “도메인 사용자” 그룹이 IAM Identity Center에 제대로 동기화되지 않습니다.	567
잘못된 MFA 보안 인증 오류	567
인증 앱으로 등록하거나 로그인하려고 시도하면 '예상치 못한 오류가 발생했습니다'라는 메시지가 나타납니다.	567
IAM Identity Center에 로그인하려고 시도할 때 "사용자가 아닌 우리 쪽에서 문제가 발생했습니다"라는 오류가 표시됩니다.	568
내 사용자가 IAM Identity Center로부터 이메일을 받지 못하고 있습니다.	568
오류: 관리 계정에 프로비저닝된 권한 세트에 대한 액세스 권한을 삭제/수정/제거/할당할 수 없습니다.	568
오류: 세션 토큰을 찾을 수 없거나 세션 토큰이 유효하지 않습니다	569
신뢰할 수 있는 도메인의 그룹 멤버가 IAM Identity Center와 동기화되지 않음	569
에서 고객 관리형 키 문제 해결 AWS IAM Identity Center	569
액세스 거부됨: KMS 복호화 권한 문제	569
AWS IAM Identity Center에서 고객 관리형 KMS 키가 활성화된 관리형 애플리케이션 로그인 실패	570
AWS IAM Identity Center에서 고객 관리형 KMS 키가 활성화된 관리형 애플리케이션 설치 및/또는 사용자 할당 실패	570
KMS 권한 문제를 사용하여 고객 관리형 키 구성 AWS IAM Identity Center	571
AWS IAM Identity Center에서 고객 관리형 KMS 키가 활성화된 상태에서 액세스 포털 로그인 실패	571
의 다중 리전 설정 문제 해결 AWS IAM Identity Center	571
IAM Identity Center 인스턴스를 복제하려는 리전은 IAM Identity Center 콘솔에서 사용할 수 없습니다.	571
AWS 추가 리전의 관리형 애플리케이션 로그인 실패	572
문서 이력	573
AWS 용어집	583
.....	dlxxxiv

IAM Identity Center란 무엇인가요?

AWS IAM Identity Center 는 인력 사용자를 Kiro 및 Amazon Quick과 같은 AWS 관리형 애플리케이션과 기타 AWS 리소스에 연결하는 AWS 솔루션입니다. 기존 ID 제공업체를 연결하고 디렉터리에서 사용자와 그룹을 동기화하거나 IAM Identity Center에서 직접 사용자를 생성하고 관리할 수 있습니다. 또 다음 중 하나 또는 둘 모두에 IAM Identity Center를 사용할 수 있습니다.

- 애플리케이션에 대한 사용자 액세스
- 에 대한 사용자 액세스 AWS 계정

에 액세스하기 위해 이미 IAM을 사용하고 있습니까 AWS 계정?

AWS 관리형 애플리케이션에 액세스하기 위해 IAM Identity Center를 사용하기 위해 현재 AWS 계정 워크플로를 변경할 필요가 없습니다. AWS 계정 액세스를 위해 [IAM과 페더레이션](#)을 사용하는 경우 사용자는 항상 가지고 있는 것과 동일한 방식으로 AWS 계정에 계속 액세스할 수 있으며 기존 워크플로를 계속 사용하여 해당 액세스를 관리할 수 있습니다.

IAM Identity Center를 사용하는 이유는 무엇입니까?

IAM Identity Center는 다음과 같은 주요 기능을 통해 애플리케이션 또는 AWS 계정들 다에 대한 인력 사용자 액세스를 간소화하고 단순화합니다.

AWS 관리형 애플리케이션과의 통합

Kiro 및와 같은 [AWS 관리형 애플리케이션](#)은 IAM Identity Center와 Amazon Redshift 통합됩니다. IAM Identity Center는 AWS 관리형 애플리케이션에 사용자 및 그룹에 대한 공통 보기를 제공합니다.

애플리케이션 간 신뢰할 수 있는 ID 전파

신뢰할 수 있는 자격 증명 전파를 통해 Amazon Quick과 같은 AWS 관리형 애플리케이션은 사용자의 자격 증명들과 같은 다른 AWS 관리형 애플리케이션 Amazon Redshift 과 안전하게 공유하고 사용자의 자격 증명을 기반으로 AWS 리소스에 대한 액세스를 승인할 수 있습니다. 사용자 및 사용자가 개시한 활동을 기반으로 CloudTrail 이벤트 로그가 기록되므로 사용자 활동을 더 쉽게 감사할 수 있습니다. 이를 통해 누가 무엇을 액세스했는지 더 쉽게 파악할 수 있습니다. 엔드 투 엔드 구성 지침 등 지원되는 사용 사례에 대해서는 [신뢰할 수 있는 ID 전파 사용 사례](#)를 참조하세요.

하나의 플레이스에서 여러 AWS 계정에 권한 할당

IAM Identity Center의 다중 계정 권한을 통해 하나의 플레이스에서 여러 AWS 계정의 사용자 그룹에 권한을 할당할 수 있습니다. 일반적인 직무를 기반으로 권한을 생성하거나 보안 요구 사항에 맞는 사용자 지정 권한을 정의할 수 있습니다. 그런 다음 작업 인력 사용자에게 이러한 권한을 할당하여 특정에 대한 액세스를 제어할 수 있습니다 AWS 계정.

이러한 선택 기능은 IAM Identity Center의 [조직 인스턴스](#)에만 사용할 수 있습니다.

한 페더레이션 포인트를 통해 AWS에 대한 사용자 액세스 간소화

IAM Identity Center는 하나의 페더레이션 지점을 제공하여 여러 AWS 관리형 애플리케이션 및를 사용하는 데 필요한 관리 작업을 줄입니다 AWS 계정. IAM Identity Center를 통해 [SAML 2.0 ID](#) 제공업체 사용 시 단 한 번의 페더레이션과 단 하나의 인증서로 관리할 수 있습니다. IAM Identity Center는 신뢰할 수 있는 자격 증명 전파 사용 사례 또는 사용자가 리소스에 AWS 대한 액세스를 다른 사람과 공유할 때 사용자 및 그룹에 대한 공통 보기를 AWS 관리형 애플리케이션에 제공합니다.

IAM Identity Center에서 작동하는 일반적으로 사용되는 ID 제공업체 구성 방법에 대해서는 [IAM Identity Center의 ID 소스 자습서](#)를 참조하세요. 기존 ID 제공업체가 없는 경우 [IAM Identity Center에서 직접 사용자를 생성하고 관리](#)할 수 있습니다.

두 가지 인스턴스 유형

IAM Identity Center는 조직 인스턴스와 계정 인스턴스라는 두 가지 유형의 인스턴스를 지원합니다. 조직 인스턴스가 모범 사례입니다. 에 대한 액세스를 관리할 수 있는 유일한 인스턴스 AWS 계정이며 애플리케이션의 모든 프로덕션 사용에 권장됩니다. 조직 인스턴스는 AWS Organizations 관리 계정에 배포되며 사용자 액세스를 관리할 단일 지점을 제공합니다 AWS.

계정 인스턴스는 활성화된 AWS 계정 에 바인딩됩니다. IAM Identity Center의 계정 인스턴스는 일부 AWS 관리형 애플리케이션의 격리된 배포를 지원하는 경우에만 사용합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

사용자를 위한 사용자 친화적 웹 포털 액세스

AWS 액세스 포털은 사용자에게 할당된 모든 애플리케이션 AWS 계정또는 둘 다에 대한 원활한 액세스를 제공하는 사용자 친화적인 웹 포털입니다.

AWS 계정 및 애플리케이션에 대한 다중 리전 액세스

IAM Identity Center 인스턴스를 추가 리전에 복제하면 작업 인력은 활성화된 모든 리전을 통해 할당된 AWS 계정 및 애플리케이션에 액세스하고 활성화된 각 리전에 AWS 관리형 애플리케이션을 배포할 수 있습니다.

IAM Identity Center 이름 변경

2022년 7월 26일에 AWS Single Sign-On의 이름이 로 변경되었습니다 AWS IAM Identity Center.

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 identitystore를 포함하는 [서비스 엔드포인트](#)
- AWS::SSO 접두사를 포함하는 [CloudFormation](#) 리소스
- AWSServiceRoleForSSO를 포함하는 [서비스 연결 역할](#)
- sso 및 singlessignon를 포함하는 콘솔 URL
- singlessignon를 포함하는 설명서 URL

IAM Identity Center 시작하기

다음에서는 IAM Identity Center를 시작하는 방법을 간략하게 설명합니다.

1. IAM Identity Center 활성화

[IAM Identity Center를 활성화](#)하면 두 가지 유형의 IAM Identity Center 인스턴스 중에서 선택할 수 있습니다. 조직 [인스턴스](#)(권장) 및 [계정 인스턴스](#) 유형입니다. 이러한 인스턴스 유형의 다양한 기능에 대한 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#)를 참조하세요.

Note

IAM Identity Center가 활성화된 후 다음 중 하나를 수행하여 [IAM Identity Center 콘솔](#)에 로그인하고 열 수 있습니다.

- 조직 인스턴스 - 관리 계정의 관리 권한이 있는 자격 증명을 AWS 사용하여 로그인합니다.
- 계정 인스턴스 - IAM Identity Center AWS 계정 가 활성화된에서 관리 권한이 있는 자격 증명을 AWS 사용하여 로그인합니다.

2. IAM Identity Center에 자격 증명 소스 연결

IAM Identity Center 콘솔에서 사용하려는 자격 증명 소스를 확인합니다. 자격 증명 소스는 다음을 참조하세요.

- 외부 자격 증명 공급자 - 인력 사용자를 관리할 기존 자격 증명 공급자가 있는 경우 IAM Identity Center에 연결할 수 있습니다. IAM Identity Center에서 작동하는 일반적으로 사용되는 자격 증명 공급자 구성 방법에 대해서는 [IAM Identity Center의 ID 소스 자습서](#) 섹션을 참조하세요.
- Active Directory - Active Directory를 사용하여 인력 사용자를 관리하는 경우 IAM Identity Center에 연결할 수 있습니다. 자세한 내용은 [Active Directory를 ID 소스로 사용](#) 단원을 참조하십시오.
- IAM Identity Center - 또는 [IAM Identity Center에서 사용자 및 그룹을 직접 생성하고 관리](#)할 수 있습니다.

Note

현재 IAM Identity Center에서 다중 리전 설정을 활용하려면 외부 자격 증명 공급자를 자격 증명 소스로 사용해야 합니다. 이 설정의 이점에 대한 자세한 내용은 [여러에서 IAM Identity Center 사용 AWS 리전](#).

3. 에 대한 사용자 액세스 설정 AWS 계정 (조직 인스턴스만 해당)

IAM Identity Center의 조직 인스턴스를 사용하는 경우 [권한 세트를](#) 사용하여 사용자에게 AWS 계정 및 리소스에 대한 액세스 권한을 부여하여 사용자 또는 그룹 액세스 권한을 할당 AWS 계정할 수 있습니다.

4. 애플리케이션에 대한 사용자 액세스 설정

IAM Identity Center를 사용하면 사용자에게 두 가지 유형의 애플리케이션에 대한 액세스 권한을 부여할 수 있습니다.

a. [AWS 관리형 애플리케이션](#)

- Amazon Q Business AWS CLI 및 Amazon Redshift와 같은 AWS 관리형 애플리케이션에서 IAM Identity Center를 사용할 수 있습니다. 자세한 내용은 [AWS 관리형 애플리케이션](#) 및 [AWS CLI와 IAM Identity Center 통합](#) 섹션을 참조하세요.

b. [고객 관리형 애플리케이션](#)

- 다음 유형의 고객 관리형 애플리케이션 중 하나를 IAM Identity Center와 통합할 수 있습니다.
 - [IAM Identity Center 카탈로그에 나열된 애플리케이션](#)
 - [사용자 정의 애플리케이션](#)
- 애플리케이션을 구성한 후 [사용자에게 애플리케이션에 대한 액세스 권한을 할당](#)할 수 있습니다.

5. 사용자에게 AWS 액세스 포털에 대한 로그인 지침 제공

AWS 액세스 포털은 사용자에게 할당된 모든 애플리케이션 AWS 계정 또는 둘 다에 대한 원활한 액세스를 제공하는 웹 포털입니다. IAM Identity Center의 신규 사용자는 AWS 액세스 포털에 로그인 하기 전에 사용자 자격 증명을 활성화해야 합니다.

AWS 액세스 포털에 로그인하는 방법에 대한 자세한 내용은 AWS Sign-In 사용 설명서의 [AWS 액세스 포털에 로그인](#)을 참조하세요. AWS 액세스 포털의 로그인 프로세스에 대한 자세한 내용은 [AWS 액세스 포털에 로그인](#)을 참조하세요.

IAM Identity Center 전제 조건 및 고려 사항

IAM Identity Center를 사용하여 AWS 관리형 애플리케이션 전용, AWS 계정 전용 또는 둘 다에 액세스 할 수 있습니다. IAM 페더레이션을 사용하여에 대한 액세스를 관리하는 경우 애플리케이션 액세스에 IAM Identity Center를 사용하는 동안 계속 그렇게 AWS 계정할 수 있습니다.

IAM Identity Center를 활성화하기 전에 다음 사항을 고려합니다.

- AWS 리전

먼저 IAM Identity Center의 각 인스턴스에 대해 [지원되는](#) 단일 리전에서 IAM Identity Center를 활성화합니다. AWS 계정에 대한 Single Sign-On 액세스에 IAM Identity Center를 사용하려면 조직의 모든 사용자가 리전에 액세스할 수 있어야 합니다. 애플리케이션 액세스에 IAM Identity Center를 사용하려는 경우 Amazon SageMaker AI와 같은 일부 AWS 관리형 애플리케이션은 지원하는 리전에서만 작동할 수 있습니다. 또한 대부분의 AWS 관리형 애플리케이션은 애플리케이션과 동일한 리전에서 IAM Identity Center를 사용할 수 있어야 합니다. 이는 동일한 리전에 공동 배치하거나 지원되는 경우 IAM Identity Center 인스턴스를 AWS 관리형 애플리케이션의 원하는 배포 리전에 복제하여 달성할 수 있습니다. 자세한 내용은 [선택 시 고려 사항 AWS 리전](#) 단원을 참조하십시오.

- 애플리케이션 액세스만

IAM Identity Center는 기존 자격 증명 공급자를 사용하여 Kiro와 같은 애플리케이션에 대한 사용자 액세스에만 사용할 수 있습니다. 자세한 내용은 [애플리케이션에 대한 사용자 액세스에만 IAM Identity Center 사용](#) 단원을 참조하십시오.

 Note

애플리케이션 리소스에 대한 액세스는 애플리케이션 소유자가 독립적으로 관리합니다.

- IAM 역할 할당량

IAM Identity Center는 IAM 역할을 생성하여 사용자에게 리소스에 대한 권한을 제공합니다. 자세한 내용은 [IAM Identity Center에서 생성한 IAM 역할](#) 단원을 참조하십시오.

- IAM Identity Center 및 AWS Organizations

AWS Organizations 는 IAM Identity Center와 함께 사용하는 것이 좋지만 필수는 아닙니다. 조직을 설정하지 않았어도 설정할 필요는 없습니다. 이미를 설정했고 조직에 IAM Identity Center를 추가 AWS Organizations 하려는 경우 모든 AWS Organizations 기능이 활성화되어 있는지 확인합니다. 자세한 내용은 [IAM Identity Center 및 AWS Organizations](#) 단원을 참조하십시오.

액세스 포털 및 IAM Identity Center 콘솔을 포함한 IAM Identity Center 웹 인터페이스는 지원되는 웹 브라우저를 통해 사람이 액세스하도록 설계되었습니다. 호환되는 브라우저에는 Microsoft Edge, Mozilla Firefox, Google Chrome 및 Apple Safari의 최신 세 가지 버전이 포함됩니다. 브라우저 기반이 아닌 경로를 사용하여 이러한 엔드포인트에 액세스하는 것은 지원되지 않습니다. IAM Identity Center 서비스에 프로그래밍 방식으로 액세스하려면 IAM Identity Center 및 Identity Store APIs 참조 가이드에서 사용할 수 있는 문서화된 API를 사용하는 것이 좋습니다.

선택 시 고려 사항 AWS 리전

원하는 대로 지원되는 단일에서 IAM Identity Center를 활성화할 수 있으며 전 세계 사용자가 사용할 수 있는 AWS 리전 있습니다. 이러한 글로벌 가용성을 통해 여러 AWS 계정 및 애플리케이션에 대한 사용자 액세스를 더 쉽게 구성할 수 있습니다. 다음은 AWS 리전을 선택하기 위한 주요 고려 사항입니다.

- 사용자의 지리적 위치 - 대부분의 최종 사용자와 지리적으로 가장 가까운 리전을 선택하면 Amazon SageMaker AI와 같은 AWS 액세스 포털 및 AWS 관리형 애플리케이션에 대한 액세스 지연 시간이 줄어듭니다.
- 옵트인 리전(기본적으로 비활성화된 리전) - 옵트인 리전은 기본적으로 비활성화 AWS 리전 된 입니다. 옵트인 리전을 사용하려면 이를 활성화해야 합니다. 자세한 내용은 [옵트인 리전에서 IAM Identity Center 관리](#)를 참조하세요.
- IAM Identity Center를 추가 리전으로 복제 - IAM Identity Center를 추가로 복제하려는 경우 기본적으로 활성화된 리전을 선택해야 AWS 리전합니다. 자세한 내용은 [여러에서 IAM Identity Center 사용 AWS 리전](#) 단원을 참조하십시오.
- AWS 관리형 애플리케이션을 위한 배포 리전 선택 - AWS 관리형 애플리케이션은 사용 가능한 AWS 리전 에서만 작동할 수 있습니다. 많은 AWS 관리형 애플리케이션은 IAM Identity Center가 활성화되거나 복제되는 리전(기본 또는 추가 리전)에서만 작동할 수 있습니다. IAM Identity Center 인스턴스가 추가 리전으로의 복제를 지원하는지 확인하려면 섹션을 참조하세요 [여러에서 IAM Identity Center 사용 AWS 리전](#). 복제가 옵션이 아닌 경우 AWS 관리형 애플리케이션을 사용하려는 리전에서 IAM Identity Center를 활성화하는 것이 좋습니다.
- 디지털 주권-디지털 주권 규정 또는 회사 정책에 따라 특정 AWS 리전을 사용해야 할 수 있습니다. 회사의 법률 부서에 문의하세요.
- 자격 증명 소스 - [AWS Managed Microsoft AD](#) 또는 [Active Directory\(AD\)](#)의 자체 관리형 디렉터리를 자격 증명 소스로 사용하는 경우 해당 홈 리전은 IAM Identity Center를 활성화한 AWS 리전 와 일치해야 합니다.
- Amazon Simple Email Service를 사용한 리전 간 이메일 - 일부 리전에서 IAM Identity Center는 다른 리전의 [Amazon Simple Email Service\(Amazon SES\)](#)를 호출하여 이메일을 보낼 수 있습니다. 이러한 리전 간 호출에서 IAM Identity Center는 특정 사용자 속성을 다른 리전으로 전송합니다. 자세한 내용은 [Amazon SES를 사용한 리전 간 이메일](#) 단원을 참조하십시오.
- AWS Control Tower -에서 IAM Identity Center의 조직 인스턴스를 활성화하는 경우 인스턴스는 AWS Control Tower AWS Control Tower 랜딩 존과 동일한 리전에 생성됩니다.

주제

- [IAM Identity Center 리전 데이터 스토리지 및 작업](#)

- [전환 AWS 리전](#)
- [IAM Identity Center가 활성화된 AWS 리전의 비활성화](#)

IAM Identity Center 리전 데이터 스토리지 및 작업

IAM Identity Center에서 AWS 리전 전반에 걸쳐 데이터 스토리지 및 작업을 처리하는 방법을 알아봅니다.

IAM Identity Center에서 데이터를 저장하는 방법 이해

IAM Identity Center를 활성화하면 IAM Identity Center에서 구성하는 모든 데이터가 IAM Identity Center를 활성화한 리전에 저장됩니다. 이 데이터에는 디렉터리 구성, 권한 세트, 애플리케이션 인스턴스 및 AWS 계정 애플리케이션에 대한 사용자 할당이 포함됩니다. IAM Identity Center ID 스토어를 사용하는 경우, IAM Identity Center에서 생성하는 모든 사용자와 그룹도 같은 리전에 저장됩니다. IAM Identity Center 인스턴스를 추가 리전에 복제하면 IAM Identity Center는 사용자, 그룹, 권한 세트 및 할당, 기타 메타데이터 및 구성을 해당 리전에 자동으로 복제합니다.

Amazon SES를 사용한 리전 간 이메일

IAM Identity Center는 최종 사용자가 두 번째 인증 요소인 일회용 암호(OTP)로 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 초대장을 받는 경우와 같은 특정 ID 및 보안 인증 관리 이벤트를 위해 전송됩니다. Amazon SES는 IAM Identity Center AWS 리전 가 지원하는의 하위 집합에서 사용할 수 있습니다.

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.

IAM Identity Center 리전 코드	IAM Identity Center 리전 이름	Amazon SES 리전 코드	Amazon SES 리전 이름
ap-east-1	아시아 태평양(홍콩)	ap-northeast-2	아시아 태평양(서울)
ap-east-2	아시아 태평양(타이베이)	ap-northeast-1	아시아 태평양(도쿄)
ap-south-2	아시아 태평양(하이데라바드)	ap-south-1	아시아 태평양(뭄바이)

IAM Identity Center 리전 코드	IAM Identity Center 리전 이름	Amazon SES 리전 코드	Amazon SES 리전 이름
ap-southeast-4	아시아 태평양(멜버른)	ap-southeast-2	아시아 태평양(시드니)
ap-southeast-5	아시아 태평양(말레이시아)	ap-southeast-1	아시아 태평양(싱가포르)
ap-southeast-6	아시아 태평양(뉴질랜드)	ap-southeast-2	아시아 태평양(시드니)
ap-southeast-7	아시아 태평양(태국)	ap-northeast-3	아시아 태평양(오사카)
ca-west-1	캐나다 서부(캘거리)	ca-central-1	캐나다(중부)
eu-south-2	유럽(스페인)	eu-west-3	유럽(파리)
eu-central-2	유럽(취리히)	eu-central-1	유럽(프랑크푸르트)
mx-central-1	멕시코(중부)	us-east-2	미국 동부(오하이오)
me-central-1	중동(UAE)	eu-central-1	유럽(프랑크푸르트)
us-gov-east-1	AWS GovCloud(미국 동부)	us-gov-west-1	AWS GovCloud(미국 서부)

이러한 리전 간 호출에서 IAM Identity Center는 다음과 같은 사용자 속성을 전송할 수 있습니다.

- 이메일 주소
- 이름
- 성
- 의 계정 AWS Organizations
- AWS 액세스 포털 URL
- 사용자 이름
- 디렉터리 ID
- 사용자 ID

옵트인 리전(기본값으로 비활성화된 리전)에서의 IAM Identity Center 관리

대부분은 기본적으로 모든 AWS 서비스의 작업에 대해 AWS 리전 활성화되지만 IAM Identity Center를 사용하려면 다음 [옵트인 리전](#)을 활성화해야 합니다.

- 아프리카(케이프타운)
- 아시아 태평양(홍콩)
- 아시아 태평양(타이베이)
- 아시아 태평양(하이데라바드)
- 아시아 태평양(자카르타)
- 아시아 태평양(멜버른)
- 아시아 태평양(말레이시아)
- 아시아 태평양(뉴질랜드)
- 아시아 태평양(태국)
- 캐나다 서부(캘거리)
- 유럽(밀라노)
- 유럽(스페인)
- 유럽(취리히)
- 이스라엘(텔아비브)
- 멕시코(중부)
- Middle East (Bahrain)
- 중동(UAE)

옵트인 리전에 IAM Identity Center를 배포하는 경우 IAM Identity Center에 대한 액세스를 관리하려는 모든 계정에서 이 리전을 활성화해야 합니다. 모든 계정에는 해당 리전에서 리소스를 생성할지 여부와 관계없이 이 구성이 필요합니다. 조직의 현재 계정에 대해 리전을 활성화할 수 있으며 새 계정을 추가할 때 이 작업을 반복해야 합니다. 지침은 AWS Organizations 사용 설명서의 [조직에서 리전 활성화 또는 비활성화](#)를 참조하세요. 이러한 추가 단계를 반복하지 않기 위해 [기본적으로 활성화된 리전](#)에 IAM Identity Center를 배포하도록 선택할 수 있습니다.

Note

액세스 AWS 포털에서 AWS 멤버 계정에 액세스할 수 있도록 IAM Identity Center 인스턴스가 위치한 옵트인 리전과 동일한 리전에 AWS 멤버 계정을 옵트인해야 합니다.

옵트인 리전에 저장된 메타데이터

옵트인에서 관리 계정에 대해 IAM Identity Center를 활성화하면 모든 멤버 계정에 대한 AWS 리전다음 IAM Identity Center 메타데이터가 리전에 저장됩니다.

- 계정 ID
- 계정 이름
- 계정 이메일
- IAM Identity Center가 구성원 계정에 생성하는 IAM 역할의 Amazon 리소스 이름(ARN)

AWS 리전 기본적으로 활성화된

다음 리전은 기본적으로 활성화되어 있으며 이러한 리전에서 IAM Identity Center를 활성화할 수 있습니다.

- 미국 동부(오하이오)
- 미국 동부(버지니아 북부)
- 미국 서부(오레곤)
- 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)

전환 AWS 리전

비활성화해야 할 리전이 아닌 사용자가 계속 사용할 수 있도록 하려는 리전에 IAM Identity Center를 설치하는 것이 좋습니다. 자세한 내용은 [선택 시 고려 사항 AWS 리전](#) 단원을 참조하십시오.

[현재 IAM Identity Center 인스턴스를 삭제](#)하고 다른 리전에서 인스턴스를 생성하는 경우에만 IAM Identity Center 리전을 전환할 수 있습니다. 기존 IAM Identity Center 인스턴스에서 AWS 관리형 애플리케이션을 이미 활성화한 경우 IAM Identity Center를 삭제하기 전에 애플리케이션을 비활성화합니다. AWS 관리형 애플리케이션 비활성화에 대한 지침은 [섹션을 참조하세요](#) [AWS 관리형 애플리케이션 비활성화](#).

Note

다른 리전에 AWS 관리형 애플리케이션을 배포할 수 있도록 IAM Identity Center 리전을 전환하는 것을 고려하는 경우 대신 IAM Identity Center 인스턴스를 해당 리전으로 복제하는 것이 좋습니다. 자세한 내용은 [여러에서 IAM Identity Center 사용 AWS 리전](#) 단원을 참조하십시오.

새 리전의 구성 고려 사항

새 IAM Identity Center 인스턴스에서 사용자, 그룹, 권한 세트, 애플리케이션 및 할당을 다시 생성해야 합니다. IAM Identity Center 계정 및 애플리케이션 할당 [API](#)를 사용하여 구성의 스냅샷을 가져온 후 해당 스냅샷을 사용하여 새 리전에서 구성을 다시 빌드할 수 있습니다. 다른 리전으로 전환하면 [AWS 액세스 포털](#)의 URL도 변경되어 사용자에게 AWS 계정 및 애플리케이션에 대한 Single Sign-On 액세스 권한을 제공합니다. 새 인스턴스의 관리 콘솔을 통해 일부 IAM Identity Center 구성을 다시 생성해야 할 수도 있습니다.

IAM Identity Center가 활성화된 AWS 리전 의 비활성화

IAM Identity Center가 설치된 AWS 리전 를 비활성화하면 IAM Identity Center도 비활성화됩니다. 리전에서 IAM Identity Center가 비활성화되면 해당 리전의 사용자는 AWS 계정 및 애플리케이션에 대한 Single Sign-On 액세스 권한을 가질 수 없습니다.

[옵트인 AWS 리전](#)에서 IAM Identity Center를 다시 활성화하려면 리전을 다시 활성화해야 합니다. IAM Identity Center는 일시 중지된 모든 이벤트를 다시 처리해야 하므로 IAM Identity Center를 다시 활성화하는 데는 시간이 걸릴 수 있습니다.

Note

IAM Identity Center AWS 계정 내에서 사용하도록 활성화된에 대한 액세스만 관리할 수 있습니다 AWS 리전. 조직의 모든 계정에서 액세스를 관리하려면 IAM Identity Center와 함께 사용하도록 AWS 리전 자동으로 활성화된의 관리 계정에서 IAM Identity Center를 활성화합니다.

활성화 및 비활성화에 대한 자세한 내용은 AWS 일반 AWS 리전참조의 [관리를 AWS 리전](#) 참조하세요.

애플리케이션에 대한 사용자 액세스에만 IAM Identity Center 사용

IAM Identity Center를 사용하여 Kiro와 같은 애플리케이션 AWS 계정 또는 둘 다에 액세스할 수 있습니다. 기존 ID 제공업체를 연결하고 디렉터리에서 사용자와 그룹을 동기화하거나 [IAM Identity Center에서 직접 사용자를 생성하고 관리](#)할 수 있습니다. 기존 ID 제공업체를 IAM Identity Center에 연결하는 방법에 대한 자세한 내용은 [IAM Identity Center의 ID 소스 자습서](#)를 참조하세요.

에 액세스하기 위해 이미 IAM을 사용하고 있습니까 AWS 계정?

AWS 관리형 애플리케이션에 액세스하기 위해 IAM Identity Center를 사용하기 위해 현재 AWS 계정 워크플로를 변경할 필요가 없습니다. AWS 계정 액세스에 [IAM과 연동](#)을 사용하는 경우 사용자는 항상 가지고 있는 것과 동일한 방식으로 AWS 계정에 계속 액세스할 수 있으며 기존 워크플로를 계속 사용하여 해당 액세스를 관리할 수 있습니다.

IAM Identity Center에서 생성한 IAM 역할

AWS 계정에 사용자를 할당하면 IAM Identity Center는 사용자에게 리소스에 대한 권한을 부여하는 IAM 역할을 생성합니다.

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 AWS 액세스 포털 또는를 사용하여 정의한 권한 있는 사용자가 역할을 수임하도록 허용합니다 AWS CLI. 권한 세트를 수정하면 IAM Identity Center에서 해당 IAM 정책 및 역할이 그에 따라 업데이트되도록 합니다. IAM Identity Center 인스턴스를 추가 리전에 복제해도 기존 IAM 역할에는 영향을 주지 않으며 새 IAM 역할이 생성되지 않습니다.

Note

권한 세트는 애플리케이션에 권한을 부여하는 데 사용되지 않습니다.

에서 IAM 역할을 이미 구성한 경우 계정이 IAM 역할에 대한 할당량에 근접하고 있는지 확인하는 AWS 계정것이 좋습니다. 계정당 IAM 역할의 기본 할당량은 역할 1,000개입니다. 자세한 내용은 [IAM 객체 할당량](#)을 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 요청](#)을 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 Identity Center 및 AWS Organizations

AWS Organizations 는 IAM Identity Center와 함께 사용하는 것이 좋지만 필수는 아닙니다. 조직을 설정하지 않았어도 설정할 필요는 없습니다. IAM Identity Center를 활성화하면 서비스를 활성화할지 여부를 선택합니다 AWS Organizations. 조직을 설정하면 조직을 설정하는 AWS 계정 이 조직의 관리 계정이 됩니다. AWS 계정 의 루트 사용자는 이제 조직 관리 계정의 소유자입니다. 조직에 추가로 초대하는 모든 AWS 계정 은 구성원 계정입니다. 관리 계정은 조직 리소스, 조직 단위 및 구성원 계정을 관리하는 정책을 생성합니다. 권한은 관리 계정에 의해 구성원 계정에 위임됩니다.

Note

IAM Identity Center의 조직 인스턴스를 생성하는를 사용하여 IAM Identity Center를 활성화 AWS Organizations하는 것이 좋습니다. 조직 인스턴스는 IAM Identity Center의 모든 기능을 지원하고 중앙 관리 기능을 제공하므로 권장되는 모범 사례입니다. 자세한 내용은 [IAM Identity Center의 조직 인스턴스 관리](#) 단원을 참조하십시오.

이미를 설정했고 조직에 IAM Identity Center를 추가 AWS Organizations 하려는 경우 모든 AWS Organizations 기능이 활성화되어 있는지 확인합니다. 조직을 생성할 때 모든 기능 활성화가 기본값입니다. 자세한 내용은AWS Organizations 사용 설명서에서 [조직 내 모든 기능 활성화](#)를 참조하세요.

IAM Identity Center의 조직 인스턴스를 활성화하려면 관리 자격 증명이 있는 사용자 또는 루트 사용자로 AWS Organizations 관리 계정에 AWS Management Console 로그인하여에 로그인해야 합니다(다

른 관리 사용자가 없는 경우 권장되지 않음). 자세한 내용은 AWS Organizations 사용 설명서의 [AWS 조직 생성 및 관리](#)를 참조하세요.

AWS Organizations 멤버 계정의 관리 자격 증명으로 로그인하면 IAM Identity Center의 계정 인스턴스를 활성화할 수 있습니다. 계정 인스턴스는 기능이 제한되어 있으며 단일 AWS 계정에 바인딩됩니다.

IAM Identity Center의 조직 및 계정 인스턴스

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

- 조직 인스턴스(권장)

AWS Organizations 관리 계정에서 활성화하는 IAM Identity Center의 인스턴스입니다. 조직 인스턴스는 IAM Identity Center의 모든 기능을 지원합니다. 계정 인스턴스 대신 조직 인스턴스를 배포하여 관리 지점 수를 최소화하는 것이 좋습니다.

- 계정 인스턴스

단일에 바인딩 AWS 계정되고 IAM Identity Center가 활성화된 AWS 계정 및 AWS 리전 내에서만 표시되는 IAM Identity Center의 인스턴스입니다. 더 간단한 단일 계정 시나리오에는 계정 인스턴스를 사용합니다. 다음 중 하나를 통해 계정 인스턴스를 생성할 수 있습니다.

- 에서 관리하지 AWS 계정 않는 AWS Organizations
- 의 멤버 계정 AWS Organizations

AWS 계정 IAM Identity Center를 활성화할 수 있는 유형

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

- AWS Organizations 관리 계정(권장) - IAM Identity Center의 [조직 인스턴스](#)를 생성하는 데 필요합니다. 조직 인스턴스를 사용하여 조직 전체에 걸쳐 다중 계정 권한 및 애플리케이션 할당을 수행할 수 있습니다.
- AWS Organizations 멤버 계정 -를 사용하여 IAM Identity Center의 [계정 인스턴스](#)를 생성하여 해당 멤버 계정 내에서 애플리케이션 할당을 활성화합니다. 구성원 수준 인스턴스가 있는 하나 이상의 계정이 조직에 존재할 수 있습니다.
- 독립 실행형 AWS 계정-를 사용하여 IAM Identity Center의 [조직 인스턴스](#) 또는 [계정 인스턴스](#)를 생성합니다. 독립 실행형 AWS 계정 는에서 관리하지 않습니다 AWS Organizations. IAM Identity

Center의 인스턴스 하나만 독립 실행형에 연결하고 해당 인스턴스를 독립 실행형 내에서 애플리케이션 할당에 AWS 계정 사용할 수 있습니다 AWS 계정.

다음 표를 사용하여 인스턴스 유형에서 제공하는 기능을 비교합니다.

기능	AWS Organizations 관리 계정의 인스턴스 (권장)	구성원 계정의 인스턴스	독립 실행형의 인스턴스 AWS 계정
사용자 관리	☑예	☑예	☑예
AWS AWS 관리형 애플리케이션에 대한 Single Sign On 액세스를 위한 액세스 포털	☑예	☑예	☑예
OAuth 2.0(OIDC) 고객 관리형 애플리케이션	☑예	☑예	☑예
다중 계정 권한	☑예	☒아니요	☒아니요
AWS에 대한 Single Sign-On 액세스를 위한 액세스 포털 AWS 계정	☑예	☒아니요	☒아니요
SAML 2.0 고객 관리형 애플리케이션	☑예	☒아니요	☒아니요
위임된 관리자가 인스턴스 관리 가능	☑예	☒아니요	☒아니요
고객 관리형 KMS 키를 사용한 저장 데이터 암호화	☑예	☒아니요	☒아니요
IAM Identity Center를 추가 리전에 복제	☑예	☒아니요	☒아니요

AWS 관리형 애플리케이션 및 IAM Identity Center에 대한 자세한 내용은 [섹션을 참조하세요](#) [AWS IAM Identity Center와 함께 사용할 수 있는 관리형 애플리케이션](#).

주제

- [IAM Identity Center의 조직 인스턴스 관리](#)
- [IAM Identity Center의 계정 인스턴스](#)
- [IAM Identity Center 인스턴스 삭제](#)

IAM Identity Center의 조직 인스턴스 관리

와 함께 IAM Identity Center를 활성화하면 IAM Identity Center의 조직 인스턴스가 AWS Organizations 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 인스턴스가 있습니다.

IAM Identity Center의 조직 인스턴스를 활성화하려면 [IAM Identity Center의 인스턴스 활성화](#)를 참조하세요.

조직 인스턴스를 사용하는 경우

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

- IAM Identity Center의 모든 기능 지원 - 조직 AWS 계정 내 여러에 대한 권한 관리, 고객 관리형 애플리케이션에 대한 액세스 할당, 다중 리전 복제를 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 생성의 중앙 제어 - 옵트인 리전(기본적으로 비활성화AWS 리전 됨)에서 IAM Identity Center 인스턴스를 조직에 배포하지 않은 한 조직의 멤버 계정에서 계정 인스턴스를 생성할 수 있는지 여부를 제어할 수 있습니다.

IAM Identity Center의 조직 인스턴스를 활성화하는 방법에 대한 지침은 [IAM Identity Center의 인스턴스 활성화](#) 섹션을 참조하세요.

IAM Identity Center의 계정 인스턴스

IAM Identity Center의 계정 인스턴스를 사용하면 지원되는 AWS 관리형 애플리케이션과 OIDC 기반 고객 관리형 애플리케이션을 배포할 수 있습니다. 계정 인스턴스는 IAM Identity Center 인력 ID 및 액세스 포털 기능을 AWS 계정활용하여 단일에서 애플리케이션의 격리된 배포를 지원합니다.

계정 인스턴스는 단일에 바인딩되며 동일한 계정 AWS 계정 및에서 지원되는 애플리케이션에 대한 사용자 및 그룹 액세스를 관리하는 데에만 사용됩니다 AWS 리전. 계정 인스턴스는 당 1개로 제한됩니다 AWS 계정. 의 멤버 계정 AWS Organizations 또는에서 관리하지 AWS 계정 않는 독립 실행형 중 하나에서 계정 인스턴스를 생성할 수 있습니다 AWS Organizations.

IAM Identity Center의 계정 인스턴스를 활성화하는 방법에 대한 지침은 [IAM Identity Center의 인스턴스 활성화](#) 섹션을 참조하고 계정 탭을 선택합니다.

계정 인스턴스를 사용하는 경우

대부분의 경우 [조직 인스턴스](#)가 권장됩니다. 계정 인스턴스는 다음 시나리오 중 하나에 해당하는 경우에만 사용됩니다.

- 지원되는 AWS 관리형 애플리케이션의 임시 평가판을 실행하여 애플리케이션이 비즈니스 요구 사항에 적합한지 확인하고자 합니다.
- 조직 전체에서 IAM Identity Center를 채택할 계획은 없지만 하나 이상의 AWS 관리형 애플리케이션을 지원하려고 합니다.
- IAM Identity Center의 조직 인스턴스가 있지만 지원되는 AWS 관리형 애플리케이션을 조직 인스턴스의 사용자와 구별되는 격리된 사용자 세트에 배포하고자 합니다.
- 운영하는 AWS 조직을 제어하지 않습니다. 예를 들어, 타사를 관리하는 AWS 조직을 제어합니다 AWS 계정.

Important

IAM Identity Center를 사용하여 여러 계정의 애플리케이션을 지원하려는 경우 조직 인스턴스를 사용합니다. 계정 인스턴스는 이 사용 사례를 지원하지 않습니다.

AWS 계정 인스턴스를 지원하는 관리형 애플리케이션

IAM Identity Center의 계정 인스턴스 [AWS IAM Identity Center](#)와 함께 사용할 수 있는 관리형 애플리케이션을 지원하는 AWS 관리형 애플리케이션은 섹션을 참조하세요. AWS 관리형 애플리케이션을 사용하여 계정 인스턴스 생성의 가용성을 확인합니다.

구성원 계정의 가용성 제한

AWS Organizations 멤버 계정에 IAM Identity Center의 계정 인스턴스를 배포하려면 다음 조건 중 하나가 true여야 합니다.

- 조직에 IAM Identity Center의 조직 인스턴스가 없습니다.
- 조직에 IAM Identity Center의 조직 인스턴스가 있으며 인스턴스 관리자가 IAM Identity Center의 계정 인스턴스 생성을 허용합니다(2023년 11월 15일 이후에 생성된 조직 인스턴스의 경우).
- 조직에 IAM Identity Center의 조직 인스턴스가 있고 인스턴스 관리자가 조직의 멤버 계정별로 계정 인스턴스 생성을 수동으로 생성하도록 활성화했습니다(2023년 11월 15일 이전에 생성된 조직 인스턴스의 경우). 지침은 [멤버 계정에서 계정 인스턴스 생성 허용](#) 섹션을 참조하세요.

위의 조건 중 하나가 충족되면 다음 조건이 모두 true여야 합니다.

- 관리자가 멤버 계정이 계정 인스턴스 생성할 수 없도록 하는 [서비스 제어 정책](#)을 생성하지 않았습니다.
- AWS 리전과 무관하게 동일한 계정에 IAM Identity Center 인스턴스가 아직 없습니다.
- IAM Identity Center를 사용할 수 AWS 리전 있는에서 작업하고 있습니다. 리전에 대한 자세한 내용은 [IAM Identity Center 리전 데이터 스토리지 및 작업](#)의 내용을 참조하세요.

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 세트를 지원하지 않으므로 AWS 계정 액세스를 지원하지 않습니다.
- 계정 인스턴스를 조직 인스턴스로 변환 또는 병합할 수 없습니다.
- 일부 [AWS 관리형 애플리케이션](#)만 계정 인스턴스를 지원합니다.
- 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 에 남아 있어야 합니다.

멤버 계정에서 계정 인스턴스 생성 허용

2023년 11월 15일 이전에 IAM Identity Center를 활성화한 경우 IAM Identity Center의 [조직 인스턴스](#)가 있으며 멤버 계정으로 계정 인스턴스를 생성할 수 있는 기능이 기본적으로 비활성화됩니다. IAM Identity Center 콘솔에서 계정 인스턴스 기능을 활성화하여 구성원 계정이 계정 인스턴스를 생성할 수 있는지 여부를 선택할 수 있습니다.

조직의 구성원 계정에서 계정 인스턴스의 생성 활성화

Important

멤버 계정에 대한 IAM Identity Center의 계정 인스턴스를 활성화하는 작업은 일회성 작업입니다. 즉, 이 작업은 되돌릴 수 없습니다. 활성화되면 서비스 제어 정책(SCP)을 생성하여 계정 인스턴스 생성을 제한할 수 있습니다. 자세한 내용은 [서비스 제어 정책으로 계정 인스턴스 생성 제어](#)를 참조하세요.

1. [IAM Identity Center 콘솔](#)을 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.

서비스 제어 정책으로 계정 인스턴스 생성 제어

멤버 계정으로 계정 인스턴스를 생성하는 기능은 IAM Identity Center를 활성화한 시기에 따라 달라집니다.

- 2023년 11월 이전 - [멤버 계정에서 계정 인스턴스 생성을 허용](#)해야 하며, 이 작업은 되돌릴 수 없습니다.
- 2023년 11월 15일 이후 - 멤버 계정은 기본적으로 계정 인스턴스를 생성할 수 있습니다.

어느 경우든 서비스 제어 정책(SCP)을 사용하여 다음을 수행할 수 있습니다.

- 모든 멤버 계정이 계정 인스턴스를 생성하지 못하도록 방지합니다.
- 특정 멤버 계정만 계정 인스턴스를 생성하도록 허용합니다.

계정 인스턴스 방지

다음 절차에 따라 멤버 계정이 IAM Identity Center의 계정 인스턴스를 생성하지 못하도록 방지하는 SCP를 생성합니다.

1. [IAM Identity Center 콘솔](#)을 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 콘솔](#)로 이동하여 SCP를 생성하거나 이를 기존 SCP에 명령문으로 연결할 수 있게 됩니다. SCPs의 기능입니다 AWS Organizations. SCP 연결에 대한 지침은 AWS Organizations 사용 설명서의 [서비스 제어 정책 연결 및 분리](#)를 참조하세요.

계정 인스턴스 제한

이 정책은 모든 계정 인스턴스 생성을 방지하는 대신 "**<ALLOWED-ACCOUNT-ID>**" 자리 표시자에 명시적으로 나열된 것을 AWS 계정 제외한 모든에 대해 IAM Identity Center의 계정 인스턴스를 생성하려는 시도를 거부합니다.

Example: 계정 인스턴스 생성을 제한하는 정책 거부

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyMemberAccountInstances",
      "Effect": "Deny",
      "Action": "sso:CreateInstance",
      "Resource": "*",
      "Condition": {
```

```

    "StringNotEquals": {
      "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
    }
  }
}
]
}

```

- ['<ALLOWED-ACCOUNT-ID>']를 IAM Identity Center의 계정 인스턴스를 생성하도록 허용할 실제 AWS 계정 ID로 바꿉니다.
- 허용되는 계정 ID는 ['111122223333', '444455556666'] 배열 형식으로 여러 개 나열할 수 있습니다.
- 이 정책을 조직 SCP에 연결하여 IAM Identity Center 계정 인스턴스 생성에 대한 중앙 집중식 제어를 적용합니다.

SCP 연결에 대한 지침은 AWS Organizations 사용 설명서의 [서비스 제어 정책 연결 및 분리](#)를 참조하세요.

IAM Identity Center 인스턴스 삭제

IAM Identity Center 인스턴스가 삭제되면 해당 인스턴스의 모든 데이터가 삭제되며 복구할 수 없습니다. 다음 표에는 IAM Identity Center에 구성되어 있는 디렉터리 유형에 따라 삭제되는 데이터가 설명되어 있습니다.

삭제되는 데이터	연결된 디렉터리 -, AWS Managed Microsoft AD AD Connector 또는 외부 ID 제공업체	IAM Identity Center ID 스토어	
에 대해 구성한 모든 권한 세트 AWS 계정	예	예	
IAM Identity Center에 서 구성한 모든 애플리 케이션	예	예	

삭제되는 데이터	연결된 디렉터리 -, AWS Managed Microsoft AD AD Connector 또는 외부 ID 제공업체	IAM Identity Center ID 스토어	
AWS 계정 및 애플리 케이션에 대해 구성된 모든 사용자 할당	☑예	☑예	
디렉터리 또는 스토어 의 모든 사용자 및 그 그룹	해당 사항 없음	☑예	

IAM Identity Center 인스턴스를 추가 리전에 복제한 경우 인스턴스를 삭제하기 전에 해당 리전을 제거해야 합니다.

IAM Identity Center 인스턴스를 삭제하려면 다음 절차를 수행하세요.

IAM Identity Center 인스턴스를 삭제하려면

1. [IAM Identity Center 콘솔](#)을 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.

IAM Identity Center 활성화

IAM Identity Center를 활성화할 때 활성화할 AWS IAM Identity Center 인스턴스 유형을 선택합니다. 서비스의 인스턴스는 AWS 환경 내에서 서비스를 한 번만 배포하는 것입니다. IAM Identity Center에서 사용할 수 있는 두 가지 인스턴스 유형은 조직 인스턴스와 계정 인스턴스입니다. 활성화할 수 있는 인스턴스 유형은 로그인한 계정 유형에 따라 다릅니다.

다음 목록은 각 유형의 AWS 계정에 대해 활성화할 수 있는 IAM Identity Center 인스턴스의 유형을 식별합니다.

- AWS Organizations 관리 계정(권장) - IAM Identity Center의 [조직 인스턴스](#)를 생성하는 데 필요합니다. 조직 인스턴스를 사용하여 조직 전체에 걸쳐 다중 계정 권한 및 애플리케이션 할당을 수행할 수 있습니다. 이 인스턴스 유형을 추가 리전에 복제하여 계정 액세스의 복원력을 높이고 AWS 애플리케이션 배포 리전을 선택할 때 유연성을 높일 수 있습니다.
- AWS Organizations 멤버 계정 -를 사용하여 IAM Identity Center의 [계정 인스턴스](#)를 생성하여 해당 멤버 계정 내에서 애플리케이션 할당을 활성화합니다. 구성원 수준 인스턴스가 있는 하나 이상의 계정이 조직에 존재할 수 있습니다.
- 독립 실행형 AWS 계정-를 사용하여 IAM Identity Center의 [조직 인스턴스](#) 또는 [계정 인스턴스](#)를 생성합니다. 독립 실행형 AWS 계정 는에서 관리하지 않습니다 AWS Organizations. IAM Identity Center의 인스턴스 하나만 독립 실행형에 연결하고 해당 인스턴스를 독립 실행형 내의 애플리케이션 할당에 AWS 계정 사용할 수 있습니다 AWS 계정.

Important

조직 관리 계정은 서비스 제어 정책을 사용하여 [조직 멤버 계정이 IAM Identity Center의 계정 인스턴스를 생성](#)할 수 있는지 여부를 제어할 수 있습니다.

프리 티어 계정을 사용하는 경우 AWS 조직을 생성하면 사용한 pay-as-you-go 요금으로 계정을 유료 플랜으로 자동 업그레이드합니다. 프리 티어 크레딧은 즉시 만료됩니다. 자세한 내용은 [AWS 프리 티어 FAQs](#).

다양한 인스턴스 유형에서 제공하는 다양한 기능을 비교하려면 [IAM Identity Center의 조직 및 계정 인스턴스](#) 섹션을 참조하세요.

IAM Identity Center를 활성화하기 전에 [IAM Identity Center 전제 조건 및 고려 사항](#) 섹션을 검토하는 것이 좋습니다.

IAM Identity Center의 인스턴스 활성화

조직 또는 계정 인스턴스 중 활성화하려는 IAM Identity Center 인스턴스 유형의 탭을 선택합니다.

Organization (recommended)

1. 다음 중 하나를 수행하여 AWS Management Console에 로그인합니다.
 - 신규 사용자 AWS (루트 사용자) - 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
 - 독립형 AWS 계정 (IAM 자격 증명)과 AWS 함께를 이미 사용 중 - 관리 권한이 있는 IAM 자격 증명을 사용하여 로그인합니다.
 - 이미 사용 중 AWS Organizations (IAM 자격 증명) - 관리 계정 자격 증명을 사용하여 로그인합니다.
2. [IAM Identity Center 콘솔](#)을 엽니다.
3. (선택 사항) 기본 관리형 키가 아닌 고객 AWS 관리형 KMS 키를 저장 시 암호화에 사용하려면 IAM Identity Center 저장 시 데이터 암호화를 위한 키 섹션에서 고객 관리형 키를 구성합니다. 자세한 정보는 [에서 고객 관리형 KMS 키 구현 AWS IAM Identity Center](#) 섹션을 참조하세요.

Important

KMS 고객 관리형 키 사용에 필요한 권한을 구성한 경우에만 이 단계를 수행합니다. 적절한 권한이 없으면 이 단계가 실패하거나 IAM Identity Center 관리 및 AWS 관리형 애플리케이션을 중단시킬 수 있습니다.

4. IAM Identity Center 활성화에서 활성화를 선택합니다.
5. AWS Organizations를 사용하여 IAM Identity Center 활성화 페이지에서 정보를 검토한 다음 활성화를 선택하여 프로세스를 완료합니다.

Note

AWS Organizations 는 단일 AWS 리전에서만 IAM Identity Center를 활성화할 수 있습니다. IAM Identity Center를 활성화한 후 IAM Identity Center가 활성화된 리전을 변경해야 하는 경우 현재 인스턴스를 [삭제](#)하고 다른 리전에서 인스턴스를 생성해야 합니다.

조직 인스턴스를 활성화한 후 다음 단계를 수행하여 환경 설정을 완료하는 것이 좋습니다.

- 선택한 자격 증명 소스를 사용하고 있는지 확인합니다. ID 소스가 이미 할당된 경우 계속 사용할 수 있습니다. 자세한 내용은 [IAM Identity Center에서 ID 소스 확인](#) 단원을 참조하십시오.
- 멤버 계정을 위임된 관리자 계정으로 등록합니다. 자세한 내용은 [위임된 관리](#) 단원을 참조하십시오.
- IAM Identity Center는 AWS 리소스에 대한 액세스 포털을 제공합니다. 차세대 방화벽(NGFW) 또는 보안 웹 게이트웨이(SWG)와 같은 웹 콘텐츠 필터링 솔루션을 사용하여 특정 AWS 도메인 또는 URL 엔드포인트에 대한 액세스를 필터링하는 경우 섹션을 참조하세요 [에 대한 액세스를 허용하도록 방화벽 및 게이트웨이 업데이트 AWS 액세스 포털](#).

Account

1. 다음 중 하나를 수행하여 AWS Management Console에 로그인합니다.
 - 신규 사용자 AWS (루트 사용자) - 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
 - 이미 사용 중 AWS (IAM 자격 증명) - 관리 권한이 있는 IAM 자격 증명을 사용하여 로그인합니다.
 - 이미 사용 중 AWS Organizations (IAM 자격 증명) - 멤버 계정 관리 자격 증명을 사용하여 로그인합니다.
2. [IAM Identity Center 콘솔](#)을 엽니다.
3. 를 처음 AWS 사용하거나 독립 실행형이 있는 경우 IAM Identity Center 활성화 AWS 계정에서 활성화를 선택합니다.

AWS Organizations를 사용하여 IAM Identity Center 활성화 페이지가 표시됩니다. 이 옵션은 권장 사항이지만 필수는 아닙니다.

IAM Identity Center의 계정 인스턴스 활성화 링크를 선택합니다.

4. AWS Organizations 멤버 계정의 관리자인 경우 IAM Identity Center의 계정 인스턴스 활성화에서 계정 인스턴스 활성화를 선택합니다.
5. IAM Identity Center의 계정 인스턴스 활성화 페이지에서 정보를 검토하고 선택적으로 이 계정 인스턴스와 연결할 태그를 추가합니다. 그런 다음 활성화를 선택하여 프로세스를 완료합니다.

Note

AWS 계정이 조직의 멤버인 경우 IAM Identity Center의 계정 인스턴스를 활성화하는 기능에 제한이 있을 수 있습니다.

- 조직에서 2023년 11월 15일 이전에 IAM Identity Center를 활성화한 경우 멤버 계정이 계정 인스턴스를 생성할 수 있는 기능은 기본적으로 비활성화되어 있으므로 조직의 관리 계정에서 활성화해야 합니다.
- 조직에서 2023년 11월 15일 이후에 IAM Identity Center를 활성화한 경우에는 멤버 계정이 계정 인스턴스를 생성할 수 있는 기능이 기본적으로 활성화되어 있습니다. 그러나 서비스 제어 정책을 사용하여 조직 내에 IAM Identity Center의 계정 인스턴스가 생성되지 않도록 할 수 있습니다.

자세한 내용은 [the section called “멤버 계정에서 계정 인스턴스 생성 허용”](#) 및 [the section called “계정 인스턴스 생성을 위한 SCP”](#) 섹션을 참조하세요.

IAM Identity Center에서 ID 소스 확인

IAM Identity Center의 ID 소스는 사용자 및 그룹을 관리하는 위치를 정의합니다. IAM Identity Center를 활성화한 후 선택한 ID 소스를 사용하고 있는지 확인합니다. ID 소스가 이미 할당된 경우 계속 사용할 수 있습니다.

Active Directory 또는 외부 ID 제공업체를 통해 사용자 및 그룹을 관리하고 있다면, IAM Identity Center를 활성화하고 ID 소스를 선택할 때 해당 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 관리 사용자를 포함한 모든 사용자는 AWS 계정 및 애플리케이션에 대한 Single Sign-On 액세스 권한을 잃게 됩니다. 자세한 내용은 [ID 소스 변경 시 고려 사항](#) 단원을 참조하십시오.

자격 증명 소스를 확인하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.

2. 대시보드 페이지의 권장 설정 단계 섹션에서 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. 다른 외부 자격 증명 공급자를 아직 사용하지 않는 경우 사용자 및 그룹 생성을 시작하고 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

Directory Service 를 사용하여 AWS Managed Microsoft AD 디렉터리의 사용자 및 그룹을 이미 관리하거나 자체 관리형 디렉터리를 관리하는 경우 IAM Identity Center를 활성화할 때 해당 디렉터리를 연결하는 Active Directory (AD)가 좋습니다. 기본 Identity Center 디렉터리에 사용자 및 그룹을 생성하지 마세요. IAM Identity Center는 AWS Directory Service 에서 제공하는 연결을 사용하여 Active Directory의 소스 디렉터리에 있는 사용자, 그룹 및 구성원 정보를 IAM Identity Center ID 스토어로 동기화합니다. 자세한 내용은 [Microsoft AD 디렉터리](#) 단원을 참조하십시오.

Note

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

외부 ID 제공업체

Okta 또는 Microsoft Entra ID 등 외부 ID 제공업체(IdP)의 경우, IAM Identity Center를 사용해 SAML(Security Assertion Markup Language) 2.0 표준으로 IdP의 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 [IAM Identity Center의 ID 소스 자습서](#)를 참조하세요.

Note

외부 ID 제공업체를 사용할 계획이라면 IAM Identity Center가 아닌 외부 IdP에서 다중 인증 (MFA) 설정을 관리한다는 점에 유의하세요. 외부 ID 제공업체에 대해 IAM Identity Center의 MFA가 지원되지 않습니다. 자세한 내용은 [사용자에게 MFA에 대한 메시지 표시](#) 단원을 참조하십시오.

Note

IAM Identity Center를 추가 리전에 복제하려는 경우 외부 ID 제공업체를 구성해야 합니다. 사전 조건을 포함한 자세한 내용은 섹션을 참조하세요 [여러에서 IAM Identity Center 사용 AWS 리전](#).

에 대한 액세스를 허용하도록 방화벽 및 게이트웨이 업데이트 AWS 액세스 포털

AWS 액세스 포털은 사용자에게 Office 365, Concur, Salesforce 등과 같이 AWS 계정 가장 일반적으로 사용되는 모든 클라우드 애플리케이션에 대한 Single Sign-On 액세스를 제공합니다. 포털에서 AWS 계정 또는 애플리케이션 아이콘을 선택하여 여러 애플리케이션을 빠르게 시작할 수 있습니다.

Note

AWS 관리형 애플리케이션은 IAM Identity Center와 통합되어 인증 및 디렉터리 서비스에 사용하지만 애플리케이션 액세스에는 AWS 액세스 포털을 사용하지 않을 수 있습니다.

차세대 방화벽(NGFW) 또는 보안 웹 게이트웨이(SWG)와 같은 웹 콘텐츠 필터링 솔루션을 사용하여 특정 AWS 도메인 또는 URL 엔드포인트에 대한 액세스를 필터링하는 경우 AWS 액세스 포털과 연결된 도메인 및 URL 엔드포인트를 허용 목록에 추가해야 합니다.

다음 목록은 웹 콘텐츠 필터링 솔루션 허용 목록에 추가할 IPv4 및 듀얼 스택 도메인과 URL 엔드포인트를 제공합니다.

IPv4 허용 목록

- *[Directory ID or alias].awsapps.com*
- *[Identity Center instance ID].[Region].portal.amazonaws.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].prod.pr.panorama.console.api.aws/panoramamaroute*
- *[Region].signin.aws*
- *[Region].signin.aws.amazon.com*
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

듀얼 스택 허용 목록

- *[Identity Center instance ID].portal.[Region].app.aws*
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region].sso.signin.aws*
- *[Region].signin.aws.amazon.com*
- signin.aws.amazon.com

- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

통합 허용 목록(IPv4 + 이전 버전과의 호환성을 갖춘 듀얼 스택)

- *[Directory ID or alias].awsapps.com*
- *[Identity Center instance ID].[Region].portal.amazonaws.com*
- *[Identity Centers instance ID].portal.[Region].app.aws*
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- oidc.*[Region]*.api.aws
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- sso.*[Region]*.api.aws
- *.sso-portal.*[Region]*.amazonaws.com
- portal.sso.*[Region]*.api.aws
- *[Region]*.prod.pr.panorama.console.api.aws/panoramamaroute
- *[Region]*.signin.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

도메인 및 URL 엔드포인트 허용 목록에 대한 고려 사항

AWS 액세스 포털의 허용 목록 요구 사항 외에도 사용하는 다른 서비스 및 애플리케이션에는 도메인 허용 목록이 필요할 수 있습니다.

- 액세스 포털에서 AWS 계정 AWS Management Console 및 IAM Identity Center 콘솔에 AWS 액세스하려면 추가 도메인을 허용해야 합니다. AWS Management Console 도메인 목록은 AWS Management Console 시작 안내서의 [문제 해결](#)을 참조하세요.
- AWS 액세스 포털에서 AWS 관리형 애플리케이션에 액세스하려면 해당 도메인을 허용 목록에 추가해야 합니다. 지침은 해당 서비스 설명서를 참조하세요.
- 외부 IdPs(예: Okta 및 Microsoft Entra ID)와 같은 외부 소프트웨어를 사용하는 경우 허용 목록에 도메인을 포함해야 합니다.

IAM Identity Center의 ID 소스 자습서

AWS Organizations 관리 계정의 기존 ID 소스를 [IAM Identity Center의 조직 인스턴스에](#) 연결할 수 있습니다. 기존 ID 제공업체가 없는 경우 기본 IAM Identity Center 디렉터리에서 직접 사용자를 생성하고 관리할 수 있습니다. 조직당 ID 소스를 하나 가질 수 있습니다.

이 섹션의 자습서에서는 일반적으로 사용되는 자격 증명 소스로 IAM Identity Center의 조직 인스턴스를 설정하고, 관리 사용자를 생성하고, IAM Identity Center를 사용하여 액세스 권한을 관리하는 경우 권한 세트를 AWS 계정생성하고 구성하는 방법을 설명합니다. 애플리케이션 액세스용으로만 IAM Identity Center를 사용하는 경우 권한 세트를 사용할 필요가 없습니다.

이러한 자습서에서는 IAM Identity Center의 계정 인스턴스를 설정하는 방법을 설명하지 않습니다. 계정 인스턴스를 사용하여 사용자 및 그룹을 애플리케이션에 할당할 수 있지만 이 인스턴스 유형을 사용하여 AWS 계정에 대한 사용자 액세스를 관리할 수는 없습니다. 자세한 내용은 [IAM Identity Center의 계정 인스턴스](#) 단원을 참조하십시오.

Note

이 자습서를 시작하기 전에 IAM Identity Center를 활성화합니다. 자세한 내용은 [IAM Identity Center 활성화](#) 단원을 참조하십시오.

주제

- [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.](#)
- [자습서 비디오](#)

Active Directory를 ID 소스로 사용

Directory Service 또는 Active Directory(AD)의 자체 관리형 AWS Managed Microsoft AD 디렉터리를 사용하여 디렉터리의 사용자를 관리하는 경우 해당 사용자와 함께 작동하도록 IAM Identity Center ID 소스를 변경할 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.

- 를 사용하는 경우 AWS Managed Microsoft AD 디렉터리가 설정된 AWS 리전 동일한에서 IAM Identity Center를 활성화해야 AWS Managed Microsoft AD입니다. 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 사용합니다.
- 관리 계정에 있는 Active Directory를 사용합니다.

에 설정된 기존 AD 커넥터 또는 AWS Managed Microsoft AD 디렉터리가 있어야 하며 AWS Organizations 관리 계정 내에 있어야 AWS Directory Service합니다. 한 번에 하나의 AD Connector 디렉터리 또는 AWS Managed Microsoft AD 의 디렉터리 한 개에만 연결할 수 있습니다. 여러 도메인이나 포리스트를 지원해야 하는 경우 AWS Managed Microsoft AD를 사용합니다. 자세한 내용은 다음을 참조하세요.

- [의 디렉터를 IAM Identity Center AWS Managed Microsoft AD 에 연결](#)
- [Active Directory의 자체 관리형 디렉터를 IAM Identity Center에 연결](#)
- 위임된 관리자 계정에 있는 Active Directory를 사용합니다.

IAM Identity Center 위임된 관리자를 활성화하고 Active Directory를 IAM Identity Center ID 소스로 사용하려는 경우 위임된 관리자 계정에 있는 디렉터리에 설정된 기존 AD 커넥터 또는 AWS Managed Microsoft AD AWS 디렉터를 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

Active Directory에서 AWS Managed Microsoft AD 디렉터리 또는 자체 관리형 디렉터리를 연결할 계획이고 RADIUS MFA를와 함께 사용하지 않는 경우 IAM Identity Center에서 MFA를 AWS Directory Service활성화합니다.

AWS Managed Microsoft AD

1. [Microsoft AD 디렉터리](#)에서 지침을 검토하세요.
2. [의 디렉터리를 IAM Identity Center AWS Managed Microsoft AD 에 연결](#) 단원의 단계를 따르세요.
3. 관리자 권한을 부여하려는 사용자가 IAM Identity Center와 동기화하도록 Active Directory를 구성합니다. 자세한 내용은 [관리 사용자의 IAM Identity Center 동기화](#) 단원을 참조하십시오.

Active Directory의 자체 관리형 디렉터리

1. [Microsoft AD 디렉터리](#)에서 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 내용은 [관리 사용자의 IAM Identity Center 동기화](#) 단원을 참조하십시오.

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 콘솔](#)을 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 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](#) 단원을 참조하십시오.

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. 자세한 내용은 [외부 ID 제공업체와의 SAML 및 SCIM ID 페더레이션 사용](#) 단원을 참조하십시오.

Note

CyberArk는 현재 AWS IAM Identity Center 애플리케이션에서 SAML 다중 어설션 소비 서비스(ACS) URLs을 지원하지 않습니다. IAM Identity Center에서 [다중 리전 지원을](#) 완전히 활용하려면 SAML 기능이 필요합니다. IAM Identity Center를 추가 리전에 복제하려는 경우 단일 ACS URL을 사용하면 해당 추가 리전의 사용자 경험에 영향을 미칠 수 있습니다. 기본 리전은 계속 정상적으로 작동합니다. 이 기능을 활성화하려면 IdP 공급업체와 협력하는 것이 좋습니다. 단일 ACS URL을 사용하는 추가 리전의 사용자 경험에 대한 자세한 내용은 [the section called “여러 ACS URLs 없이 AWS 관리형 애플리케이션 사용”](#) 및 섹션을 참조하세요. [the section called “AWS 계정 여러 ACS URLs 없이 복원력에 액세스”](#).

SCIM 배포를 시작하기 전에 먼저 [자동 프로비저닝을 사용할 때 고려 사항](#)을 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: CyberArk에서 프로비저닝 구성](#)
- [\(선택 사항\) 3단계: IAM Identity Center에서 액세스 제어\(ABAC\)에 사용되는 CyberArk 사용자 속성 구성](#)
- [\(선택 사항\) 액세스 제어에 속성 전달](#)

사전 조건

시작하기 전에 다음을 준비해야 합니다.

- CyberArk 구독 또는 무료 평가판. 무료 평가판을 신청하려면 [CyberArk](#)를 방문하세요.
- IAM Identity Center 활성화 계정([무료](#)). 자세한 내용은 [IAM Identity Center 활성화](#)를 참조하세요.
- [IAM Identity Center 센터 CyberArk 설명서](#)에 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 상태에서에서만 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 콘솔](#)을 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 SCIM 엔드포인트와 액세스 토큰을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.
 - a. SCIM 엔드포인트-예: `https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. 액세스 토큰 - 토큰 표시를 선택하여 값을 복사합니다.

Warning

SCIM 엔드포인트와 액세스 토큰을 가져올 수 있는 유일한 시간입니다. 계속 진행하기 전에 이 값을 복사해야 합니다. 이 자습서의 후반부에 이 값을 입력하여 IdP에서 자동 프로비저닝을 구성할 수 있습니다.

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 [사전 조건](#)를 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. [사전 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.
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

이는 IAM Identity Center가 AWS 리소스에 대한 액세스를 관리하도록 속성을 구성하도록 선택한 CyberArk 경우의 선택적 절차입니다. 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 전달](#)을 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 사용하는 경우 Google Workspace의 사용자를 IAM Identity CenterGoogle Workspace에 통합하여 AWS 리소스에 대한 액세스 권한을 부여할 수 있습니다. IAM Identity Center ID 소스를 기본 IAM Identity Center ID 소스에서 Google Workspace로 변경하여 이 통합을 달성할 수 있습니다.

Note

Google Workspace는 현재 AWS IAM Identity Center 애플리케이션에서 SAML 다중 어설션 소비 서비스(ACS) URLs을 지원하지 않습니다. IAM Identity Center에서 [다중 리전 지원을](#) 완전히 활용하려면 SAML 기능이 필요합니다. IAM Identity Center를 추가 리전에 복제하려는 경우 단일 ACS URL을 사용하면 해당 추가 리전의 사용자 경험에 영향을 미칠 수 있습니다. 기본 리전은 계속 정상적으로 작동합니다. 이 기능을 활성화하려면 IdP 공급업체와 협력하는 것이 좋습니다. 단일 ACS URL을 사용하는 추가 리전의 사용자 경험에 대한 자세한 내용은 [the section called “여러 ACS URLs 없이 AWS 관리형 애플리케이션 사용”](#) 및 섹션을 참조하세요. [the section called “AWS 계정 여러 ACS URLs 없이 복원력에 액세스”](#).

Google Workspace의 사용자 정보는 [SCIM\(System for Cross-domain Identity Management\) 2.0 프로토콜](#)을 사용하여 IAM Identity Center에 동기화됩니다. 자세한 내용은 [외부 ID 제공업체와의 SAML 및 SCIM ID 페더레이션 사용](#) 단원을 참조하십시오.

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 수행하기 위해 Google Workspace를 ID 제공업체로 설정하고 IAM Identity Center와 연결해야 합니다.

목표

이 자습서의 단계는 Google Workspace와 간의 SAML 연결을 설정하는 방법을 안내합니다 AWS. 나중에 SCIM을 사용하여 Google Workspace에서 사용자를 동기화합니다. 모든 것이 올바르게 구성되었는지 확인하려면 구성 단계를 완료한 후 Google Workspace 사용자로 로그인하고 AWS 리소스에 대한 액세스를 확인합니다. 이 자습서는 소규모 Google Workspace 디렉터리 테스트 환경을 기반으로 합니다. 이 자습서에는 그룹 및 조직 단위와 같은 디렉터리 구조는 포함되지 않습니다. 이 자습서를 완료하면 사용자가 자격 Google Workspace 증명을 사용하여 AWS 액세스 포털에 액세스할 수 있습니다.

Note

Google Workspace 무료 평가판을 신청하려면 Google's 웹사이트에서 [Google Workspace](#)를 방문하세요.

IAM Identity Center를 아직 활성화하지 않은 경우 [IAM Identity Center 활성화](#)의 내용을 참조하세요.

고려 사항

- Google Workspace 및 IAM Identity Center 간에 SCIM 프로비저닝을 구성하기 전에 먼저 [자동 프로비저닝을 사용할 때 고려 사항](#) 검토가 권장됩니다.
- 현재 Google Workspace로부터의 SCIM 자동 동기화는 사용자 프로비저닝으로 제한됩니다. 자동 그룹 프로비저닝은 현재 지원되지 않습니다. AWS CLI Identity Store [create-group](#) 명령 또는 AWS Identity and Access Management (IAM) API [CreateGroup](#)을 사용하여 그룹을 수동으로 생성할 수 있습니다. 또는 [ssosync](#)를 사용하여 Google Workspace 사용자와 그룹을 IAM Identity Center로 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 여러개인 사용자는 동기화되지 않습니다. 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 Google Workspace의 SCIM을 사용하여 해당 사용자를 덮어쓰고 동기화합니다.
- ID 소스를 변경할 때 고려해야 할 추가 사항이 있습니다. 자세한 내용은 [the section called “IAM Identity Center에서 외부 IdP로 변경”](#) 단원을 참조하십시오.

1단계: Google Workspace: SAML 애플리케이션 구성

1. 슈퍼 관리자 권한이 있는 계정을 사용하여 Google 관리 콘솔에 로그인합니다.
2. Google 관리 콘솔의 왼쪽 탐색 패널에서 앱을 선택한 다음 웹 및 모바일 앱을 선택합니다.

3. 앱 추가 드롭다운 목록에서 앱 검색을 선택합니다.
4. 검색 상자에 Amazon Web Services를 입력한 다음 목록에서 Amazon Web Services(SAML) 앱을 선택합니다.
5. Google ID 제공업체 세부 정보-Amazon Web Services 페이지에서 다음 중 하나를 수행할 수 있습니다.
 - a. IdP 메타데이터를 다운로드합니다.
 - b. SSO URL, 엔터티 ID URL 및 인증서 정보를 복사합니다.

2단계에서는 XML 파일 또는 URL 정보가 필요합니다.

6. Google 관리자 콘솔의 다음 단계로 이동하기 전에 이 페이지를 열어 두고 IAM Identity Center 콘솔로 이동합니다.

2단계: IAM Identity Center 및 Google Workspace: IAM Identity Center ID 소스를 변경하고 Google Workspace를 SAML ID 제공업체로 설정합니다.

1. 관리 권한이 있는 역할을 사용하여 [IAM Identity Center 콘솔](#)에 로그인합니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 설정 페이지에서 작업을 선택한 다음 ID 소스 변경을 선택합니다.
 - IAM Identity Center를 활성화하지 않은 경우 자세한 내용은 [IAM Identity Center 활성화](#)를 참조하세요. IAM Identity Center를 처음 활성화하고 액세스한 후에는 대시보드에 도착하여 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 Identity Provider 메타데이터 섹션에서 다음 중 하나를 수행해야 합니다.
 - i. IAM Identity Center 콘솔에서 Google SAML 메타데이터를 IdP SAML 메타데이터로 업로드합니다.
 - ii. Google SSO URL을 IdP 로그인 URL 필드에 복사하여 붙여넣고, Google 발급자 URL을 IdP 발급자 URL 필드에 붙여넣고, Google 인증서를 IdP 인증서로 업로드합니다.

6. IAM Identity Center 콘솔의 Identity Provider 메타데이터 섹션에 Google 메타데이터를 제공한 후 IAM Identity Assertion Consumer Service(ACS) URL 및 IAM Identity Center 발급자 URL을 복사합니다. 다음 단계에서 Google 관리자 콘솔에서 이러한 URLs을 제공해야 합니다.
7. IAM Identity Center 콘솔을 사용하여 페이지를 열어 두고 Google 관리자 콘솔로 돌아갑니다. Amazon Web Services-서비스 공급자 세부 정보 페이지에 있어야 합니다. 계속을 선택합니다.
8. 서비스 공급자 세부 정보 페이지에서 ACS URL 및 엔터티 ID 값을 입력합니다. 이전 단계에서 이러한 값을 복사했으며 IAM Identity Center 콘솔에서 찾을 수 있습니다.
 - IAM Identity Center Assertion Consumer Service(ACS) URL을 ACS URL 필드에 붙여넣습니다.
 - IAM Identity Center 발급자 URL을 Entity ID 필드에 붙여 넣습니다.
9. 서비스 공급자 세부 정보 페이지에서 다음과 같이 이름 ID 아래의 필드를 입력합니다.
 - 이름 ID 형식의 경우 이메일을 선택합니다.
 - 이름 ID의 경우 기본 정보 > 기본 이메일을 선택합니다.
10. 계속을 선택합니다.
11. 속성 매핑 페이지의 속성 아래에서 매핑 추가를 선택하고 Google 디렉터리 속성에서 이 필드를 구성합니다.
 - `https://aws.amazon.com/SAML/Attributes/RoleSessionName` 앱 속성의 경우 Google Directory 속성 에서 기본 정보, 기본 이메일 필드를 선택합니다.
 - `https://aws.amazon.com/SAML/Attributes/Role` 앱 속성에서 Google Directory 속성을 선택합니다. Google 디렉터리 속성은 부서일 수도 있습니다.
12. 완료를 클릭합니다.
13. IAM Identity Center 콘솔로 돌아가서 다음을 선택합니다. 검토 및 확인 페이지에서 정보를 검토한 다음 제공된 공간에 ACCEPT를 입력합니다. ID 소스 변경을 선택합니다.

이제 Google Workspace에서 Amazon Web Services 앱을 활성화하여 사용자가 IAM Identity Center에 프로비저닝할 준비가 되었습니다.

3단계: Google Workspace: 앱 활성화

1. 앱과 웹 및 모바일 앱에서 찾을 수 있는 Google 관리 콘솔과 AWS IAM Identity Center 애플리케이션으로 돌아갑니다.
2. 사용자 액세스 패널의 사용자 액세스 옆에서 아래쪽 화살표를 선택하여 사용자 액세스 확장을 선택하여 서비스 상태 패널을 표시합니다.

3. 서비스 상태에서 모든 사용자에게 대해 커짐을 선택한 다음 저장을 선택합니다.

Note

최소 권한 원칙을 유지하는 데 도움이 되도록 이 자습서를 완료한 후 서비스 상태를 모든 사용자에게 대해 꺼짐으로 변경하는 것이 좋습니다. AWS에 대한 액세스 권한이 필요한 사용자만 서비스를 활성화해야 합니다. Google Workspace 그룹 또는 조직 단위를 사용하여 특정 사용자 하위 세트에 대한 액세스 권한을 사용자에게 부여할 수 있습니다.

4단계: IAM Identity Center: IAM Identity Center 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. 이후 자습서의 5단계에서는 이 값을 입력하여 Google Workspace에서 프로비저닝을 구성합니다.
 - a. SCIM 엔드포인트 - 예:
 - IPv4 `https://scim.Region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - 듀얼 스택 `https://scim.Region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. 액세스 토큰 - 토큰 표시를 선택하여 값을 복사합니다.

Warning

SCIM 엔드포인트와 액세스 토큰을 가져올 수 있는 유일한 시간입니다. 계속 진행하기 전에 이 값을 복사해야 합니다.

4. 닫기를 선택하세요.

이제 IAM Identity Center 콘솔에서 프로비저닝을 설정했으므로 Google Workspace에서 자동 프로비저닝 IAM Identity Center 커넥터를 사용하여 남은 작업을 완료합니다.

5단계: Google Workspace에서 자동 프로비저닝 구성

1. 앱 및 웹 및 모바일 앱에서 찾을 수 있는 Google 관리자 콘솔과 AWS IAM Identity Center 애플리케이션으로 돌아갑니다. 자동 프로비저닝 섹션에서 자동 프로비저닝 구성을 선택합니다.
2. 이전 절차에서 IAM Identity Center 콘솔에서 액세스 토큰 값을 복사했습니다. 해당 값을 `액세스 토큰` 필드에 붙여 넣고 계속을 선택합니다. 또한 이전 절차에서 IAM Identity Center 콘솔에서 SCIM 엔드포인트 값을 복사했습니다. 해당 값을 Endpoint URL 필드에 붙여넣고 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 범위에서 Google Workspace 디렉터리가 있는 그룹을 선택하여 Amazon Web Services 앱에 대한 액세스를 제공할 수 있습니다. 이 단계를 건너뛰고 계속을 선택합니다.
5. 프로비저닝 해제에서 사용자의 액세스를 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. 정보가 Google Workspace 디렉터리의 정보와 일치해야 합니다.

축하합니다!

Google Workspace 및 간에 SAML 연결을 성공적으로 설정하고 자동 프로비저닝이 작동하는지 확인 AWS 했습니다. 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.

액세스 제어에 속성 전달-선택 사항

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 전달](#)을 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.

에 액세스 권한 할당 AWS 계정

다음 단계는에 대한 액세스 권한만 부여하는 데 AWS 계정 만 필요합니다. 이러한 단계는 AWS 애플리케이션에 대한 액세스 권한을 부여하는 데 필요하지 않습니다.

Note

이 단계를 완료하려면 IAM Identity Center의 조직 인스턴스가 필요합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

1단계: IAM Identity Center: Google Workspace 사용자에게 계정에 대한 액세스 권한 부여

1. IAM Identity Center 콘솔로 돌아갑니다. 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. 그리고 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 세트 정책 섹션에서 AdministratorAccess를 선택합니다.
- 다음을 선택합니다.
- ii. 2단계: 권한 세트 세부 정보 지정 페이지에서 기본 설정을 유지하고 다음을 선택합니다.

기본 설정에서는 세션 지속 시간이 1시간으로 설정된 *AdministratorAccess*라는 권한 세트를 생성합니다.

- iii. 3단계: 검토 및 생성에서 권한 세트 유형이 AWS 관리형 정책 AdministratorAccess를 사용하는지 확인합니다. 생성(Create)을 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 세트가 목록에 표시됩니다. 권한 세트의 확인란을 선택하고 다음을 선택합니다.
- c. 3단계: 검토 및 제출에서 선택한 사용자 및 권한 세트를 검토한 다음 제출을 선택합니다.

페이지는가 구성 AWS 계정 중이라는 메시지로 업데이트됩니다. 프로세스가 완료될 때까지 기다립니다.

AWS 계정 페이지로 돌아갑니다. 알림 메시지는가 재프로비저닝되었고 업데이트된 권한 세트 AWS 계정 가 적용되었음을 알려줍니다. 사용자가 로그인하면 *AdministratorAccess* 역할을 선택할 수 있는 옵션이 제공됩니다.

Note

Google Workspace의 SCIM 자동 동기화는 사용자 프로비저닝만 지원합니다. 자동 그룹 프로비저닝은 현재 지원되지 않습니다. AWS Management Console을 사용하여 Google Workspace 사용자에게 대한 그룹을 생성할 수는 없습니다. 사용자를 프로비저닝한 후 AWS CLI Identity Store [create-group](#) 명령 또는 IAM API [CreateGroup](#)을 사용하여 그룹을 생성할 수 있습니다.

2단계: Google Workspace: AWS 리소스에 대한 Google Workspace 사용자 액세스 확인

1. 테스트 사용자 계정을 사용하여 Google에 로그인합니다. Google Workspace에 사용자를 추가하는 방법을 알아보려면 [Google Workspace 설명서](#)를 참조하세요.
2. Google apps런처(와플 모양) 아이콘을 선택합니다.
3. 사용자 지정 Google Workspace 앱이 있는 앱 목록 하단으로 스크롤합니다. Amazon Web Services 앱이 표시됩니다.

4. Amazon Web Services 앱을 선택합니다. AWS 액세스 포털에 로그인했으며 AWS 계정 아이콘을 볼 수 있습니다. 해당 아이콘을 확장하여 사용자가 액세스할 수 있는 AWS 계정 목록을 확인합니다. 이 자습서에서는 단일 계정만 사용했으므로 아이콘을 확장하면 하나의 계정만 표시됩니다.
5. 계정을 선택하면 사용자에게 제공되는 권한 세트가 표시됩니다. 이 자습서에서는 AdministratorAccess 권한 세트를 생성했습니다.
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.

다음 단계

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

- AWS CLI Identity Store [create-group](#) 명령 또는 IAM API [CreateGroup](#)을 사용하여 사용자를 위한 그룹을 생성합니다.

그룹은 AWS 계정 및 애플리케이션에 대한 액세스를 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.

- 직무에 따라 권한을 구성합니다. [권한 세트 생성](#)을 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 관리](#)하는 방법을 검토하세요.

문제 해결

Google Workspace를 사용한 일반적인 SCIM 및 SAML 문제 해결은 다음 섹션을 참조하세요.

- [특정 사용자가 외부 SCIM 공급자로부터 IAM Identity Center로 동기화하지 못함](#)
- [IAM Identity Center에서 생성된 SAML 어설션 콘텐츠 관련 문제](#)
- [외부 ID 제공업체에서 사용자 또는 그룹을 프로비저닝할 때의 중복 사용자 또는 그룹 오류](#)
- Google Workspace 문제 해결은 [Google Workspace 설명서](#)를 참조하세요.

다음 리소스는 작업 시 문제를 해결하는 데 도움이 될 수 있습니다. AWS

- [AWS re:Post](#)-문제를 해결할 때 도움이 되는 FAQ와 기타 리소스 링크를 찾을 수 있습니다.
- [AWS Support](#)-기술 지원 받기

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 [SAML\(Security Assertion Markup Language\) 2.0](#) 프로토콜을 사용합니다. 자세한 내용은 [외부 ID 제공업체와의 SAML 및 SCIM ID 페더레이션 사용](#) 단원을 참조하십시오.

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 사항](#)을 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 [JumpCloud](#)를 방문하세요.
- IAM Identity Center 지원 계정([무료](#)). 자세한 내용은 [IAM Identity Center 활성화](#)를 참조하세요.
- [IAM Identity Center 센터 JumpCloud 설명서](#)에 설명된 대로 JumpCloud 계정에서 IAM Identity Center로의 SAML 연결을 수행합니다.
- IAM Identity Center를 추가 리전에 복제한 경우 AWS 관리형 애플리케이션 및 해당 리전 AWS 계정에서 액세스할 수 있도록 ID 제공업체 구성을 업데이트해야 합니다. 자세한 내용은 [the section called “3단계: 외부 IdP 설정 업데이트”](#) 섹션을 참조하세요. 자세한 내용은 JumpCloud 설명서를 참조하세요.
- 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.

- 의 AWS Single Sign-On 커넥터와 연결된 그룹만 SCIM과 동기화 JumpCloud됩니다.
- 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.

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 콘솔](#)을 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 SCIM 엔드포인트와 액세스 토큰을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.
 - a. SCIM 엔드포인트-예: `https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. 액세스 토큰 - 토큰 표시를 선택하여 값을 복사합니다.

Warning

SCIM 엔드포인트와 액세스 토큰을 가져올 수 있는 유일한 시간입니다. 계속 진행하기 전에 이 값을 복사해야 합니다. 이 자습서의 후반부에 이 값을 입력하여 IdP에서 자동 프로비저닝을 구성할 수 있습니다.

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 조건](#)을 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 참조하세요.
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.
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 IAM Identity Center가 AWS 리소스에 대한 액세스를 관리하도록 속성을 구성하도록 선택한 JumpCloud 경우의 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 구성](#)을 참조하세요.

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 두 번째 탭인 IAM Identity Center를 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. 예: `https://aws.amazon.com/SAML/Attributes/AccessControl:Email`.
 - 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 전달](#)을 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.

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

AWS IAM Identity Center 는 [SAML\(Security Assertion Markup Language\) 2.0](#)과의 통합과 SCIM(System for Cross-domain Identity Management) 2.0 프로토콜을 사용하여 Microsoft Entra ID (이전에는 Azure Active Directory 또는 라고 함 Azure AD)에서 IAM Identity Center로 사용자 및 그룹 정보의 [자동 프로비저닝](#)(동기화)을 지원합니다. [SCIM 프로필](#) 자세한 내용은 [외부 ID 제공업체와의 SAML 및 SCIM ID 페더레이션 사용](#) 단원을 참조하십시오.

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 설명서에서 [Quickstart: 테넌트 설정](#)을 참조하십시오.
- AWS IAM Identity Center 활성화된 계정입니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [IAM Identity Center 활성화](#)를 참조하십시오.

고려 사항

다음은 SCIM v2 프로토콜을 사용하여 프로덕션 환경에서 IAM Identity Center를 통해 [자동 프로비저닝](#)을 구현하는 방법에 영향을 미칠 수 있는 Microsoft Entra ID 관련 중요 고려 사항입니다.

자동 프로비저닝

SCIM 배포를 시작하기 전에 먼저 [자동 프로비저닝을 사용할 때 고려 사항](#)의 내용을 검토하는 것이 좋습니다.

액세스 제어를 위한 속성

액세스 제어 속성은 자격 증명 소스의 누가 AWS 리소스에 액세스할 수 있는지 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 설명서의 [할당 기반 범위 지정](#)을 참조하세요. 또는 [IAM Identity Center 구성 가능 AD 동기화](#)를 사용하여 IAM Identity Center와 Active Directory 그룹을 통합할 수 있습니다.

동적 그룹

Microsoft Entra ID 사용자 프로비저닝 서비스는 [동적 그룹](#)의 사용자를 읽거나 프로비저닝할 수 없습니다. 동적 그룹을 사용하는 동안의 사용자 및 그룹 구조와 IAM Identity Center에 표시되는 방식을 보여주는 예는 아래를 참조하세요. 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 명심하세요.

- 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 설명서의 [미리 보기 제한 사항](#)을 참조하세요.

1단계: Microsoft 테넌트 준비

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

Step 1.1 >

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

이 절차에서는에 AWS IAM Identity Center 엔터프라이즈 애플리케이션을 설치합니다Microsoft Entra ID. SAML 연결을 구성하려면 나중 에이 애플리케이션이 필요합니다 AWS.

1. [Microsoft Entra 관리 센터](#)에 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**를 입력합니다.
4. 결과에서 AWS IAM Identity Center를 선택합니다.
5. 생성(Create)을 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. 암호에서 강력한 암호를 입력하거나 눈 모양 아이콘을 선택하여 자동 생성된 암호를 표시한 후 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:에 권한을 할당하기 전에 Nikki의 경험 테스트 AWS IAM Identity Center

이 절차에서는 Nikki가 Microsoft [내 계정 포털](#)에 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 창에서 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 자격 증명 > 애플리케이션 > 엔터프라이즈 애플리케이션으로 이동한 후 목록에서 AWS IAM Identity Center를 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 내 AWS 계정 페이지에서 리전을 관리하는 데 필요한 계정 권한을 Nikki에 부여하는 데 사용됩니다 AWS Management Console. Nikki 계정에서 다른 정보를 보거나 관리할 수 있는 기타 모든 권한은 기본적으로 거부됩니다.

1. [IAM Identity Center 콘솔](#)을 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**

- 리소스 추가 옆에 있는 추가를 선택합니다.
- 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": [
        "*"
      ]
    }
  ]
}
```

- 다음을 선택합니다.
- 권한 세트 세부 정보 지정 페이지의 권한 세트 이름에서 **RegionalAdmin**을 입력하고 다음을 선택합니다.
- 검토 및 생성 페이지에서 생성을 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 콘솔](#)을 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

여기서 Nikki AWS 계정 가 리전을 관리하는를 찾은 다음 액세스 AWS 포털에 성공적으로 액세스하는 데 필요한 권한을 할당합니다.

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 다중 계정 권한에서 AWS 계정을 선택합니다.
3. Nikki에게 리전을 관리할 수 있는 액세스 권한을 부여하려는 계정 이름(예: #####) 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.
5. Example

<caption>On the 권한 세트 선택 page, choose the RegionalAdmin permission set created in Step 2.1, and then choose 다음.</caption>

6. 검토 및 제출 페이지에서 선택 내용을 검토한 후 제출을 선택합니다.

3단계: SAML 연결 구성 및 테스트

이 단계에서는 IAM Identity Center의 외부 IdP 설정과 Microsoft Entra ID 함께의 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 연결을 구성할 때 입력해야 하는 메타데이터 파일과 AWS 특정 로그인 URLMicrosoft Entra ID을 검색합니다.

1. [IAM Identity Center 콘솔](#)에서 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 제공업체 구성 페이지의 서비스 제공업체 메타데이터에서 기본 IPv4 또는 듀얼 스택을 선택합니다. 자격 증명 소스 변경을 완료한 후 서비스 공급자 메타데이터 파일을 다운로드할 수 있습니다.
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 이동하여에서 AWS IAM Identity Center 엔터프라이즈 애플리케이션을 구성합니다Microsoft Entra ID. 나중에 이 페이지로 돌아와 프로세스를 완료하게 됩니다.

Step 3.2 >

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

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 Center를 선택합니다.
2. 왼쪽에서 2를 선택합니다. Single Sign-On을 설정합니다.
3. SAML로 Single Sign-On 설정 페이지에서 SAML을 선택합니다. 그런 다음 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 회신 URL(어설션 소비자 서비스 URL) 값이 모두 엔드포인트를 가리키는지 확인합니다 AWS.

- 식별자 - IAM Identity Center의 발급자 URL입니다. IPv4-only 엔드포인트를 사용하는지 아니면 듀얼 스택 엔드포인트를 사용하는지에 관계없이 동일한 값이 적용됩니다.
 - 회신 URL(Assertion Consumer Service URL) - 여기의 값에는 IAM Identity Center의 활성화된 모든 리전의 IPv4-only 및 듀얼 스택 엔드포인트가 모두 포함됩니다. 사용자가에서 Amazon Web Services 애플리케이션을 시작할 때 기본 리전으로 리디렉션되도록 기본 리전의 ACS URL을 기본 URL로 사용할 수 있습니다Microsoft Entra ID. ACS URLs[기본 및 추가의 ACS 엔드포인트 AWS 리전](#).
 - (선택 사항) IAM Identity Center를 추가 리전에 복제한 경우 각 추가 리전의 AWS 액세스 포털에 Microsoft Entra ID 대해에서 북마크 앱을 생성할 수도 있습니다. 이를 통해 사용자에서 추가 리전의 AWS 액세스 포털에 액세스할 수 있습니다Microsoft Entra ID. 사용자에게의 북마크 앱에 액세스할 수 있는 권한을 부여해야 합니다Microsoft Entra ID. 자세한 내용은 [Microsoft Entra ID 설명서를](#) 참조하세요. 나중에 IAM Identity Center를 추가 리전에 복제하려는 경우 초기 설정 후 추가 리전에 대한 액세스를 활성화하는 방법에 [Microsoft Entra ID 추가 리전에 액세스하기 위한 구성](#) 대한 지침을 보려면 섹션을 참조하세요.
5. 로그인 URL(선택 사항)에 이전 단계(**Step 3.1**)에서 복사한 AWS 액세스 포털 로그인 URL 값을 붙여 넣고 저장을 선택한 다음 X를 선택하여 창을 닫습니다.
 6. 를 사용하여 Single Sign-On을 테스트하라는 메시지가 표시되면 나중에 테스트하겠습니다를 AWS IAM Identity Center선택합니다. 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. 인증되면 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 창에서 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 디스플레이를 확인합니다.

Tip

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

Step 3.5

3.5단계: Nikki의 액세스 수준을 테스트하여 AWS 계정관리

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 계정 탭을 선택하여 계정 목록을 표시합니다. 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. 암호에서 강력한 암호를 입력하거나 눈 모양 아이콘을 선택하여 자동 생성된 암호를 표시한 후 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 콘솔](#)을 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:

- IPv4: `https://scim.aws-region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - 듀얼 스택: `https://scim.aws-region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
- b. 액세스 토큰 - 토큰 표시를 선택하여 값을 복사합니다.

 Warning

SCIM 엔드포인트와 액세스 토큰을 가져올 수 있는 유일한 시간입니다. 계속 진행하기 전에 이 값을 복사해야 합니다.

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 Center를 선택합니다.
2. 프로비저닝을 선택하고 관리에서 프로비저닝을 다시 선택합니다.
3. 프로비저닝 모드에서 자동을 선택합니다.
4. 관리자 보안 인증 정보의 테넌트 URL에서 이전 **Step 4.2**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 3.5를 사용하여 액세스 수준을 테스트할 수 있습니다.

축하합니다!

Microsoft AWS 와 간에 SAML 연결을 성공적으로 설정하고 자동 프로비저닝이 모든 것을 동기화된 상태로 유지하기 위해 작동하는지 확인했습니다. 이제 학습한 내용을 적용하여 프로덕션 환경을 보다 원활하게 설정할 수 있습니다.

5단계: ABAC 구성-선택 사항

SAML과 SCIM을 구성했으므로 속성 기반 액세스 제어(ABAC)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.

Configure user attributes in Microsoft Entra ID for access control in IAM Identity Center

IAM Identity Center에서 액세스 제어를 위해 Microsoft Entra ID에서 사용자 속성 구성

다음 절차에서는 IAM Identity Center에서 AWS 리소스에 대한 액세스를 관리하는 데 Microsoft Entra ID 사용해야 하는 속성을 결정합니다. 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](#) 섹션을 참조하세요.

1. [Microsoft Entra 관리 센터](#) 콘솔에서 ID > 애플리케이션 > 엔터프라이즈 애플리케이션으로 이동한 다음 AWS IAM Identity Center를 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*을 입력합니다. IAM Identity Center에서 *AttributeName*을 예상하는 속성의 이름으로 바꿉니다. 예를 들어 AccessControl:Department입니다.
 - c. 네임스페이스에 <https://aws.amazon.com/SAML/Attributes>를 입력합니다.
 - d. 소스에서 속성을 선택합니다.
 - e. 소스 속성의 경우 드롭다운 목록을 사용하여 Microsoft Entra ID 사용자 속성을 선택합니다. 예를 들어 user.department입니다.
5. SAML 어설션에서 IAM Identity Center로 전송해야 하는 각 속성에 대해 이전 단계를 반복합니다.
6. 저장을 선택합니다.

Configure ABAC using IAM Identity Center

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 전달](#)을 참조하세요.

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

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

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

에 액세스 권한 할당 AWS 계정

다음 단계는에 대한 액세스 권한만 부여하는 데 AWS 계정 만 필요합니다. 이러한 단계는 AWS 애플리케이션에 대한 액세스 권한을 부여하는 데 필요하지 않습니다.

Note

이 단계를 완료하려면 IAM Identity Center의 조직 인스턴스가 필요합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

1단계: IAM Identity Center: Microsoft Entra ID 사용자에게 계정에 대한 액세스 권한 부여

1. IAM Identity Center 콘솔로 돌아갑니다. 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. 그리고 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 세트 정책 섹션에서 AdministratorAccess를 선택합니다.
 다음을 선택합니다.
 - ii. 2단계: 권한 세트 세부 정보 지정 페이지에서 기본 설정을 유지하고 다음을 선택합니다.

기본 설정에서는 세션 지속 시간이 1시간으로 설정된 **AdministratorAccess**라는 권한 세트를 생성합니다.
 - iii. 3단계: 검토 및 생성에서 권한 세트 유형이 AWS 관리형 정책 AdministratorAccess를 사용하는지 확인합니다. 생성(Create)을 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 세트가 목록에 표시됩니다. 권한 세트의 확인란을 선택하고 다음을 선택합니다.
 - c. 3단계: 검토 및 제출에서 선택한 사용자 및 권한 세트를 검토한 다음 제출을 선택합니다.

페이지는 구성 AWS 계정 중인 메시지로 업데이트됩니다. 프로세스가 완료될 때까지 기다립니다.

AWS 계정 페이지로 돌아갑니다. 알림 메시지가 재프로비저닝되었고 업데이트된 권한 세트 AWS 계정 가 적용되었음을 알려줍니다. 사용자가 로그인하면 **AdministratorAccess** 역할을 선택할 수 있는 옵션이 제공됩니다.

2단계: Microsoft Entra ID: AWS 리소스에 대한 Microsoft Entra ID 사용자 액세스 확인

1. Microsoft Entra ID 콘솔로 돌아가서 IAM Identity Center SAML 기반 로그인 애플리케이션으로 이동합니다.
2. 사용자 및 그룹을 선택하고 사용자 또는 그룹 추가를 선택합니다. 4단계의 이 자습서에서 생성한 사용자를 Microsoft Entra ID 애플리케이션에 추가합니다. 사용자를 추가하면 사용자가 AWS에 로그인할 수 있습니다. 4단계에서 생성한 사용자를 검색합니다. 이 단계를 따른 경우 **RichardRoe**가 됩니다.
 - 데모는 [Microsoft Entra ID를 사용하여 기존 IAM Identity Center 인스턴스 페더레이션을 참조하세요](#).

Microsoft Entra ID IAM Identity Center의 추가 리전에 액세스하기 위한 구성 - 선택 사항

IAM Identity Center를 추가 리전에 복제한 경우 추가 리전을 AWS 계정 통해 AWS 관리형 애플리케이션 및에 액세스할 수 있도록 ID 제공업체 구성을 업데이트해야 합니다. 아래 단계는 절차를 안내합니다. 사전 조건을 포함하여이 주제에 대한 자세한 내용은 섹션을 참조하세요 [여러에서 IAM Identity Center 사용 AWS 리전](#).

1. 에 설명된 대로 IAM Identity Center 콘솔에서 추가 리전의 ACS URLs을 검색합니다 [기본 및 추가의 ACS 엔드포인트 AWS 리전](#).
2. [Microsoft Entra 관리 센터](#) 콘솔에서 ID > 애플리케이션 > 엔터프라이즈 애플리케이션으로 이동한 다음 AWS IAM Identity Center을 선택합니다.
3. 왼쪽에서 2를 선택합니다. Single Sign-On을 설정합니다.
4. 기본 SAML 구성 페이지의 회신 URL(어설션 소비자 서비스 URL) 섹션에서 각 추가 리전의 ACS URL에 대한 회신 URL 추가를 선택합니다. 사용자가에서 AWS IAM Identity Center 애플리케이션을 시작할 때 기본 리전으로 계속 리디렉션되도록 기본 리전의 ACS URL을 기본 URL로 유지할 수 있습니다Microsoft Entra ID.
5. ACS URLs 추가가 완료되면 AWS IAM Identity Center 애플리케이션을 저장합니다.
6. 각 추가 리전의 AWS 액세스 포털에 Microsoft Entra ID 대해에서 북마크 앱을 생성할 수 있습니다. 이를 통해 사용자는에서 추가 리전의 AWS 액세스 포털에 액세스할 수 있습니다Microsoft Entra ID. 사용자에게의 북마크 앱에 액세스할 수 있는 권한을 부여해야 합니다Microsoft Entra ID. 자세한 내용은 [Microsoft Entra ID 설명서를](#) 참조하세요.

7. 각 추가 리전에서 AWS 액세스 포털에 로그인할 수 있는지 확인합니다. [AWS 액세스 포털 URLs](#)로 이동하거나에서 북마크 앱을 시작합니다Microsoft Entra ID.

문제 해결

Microsoft Entra ID를 사용한 일반적인 SCIM 및 SAML 문제 해결은 다음 섹션을 참조하세요.

- [Microsoft Entra ID 및 IAM Identity Center와의 동기화 문제](#)
- [특정 사용자가 외부 SCIM 공급자로부터 IAM Identity Center로 동기화하지 못함](#)
- [IAM Identity Center에서 생성된 SAML 어설션 콘텐츠 관련 문제](#)
- [외부 ID 제공업체에서 사용자 또는 그룹을 프로비저닝할 때의 중복 사용자 또는 그룹 오류](#)
- [추가 리소스](#)

Microsoft Entra ID 및 IAM Identity Center와의 동기화 문제

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"}
```

AWS CloudTrail 실패한 이벤트를 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 [문제 해결](#)을 참조하세요.

Microsoft Entra ID 게스트 계정 동기화

Microsoft Entra ID 게스트 사용자를 IAM Identity Center에 동기화하려면 다음 절차를 참조하세요.

Microsoft Entra ID 게스트 사용자의 이메일이 Microsoft Entra ID 사용자와 다릅니다. 이 차이는 Microsoft Entra ID 게스트 사용자를 IAM Identity Center와 동기화하려고 할 때 문제를 일으킵니다. 예를 들어 게스트 사용자의 다음 이메일 주소를 참조하세요.

exampleuser_domain.com#EXT#@domain.onmicrosoft.com.

IAM Identity Center의 이메일 주소에는 **#EXT#@domain** 형식이 포함되지 않아야 합니다.

1. [Microsoft Entra 관리 센터](#)에 로그인하고 ID > 애플리케이션 > 엔터프라이즈 애플리케이션으로 이동한 다음 AWS IAM Identity Center를 선택합니다.
2. 왼쪽 창의 Single Sign On 탭으로 이동합니다.
3. 사용자 속성 및 클레임 옆에 나타나는 편집을 선택합니다.
4. 필수 클레임 다음에 고유 사용자 식별자(이름 ID)를 선택합니다.
5. Microsoft Entra ID 사용자와 게스트 사용자에 대해 두 가지 클레임 조건을 생성합니다.
 - a. Microsoft Entra ID 사용자의 경우 소스 속성이 user.userprincipalname로 설정된 멤버에 대한 사용자 유형을 생성합니다.
 - b. Microsoft Entra ID 게스트 사용자의 경우 소스 속성이 user.mail로 설정된 외부 게스트의 사용자 유형을 생성합니다.
 - c. 저장을 선택하고 Microsoft Entra ID 게스트 사용자로 로그인을 다시 시도합니다.

추가 리소스

- 일반 SCIM 문제 해결 팁은 [IAM Identity Center 문제 해결](#) 섹션을 참조하세요.
- Microsoft Entra ID 문제 해결은 [Microsoft 설명서](#)를 참조하세요.
- 여러의 페더레이션에 대한 자세한 내용은 [AWS 계정 를 사용하여 보안을 Azure Active Directory Federation](#) AWS 계정참조하세요.

다음 리소스는 작업 시 문제를 해결하는 데 도움이 될 수 있습니다. AWS

- [AWS re:Post](#)-문제를 해결할 때 도움이 되는 FAQ와 기타 리소스 링크를 찾을 수 있습니다.
- [AWS Support](#)-기술 지원 받기

Okta 및 IAM Identity Center를 사용하여 SAML 및 SCIM 구성

[SCIM\(System for Cross-domain Identity Management\) v2.0 프로토콜](#)을 사용하여 Okta의 사용자 및 그룹 정보를 IAM Identity Center로 자동 프로비저닝(동기화)할 수 있습니다. 자세한 내용은 [외부 ID 제공 업체와의 SAML 및 SCIM ID 페더레이션 사용](#) 단원을 참조하십시오.

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 계정 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

Okta와 IAM Identity Center 모두에서 관리 오버헤드를 최소화하려면 개별 사용자 대신 그룹을 할당하고 푸시하는 것이 좋습니다.

- 사용자 가져오기 - 사용자를 IAM Identity Center에서 로 가져올 수 있습니다Okta.

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 액세스를 확인합니다.

SAML을 통해 IAM Identity CenterOkta에 연결할 때 다음 기능이 지원됩니다.

- IdP 시작 SAML 로그인 - 사용자는 Okta 포털을 통해 로그인하고 IAM Identity Center에 액세스할 수 있습니다.
- SP 시작 SAML 로그인 - 사용자는 AWS 액세스 포털에 액세스하여 Okta 포털을 통해 로그인하도록 리디렉션합니다.

Note

Okta's [IAM Identity Center 애플리케이션](#)이 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.

IAM Identity Center를 아직 활성화하지 않은 경우 [IAM Identity Center 활성화](#)의 내용을 참조하세요.

고려 사항

- Okta 및 IAM Identity Center 간에 SCIM 프로비저닝을 구성하기 전에 먼저 [자동 프로비저닝을 사용할 때 고려 사항](#) 검토가 권장됩니다.
- 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 여러개인 사용자는 동기화되지 않습니다. 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.
- IAM Identity Center와 함께 Okta를 사용하는 경우 IAM Identity Center는 일반적으로 Okta에서 애플리케이션으로 구성됩니다. 이를 통해 IAM Identity Center의 여러 인스턴스를 여러 애플리케이션으로 구성하여 Okta의 단일 인스턴스 내에서 여러 AWS 조직에 대한 액세스를 지원할 수 있습니다.
- 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.

- IAM Identity Center를 추가 리전에 복제한 경우 관리 AWS 형 애플리케이션 및 추가 리전을 AWS 계정 통해 액세스할 수 있도록 ID 제공업체 구성을 업데이트해야 합니다. 사전 조건을 포함한 자세한 내용은 섹션을 참조하세요 [여러에서 IAM Identity Center 사용 AWS 리전](#). Okta별 단계는에 설명되어 있습니다. [Okta 추가 리전에 액세스하기 위한 구성](#)

1단계: Okta: 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 입력하고 앱을 AWS IAM Identity Center 선택하여 IAM Identity Center 앱을 추가합니다.
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.xml로 저장합니다.

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

2단계: Okta를 IAM Identity Center의 ID 소스로 구성

1. 관리 권한이 있는 사용자로 [IAM Identity Center 콘솔](#)을 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 쉽게 액세스할 수 있도록 다음 항목을 텍스트 파일에 복사합니다.
 - IAM Identity Center Assertion Consumer Service(ACS) URL - IPv4-only 및 듀얼 스택 ACS URLs. 또한 IAM Identity Center 인스턴스가 여러 리전에서 활성화된 경우 각 추가 리전에는 자체 IPv4-only 및 듀얼 스택 ACS URLs. ACS URLs [기본 및 추가의 ACS 엔드포인트 AWS 리전](#).

- IAM Identity Center 발급자 URL

이후 자습서에서는 이러한 값을 업데이트합니다.

- b. ID 제공업체 메타데이터의 IdP SAML 메타데이터에서 파일 선택을 선택한 다음 이전 단계에서 생성한 `metadata.xml` 파일을 선택합니다.
 - c. 다음을 선택합니다.
6. 고지 사항을 읽고 진행할 준비가 되면 ACCEPT를 입력합니다.
 7. ID 소스 변경을 선택합니다.

AWS 콘솔을 열어 두면 다음 단계에서이 콘솔을 계속 사용할 수 있습니다.

8. 로 돌아가서 AWS IAM Identity Center 앱의 로그인 탭을 Okta admin dashboard 선택한 다음 편집을 선택합니다.
9. 고급 로그인 설정에서 다음을 입력합니다.
 - ACS URL에 IAM Identity Center Assertion Consumer Service(ACS) URL에 복사한 값(들)을 입력합니다. 사용자가에서 Amazon Web Services 애플리케이션을 시작할 때 기본 리전으로 리디렉션되도록 기본 리전의 ACS URL을 기본 URL로 사용할 수 있습니다Okta.
 - (선택 사항) IAM Identity Center를 추가 리전에 복제한 경우 각 추가 리전의 AWS 액세스 포털에 Okta 대해에서 북마크 앱을 생성할 수도 있습니다. 이를 통해 사용자는에서 추가 리전의 AWS 액세스 포털에 액세스할 수 있습니다Okta. 사용자에게의 북마크 앱에 액세스할 수 있는 권한을 부여해야 합니다Okta. 자세한 내용은 [Okta 설명서를](#) 참조하세요. 나중에 IAM Identity Center를 추가 리전에 복제하려는 경우이 초기 설정 후 추가 리전에 대한 액세스를 활성화하는 방법에 [Okta 추가 리전에 액세스하기 위한 구성](#) 대한 지침을 보려면 섹션을 참조하세요.
 - 발급자 URL의 경우 IAM Identity Center 발급자 URL에서 복사한 값을 입력합니다.
 - 애플리케이션 사용자 이름 형식의 경우 메뉴에서 옵션 중 하나를 선택합니다.

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

10. 저장을 선택합니다.

이제 Okta에서 IAM Identity Center로 사용자를 프로비저닝할 준비가 되었습니다. Okta admin dashboard를 열린 상태로 두고 IAM Identity Center 콘솔로 돌아가 다음 단계를 진행합니다.

3단계: IAM Identity Center 및 Okta: Okta 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.
 - a. SCIM 엔드포인트 - 엔드포인트 형식은 구성에 따라 다릅니다.
 - IPv4: `https://scim.us-east-2.amazonaws.com/111111111111-2222-3333-4444-5555555555/scim/v2`
 - 듀얼 스택: `https://scim.us-east-2.api.aws/111111111111-2222-3333-4444-5555555555/scim/v2`
 - b. 액세스 토큰 - 토큰 표시를 선택하여 값을 복사합니다.

Warning

SCIM 엔드포인트와 액세스 토큰을 가져올 수 있는 유일한 시간입니다. 계속 진행하기 전에 이 값을 복사해야 합니다. 이 자습서의 후반부에서 이 값을 입력하여 Okta에서 자동 프로비저닝을 구성합니다.

3. 달기를 선택하세요.
4. Okta admin dashboard로 돌아가서 IAM Identity Center 앱으로 이동합니다.
5. IAM Identity Center 앱 페이지에서 프로비저닝 탭을 선택한 다음 설정의 왼쪽 탐색 메뉴에서 통합을 선택합니다.
6. 편집을 선택한 다음 API 통합 활성화 옆의 확인란을 선택하여 자동 프로비저닝을 활성화합니다.
7. 이 단계의 앞부분Okta에서 복사 AWS IAM Identity Center 한의 SCIM 프로비저닝 값으로 구성합니다.
 - a. 기본 URL 필드에 SCIM 엔드포인트 값을 입력합니다.
 - 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 설정 섹션으로 이동합니다.

10. 설정에서 대상 앱을 선택하고, 활성화하려는 각 앱으로 프로비저닝 기능에 대해 활성화 확인란을 선택합니다. 이 자습서에서는 모든 옵션을 선택합니다.
11. 저장을 선택합니다.

이제 Okta의 사용자를 IAM Identity Center와 동기화할 준비가 되었습니다.

4단계: Okta: Okta의 사용자를 IAM Identity Center와 동기화

기본적으로 Okta IAM Identity Center 앱에는 어떤 사용자 또는 그룹도 할당되지 않습니다. 프로비저닝 그룹은 그룹 구성원인 사용자를 프로비저닝합니다. 그룹 및 사용자를 동기화하려면 다음 단계를 완료하세요 AWS IAM Identity Center.

1. OktalIAM 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 Center와 동기화할 Okta 그룹을 선택합니다. 저장을 선택합니다.

그룹과 구성원이 IAM Identity Center로 푸시되면 그룹 상태가 활성으로 변경됩니다.

3. 할당 탭으로 돌아갑니다.
4. IAM Identity Center에 개별 Okta 사용자를 추가하려면 다음 단계를 수행합니다.
 - a. 할당 페이지에서 할당을 선택한 다음 사람에게 할당을 선택합니다.
 - b. 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 사용자 및 그룹을 할당할 수도 있습니다. Okta admin dashboard. 이를 위해 설정 아이콘을 선택하고 사용자에게 할당 또는 그룹에 할당을 선택한 다음 사용자나 그룹을 지정합니다.

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

축하합니다!

Okta 및 간에 SAML 연결을 성공적으로 설정하고 자동 프로비저닝이 작동하는지 확인 AWS 했습니다. 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.

액세스 제어에 속성 전달-선택 사항

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 전달](#)을 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.

에 액세스 권한 할당 AWS 계정

다음 단계는에 대한 액세스 권한만 부여하는 데 AWS 계정 만 필요합니다. 이러한 단계는 AWS 애플리케이션에 대한 액세스 권한을 부여하는 데 필요하지 않습니다.

Note

이 단계를 완료하려면 IAM Identity Center의 조직 인스턴스가 필요합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

1단계: IAM Identity Center: Okta 사용자에게 계정에 대한 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. 그리고 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 세트 정책 섹션에서 AdministratorAccess를 선택합니다.

다음을 선택합니다.

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

기본 설정에서는 세션 지속 시간이 1시간으로 설정된 *AdministratorAccess*라는 권한 세트를 생성합니다.

- iii. 3단계: 검토 및 생성에서 권한 세트 유형이 AWS 관리형 정책 AdministratorAccess를 사용하는지 확인합니다. 생성(Create)을 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 세트가 목록에 표시됩니다. 권한 세트의 확인란을 선택하고 다음을 선택합니다.

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

페이지는 구성 AWS 계정 중인 메시지로 업데이트됩니다. 프로세스가 완료될 때까지 기다립니다.

AWS 계정 페이지로 돌아갑니다. 알림 메시지가 재프로비저닝되었고 업데이트된 권한 세트 AWS 계정 가 적용되었음을 알려줍니다. 사용자가 로그인하면 *AdministratorAccess* 역할을 선택할 수 있는 옵션이 제공됩니다.

2단계: Okta: AWS 리소스에 대한 Okta 사용자 액세스 확인

1. 테스트 사용자 계정을 사용하여 Okta dashboard에 로그인합니다.
2. 내 앱에서 AWS IAM Identity Center 아이콘을 선택합니다.
3. AWS 계정 아이콘이 표시됩니다. 해당 아이콘을 확장하여 사용자가 액세스할 수 있는 AWS 계정 목록을 확인합니다. 이 자습서에서는 단일 계정만 사용했으므로 아이콘을 확장하면 하나의 계정만 표시됩니다.
4. 계정을 선택하면 사용자에게 제공되는 권한 세트가 표시됩니다. 이 자습서에서는 AdministratorAccess 권한 세트를 생성했습니다.
5. 권한 세트 옆에는 해당 권한 세트에 사용할 수 있는 액세스 유형에 대한 링크가 있습니다. 권한 세트를 생성할 때 AWS Management Console 및 프로그래밍 방식 액세스 모두에 대한 액세스를 지정했습니다. 관리 콘솔을 선택하면 AWS Management Console이 열립니다.
6. 사용자가 AWS Management Console에 로그인합니다.

AWS 액세스 포털을 사용할 수도 있습니다. 그러면 AWS 액세스 Okta 포털로 이동하기 전에 포털을 통해 로그인하도록 리디렉션됩니다. 이 경로는 SP가 시작한 SAML 로그인 흐름을 따릅니다.

Okta IAM Identity Center의 추가 리전에 액세스하기 위한 구성 - 선택 사항

IAM Identity Center를 추가 리전에 복제한 경우 추가 리전을 AWS 계정 통해 AWS 관리형 애플리케이션 및에 액세스할 수 있도록 ID 제공업체 구성을 업데이트해야 합니다. 아래 단계는 절차를 안내합니다. 사전 조건을 포함하여이 주제에 대한 자세한 내용은 섹션을 참조하세요 [여러에서 IAM Identity Center 사용 AWS 리전](#).

1. 에 설명된 대로 IAM Identity Center 콘솔에서 추가 리전의 ACS URLs을 검색합니다 [기본 및 추가의 ACS 엔드포인트 AWS 리전](#).
2. Okta 관리자 대시보드의 탐색 창에서 애플리케이션을 선택한 다음 확장된 목록에서 애플리케이션을 다시 선택합니다.
3. AWS IAM Identity Center 애플리케이션을 선택합니다.
4. 로그인(Sign On) 탭을 선택합니다.
5. 고급 로그인 설정 및 기타 요청 가능한 SSO URLs에서 각 추가 리전의 ACS URL에 대해 다른 추가를 선택하고 ACS URL을 텍스트 필드에 붙여 넣습니다.
6. ACS URLs 추가가 완료되면 AWS IAM Identity Center 애플리케이션을 저장합니다.
7. 에서 각 추가 리전의 AWS 액세스 포털에 Okta 대한 북마크 앱을 생성할 수 있습니다. 이를 통해 사용자는에서 추가 리전의 AWS 액세스 포털에 액세스할 수 있습니다Okta. 사용자에게의 북마크 앱에 액세스할 수 있는 권한을 부여해야 합니다Okta. 자세한 내용은 [Okta 설명서를](#) 참조하세요.
8. 각 추가 리전에서 AWS 액세스 포털에 로그인할 수 있는지 확인합니다. [AWS 액세스 포털 URLs](#)로 이동하거나에서 북마크 앱을 시작합니다Okta.

다음 단계

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

- 에 대한 액세스 권한을 부여합니다. 단원을 AWS 계정참조하십시오 [에 사용자 또는 그룹 액세스 할당 AWS 계정](#).
- 클라우드 애플리케이션에 대한 액세스 권한을 부여하려면 [IAM Identity Center 콘솔에서 애플리케이션에 사용자 액세스 권한 할당](#)의 내용을 참조하세요.
- 직무에 따라 권한을 구성합니다. [권한 세트 생성](#)을 참조하세요.

문제 해결

Okta를 사용한 일반적인 SCIM 및 SAML 문제 해결은 다음 섹션을 참조하세요.

- [IAM Identity Center에서 삭제된 사용자 및 그룹 재프로비저닝](#)
- [Okta의 자동 프로비저닝 오류](#)
- [특정 사용자가 외부 SCIM 공급자로부터 IAM Identity Center로 동기화하지 못함](#)
- [IAM Identity Center에서 생성된 SAML 어설션 콘텐츠 관련 문제](#)
- [외부 ID 제공업체에서 사용자 또는 그룹을 프로비저닝할 때의 중복 사용자 또는 그룹 오류](#)
- [추가 리소스](#)

IAM Identity Center에서 삭제된 사용자 및 그룹 재프로비저닝

- 동기화된 다음 IAM Identity Center에서 삭제된 Okta의 사용자 또는 그룹을 변경하려는 경우 Okta 콘솔에서 다음 오류 메시지를 받을 수 있습니다.
 - 사용자 *Jane Doe*를 앱으로 자동 프로필 푸시 AWS IAM Identity Center 실패:
*jane_doe@example.com*에 대한 프로필 업데이트를 푸시하는 동안 오류 발생: *xxxxx-xxxxxx-xxxxxx-xxxxxx* 사용자에게 대해 반환된 사용자가 없음
 - 연결된 그룹이 누락되었습니다 AWS IAM Identity Center. 연결된 그룹을 변경하여 그룹 멤버십 푸시를 재개합니다.
- 동기화 및 삭제된 IAM Identity Center 사용자 또는 그룹에 대한 Okta의 시스템 로그에서 다음 오류 메시지를 받을 수도 있습니다.
 - Okta 오류: Eventfailed application.provision.user.push_profile : 사용자에게 대해 반환된 사용자가 없음 *xxxxxx-xxxxxx-xxxxxx-xxxxxx*
 - Okta 오류: application.provision.group_push.mapping.update.or.delete.failed.with.error : 연결된 그룹이 누락되었습니다 AWS IAM Identity Center. 연결된 그룹을 변경하여 그룹 멤버십 푸시를 재개합니다.

Warning

SCIM을 사용하여 Okta와 IAM Identity Center와 동기화한 경우 IAM Identity Center가 아닌 Okta에서 사용자 및 그룹을 삭제해야 합니다.

삭제된 IAM Identity Center 사용자 문제 해결

삭제된 IAM Identity Center 사용자와 관련된 이 문제를 해결하려면 사용자를 Okta에서 삭제해야 합니다. 필요한 경우 이러한 사용자도 Okta에서 다시 생성해야 합니다. 사용자가 Okta에서 다시 생성되면 SCIM을 통해 IAM Identity Center로 다시 프로비저닝됩니다. 사용자 삭제에 대한 자세한 내용은 [Okta 설명서](#)를 참조하세요.

Note

IAM Identity Center에 대한 Okta 사용자의 액세스 권한을 제거해야 하는 경우 먼저 그룹 푸시에서 제거한 다음 Okta에서 할당 그룹에서 제거해야 합니다. 이렇게 하면 사용자가 IAM Identity Center의 연결된 그룹 멤버십에서 제거됩니다. 그룹 푸시 문제 해결에 대한 자세한 내용은 [Okta 설명서](#)를 참조하세요.

삭제된 IAM Identity Center 그룹 문제 해결

삭제된 IAM Identity Center 그룹에서 이 문제를 해결하려면 Okta에서 그룹을 삭제해야 합니다. 필요한 경우 그룹 푸시를 사용하여 Okta에서 이러한 그룹을 다시 생성해야 합니다. Okta에서 사용자를 다시 생성하면 SCIM을 통해 IAM Identity Center로 다시 프로비저닝됩니다. 그룹 삭제에 대한 자세한 내용은 [Okta 설명서](#)를 참조하세요.

Okta의 자동 프로비저닝 오류

Okta의 오류가 발생하면 다음을 수행하세요.

사용자 Jane Doe의 앱 자동 프로비저닝 AWS IAM Identity Center 실패: 일치하는 사용자를 찾을 수 없음

자세한 정보는 [Okta 설명서](#)를 참조하세요.

추가 리소스

- 일반 SCIM 문제 해결 팁은 [IAM Identity Center 문제 해결](#) 섹션을 참조하세요.

다음 리소스는 작업 시 문제를 해결하는 데 도움이 될 수 있습니다. AWS

- [AWS re:Post](#)-문제를 해결할 때 도움이 되는 FAQ와 기타 리소스 링크를 찾을 수 있습니다.
- [AWS Support](#)-기술 지원 받기

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. 자세한 내용은 [외부 ID 제공업체와의 SAML 및 SCIM ID 페더레이션 사용](#) 단원을 참조하십시오.

Note

OneLogin는 현재 AWS IAM Identity Center 애플리케이션에서 SAML 다중 어설션 소비 서비스(ACS) URLs을 지원하지 않습니다. IAM Identity Center에서 [다중 리전 지원을](#) 완전히 활용하려면 SAML 기능이 필요합니다. IAM Identity Center를 추가 리전에 복제하려는 경우 단일 ACS URL을 사용하면 해당 추가 리전의 사용자 경험에 영향을 미칠 수 있습니다. 기본 리전은 계속 정상적으로 작동합니다. 이 기능을 활성화하려면 IdP 공급업체와 협력하는 것이 좋습니다. 단일 ACS URL을 사용하는 추가 리전의 사용자 경험에 대한 자세한 내용은 [the section called “여러 ACS URLs 없이 AWS 관리형 애플리케이션 사용”](#) 및 섹션을 참조하십시오. [the section called “AWS 계정 여러 ACS URLs 없이 복원력에 액세스”](#).

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 사항](#)을 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 [OneLogin 웹사이트에서](#) 무료 평가판 또는 개발자 계정을 얻을 수 있습니다.
- IAM Identity Center 활성화 계정([무료](#)). 자세한 내용은 [IAM Identity Center 활성화](#)를 참조하세요.
- OneLogin 계정에서 IAM Identity Center로 SAML 연결을 수행합니다. 자세한 내용은 AWS Partner Network Blog에서 [OneLogin 및 AWS간의 Single Sign-On 활성화](#)를 참조하세요.

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 콘솔](#)을 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 SCIM 엔드포인트와 액세스 토큰을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.
 - a. SCIM 엔드포인트-예: `https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. 액세스 토큰 - 토큰 표시를 선택하여 값을 복사합니다.

⚠ Warning

SCIM 엔드포인트와 액세스 토큰을 가져올 수 있는 유일한 시간입니다. 계속 진행하기 전에 이 값을 복사해야 합니다. 이 자습서의 후반부에 이 값을 입력하여 IdP에서 자동 프로비저닝을 구성할 수 있습니다.

5. 달기를 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 OneLogin 위해에서 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 AWS간의 Single Sign-On 활성화](#)를 참조하세요.

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 탐색 창에서 구성을 선택합니다.
3. 이전 절차에서 IAM Identity Center에서 SCIM 엔드포인트 값을 복사했습니다. 해당 값을 OneLogin의 SCIM 기본 URL 필드에 붙여넣습니다. 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. 탐색 창에서 Provisioning(프로비저닝)을 선택합니다.
6. 프로비저닝 활성화, 사용자 생성, 사용자 삭제 및 사용자 업데이트 체크박스를 선택한 다음 저장을 선택합니다.
7. 탐색 창에서 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 섹션을 취소하고 저장을 클릭합니다.

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

이는 IAM Identity Center에서 AWS 리소스에 대한 액세스를 관리하는 데 사용할 속성을 구성하도록 선택한 OneLogin 경우의 선택적 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 참조하세요.

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 탐색 창에서 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. 플러그에서 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 전달](#)을 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.

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 [OneLogin웹사이트](#)를 참조하세요.

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. 자세한 내용은 [외부 ID 제공업체와의 SAML 및 SCIM ID 페더레이션 사용](#) 단원을 참조하십시오.

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 문의하세요.

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 사항](#)을 검토하는 것이 좋습니다. 그 후, 다음 섹션에서 추가 고려 사항을 계속 검토합니다.

주제

- [사전 조건](#)
- [고려 사항](#)
- [1단계: IAM Identity Center 프로비저닝 활성화](#)
- [2단계: PingFederate에서 프로비저닝 구성](#)
- [\(선택 사항\) 3단계: IAM Identity Center에서 액세스 제어에 사용되는 PingFederate의 사용자 속성 구성](#)
- [\(선택 사항\) 액세스 제어에 속성 전달](#)
- [문제 해결](#)

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 커넥터](#)를 참조하세요.
- IAM Identity Center 활성화 계정([무료](#)). 자세한 내용은 [IAM Identity Center 활성화](#)를 참조하세요.
- PingFederate 인스턴스에서 IAM Identity Center로 SAML 연결을 수행합니다. 이 연결을 구성하는 방법에 대한 지침은 PingFederate 설명서를 참조하세요. 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.

- IAM Identity Center를 추가 리전에 복제한 경우 AWS 관리형 애플리케이션 및 해당 리전 AWS 계정에서 액세스할 수 있도록 ID 제공업체 구성을 업데이트해야 합니다. 자세한 내용은 [the section called “3단계: 외부 IdP 설정 업데이트”](#) 섹션을 참조하세요. 자세한 내용은 PingFederate 설명서를 참조하세요.

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 콘솔](#)을 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 SCIM 엔드포인트와 액세스 토큰을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.
 - a. SCIM 엔드포인트-예: `https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. 액세스 토큰 - 토큰 표시를 선택하여 값을 복사합니다.

⚠ Warning

SCIM 엔드포인트와 액세스 토큰을 가져올 수 있는 유일한 시간입니다. 계속 진행하기 전에 이 값을 복사해야 합니다. 이 자습서의 후반부에 이 값을 입력하여 IdP에서 자동 프로비저닝을 구성할 수 있습니다.

5. 달기를 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 조건](#)을 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 참조하세요. 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 PingFederate와고가용성 구성을 사용하지 않는 경우 STANDALONE를 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. 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. 소스 페이지에서 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 참조하세요.

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 UserPrincipalName를 userName으로 지정할 수 있습니다.
 - b. * 접미사가 붙은 다른 필드는 사용자의 null이 아닌 속성에 매핑되어야 합니다.
14. 활성화 및 요약 페이지에서 채널 상태를 활성화로 설정하여 구성을 저장한 후 즉시 동기화가 시작 되도록 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 Identity Center에서 액세스 제어에 사용되는 PingFederate의 사용자 속성 구성

이는 IAM Identity Center에서 AWS 리소스에 대한 액세스를 관리하는 데 사용할 속성을 구성하도록 선택한 PingFederate 경우의 선택적 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 참조하세요.

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:uri`를 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 참조하세요.

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 전달](#)을 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.

문제 해결

PingFederate를 사용한 일반적인 SCIM 및 SAML 문제 해결은 다음 섹션을 참조하세요.

- [특정 사용자가 외부 SCIM 공급자로부터 IAM Identity Center로 동기화하지 못함](#)
- [IAM Identity Center에서 생성된 SAML 어설션 콘텐츠 관련 문제](#)
- [외부 ID 제공업체에서 사용자 또는 그룹을 프로비저닝할 때의 중복 사용자 또는 그룹 오류](#)
- PingFederate에 대한 자세한 내용은 [PingFederate 설명서](#)를 참조하세요.

다음 리소스는 작업 시 문제를 해결하는 데 도움이 될 수 있습니다. AWS

- [AWS re:Post](#)-문제를 해결할 때 도움이 되는 FAQ와 기타 리소스 링크를 찾을 수 있습니다.
- [AWS Support](#)-기술 지원 받기

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.

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 사항](#)을 검토하는 것이 좋습니다. 그 후, 다음 섹션에서 추가 고려 사항을 계속 검토합니다.

주제

- [사전 조건](#)
- [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](#)
- [문제 해결](#)

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 참조하세요.
- IAM Identity Center 활성화 계정([무료](#)). 자세한 내용은 [IAM Identity Center 활성화](#)를 참조하세요.
- 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 추가](#)를 참조하세요.
- PingOne 인스턴스에서 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 참조하세요.
- IAM Identity Center를 추가 리전에 복제한 경우 AWS 관리형 애플리케이션 및 해당 리전 AWS 계정에서 액세스할 수 있도록 ID 제공업체 구성을 업데이트해야 합니다. 자세한 내용은 [the section called “3단계: 외부 IdP 설정 업데이트”](#) 섹션을 참조하세요. 자세한 내용은 PingOne 설명서를 참조하세요.

고려 사항

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

- PingOne은 SCIM을 통한 그룹 프로비저닝을 지원하지 않습니다. Ping의 SCIM 그룹 지원에 대한 최신 정보는 PingOne로 문의하세요.
- 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 [SCIM을 사용하여 외부 ID 제공업체의 사용자 및 그룹 프로비저닝](#)을 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 emailAddress를 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 해결하려면 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 콘솔](#)을 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 SCIM 엔드포인트와 액세스 토큰을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.
 - a. SCIM 엔드포인트-예: `https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`

- b. 액세스 토큰 - 토큰 표시를 선택하여 값을 복사합니다.

Warning

SCIM 엔드포인트와 액세스 토큰을 가져올 수 있는 유일한 시간입니다. 계속 진행하기 전에 이 값을 복사해야 합니다. 이 자습서의 후반부에 이 값을 입력하여 IdP에서 자동 프로비저닝을 구성할 수 있습니다.

5. 달기를 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 조건](#)을 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 참조하세요.
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. 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 [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 문의하세요.

(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 선택한 PingOne 경우의 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 참조하세요.

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 계속을 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 전달](#)을 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.

문제 해결

PingOne를 사용한 일반적인 SCIM 및 SAML 문제 해결은 다음 섹션을 참조하세요.

- [특정 사용자가 외부 SCIM 공급자로부터 IAM Identity Center로 동기화하지 못함](#)
- [IAM Identity Center에서 생성된 SAML 어설션 콘텐츠 관련 문제](#)
- [외부 ID 제공업체에서 사용자 또는 그룹을 프로비저닝할 때의 중복 사용자 또는 그룹 오류](#)
- PingOne에 대한 자세한 내용은 [PingOne 설명서](#)를 참조하세요.

다음 리소스는 작업 시 문제를 해결하는 데 도움이 될 수 있습니다. AWS

- [AWS re:Post](#)-문제를 해결할 때 도움이 되는 FAQ와 기타 리소스 링크를 찾을 수 있습니다.
- [AWS Support](#)-기술 지원 받기

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 Microsoft Active Directory, Microsoft Entra ID 또는 Okta 등과 같은 다른 ID 제공업체를 사용하는 경우 기본 구성을 사용하는 대신 해당 ID 소스를 IAM Identity Center와 통합하는 것을 고려해 보세요.

목표

이 자습서에서는 기본 디렉터를 ID 소스로 사용하고 IAM Identity Center 조직 인스턴스를 사용하여 관리 사용자를 설정하고 테스트합니다. 이 관리 사용자는 사용자 및 그룹을 생성 및 관리하고 권한 세트를 사용하여 AWS 액세스 권한을 부여합니다. 다음 단계에서는 다음을 생성합니다.

- *Nikki Wolf*라는 관리 사용자
- *Admin team*이라는 그룹
- *AdminAccess*라는 권한 세트

모든 사항이 올바르게 생성되었는지 확인하려면 로그인하고 관리 사용자의 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. 또는 사용자에게 애플리케이션에 대한 액세스 권한을 부여하려는 경우 이 절차의 [1단계](#)를 진행하여 [애플리케이션 액세스를 구성](#)할 수 있습니다.

사전 조건

이 자습서를 완료하려면 다음과 같은 사전 조건이 필요합니다.

- [IAM Identity Center 활성화](#)를 활성화하고 [IAM Identity Center의 조직 인스턴스](#)를 확보합니다.
 - IAM Identity Center의 [계정 인스턴스](#)를 보유하고 있는 경우 사용자 및 그룹을 생성하고 애플리케이션에 대한 액세스 권한을 부여할 수 있습니다. 자세한 내용은 [애플리케이션 액세스](#)를 참조하세요.
- 예 로그인 AWS Management Console 하고 IAM Identity Center 콘솔에 다음과 같이 액세스합니다.
 - 신규 사용자 AWS (루트 사용자) - AWS 계정 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
 - 이미 사용 중 AWS (IAM 자격 증명) - 관리 권한이 있는 IAM 자격 증명을 사용하여 로그인합니다.

- 에 로그인하는 방법에 대한 자세한 내용은 가이드를 AWS Management Console참조하세요.
[AWS Sign-In](#)
- IAM Identity Center 사용자에게 대해 다중 인증을 구성할 수 있습니다. 자세한 내용은 [IAM Identity Center에서 MFA 구성](#) 단원을 참조하십시오.

1단계: 사용자 추가

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. IAM Identity Center 콘솔의 탐색 창에서 사용자를 선택하고 사용자 추가를 선택합니다.
3. 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 나중에 변경할 수 없습니다.

- 암호 - 이 사용자에게 암호 설정 지침이 포함된 이메일 보내기(권장)를 선택합니다.

이 옵션을 선택하면 Amazon Web Services에서 사용자에게 IAM Identity Center 가입 초대라는 제목의 이메일을 발송합니다. 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.
4. 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.
5. 그룹 영역에서 새로 고침 버튼을 선택합니다. *Admin team* 그룹이 목록에 표시됩니다.

Admin team 옆에 있는 확인란을 선택하고 다음을 선택합니다.

6. 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

Important

[IAM Identity Center의 조직 인스턴스](#)를 활성화한 경우에만 다음 단계를 진행합니다.

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. 그리고 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 세트 정책 섹션에서 `AdministratorAccess`를 선택합니다.

다음을 선택합니다.

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

기본 설정에서는 세션 지속 시간이 1시간으로 설정된 `AdministratorAccess`라는 권한 세트를 생성합니다. 권한 세트 이름 필드에 새 이름을 입력하여 권한 세트의 이름을 변경할 수 있습니다.

- iii. 3단계: 검토 및 생성에서 권한 세트 유형이 AWS 관리형 정책 `AdministratorAccess`를 사용하는지 확인합니다. 생성(Create)을 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 세트가 목록에 표시됩니다. 권한 세트의 체크박스를 선택하고 다음을 누릅니다.

- c. 3단계: 할당 검토 및 제출 페이지에서 `Admin team` 그룹이 선택되어 있고 `AdministratorAccess` 권한 세트가 선택되어 있는지 확인한 다음 제출을 선택합니다.

페이지는 구성 AWS 계정 중인 메시지로 업데이트됩니다. 프로세스가 완료될 때까지 기다립니다.

AWS 계정 페이지로 돌아갑니다. 알림 메시지가 재프로비저닝되었고 업데이트된 권한 세트 AWS 계정 가 적용되었음을 알려줍니다.

축하합니다!

첫 번째 사용자, 그룹 및 권한 세트를 성공적으로 설정했습니다.

이 자습서의 다음 부분에서는 관리 자격 증명으로 액세스 포털에 로그인하고 암호를 설정하여 `Nikki#` AWS 액세스를 테스트합니다. 이제 콘솔에서 로그아웃합니다.

3단계: 사용자 액세스 테스트

Nikki Wolf가 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 사용자 **Nikki Wolf**를 추가했을 때 **Nikki**가 암호 설정 안내 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 설정하고 [MFA 디바이스를 등록](#)할 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 액세스 포털이 열리고 액세스할 수 있는 조직과 애플리케이션이 표시됩니다.

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

각 권한 세트에 대해 역할 또는 액세스 키의 두 가지 관리 방법을 사용할 수 있습니다.

- 역할, 예: **AdministratorAccess**- AWS Console Home를 엽니다.
- 액세스 키 - AWS CLI 또는 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 내용은 [AWS CLI AWS SDKs에 대한 IAM Identity Center 사용자 자격 증명 가져오기](#) 단원을 참조하십시오.

4. 역할 링크를 선택하여 AWS Console Home에 로그인합니다.

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 따르면 관리자를 생성한 후 보다 제한적인 권한 세트를 생성하여 동일한 사용자에게 할당하세요. 이렇게 하면 관리 권한이 아닌 필요한 권한 AWS 계정으로만 액세스할 수 있습니다.

사용자가 계정 활성화 [초대를 수락](#)하고 AWS 액세스 포털에 로그인한 후 포털에 표시되는 유일한 항목은 할당된 AWS 계정, 역할 및 애플리케이션에 대한 항목입니다.

자습서 비디오

추가 리소스로 다음 비디오 자습서를 사용하여 외부 ID 제공업체 설정에 대해 자세히 알아볼 수 있습니다.

- [에서 외부 자격 증명 공급자 간 마이그레이션 AWS IAM Identity Center](#)
- [기존 AWS IAM Identity Center 인스턴스와 연동 Microsoft Entra ID](#)

IAM Identity Center에서 인력 설정

IAM Identity Center는 인력 사용자를 Kiro 및 Amazon Quick과 같은 AWS 관리형 애플리케이션과 기타 AWS 리소스에 연결하는 AWS 솔루션입니다. 기존 ID 제공업체를 연결하고 디렉터리에서 사용자와 그룹을 동기화하거나 IAM Identity Center에서 직접 사용자를 생성하고 관리할 수 있습니다.

에 액세스하기 위해 이미 IAM을 사용하고 있습니까 AWS 계정?

AWS 관리형 애플리케이션에 액세스하기 위해 IAM Identity Center를 사용하기 위해 현재 AWS 계정 워크플로를 변경할 필요가 없습니다. AWS 계정 액세스에 [IAM과 연동을](#) 사용하는 경우 사용자는 항상 가지고 있는 것과 동일한 방식으로 AWS 계정 에 계속 액세스할 수 있으며 기존 워크플로를 계속 사용하여 해당 액세스를 관리할 수 있습니다.

조직의 자격 증명 관리 전략 및 기존 인프라에 가장 적합한 접근 방식을 선택합니다.

주제

- [IAM Identity Center에서의 사용자, 그룹 및 프로비저닝](#)
- [ID 소스 관리](#)
- [Identity Center 디렉터리에서 사용자 관리](#)

IAM Identity Center에서의 사용자, 그룹 및 프로비저닝

IAM Identity Center를 사용하면 로그인할 수 있는 사용자와 액세스할 수 있는 리소스를 제어할 수 있습니다. 로그인하려면 사용자를 프로비저닝해야 합니다. 그런 다음 프로비저닝된 사용자 또는 그룹에만 액세스 권한을 할당할 수 있습니다. IAM Identity Center에서의 사용자, 그룹 및 프로비저닝에 대해 알아보십시오.

사용자 이름 및 이메일 주소 고유성

IAM Identity Center를 사용하려면 각 사용자에게 고유한 사용자 이름이 있어야 합니다. 사용자 이름은 사용자의 기본 식별자입니다. 사용자 이름은 사용자의 이메일 주소와 일치하지 않아도 됩니다. 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 중첩된 그룹(그룹 내 그룹)을 지원하지 않습니다. 그룹은 AWS 계정 및 애

폴리리케이션에 대한 액세스를 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 직접 사용자 및 그룹을 생성하거나 자격 증명 소스를 IAM Identity Center에 연결할 수 있습니다. IAM Identity Center를 사용하면 사용자와 그룹에게 연결된 애플리케이션 및 AWS 계정에 대한 액세스 권한을 할당할 수 있습니다.

IAM Identity Center에서의 프로비저닝은 사용하는 ID 소스에 따라 달라집니다. 자세한 내용은 [ID 소스 관리](#) 단원을 참조하십시오.

사용자 및 그룹 프로비저닝

프로비저닝 해제는 IAM Identity Center에서 사용자 및 그룹 정보를 제거하는 프로세스입니다.

IAM Identity Center에서 Active Directory 또는 외부 ID 제공업체를 사용하는 경우 IAM Identity Center가 아닌 해당 자격 증명 소스에서 사용자 및 그룹을 제거해야 합니다. 자격 증명 소스가 Active Directory 또는 외부 ID 제공업체인 경우 IAM Identity Center 사용자 및 그룹을 삭제해도 완전히 제거되지 않습니다.

IAM Identity Center 사용자 또는 그룹의 프로비저닝을 해제해야 하는 경우 먼저 프로비저닝을 해제하려는 사용자 또는 그룹에 대한 애플리케이션이나 [권한 세트의 할당을 제거](#)해야 합니다. 그렇지 않으면 IAM Identity Center에 할당되지 않은 권한 세트와 애플리케이션 할당이 남게 됩니다.

ID 소스 관리

IAM Identity Center의 ID 소스는 사용자 및 그룹을 관리하는 위치를 정의합니다. 자격 증명 소스를 구성한 후 사용자 또는 그룹을 조회하여, AWS 계정애플리케이션 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.

- [외부 ID 제공업체](#) - Okta 또는 Microsoft Entra ID와 같은 외부 ID 제공업체(idP)에서 사용자를 관리하려는 경우 이 옵션을 선택합니다.

- [온프레미스 또는 AWS 관리형 Active Directory](#) -를 연결하려면이 옵션을 선택합니다Active Directory (AD).
- [ID Center 디렉터리](#) – IAM Identity Center를 처음 활성화하면 다른 ID 소스를 선택하지 않는 한 자동으로 Identity Center 디렉터리가 기본 ID 소스로 구성됩니다. Identity Center 디렉터를 사용하면 사용자 및 그룹을 생성하고 AWS 계정 및 애플리케이션에 대한 액세스 수준을 할당할 수 있습니다.

Note

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

주제

- [ID 소스 변경 시 고려 사항](#)
- [ID 소스 변경](#)
- [IAM Identity Center에서 지원되는 사용자 및 그룹 속성](#)
- [외부 ID 제공업체](#)
- [Microsoft AD 디렉터리](#)

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 관리 사용자를 포함한 모든 사용자는 AWS 계정 및 애플리케이션에 대한 Single Sign-On 액세스 권한을 잃게 됩니다.

IAM Identity Center의 ID 소스를 변경하기 전에 다음 고려 사항을 검토한 후 진행하세요. ID 소스 변경을 계속 진행하려면 [ID 소스 변경](#)에서 자세한 내용을 확인하세요.

IAM Identity Center 디렉터리와 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.

⚠ Important

IAM Identity Center에서 Active Directory로 또는 Active Directory에서 ID 소스 유형을 변경할 경우 Identity Store ID가 변경됩니다. 이는 다음과 같은 의미를 가집니다.

- 기본 AWS 액세스 포털 URL이 변경됩니다. 새 URL을 작업 인력에게 전달하고 해당 URL이 참조되는 즐겨찾기, 게이트웨이 또는 방화벽 허용 목록 및 구성을 업데이트해야 합니다. 사용자의 사용 종단을 최소화하려면 예약된 유지 관리 기간에 이 변경을 수행하는 것이 좋습니다.
- IAM Identity Center에서 유휴 시 암호화에 고객 관리형 KMS 키를 사용하고 있고 암호화 컨텍스트로 KMS 키 정책을 구성한 경우 Identity Store의 암호화 컨텍스트가 변경됩니다. 예를 들어 Identity Store ARN 'arn:aws:identitystore::123456789012:identitystore/d-922763e9b3'에서 'd-922763e9b3'이 Identity Store ID입니다. 이 전환 중에 서비스 종단을 방지하려면 와일드카드 패턴 'arn:aws:identitystore::123456789012:identitystore/*'를 사용하여 KMS 키 정책을 일시적으로 수정합니다.

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 (Active Directory 또는 동기화된 ID에서) 삭제되더라도 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 Identity Center와 Active Directory 간에 ID 소스를 변경하면 AWS 액세스 포털의 URL도 변경됩니다.

- Identity Store API를 사용하여 IAM Identity Center 콘솔에서 사용자를 삭제하거나 비활성화하는 경우 활성 세션이 있는 사용자는 통합 애플리케이션과 계정에 계속 액세스할 수 있습니다. 인증 세션 지속 시간 및 사용자 동작에 대해서는 [IAM Identity Center의 인증 세션 이해](#)을 참조하세요.

IAM Identity Center에서 사용자 및 그룹을 프로비저닝하는 방법에 대한 자세한 내용은 [Microsoft AD 디렉터리](#)를 참조하세요.

IAM Identity Center에서 외부 IdP로 변경

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

- 할당과 멤버십은 올바른 어설션에서 작동합니다 – 사용자 할당, 그룹 할당, 그룹 멤버십은 새 IdP가 올바른 어설션(예: SAML nameID)을 보내는 한 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 또는 그룹을 변경해도 외부 IdP가 자동으로 업데이트되지 않습니다.
- SCIM 프로비저닝 – SCIM 프로비저닝을 사용하고 있는 경우 ID 제공업체의 사용자 및 그룹 변경 사항은 ID 제공업체가 해당 변경 사항을 IAM Identity Center로 전송한 이후에만 IAM Identity Center에 반영됩니다. [자동 프로비저닝을 사용할 때 고려 사항](#)(를) 참조하세요.
- 롤백-언제든지 IAM Identity Center를 ID 소스로 사용하도록 되돌릴 수 있습니다. [외부 IdP에서 IAM Identity Center로 변경](#)(를) 참조하세요.
- 기존 사용자 세션은 세션 지속시간 만료 시 취소됩니다 – ID 소스를 외부 ID 제공업체로 변경하면 활성 사용자 세션은 콘솔에 구성된 최대 세션 지속 시간에서 남은 시간 동안 유지됩니다. 예를 들어 AWS 액세스 포털 세션 기간이 8시간으로 설정되어 있고 4시간 후에 자격 증명 소스를 변경한 경우 활성 사용자 세션은 추가로 4시간 동안 유지됩니다. 사용자 세션을 취소하려면 [the section called “직원 사용자의 활성 세션 종료”](#)을 참조하세요.

Identity Store API를 사용하여 IAM Identity Center 콘솔에서 사용자를 삭제하거나 비활성화하는 경우 활성 세션이 있는 사용자는 통합 애플리케이션과 계정에 계속 액세스할 수 있습니다. 인증 세션 지속 시간 및 사용자 동작에 대해서는 [IAM Identity Center의 인증 세션 이해](#)을 참조하세요.

Note

사용자를 삭제한 후에는 IAM Identity Center 콘솔에서 사용자 세션을 취소할 수 없습니다.

IAM Identity Center에서 사용자 및 그룹을 프로비저닝하는 방법에 대한 자세한 내용은 [외부 ID 제공업체](#)를 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.
- 기존 사용자 세션은 세션 지속시간 만료 시 취소됩니다 - ID 소스를 외부 ID 제공업체로 변경하면 활성 사용자 세션은 콘솔에 구성된 최대 세션 지속 시간에서 남은 시간 동안 유지됩니다. 예를 들어 AWS 액세스 포털 세션 기간이 8시간이고 네 번째 시간에 자격 증명 소스를 변경한 경우 활성 사용자 세션은 추가로 4시간 동안 계속 실행됩니다. 사용자 세션을 취소하려면 [the section called “직원 사용자의 활성 세션 종료”](#)를 참조하세요.

Identity Store API를 사용하여 IAM Identity Center 콘솔에서 사용자를 삭제하거나 비활성화하는 경우 활성 세션이 있는 사용자는 통합 애플리케이션과 계정에 계속 액세스할 수 있습니다. 인증 세션 지속 시간 및 사용자 동작에 대해서는 [IAM Identity Center의 인증 세션 이해](#)를 참조하세요.

Note

사용자를 삭제한 후에는 IAM Identity Center 콘솔에서 사용자 세션을 취소할 수 없습니다.

- 다중 리전 지원 - IAM Identity Center를 추가 리전에 복제했거나 복제하려는 경우 외부 ID 제공업체를 ID 소스로 사용해야 합니다. 기타 사전 조건을 포함한 자세한 내용은 [여러에서 IAM Identity Center 사용 AWS 리전](#).

IAM Identity Center에서 사용자 및 그룹을 프로비저닝하는 방법에 대한 자세한 내용은 [Identity Center 디렉터리에서 사용자 관리](#)를 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, 그룹 멤버십은 새 IdP가 올바른 어설션(예: SAML nameID)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 SCIM 활성화 시 새 공급자가 사용자 및 그룹을 올바르게 일차하도록 이 가이드의 IdP 관련 정보 및 IdP에서 제공한 설명서를 검토할 것을 권장합니다.
- 기존 사용자 세션은 세션 지속시간 만료 시 취소됩니다 – ID 소스를 외부 ID 제공업체로 변경하면 활성 사용자 세션은 콘솔에 구성된 최대 세션 지속 시간에서 남은 시간 동안 유지됩니다. 예를 들어 AWS 액세스 포털 세션 기간이 8시간이고 네 번째 시간에 자격 증명 소스를 변경한 경우 활성 사용자 세션은 추가로 4시간 동안 유지됩니다. 사용자 세션을 취소하려면 [the section called “직원 사용자의 활성 세션 종료”](#)를 참조하세요.

Identity Store API를 사용하여 IAM Identity Center 콘솔에서 사용자를 삭제하거나 비활성화하는 경우 활성 세션이 있는 사용자는 통합 애플리케이션과 계정에 계속 액세스할 수 있습니다. 인증 세션 지속 시간 및 사용자 동작에 대해서는 [IAM Identity Center의 인증 세션 이해](#)를 참조하세요.

Note

사용자를 삭제한 후에는 IAM Identity Center 콘솔에서 사용자 세션을 취소할 수 없습니다.

IAM Identity Center에서 사용자 및 그룹을 프로비저닝하는 방법에 대한 자세한 내용은 [외부 ID 제공업체](#)를 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.
- Identity Store API를 사용하여 IAM Identity Center 콘솔에서 사용자를 삭제하거나 비활성화하는 경우 활성 세션이 있는 사용자는 통합 애플리케이션과 계정에 계속 액세스할 수 있습니다. 인증 세션 지속 시간 및 사용자 동작에 대해서는 [IAM Identity Center의 인증 세션 이해](#)를 참조하세요.
- 다중 리전 지원 - IAM Identity Center를 추가 리전에 복제했거나 복제하려는 경우 외부 ID 제공업체를 ID 소스로 사용해야 합니다. 기타 사전 조건을 포함한 자세한 내용은 섹션을 참조하세요 [여러에서 IAM Identity Center 사용 AWS 리전](#).

IAM Identity Center에서 사용자 및 그룹을 프로비저닝하는 방법에 대한 자세한 내용은 [Microsoft AD 디렉터리](#)를 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 사항](#)에 있는 정보를 검토하세요. 이 절차를 완료하려면 IAM Identity Center의 조직 인스턴스가 필요합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

Warning

현재 배포에 따라 이 변경으로 인해 IAM Identity Center에서 구성한 모든 사용자 및 그룹 할당이 제거됩니다. 이렇게 변경하면에서 권한 세트 IAM 역할도 제거됩니다 AWS 계정. 따라서 리소스 정책을 업데이트해야 할 수 있으며, 이로 인해 AWS KMS 키 및 Amazon EKS 클러스터에 대한 액세스가 중단되지 않도록 해야 합니다. 자세한 내용은 [리소스 정책](#), [Amazon EKS 클러스터 구성 맵 및 AWS KMS 키 정책에서 권한 세트 참조](#)를 참조하세요.

이 경우 IAM Identity Center의 관리 사용자를 포함한 모든 사용자와 그룹은 AWS 계정 및 애플리케이션에 대한 Single Sign-On 액세스 권한을 잃게 됩니다.

ID 소스를 변경하려면

1. [IAM Identity Center 콘솔](#)을 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.

Note

IAM Identity Center를 추가 리전에 복제한 경우 ID 소스 유형을 변경할 수 없습니다. 현재 외부 IdP로 바꿀 수 있습니다. 자격 증명 소스 유형을 변경하려면 먼저 모든 추가 리전을 제거해야 합니다. 자세한 내용은 [여러에서 IAM Identity Center 사용 AWS 리전](#) 섹션을 참조하세요.

외부 ID 공급자로 전환하는 경우 [외부 ID 제공업체에 연결하는 방법](#)의 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 수행하세요.
 - 안내에 따른 설정 시작을 선택합니다. 안내된 설정 프로세스를 완료하는 방법에 대한 자세한 내용은 [설정 안내](#)을 참조하세요.
 - ID 소스 섹션에서 작업을 선택한 다음 동기화 관리를 선택하여 동기화 범위, 동기화할 사용자 및 그룹 목록을 구성합니다.

IAM Identity Center에서 지원되는 사용자 및 그룹 속성

이 가이드에서는 IAM Identity Center의 SCIM 속성 지원에 대한 참조를 제공합니다. IAM Identity Center ID 스토어에서 지원되는 SCIM 사양의 사용자와 그룹 속성을 나열하고 지원되지 않는 특정 속성과 하위 속성을 식별합니다.

속성은 개별 사용자 또는 그룹 개체를 정의하고 식별하는 데 도움이 되는 정보(예: name, email 또는 members)입니다. IAM Identity Center는 수동 입력과 자동 SCIM 프로비저닝을 통해 가장 일반적으로 사용되는 속성을 지원합니다.

- 도메인 간 ID 관리 시스템(SCIM) 사양에 대한 자세한 내용은 <https://tools.ietf.org/html/rfc7642> 섹션을 참조하세요.
- 수동 및 자동 프로비저닝에 대한 내용은 [사용자가 외부 IdP일 경우 프로비저닝](#) 섹션을 참조하세요.
- 속성 매핑에 대한 내용은 [IAM Identity Center와 외부 ID 제공업체 디렉터리 간의 속성 매핑](#)을 참조하세요.

IAM Identity Center는 자동 프로비저닝 사용 사례에서 SCIM을 지원하므로 몇 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.

지원되지 않는 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

지원되지 않는 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)

외부 ID 제공업체

IAM Identity Center를 사용하여 보안 어설션 마크업 언어(SAML) 2.0 및 도메인 간 ID 관리 시스템(SCIM) 프로토콜을 통해 외부 ID 제공업체(IdP)의 기존 인력 ID에 연결할 수 있습니다. 이렇게 하면 사용자가 회사 보안 인증으로 AWS 액세스 포털에 로그인할 수 있습니다. 그런 다음 외부 IdP에 호스팅된 할당 계정, 역할 및 애플리케이션으로 이동할 수 있습니다.

예를 들어 Okta 또는 Microsoft Entra ID와 같은 외부 IdP를 IAM Identity Center에 연결할 수 있습니다. 그런 다음 사용자는 기존 Okta 또는 Microsoft Entra ID 자격 증명을 사용하여 AWS 액세스 포털에 로그인할 수 있습니다. 사용자가 로그인한 후 수행할 수 있는 작업을 제어하려면 AWS 조직의 모든 계정 및 애플리케이션에 중앙에서 액세스 권한을 할당하면 됩니다. 또한 개발자는 기존 자격 증명을 사용하여 AWS Command Line Interface (AWS CLI)에 간단히 로그인하고 자동 단기 자격 증명 생성 및 교체의 이점을 누릴 수 있습니다.

Active Directory 또는에서 자체 관리형 디렉터리를 사용하는 경우 섹션을 AWS Managed Microsoft AD 참조하세요 [Microsoft AD 디렉터리](#).

Note

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 AWS 계정 또는 애플리케이션에 할당하기 전에 해당하는 모든 사용자 및 그룹을 IAM Identity Center에 프로비저닝해야 합니다. 이를 위해 사용자 및 그룹에 대해 [SCIM을 사용하여 외부 ID 제공업체의 사용자 및 그룹 프로비저닝](#) 구성을 수행하거나 [수동 프로비저닝](#)을 사용할 수 있습니다. 사용자를 프로비저닝하는 방법에 관계없이 IAM Identity Center는 AWS Management Console, 명령줄 인터페이스 및 애플리케이션 인증을 외부 IdP로 리디렉션합니다. 그러면 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.

주제

- [외부 ID 제공업체에 연결하는 방법](#)
- [IAM Identity Center에서 외부 ID 제공업체 메타데이터를 변경하는 방법](#)
- [외부 ID 제공업체와의 SAML 및 SCIM ID 페더레이션 사용](#)

- [SCIM 프로파일 및 SAML 2.0 구현](#)

외부 ID 제공업체에 연결하는 방법

지원되는 외부 IdP에는 다양한 사전 조건, 고려 사항, 프로비저닝 절차가 적용됩니다. 몇몇 IdP에 대해서는 단계별 자습서를 이용할 수 있습니다.

- [CyberArk](#)
- [Google Workspace](#)
- [JumpCloud](#)
- [Microsoft Entra ID](#)
- [Okta](#)
- [OneLogin](#)
- [Ping Identity](#)

IAM Identity Center가 지원하는 외부 IdP 고려 사항에 대한 자세한 내용은 [외부 ID 제공업체와의 SAML 및 SCIM ID 페더레이션 사용](#)을 참조하세요.

다음 절차는 모든 외부 ID 제공업체에서 사용되는 절차에 대한 일반적인 개요를 제공합니다.

외부 ID 제공업체에 연결하려면

1. [IAM Identity Center 콘솔](#)을 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.

Note

다운로드하는 SAML 메타데이터 파일에는 IPv4-only 및 듀얼 스택 어설션 소비자 서비스(ACS) URLs. 또한 IAM Identity Center가 추가 리전에 복제되는 경우 메타데이터

파일에는 각 추가 리전에 대한 ACS URLs 포함됩니다. 외부 IdP에 ACS URLs 수 제한이 있는 경우 불필요한 ACS URLs. 예를 들어 조직에서 듀얼 스택 엔드포인트를 완전히 채택하고 더 이상 IP4v-only 엔드포인트를 사용하지 않는 경우 후자를 제거할 수 있습니다. 다른 방법은 메타데이터 파일을 사용하지 않고 ACS URLs IdP에 붙여넣는 것입니다.

- 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.

IAM Identity Center에서 외부 ID 제공업체 메타데이터를 변경하는 방법

이전에 IAM Identity Center에 제공한 외부 ID 제공업체의 메타데이터를 변경할 수 있습니다. 이러한 변경 사항은 IAM Identity Center를 통해 AWS 리소스에 로그인하고 액세스하는 사용자의 기능에 영향을 미칩니다. 다음 절차는 IAM Identity Center에 저장된 외부 IdP의 메타데이터를 업데이트하는 방법을 설명합니다. 이 절차를 완료하려면 IAM Identity Center의 조직 인스턴스가 필요합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

외부 ID 제공업체의 메타데이터를 변경하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택합니다. 작업을 선택한 다음 인증 관리를 선택합니다.
4. ID 제공업체 메타데이터 섹션에서 IdP 메타데이터 편집을 선택합니다. 이 페이지에서 외부 IdP의 IdP 로그인 URL 및 IdP 발급자 URL을 변경할 수 있습니다. 필요한 모든 변경을 수행했으면 변경 사항 저장을 선택합니다.

외부 ID 제공업체와의 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>)의 addr-spec을 준수하는("name@domain.com") 문자열(<https://tools.ietf.org/html/rfc2822#section-3.4.1>)이어야 합니다.
 - 메타데이터 파일은 75,000자를 초과할 수 없습니다.
 - 메타데이터에는 로그인 URL의 일부로 EntityID, X509 인증서 및 SingleSignOnService가 포함되어야 합니다.
 - 암호화 키는 지원되지 않습니다.
 - IAM Identity Center는 외부 IdP로 보내는 SAML 인증 요청에 대한 서명을 지원하지 않습니다.
 - IAM Identity Center를 추가 리전에 복제하고 다중 리전 IAM Identity Center의 이점을 최대한 활용하려는 경우 IdP는 여러 어설션 소비자 서비스(ACS) URLs을 지원해야 합니다. 자세한 내용은 [여러에서 IAM Identity Center 사용 AWS 리전](#) 단원을 참조하십시오. 단일 ACS URL을 사용하면 추가 리전의 사용자 경험에 영향을 미칠 수 있습니다. 기본 리전은 계속 정상적으로 작동합니다. 단일 ACS URL을 사용하는 추가 리전의 사용자 경험에 대한 자세한 내용은 [the section called “여러 ACS URLs 없이 AWS 관리형 애플리케이션 사용”](#) 및 섹션을 참조하세요 [the section called “AWS 계정 여러 ACS URLs 없이 복원력에 액세스”](#).
- SCIM
 - IAM Identity Center 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 3월의 FastFed Basic SCIM 프로파일 1.0(https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4) 초안에 명시된 상호 운용성 요구 사항을 기반으로 합니다. 현재 구현에 있어 이러한 문서와 IAM Identity Center 간의 차이점은 IAM Identity Center SCIM 구현 개발자 가이드의 [지원되는 API 운영](#) 섹션에 설명되어 있습니다.

위에서 언급한 표준 및 고려 사항을 준수하지 않는 IdP는 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 ExternalIdPDirectoryLogin을 필터링하여 로그
- IdP 관련 로그 및/또는 디버그 로그
- [IAM Identity Center 문제 해결](#)

Note

[IAM Identity Center의 ID 소스 자습서](#)에 포함된 IdP를 비롯해 일부 IdP는 IAM Identity Center 전용으로 구축된 “애플리케이션” 또는 “커넥터”의 형태로 IAM Identity Center에 대한 간소화된 구성 환경을 제공합니다. IdP가 이 옵션을 제공하는 경우 IAM Identity Center용으로 특별히 구축된 항목을 신중하게 선택하면서 이 옵션을 사용하는 것이 좋습니다. “AWS”, “AWS 페더레이션” 또는 유사한 일반 “AWS” 이름이라는 다른 항목은 다른 페더레이션 접근 방식 및/또는 엔드 포인트를 사용할 수 있으며 IAM Identity Center에서 예상대로 작동하지 않을 수 있습니다.

SCIM 프로파일 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\(SAML\) 2.0](#)을 사용하여 ID 페더레이션을 지원합니다. 이를 통해 IAM Identity Center는 외부 ID 제공업체(IdP)의 ID를 인증할 수 있습니다. 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 사용하면 사용자가 기존 자격 증명 공급자 자격 증명을 기반으로 애플리케이션에 액세스 AWS 계정 하고 구성할 수 있습니다.

IAM Identity Center는 IAM Identity Center 스토어 AWS Managed Microsoft AD또는 외부 ID 제공업체에 SAML IdP 기능을 추가합니다. 그런 다음 사용자는 , AWS Management Console 및와 같은 및 타사 애플리케이션을 포함하여 SAML을 지원하는 서비스에 Single Sign-OnMicrosoft 365할 수 Concur있습니니다Salesforce.

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 프로파일

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 [SCIM을 사용하여 외부 ID 제공업체의 사용자 및 그룹 프로비저닝](#) 단원을 참조하세요. IAM Identity Center의 SCIM 구현에 대한 자세한 내용은 [IAM Identity Center SCIM 구현 개발자 가이드](#)를 참조하세요.

주제

- [SCIM을 사용하여 외부 ID 제공업체의 사용자 및 그룹 프로비저닝](#)
- [SAML 2.0 인증서 교체](#)

SCIM을 사용하여 외부 ID 제공업체의 사용자 및 그룹 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](#)
- [액세스 토큰 생성](#)
- [자동 프로비저닝 활성화](#)
- [액세스 토큰 삭제](#)
- [자동 프로비저닝 비활성화](#)
- [액세스 토큰 교체](#)
- [자동 프로비저닝된 리소스 감사 및 조정](#)
- [수동 프로비저닝](#)

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 사항에 대해서는 해당 IdP에 사용할 수 있는 [IAM Identity Center의 ID 소스 자습서](#)를 참조하세요.

- 기본 이메일 주소를 프로비저닝하는 경우 이 속성 값은 각 사용자마다 고유해야 합니다. 일부 IdP에서는 기본 이메일 주소가 실제 이메일 주소가 아닐 수 있습니다. 예를 들어 이메일처럼 보이는 범용 사용자 이름(UPN)일 수 있습니다. 이러한 IdP에는 사용자의 실제 이메일 주소가 포함된 보조 또는 “기타” 이메일 주소가 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 사용자에게 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 사용자에게 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 경우 사용자가 AWS 권한, 할당 또는 권한을 잃지 않습니다.
- 아직 애플리케이션에 할당되지 않았거나 IAM Identity Center에 프로비저닝할 수 없는 AWS 계정 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 제공업체가 관리하며 구현에 따라 다를 수 있습니다. 사용자 프로비저닝 해제에 대한 자세한 내용은 ID 제공업체에 문의하세요.
- IdP에 대해 SCIM으로 자동 프로비저닝을 설정한 후에는 더 이상 IAM Identity Center 콘솔에서 사용자를 추가하거나 편집할 수 없습니다. 사용자를 추가하거나 수정해야 할 경우 외부 IdP 또는 ID 소스에서 이를 수행해야 합니다.

IAM Identity Center의 SCIM 구현에 대한 자세한 내용은 [IAM Identity Center SCIM 구현 개발자 가이드](#)를 참조하세요.

액세스 토큰 만료를 모니터링하는 방법

SCIM 액세스 토큰의 유효 기간은 1년으로 생성됩니다. SCIM 액세스 토큰이 90일 이내에 만료되도록 설정된 경우는 토큰 교체에 도움이 되도록 IAM Identity Center 콘솔과 AWS Health 대시보드를 통해 알림을 AWS 보냅니다. 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 SCIM 액세스 토큰이 만료될 때까지 매주 90~60일, 매주 2회 60~30일, 매주 3회 30~15일, 매일 15일 갱신됩니다.

액세스 토큰 생성

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 프로비저닝 활성화](#) 단원을 참조하세요.

새 액세스 토큰을 생성하려면

1. [IAM Identity Center 콘솔](#)의 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. 달기를 선택하세요.

자동 프로비저닝 활성화

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 해당 IdP용 [IAM Identity Center의 ID 소스 자습서](#)를 참조하세요.

IAM Identity Center에서 자동 프로비저닝을 활성화하려면

1. 사전 필수 조건을 완료한 후 [IAM Identity Center 콘솔](#)을 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 SCIM 엔드포인트와 액세스 토큰을 복사합니다. 나중에 IdP에서 프로비저닝을 구성할 때 이를 붙여넣어야 합니다.
 - a. SCIM 엔드포인트-예: `https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. 액세스 토큰 - 토큰 표시를 선택하여 값을 복사합니다.

Warning

SCIM 엔드포인트와 액세스 토큰을 가져올 수 있는 유일한 시간입니다. 계속 진행하기 전에 이 값을 복사해야 합니다. 이 자습서의 후반부에 이 값을 입력하여 IdP에서 자동 프로비저닝을 구성할 수 있습니다.

5. 달기를 선택하세요.

이 절차를 완료한 후에는 IdP에서 자동 프로비저닝을 구성해야 합니다. 자세한 내용은 해당 IdP용 [IAM Identity Center의 ID 소스 자습서](#)를 참조하세요.

액세스 토큰 삭제

다음 절차를 사용하여 IAM Identity Center 콘솔에서 기존 액세스 토큰을 삭제합니다.

기존 액세스 토큰을 삭제하려면

1. [IAM Identity Center 콘솔](#)의 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.

자동 프로비저닝 비활성화

다음 절차에 따라 IAM Identity Center 콘솔에서 자동 프로비저닝을 비활성화합니다.

Important

이 절차를 시작하기 전에 액세스 토큰을 삭제해야 합니다. 자세한 내용은 [액세스 토큰 삭제](#) 단원을 참조하세요.

IAM Identity Center 콘솔에서 자동 프로비저닝을 비활성화하려면

1. [IAM Identity Center 콘솔](#)의 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 비활성화를 입력한 다음 자동 프로비저닝 비활성화를 선택합니다.

액세스 토큰 교체

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 콘솔](#)의 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. [액세스 토큰 생성](#)의 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](#) 단계에 따라 앞서 기록해 둔 이전 액세스 토큰을 삭제합니다. 토큰 생성 날짜를 제거할 토큰에 대한 힌트로 사용할 수도 있습니다.

자동 프로비저닝된 리소스 감사 및 조정

SCIM은 ID 소스에서 IAM Identity Center로 사용자, 그룹, 그룹 멤버십을 자동으로 프로비저닝할 수 있도록 지원합니다. 이 안내서는 이러한 리소스를 확인하고 조정하여 정확한 동기화를 유지하는 데 도움을 줍니다.

리소스를 감사하는 이유는 무엇인가요?

정기적인 감사는 액세스 제어를 정확하게 유지하고 ID 제공업체(IdP)가 IAM Identity Center와 올바르게 동기화를 유지하는 데 도움을 줍니다. 이는 보안 규정 준수 및 액세스 관리에 있어 특히 중요합니다.

감사 가능한 리소스:

- Users
- 그룹
- 그룹 멤버십

AWS Identity Store [APIs](#) 또는 [CLI 명령](#)을 사용하여 감사 및 조정을 수행할 수 있습니다. 다음 예제에서는 AWS CLI 명령을 사용합니다. API를 사용한 대안은 아이덴티티 스토어 API 참조의 [해당 작업](#)을 참조하세요.

리소스 감사 방법

다음은 AWS CLI 명령을 사용하여 이러한 리소스를 감사하는 방법에 대한 예제입니다.

시작하기 전에 다음을 갖추었는지 확인하세요.

- IAM Identity Center에 대한 관리자 액세스 권한.
- AWS CLI 가 설치 및 구성되었습니다. 자세한 내용은 [AWS 명령줄 인터페이스 사용 설명서](#)를 참조하세요.
- 아이덴티티 스토어 명령에 필요한 IAM 권한.

1단계: 현재 리소스 나열

를 사용하여 현재 리소스를 볼 수 있습니다 AWS CLI.

Note

를 사용할 때를 지정하지 않으면 AWS CLI페이지 매김이 자동으로 처리됩니다--no-paginate. API를 직접 호출하는 경우(예: SDK 또는 사용자 지정 스크립트 사용) 응답의 NextToken을 처리해야 합니다. 이렇게 하면 여러 페이지에 걸친 모든 결과를 검색할 수 있습니다.

Example사용자

```
aws identitystore list-users \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Example그룹

```
aws identitystore list-groups \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Example그룹 멤버십

```
aws identitystore list-group-memberships \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID
```

2단계: ID 소스와 비교

나열된 리소스를 ID 소스와 비교하여 다음과 같은 불일치를 식별합니다.

- IAM Identity Center에서 프로비저닝해야 하는 리소스 누락.
- IAM Identity Center에서 제거해야 하는 추가 리소스.

Example사용자

```
# Create missing users
aws identitystore create-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-name USERNAME \
  --display-name DISPLAY_NAME \
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \
  --emails Value=EMAIL,Primary=true

# Delete extra users
aws identitystore delete-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-id USER_ID
```

Example그룹

```
# Create missing groups
aws identitystore create-group \
  --identity-store-id IDENTITY_STORE_ID \
  [group attributes]

# Delete extra groups
aws identitystore delete-group \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID
```

Example그룹 멤버십

```
# Add missing members
aws identitystore create-group-membership \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID \
  --member-id '{"UserId": "USER_ID"}'
```

```
# Remove extra members
aws identitystore delete-group-membership \
  --identity-store-id IDENTITY_STORE_ID \
  --membership-id MEMBERSHIP_ID
```

고려 사항

- 명령에는 [서비스 할당량과 API 스퀀링](#)이 적용됩니다.
- 조정 중에 많은 차이가 발견되면 AWS Identity Store를 작고 점진적으로 변경합니다. 이렇게 하면 여러 사용자에게 영향을 미치는 실수를 방지하는 데 도움이 됩니다.
- SCIM 동기화는 수동 변경 사항을 재정의할 수 있습니다. 이 동작을 이해하려면 IdP 설정을 확인하세요.

수동 프로비저닝

일부 IdP는 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 참조하십시오.

SAML 2.0 인증서 교체

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 삭제해야 합니다.

또한 일부 IdP는 여러 인증서를 지원하지 않을 수 있다는 점도 고려해야 합니다. 이 경우 해당 IdP로 인증서를 교체하면 사용자에게 일시적인 서비스 중단이 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 콘솔](#)에서 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 페이지에는 목록의 각 인증서 옆 만료 날짜 옆에 색상이 들어간 상태 표시기 아이콘이 표시됩니다. 다음은 IAM Identity Center에서 각 인증서에 표시할 아이콘을 결정하는 데 사용하는 기준에 대한 설명입니다.

- 빨간색-인증서가 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 콘솔](#)에서 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 옆에 표시된 대로 목록의 인증서 상태를 검토합니다.

Microsoft AD 디렉터리

를 사용하면 AWS Managed Microsoft AD 사용하여 Active Directory(AD)의 자체 관리형 디렉터리 또는의 디렉터리를 연결할 AWS IAM Identity Center 수 있습니다 AWS Directory Service. 이 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 를 사용하면에서 호스팅되는 독립 실행형 AWS Managed Microsoft AD 디렉터리를 설정하고 실행할 수 있습니다 AWS 클라우드. Directory Service 를 사용하여 AWS 리소스를 기존 자체 관리형 AD와 연결할 수도 있습니다. 자체 관리형 AD와 함께 작동 AWS Directory Service 하도록 구성하려면 먼저 신뢰 관계를 설정하여 클라우드로 인증을 확장해야 합니다.

IAM Identity Center는에서 제공하는 연결을 Directory Service 사용하여 소스 AD 인스턴스에 대한 패스스루 인증을 수행합니다. 를 ID 소스 AWS Managed Microsoft AD 로 사용하면 IAM Identity Center 는 AD 트러스트를 통해 연결된 도메인의 사용자 AWS Managed Microsoft AD 와 함께 작업할 수 있습니다. 4개 이상의 도메인에서 사용자를 찾으려는 경우 사용자는 IAM Identity Center에 로그인할 때 DOMAIN\user 구문을 사용자 이름으로 사용해야 합니다.

참고

- 사전 조건 단계로 AD Connector 또는 AWS Managed Microsoft AD 의 디렉터리가 AWS Organizations 관리 계정 내에 Directory Service 있는지 확인합니다.
- IAM Identity Center는 SAMBA 4 기반 Simple AD를 연결된 디렉터리로 지원하지 않습니다.
- IAM Identity Center는 FSPs 없습니다. 의 AWS Managed Microsoft AD 그룹에 신뢰할 수 있는 도메인의 멤버가 FSPs로 포함된 경우 해당 멤버는 동기화되지 않습니다.

Active Directory를 IAM Identity Center의 자격 증명 소스로 사용하는 프로세스에 대한 데모는 다음 YouTube 비디오를 참조하세요.

[Active Directory를 ID 소스로 사용 AWS IAM Identity Center | Amazon Web Services](#)

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 설정된 AWS 리전 동일한에서 IAM Identity Center를 활성화 AWS Managed Microsoft AD해야 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 사용합니다.
- 관리 계정에 있는 Active Directory를 사용합니다.

에 설정된 기존 AD 커넥터 또는 AWS Managed Microsoft AD 디렉터리가 있어야 하며 AWS Organizations 관리 계정 내에 있어야 AWS Directory Service합니다. 한 AWS Managed Microsoft AD 번에 AD Connector 디렉터리 하나 또는의 디렉터리 하나만 연결할 수 있습니다. 여러 도메인이 나 포리스트를 지원해야 하는 경우 AWS Managed Microsoft AD를 사용합니다. 자세한 내용은 다음을 참조하세요.

- [의 디렉터를 IAM Identity Center AWS Managed Microsoft AD 에 연결](#)
- [Active Directory의 자체 관리형 디렉터를 IAM Identity Center에 연결](#)
- 위임된 관리자 계정에 있는 Active Directory를 사용합니다.

IAM Identity Center 위임된 관리자를 활성화하고 Active Directory를 IAM Identity Center ID 소스로 사용하려는 경우 위임된 관리자 계정에 있는 AWS Managed Microsoft AD 디렉터리에 설정된 기존 AD 커넥터 또는 AWS 디렉터를 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 디렉터를 IAM Identity Center에 연결하는 데 도움이 될 것입니다.

디렉터리 AWS Managed Microsoft AD 또는 Active Directory의 자체 관리형 디렉터를 IAM Identity Center와 연결할 수 있습니다.

Note

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

AWS Managed Microsoft AD

1. [Microsoft AD 디렉터리](#)에서 지침을 검토하세요.
2. [의 디렉터를 IAM Identity Center AWS Managed Microsoft AD 에 연결](#) 단원의 단계를 따르세요.
3. 관리자 권한을 부여하려는 사용자가 IAM Identity Center와 동기화하도록 Active Directory를 구성합니다. 자세한 내용은 [관리 사용자의 IAM Identity Center 동기화](#) 단원을 참조하십시오.

Active Directory의 자체 관리형 디렉터리

1. [Microsoft AD 디렉터리](#)에서 지침을 검토하세요.
2. [Active Directory의 자체 관리형 디렉터를 IAM Identity Center에 연결](#) 단원의 단계를 따르세요.
3. 관리자 권한을 부여하려는 사용자가 IAM Identity Center와 동기화하도록 Active Directory를 구성합니다. 자세한 내용은 [관리 사용자의 IAM Identity Center 동기화](#) 단원을 참조하십시오.

외부 ID 제공업체(IdP)

1. [외부 ID 제공업체](#)에서 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

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

1. [IAM Identity Center 콘솔](#)을 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 사용자에게 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 내용은 [권한 집합을 생성합니다](#) 단원을 참조하십시오.

Active Directory에서 사용자를 가져올 때 프로비저닝

IAM Identity Center는에서 제공하는 연결을 사용하여 Active Directory의 소스 디렉터리에서 IAM Identity Center ID 스토어로 사용자, 그룹 및 멤버십 정보를 Directory Service 동기화합니다. 사용자 인종은 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

- [의 디렉터리를 IAM Identity Center AWS Managed Microsoft AD 에 연결](#)
- [Active Directory의 자체 관리형 디렉터리를 IAM Identity Center에 연결](#)
- [IAM Identity Center와 외부 ID 제공업체 디렉터리 간의 속성 매핑](#)
- [IAM Identity Center 구성 가능 AD 동기화](#)

의 디렉터리를 IAM Identity Center AWS Managed Microsoft AD 에 연결

다음 절차에 따라에서 AWS Managed Microsoft AD 관리하는의 디렉터리를 IAM Identity Center AWS Directory Service 에 연결합니다.

IAM Identity Center AWS Managed Microsoft AD 에 연결하려면

1. [IAM Identity Center 콘솔](#)을 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 AD의 디렉터를 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 AWS 계정 및 애플리케이션에 대한 Single Sign-On AWS 액세스 권한도 가질 수 있습니다. 이러한 사용자에 대한 Single Sign-On 액세스를 구성하려면 다음 중 하나를 수행할 수 있습니다.

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

AWS IAM Identity Center 는 도메인에서 사용자 및 그룹 정보를 읽고 사용자 및 그룹 메타데이터를 동기화할 수 있는 권한을 갖도록 양방향 신뢰가 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 협업용으로도 사용됩니다. Directory Service for Microsoft Active Directory에서 도메인으로의 신뢰는 IAM Identity Center가 인증을 위해 도메인을 신뢰하도록 허용합니다. 반대 방향의 신뢰는 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 경우](#)를 참조하세요.

Note

IAM Identity Center와 같은 AWS 애플리케이션을 사용하여 신뢰할 수 있는 도메인에서 Directory Service 디렉터리 사용자를 읽으려면 Directory Service 계정에 신뢰할 수 있는 사용자의 userAccountControl 속성에 대한 권한이 필요합니다. 이 속성에 대한 읽기 권한이 없으면 AWS 애플리케이션이 계정의 활성화 또는 비활성화 여부를 확인할 수 없습니다. 이 속성에 대한 읽기 액세스는 신뢰가 생성될 때 기본값으로 제공됩니다. 이 속성에 대한 액세스를 거부하면(권장하지 않음) Identity Center와 같은 애플리케이션이 신뢰할 수 있는 사용자를 읽을 수 없게 됩니다. 해결 방법은 AWS 예약 OU(_ 접두사)에 있는 AWS 서비스 계정의 userAccountControl 속성에 대한 읽기 액세스를 허용하는 것입니다 AWS.

- 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 연결](#)을 참조하세요. AD 커넥터 사용 시 고려 사항은 다음과 같습니다.
- IAM Identity Center를 AD Connector 디렉터리에 연결하는 경우 향후 사용자 암호 재설정은 AD 내에서 수행해야 합니다. 즉, 사용자는 AWS 액세스 포털에서 암호를 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 Directory Service 를 사용합니다.

Note

IAM Identity Center는 SAMBA4 기반 Simple AD 디렉터리에서는 작동하지 않습니다.

IAM Identity Center와 외부 ID 제공업체 디렉터리 간의 속성 매핑

속성 매핑은 IAM Identity Center에 있는 속성 유형을 Google Workspace, Microsoft Active Directory (AD), Okta와 같은 외부 ID 소스의 유사 속성과 매핑하는 데에 사용됩니다. IAM Identity Center는 ID 소스에서 사용자 속성을 검색하여 이를 IAM Identity Center 사용자 속성에 매핑합니다.

IAM Identity Center가 Google Workspace, Okta, Ping과 같은 외부 ID 제공업체(IdP)를 자격 증명 소스로 사용하도록 동기화된 경우 IdP에 속성을 매핑해야 합니다.

IAM Identity Center는 해당 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. 그러면 이러한 사용자 속성이 ID 소스에서 검색됩니다. 각 애플리케이션은 성공적인 Single Sign-On에 필요한 SAML 2.0 속성 목록을 결정합니다. 자세한 내용은 [애플리케이션의 속성을 IAM Identity Center 속성에 매핑](#) 단원을 참조하십시오.

또한 Active Directory를 자격 증명 소스로 사용하는 경우 IAM Identity Center는 Active Directory 구성 페이지의 속성 매핑 섹션에서 속성 세트를 관리합니다. 자세한 내용은 [IAM Identity Center와 Microsoft AD 디렉터리 간 사용자 속성 매핑](#) 단원을 참조하십시오.

지원되는 외부 ID 제공업체 속성

다음 표에는 지원되며 IAM Identity Center에서 [액세스 제어를 위한 속성](#) 섹션을 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}
```


IdP에서 지원되는 속성

`${path:addresses[type eq "work"].locality}``${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}``${path:userType}``${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}`

IAM Identity Center와 Microsoft AD 간의 기본 매핑

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

IAM Identity Center의 사용자 속성	Active Directory의 이 속성에 매핑
displayname	\${displayname}
emails[?primary].value *	\${mail}
externalid	\${objectguid}
name.givenname	\${givenname}
name.familyname	\${sn}
name.middlename	\${initials}
sid	\${objectsid}
username	\${userprincipalname}

* IAM Identity Center의 이메일 속성은 디렉터리 내에서 고유해야 합니다.

IAM Identity Center의 그룹 속성	Active Directory의 이 속성에 매핑
externalid	\${objectguid}
description	\${description}
displayname	\${samaccountname}@{associateddomain}

고려 사항

- 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.
- 특정 IAM Identity Center 속성은 변경할 수 없고 기본적으로 특정 Microsoft AD 디렉터리 속성에 매핑되므로 수정할 수 없습니다.

예를 들어 "사용자 이름"은 IAM Identity Center의 필수 속성입니다. "사용자 이름"을 값이 비어 있는 AD 디렉터리 속성에 매핑하는 경우 IAM Identity Center는 windowsUpn 값을 "사용자 이름"의 기본 값으로 간주합니다. 현재 매핑에서 "사용자 이름"의 속성 매핑을 변경하고자 한다면 변경 전 "사용자 이름"에 종속된 IAM Identity Center 플로가 예상대로 계속 작동하는지 확인합니다.

IAM Identity Center에서 지원되는 Microsoft AD 속성

다음 표에는 지원되고 IAM Identity Center의 사용자 속성에 매핑할 수 있는 모든 Microsoft AD 디렉터리 속성이 나열되어 있습니다.

Microsoft AD 디렉터리에서 지원되는 속성

`${samaccountname}`

`${description}`

`${objectguid}`

`${objectsid}`

`${givenname}`

`${sn}`

`${initials}`

`${mail}`

`${userprincipalname}`

`${displayname}`

`${distinguishedname}`

`${proxyaddresses[?type == "SMTP"].value}`

`${proxyaddresses[?type == "smtp"].value}`

`${useraccountcontrol}`

Microsoft AD 디렉터리에서 지원되는 속성

`${associateddomain}`

고려 사항

- 지원되는 Microsoft AD 디렉터리 속성의 조합을 IAM Identity Center의 단일 가변 속성에 매핑하도록 지정할 수 있습니다.

Microsoft AD에 지원되는 IAM Identity Center 속성

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

Active Directory용 IAM Identity Center에서 지원되는 속성

`${user:AD_GUID}`

`${user:AD_SID}`

`${user:email}`

`${user:familyName}`

`${user:givenName}`

`${user:middleName}`

`${user:name}`

`${user:preferredUsername}`

`${user:subject}`

IAM Identity Center와 Microsoft AD 디렉터리 간 사용자 속성 매핑

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 콘솔](#)을 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 **mail** 속성에 매핑하는 게 좋을 수 있습니다.
5. 변경 사항 저장을 선택합니다.

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.

- 이 방법을 통해 다음을 수행할 수 있습니다.
 - Microsoft Active Directory에서 IAM Identity Center에 자동으로 동기화되는 사용자 및 그룹을 명시적으로 정의하여 데이터 경계를 제어합니다. 언제든지 [사용자 및 그룹을 추가](#)하거나 [사용자 및 그룹을 제거](#)하여 동기화 범위를 변경할 수 있습니다.
 - 동기화된 사용자 및 그룹에 [AWS 계정에 대한 Single Sign-On 액세스 권한](#) 또는 [애플리케이션에 대한 액세스 권한](#)을 할당합니다. 애플리케이션은 AWS 관리형 애플리케이션 또는 고객 관리형 애플리케이션일 수 있습니다.
 - 필요에 따라 [동기화를 일시 중지했다가 다시 시작하여](#) 동기화 프로세스를 제어합니다. 이를 통해 프로덕션 시스템의 부하를 조절할 수 있습니다.

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 관리형 애플리케이션 또는 고객 AWS 관리형 애플리케이션에 새 사용자 AWS 계정 및 그룹 액세스 권한을 할당하려면 먼저 Active Directory에서 동기화할 사용자 및 그룹을 지정한 다음 IAM Identity Center에 동기화해야 합니다.

- 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 자식 그룹)이라고 합니다.

- 구성 가능한 AD 동기화 – 구성 가능한 AD 동기화를 사용하여 중첩 그룹을 포함하는 Active Directory 그룹에 할당하는 경우 AWS 계정 또는 애플리케이션에 대한 액세스 권한이 있는 사용자의 범위가 늘어날 수 있습니다. 이 경우 할당은 중첩 그룹의 사용자를 포함하는 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.

- 구성 가능한 AD 동기화 – 프로비저닝이 먼저 수행되며 자동으로 수행되지 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.

주제

- [구성 가능한 AD 동기화의 작동 방식](#)
- [동기화를 위한 속성 매핑을 구성합니다.](#)
- [Active Directory에서 IAM Identity Center로의 최초 동기화 설정](#)
- [동기화 범위에 사용자 및 그룹 추가](#)
- [동기화 범위에서 사용자 및 그룹을 제거합니다.](#)
- [동기화 일시 중지 및 다시 시작](#)
- [구성 가능한 AD 동기화를 위한 동기화 구성을 자동화합니다.](#)

구성 가능한 AD 동기화의 작동 방식

IAM Identity Center는 다음 프로세스를 사용하여 ID 스토어의 AD 기반 ID 데이터를 새로 고칩니다. 필수 조건에 대해 자세히 알아보려면 [필수 조건 및 고려 사항](#) 섹션을 참조하세요.

만들기

Active Directory의 자체 관리형 디렉터리 또는에서 관리하는 디렉터리를 AWS Managed Microsoft AD IAM Identity Center Directory Service에 연결한 후 IAM Identity Center ID 스토어에 동기화하려는 Active Directory 사용자 및 그룹을 명시적으로 구성할 수 있습니다. 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 자식 그룹이라고 함)도 ID 스토어에 기록됩니다.

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 Identity Center는 기본 동기화 주기로 매시간 Active Directory의 데이터를 동기화합니다. 데이터가 IAM Identity Center에 동기화되는 데는 Active Directory의 크기에 따라 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 속성 업데이트가 IAM Identity Center에 반영되려면 1회의 동기화 주기가 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 사용하는 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.

동기화를 위한 속성 매핑을 구성합니다.

사용 가능한 속성에 대한 자세한 내용은 [IAM Identity Center와 외부 ID 제공업체 디렉터리 간의 속성 매핑](#) 단원을 참조하세요.

IAM Identity Center의 속성을 디렉터리에 매핑하도록 구성하려면

1. [IAM Identity Center 콘솔](#)을 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 email을 Active Directory 사용자 디렉터리 속성 `objectguid`에 매핑하는 게 좋을 수 있습니다.

Note

그룹 속성에서 IAM Identity Center Identity Store 속성과 Active Directory 그룹 속성을 변경할 수 없습니다.

6. 변경 사항 저장을 선택합니다. 그러면 동기화 관리 페이지로 돌아갑니다.

Active Directory에서 IAM Identity Center로의 최초 동기화 설정

사용자와 그룹을 Active Directory에서 IAM Identity Center로 처음 동기화하는 경우 다음 단계를 따릅니다. 또는 [ID 소스 변경](#)에 설명된 단계에 따라 자격 증명 소스를 IAM Identity Center에서 Active Directory로 변경할 수 있습니다.

설정 안내

1. [IAM Identity Center 콘솔](#)을 엽니다.

Note

다음 단계로 이동하기 전에 IAM Identity Center 콘솔에서 AWS Managed Microsoft AD 디렉터리가 AWS 리전 위치한 중 하나를 사용하고 있는지 확인합니다.

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

Note

동기화 범위에 그룹을 추가할 때 도메인의 그룹이 아닌 신뢰할 수 있는 온프레미스 AWS Managed Microsoft AD 도메인에서 직접 그룹을 동기화합니다. 신뢰할 수 있는 도메인에서 직접 동기화된 그룹에는 IAM Identity Center가 액세스하고 성공적으로 동기화할 수 있는 실제 사용자 객체가 포함됩니다.

다음 단계에 따라 Active Directory 사용자와 그룹을 IAM Identity Center에 추가합니다.

사용자를 추가하려면

1. [IAM Identity Center 콘솔](#)을 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. 지정한 사용자가 목록에 표시되지 않는 경우 새로 고침 아이콘을 선택하여 사용자 목록을 업데이트합니다.

그룹을 추가하려면

1. [IAM Identity Center 콘솔](#)을 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. 지정한 그룹이 목록에 표시되지 않는 경우 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 콘솔](#)을 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 콘솔](#)을 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 콘솔](#)을 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 콘솔](#)을 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.

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 IAMIdentityCenterAllUsersAndGroups로 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.

Identity Center 디렉터리에서 사용자 관리

IAM Identity Center는 사용자 및 그룹에 다음과 같은 기능을 제공합니다.

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

IAM Identity Center 스토어에서 사용자 및 그룹을 관리하기 위해서는 [Identity Center 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 내용은 [사용자 및 그룹 프로비저닝](#) 단원을 참조하십시오.

ID 소스 변경

에서 사용자를 관리하려는 경우 언제든지 Identity Center 디렉터리 사용을 중지하고 대신를 사용하여 IAM Identity Center를 Microsoft AD의 디렉터리에 연결할 AWS Managed Microsoft AD수 있습니다 Directory Service. 자세한 내용은 [IAM Identity Center 디렉터리와 Active Directory 간 변경](#)의 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 변경](#)의 고려 사항을 참조하세요.

주제

- [Identity Center 디렉터리에 사용자 추가](#)
- [Identity Center 디렉터리에 그룹 추가](#)
- [그룹에 사용자 추가](#)
- [IAM Identity Center에서 그룹 삭제](#)
- [IAM Identity Center에서 사용자 삭제](#)
- [그룹에서 사용자 제거](#)
- [IAM Identity Center 디렉터리 사용자 속성 편집](#)

Identity Center 디렉터리에 사용자 추가

IAM Identity Center 디렉터리에 생성한 사용자 및 그룹은 IAM Identity Center에서만 사용할 수 있습니다. 다음 절차에 따라 Identity Center 디렉터리에 사용자를 추가합니다. 또는 AWS API 작업을 호출 [CreateUser](#)하여 사용자를 추가할 수 있습니다.

Console

사용자를 추가하려면

1. [IAM Identity Center 콘솔](#)을 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. 이 사용자에게 암호 설정 지침이 포함된 이메일 보내기 - 이 옵션을 선택하면 해당 사용자에게 Amazon Web Services를 발신자로 한 이메일이 AWS IAM Identity Center 가입 초대라는 제목으로 자동으로 발송됩니다. 이메일은 회사를 대신하여 사용자가 IAM Identity Center AWS 액세스 포털에 액세스하고 암호를 등록하도록 초대합니다. 이메일 초대는 7일 후 만료됩니다. 초대가 만료되는 경우 암호 재설정을 선택한 다음 암호 재설정 안내와 함께 사용자에게 이메일 전송을 선택하여 이메일을 다시 보낼 수 있습니다. 사용자가 초대를 수락하기 전 이메일 주소 확인을 위한 이메일 확인 링크 전송이 표시됩니다. 그러나 이 단계는 선택 사항으로 사용자가 초대를 수락하고 암호를 등록하면 사라집니다.

 Note

특정 리전에서는 IAM Identity Center가 다른 AWS 리전의 Amazon Simple Email Service를 사용하는 사용자에게 이메일을 보냅니다. 이메일 전송 방법에 대한 자세한 내용은 [Amazon SES를 사용한 리전 간 이메일](#) 단원을 참조하세요.

IAM Identity Center 서비스에서 보내는 모든 이메일은 주소 no-reply@signin.aws.com 또는 no-reply@login.awsapps.com에서 발송됩니다. 이러한 발신자 이메일 주소의 이메일은 수신하고 정크 또는 스팸으로 처리하지 않도록 이메일 시스템을 구성하는 것이 좋습니다.

- ii. 이 사용자와 공유할 수 있는 일회용 암호 생성 -이 옵션은 이메일 주소에서 사용자에게 수동으로 보낼 수 있는 AWS 액세스 포털 URL 및 암호 세부 정보를 제공합니다. 사용자는 이메일 주소를 확인해야 합니다. 이메일 확인 링크 전송을 선택하여 프로세스를 시작할 수 있습니다. 이메일 확인 링크는 7일 후 만료됩니다. 링크가 만료되는 경우 암호 재설정을 선택한 다음 일회용 암호 생성 및 사용자와 암호 공유를 선택하여 이메일 확인 링크를 다시 보낼 수 있습니다.
- c. 이메일 주소 - 이메일 주소는 고유해야 합니다.

- d. 이메일 주소 확인
- e. 이름 — 자동 프로비저닝이 작동하려면 여기에 이름을 입력해야 합니다. 자세한 내용은 [SCIM을 사용하여 외부 ID 제공업체의 사용자 및 그룹 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.

AWS CLI

사용자를 추가하려면

다음 `create-user` 명령은 Identity Center 디렉터리에 새 사용자를 생성합니다.

```
aws identitystore create-user \
  --identity-store-id d-1234567890 \
  --user-name johndoe \
  --name "GivenName=John,FamilyName=Doe" \
  --display-name "John Doe" \
  --emails "Type=work,Value=johndoe@example.com"
```

출력:

```
{
  "UserId": "1234567890-abcdef",
  "IdentityStoreId": "d-1234567890"
}
```

Note

create-user CLI 명령 또는 [CreateUser](#) API 작업으로 사용자를 생성할 때는 사용자에게 암호가 없습니다. IAM Identity Center의 설정을 업데이트하여 이러한 사용자가 처음 로그인을 시도한 후 사용자에게 확인 이메일을 보내 암호를 설정할 수 있도록 할 수 있습니다. 이 설정을 활성화하지 않으면 일회용 암호를 생성하고 사용자와 이를 공유해야 합니다. 자세한 내용은 [API로 생성된 사용자에게 일회용 암호 이메일 전송](#) 단원을 참조하십시오.

Identity Center 디렉터리에 그룹 추가

다음 절차에 따라 Identity Center 디렉터리에 그룹을 추가합니다. 또는 AWS API 작업을 호출 [CreateGroup](#)하여 그룹을 추가할 수 있습니다.

Console

그룹을 추가하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 그룹을 선택합니다.
3. 그룹 생성을 선택합니다.
4. 그룹 이름 및 설명 - 선택 사항을 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.

AWS CLI

그룹을 추가하는 방법

다음 create-group 명령은 Identity Center 디렉터리에 새 그룹을 생성합니다.

```
aws identitystore create-group \  
  --identity-store-id d-1234567890 \  
  --display-name "Developers" \  
  --description "Group that contains all developers"
```

출력:


```
{
  "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",
  "IdentityStoreId": "d-1234567890"
}
```

이 그룹을 Identity Center 디렉터리에 추가한 후 그룹에 Single Sign-On 액세스 권한을 할당할 수 있습니다. 자세한 내용은 [에 사용자 또는 그룹 액세스 할당 AWS 계정](#) 단원을 참조하십시오.

그룹에 사용자 추가

다음 절차에 따라 이전에 Identity Center 디렉터리에 생성한 그룹의 멤버로 사용자를 추가할 수 있습니다. 또는 AWS API 작업을 호출 [CreateGroupMembership](#) 하여 사용자를 그룹의 멤버로 추가할 수 있습니다.

Console

사용자를 그룹의 구성원으로 추가하려면

1. [IAM Identity Center 콘솔](#)을 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.

AWS CLI

사용자를 그룹의 구성원으로 추가하려면

다음 create-group-membership 명령은 Identity Center 디렉터리의 그룹에 사용자를 추가합니다.

```
aws identitystore create-group-membership \
  --identity-store-id d-1234567890 \
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
  --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

출력:

```
{
  "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  "IdentityStoreId": "d-1234567890"
}
```

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 Identity Center 디렉터리에서 그룹을 삭제할 수 있습니다.

Important

이 페이지의 지침은 [AWS IAM Identity Center](#)에 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 삭제](#)를 참조하세요.

Console

그룹을 삭제하려면

1. [IAM Identity Center 콘솔](#)을 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.

AWS CLI

그룹을 삭제하려면

다음 delete-group 명령은 Identity Center 디렉터리에서 지정된 그룹을 삭제합니다.

```
aws identitystore delete-group \
  --identity-store-id d-1234567890 \
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

IAM Identity Center에서 사용자 삭제

IAM Identity Center 디렉터리에서 사용자를 삭제하면 AWS 계정 및 애플리케이션에 대한 액세스가 제거됩니다. 사용자를 삭제한 후에는 이 작업을 실행 취소할 수 없습니다. 다음 절차에 따라 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 없습니다. 자세한 내용은 [IAM Identity Center의 인증 세션 이해](#) 단원을 참조하십시오.

Important

이 페이지의 지침은 [AWS IAM Identity Center](#)에 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 삭제](#)를 참조하세요.

Console

사용자 삭제

1. [IAM Identity Center 콘솔](#)을 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.

AWS CLI

사용자 삭제

다음 delete-user 명령은 Identity Center 디렉터리에서 사용자를 삭제합니다.

```
aws identitystore delete-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

그룹에서 사용자 제거

다음 절차를 따라 그룹에서 멤버를 제거합니다. 또는 AWS API 작업을 호출 [DeleteGroupMembership](#)하여 그룹에서 사용자를 제거할 수 있습니다.

Console

그룹에서 사용자 제거

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 그룹을 선택합니다.
3. 업데이트할 그룹을 선택합니다.

4. 그룹 세부 정보 페이지의 이 그룹의 사용자에서 제거할 사용자를 선택합니다.
5. 그룹에서 사용자 제거를 선택합니다.
6. 사용자 제거 대화 상자에서 그룹에서 사용자 제거를 선택하여 그룹에 할당된 계정 및 애플리케이션에 대한 사용자 액세스를 제거할지 확인합니다.

AWS CLI

그룹에서 사용자 제거

다음 `delete-group-membership` 명령은 그룹에서 멤버십을 제거합니다.

```
aws identitystore delete-group-membership
--identity-store-id d-1234567890 \
--membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

IAM Identity Center 디렉터리 사용자 속성 편집

다음 절차에 따라 Identity Center 디렉터리에서 사용자의 속성을 편집할 수 있습니다. 또는 AWS API 작업 [UpdateUser](#)를 호출하여 사용자 속성을 업데이트할 수 있습니다.

Console

IAM Identity Center에서 사용자 속성을 편집하려면

1. [IAM Identity Center 콘솔](#)을 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 매핑하는데 도움이 되도록 할 수 있습니다.

 Note

이메일 주소 속성은 편집 가능한 필드이지만 제공하는 값은 고유해야 합니다.

AWS CLI

IAM Identity Center에서 사용자 속성을 편집하려면

다음 `update-user` 명령은 사용자의 별명을 업데이트합니다.

```
aws identitystore update-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
  --operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

AWS 리소스에 대한 인력 액세스 설정

작업 인력 사용자가 IAM Identity Center를 통해 AWS 리소스를 인증하고 액세스하는 방법을 설정합니다. 이 섹션에서는 AWS 환경에 대한 인력 사용자 액세스를 관리하는 다음의 구성 요소에 대해 다룹니다.

- 인증 세션 - IAM Identity Center가 대화형 포털 세션부터 백그라운드 애플리케이션 세션에 이르는 다양한 유형의 사용자 세션을 관리하는 방식과 서로 상호 작용하는 방식을 이해합니다.
- 사용자 액세스 관리 - 세션 기간을 구성하고, 사용자 계정을 비활성화하고, 조직 전체의 액세스 블록을 구현하여 보안 및 규정 준수를 유지합니다.
- 암호 관리 - Identity Center 디렉터리에서 생성된 사용자에게 대해 암호 요구 사항을 설정하고, 사용자 자격 증명 설정을 처리하고, 사용자의 암호 재설정을 관리합니다.
- 다중 인증 - Identity Center 디렉터리에서 생성된 사용자에게 대해 사용자 로그인을 보호하기 위해 인증 앱, 보안 키 또는 내장 인증자를 사용하는 MFA로 보안을 강화합니다.

주제

- [IAM Identity Center의 인증 세션 이해](#)
- [IAM Identity Center에서 세션 지속 시간 구성](#)
- [IAM Identity Center에서 AWS 계정 및 애플리케이션에 대한 사용자 액세스 비활성화](#)
- [서비스 제어 정책과 함께 프라이빗 액세스 사용](#)
- [IAM Identity Center 디렉터리에서 사용자에게 대한 액세스 관리](#)

IAM Identity Center의 인증 세션 이해

사용자가 [AWS 액세스 포털](#)에 로그인하면 IAM Identity Center는 사용자의 확인된 자격 증명을 나타내는 인증 세션을 생성합니다.

인증되면 사용자는 관리자가 추가 로그인 없이 사용할 수 있는 권한을 부여한 모든 할당된 AWS 계정 [AWS 관리형 애플리케이션](#) 및 [고객 관리형 애플리케이션](#)에 액세스할 수 있습니다.

인증 세션 유형

사용자 대화형 세션

사용자가 AWS 액세스 포털에 로그인하면 IAM Identity Center에서 사용자 대화형 세션을 생성합니다. 이 세션은 IAM Identity Center 내에서 사용자의 인증된 상태를 나타내며 다른 세션 유형을 생성하기 위한 기반 역할을 합니다. 사용자 대화형 세션은 IAM Identity Center에 구성된 기간 동안 지속될 수 있으며, 이 기간은 최대 90일일 수 있습니다.

사용자 대화형 세션은 기본 인증 메커니즘입니다. 사용자가 로그아웃하거나 관리자가 세션을 종료하면 종료됩니다. 이러한 세션의 기간은 조직의 보안 요구 사항에 따라 신중하게 구성해야 합니다.

사용자 대화형 세션 기간 구성에 대한 자세한 내용은 [the section called “세션 지속 시간 구성”](#) 섹션을 참조하세요.

애플리케이션 세션

애플리케이션 세션은 IAM Identity Center가 Single Sign-On을 통해 설정하는 사용자와 AWS 관리형 애플리케이션(예: Kiro 또는 Amazon Quick) 간의 인증된 연결입니다.

기본적으로 애플리케이션 세션의 수명은 1시간이지만, 기본 사용자 대화형 세션이 유효한 한 자동으로 새로 고쳐집니다. 이 새로 고침 메커니즘은 보안 제어를 유지하면서 사용자에게 원활한 환경을 제공합니다. 사용자 로그아웃 또는 관리자 작업을 통해 사용자 대화형 세션이 종료되면 애플리케이션 세션은 다음 새로 고침 시도 시(일반적으로 30분 이내)에 종료됩니다.

사용자 백그라운드 세션

사용자 백그라운드 세션은 중단 없이 몇 시간 또는 며칠 동안 프로세스를 실행해야 하는 애플리케이션을 위해 설계된 연장 세션입니다. 현재 이 세션 유형은 주로 데이터 과학자가 완료하는 데 많은 시간이 걸리는 기계 학습 훈련 작업을 실행할 수 있는 [Amazon SageMaker Studio](#)에 적용됩니다.

사용자 백그라운드 세션 기간 구성에 대한 자세한 내용은 [사용자 백그라운드 세션](#)을 참조하세요.

Kiro 세션

Kiro 세션을 확장하여 IDEs를 사용하는 개발자가 최대 90일 동안 인증을 유지할 수 있도록 할 수 있습니다. 이 기능은 코드로 작업하는 동안 로그인 중단을 줄입니다.

이러한 세션은 다른 세션 유형과 독립적이며 사용자 대화형 세션 또는 기타 AWS 관리형 애플리케이션에 영향을 주지 않습니다. 이 기능은 IAM Identity Center를 활성화한 시기에 따라 기본적으로 활성화되어 있을 수 있습니다.

확장 Kiro 세션 구성에 대한 자세한 내용은 [섹션을 참조하세요???](#).

IAM Identity Center로 생성된 IAM 역할 세션

IAM Identity Center는 사용자가 AWS Management Console 또는에 액세스할 때 다른 유형의 세션을 생성합니다 AWS CLI. 이러한 경우 IAM Identity Center는 로그인 세션을 통해 사용자의 권한 세트에 지정된 IAM 역할을 수임하여 IAM 세션을 확보합니다.

Important

애플리케이션 세션과 달리, IAM 역할 세션은 일단 설정되면 독립적으로 작동합니다. 이는 권한 세트에 구성된 기간 동안 지속되며, 원래 로그인 세션의 상태와 관계없이 최대 12시간 동안 지속될 수 있습니다. 이 동작은 장기 실행 CLI 작업 또는 콘솔 세션이 예기치 않게 종료되지 않도록 보장합니다.

IAM Identity Center에서 사용자 세션을 종료하는 방법

사용자 시작

사용자가 AWS 액세스 포털에서 로그아웃하면 로그인 세션이 종료되어 사용자가 새 리소스에 액세스할 수 없습니다.

그러나 기존 애플리케이션 세션은 즉시 종료되지 않습니다. 대신, 약 30분 이내에 다음번 새로 고침을 시도하고 로그인 세션이 더 이상 유효하지 않은 것을 알게 되면 종료됩니다. 기존 IAM 역할 세션은 권한 세트 구성에 따라 만료될 때까지 계속됩니다(최대 12시간).

관리자 시작

조직 내 IAM Identity Center 관리 권한이 있는 사용자, 일반적으로 IT 관리자 또는 보안 팀은 [사용자의 세션을 종료](#)할 수 있습니다. 이 작업은 사용자가 스스로 로그아웃한 것과 동일한 방식으로 작동하므로 관리자는 필요한 경우 사용자에게 다시 로그인하도록 요구할 수 있습니다. 이 기능은 보안 정책이 변경되거나 의심스러운 활동이 감지될 때 유용합니다.

IAM Identity Center 관리자가 [사용자를 삭제](#)하거나 [사용자의 액세스를 비활성화](#)하는 경우 사용자는 AWS 액세스 포털에 대한 액세스 권한을 상실하고 새 애플리케이션 또는 IAM 역할 세션을 시작하기 위해 다시 로그인할 수 없습니다. 사용자는 30분 이내에 기존 애플리케이션 세션에 대한 액세스 권한을 잃게 됩니다. 기존의 모든 IAM 역할 세션은 IAM Identity Center 권한 세트에 구성된 세션 기간에 따라 지속됩니다. 최대 세션 기간은 12시간 일 수 있습니다.

관리자가 세션을 종료하는 경우 사용자 액세스는 어떻게 되나요?

이 참조는 관리 작업을 수행할 때 IAM Identity Center 세션이 작동하는 방식에 대한 자세한 정보를 제공합니다. 이 섹션의 표에는 AWS 액세스 포털, 애플리케이션 및 AWS 계정 세션에 대한 액세스에 대한 사용자 관리 작업 및 권한 변경의 기간과 영향이 나와 있습니다.

사용자 관리

이 표에는 사용자 관리 변경 사항이 AWS 리소스, 애플리케이션 세션 및 AWS 계정 세션에 대한 액세스에 미치는 영향이 요약되어 있습니다.

작업	사용자가 IAM Identity Center에 액세스할 수 없음	사용자가 새 애플리케이션 세션을 생성할 수 없음	사용자가 기존 애플리케이션 세션에 액세스할 수 없음	사용자가 기존 AWS 계정 세션에 액세스할 수 없음
사용자의 액세스가 비활성화됨	즉시 적용	즉시 적용	30분 이내	12시간 이내. 기간은 권한 세트에 대해 구성된 IAM 역할 세션 만료 기간에 따라 달라 집니다.
사용자가 삭제됨	즉시 적용	즉시 적용	30분 이내	12시간 이내. 기간은 권한 세트에 대해 구성된 IAM 역할 세션 만료 기간에 따라 달라 집니다.
사용자 세션이 취소됨	다시 액세스하려면 사용자가 다시 로그인해야 함	즉시 적용	30분 이내	12시간 이내. 기간은 권한 세트에 대해 구성된 IAM 역할 세션 만료 기간에 따라 달라 집니다.

작업	사용자가 IAM Identity Center에 액세스할 수 없음	사용자가 새 애플리케이션 세션을 생성할 수 없음	사용자가 기존 애플리케이션 세션에 액세스할 수 없음	사용자가 기존 AWS 계정 세션에 액세스할 수 없음
사용자 로그아웃	다시 액세스하려면 사용자가 다시 로그인해야 함	즉시 적용	30분 이내	12시간 이내. 기간은 권한 세트에 대해 구성된 IAM 역할 세션 만료 기간에 따라 달라 집니다.

그룹 멤버십

이 표에는 사용자 권한 및 그룹 멤버십의 변경 사항이 AWS 리소스, 애플리케이션 세션 및 AWS 계정 세션에 대한 액세스에 미치는 영향이 요약되어 있습니다.

작업	사용자가 IAM Identity Center에 액세스할 수 없음	사용자가 새 애플리케이션 세션을 생성할 수 없음	사용자가 기존 애플리케이션 세션에 액세스할 수 없음	사용자가 기존 AWS 계정 세션에 액세스할 수 없음
사용자로부터 제거된 애플리케이션 또는 AWS 계정 액세스	아니요 - 사용자가 IAM Identity Center에 계속 액세스할 수 있음	즉시 적용	1시간 이내	12시간 이내. 기간은 권한 세트에 대해 구성된 IAM 역할 세션 만료 기간에 따라 달라 집니다.
애플리케이션 또는 AWS 계정이 할당된 그룹에서 사용자가 제거됨	아니요 - 사용자가 IAM Identity Center에 계속 액세스할 수 있음	1시간 이내	2시간 이내	12시간 이내. 기간은 권한 세트에 대해 구성된 IAM 역할 세션 만료 기간에 따라 달라 집니다.

작업	사용자가 IAM Identity Center에 액세스할 수 없음	사용자가 새 애플리케이션 세션을 생성할 수 없음	사용자가 기존 애플리케이션 세션에 액세스할 수 없음	사용자가 기존 AWS 계정 세션에 액세스할 수 없음
그룹에서 제거된 애플리케이션 또는 AWS 계정 액세스	아니요 - 사용자가 IAM Identity Center에 계속 액세스할 수 있음	즉시 적용	1시간 이내	12시간 이내. 기간은 권한 세트에 대해 구성된 IAM 역할 세션 만료 기간에 따라 달라 집니다.

Note

AWS 액세스 포털 및 에는 해당 그룹에서 사용자를 추가하거나 제거한 후 1시간 이내에 업데이트된 사용자 권한이 반영 AWS CLI 됩니다.

타이밍 차이 이해

- 즉시 적용 - 즉시 재인증이 필요한 작업입니다.
- 30분~2시간 이내 - 애플리케이션 세션은 IAM Identity Center에 확인하고 변경 사항을 발견하는 데 시간이 필요합니다.
- 12시간 이내 - IAM 역할 세션은 독립적으로 작동하며 구성된 기간이 만료될 때만 종료됩니다.

단일 로그아웃

IAM Identity Center는 [자격 증명 소스](#) 역할을 하는 자격 증명 공급자가 시작한 SAML Single Logout(사용자가 로그아웃할 때 연결된 모든 애플리케이션에서 사용자를 자동으로 로그아웃시키는 프로토콜)을 지원하지 않습니다. 또한 IAM Identity Center를 자격 증명 공급자로 사용하는 [SAML 2.0 애플리케이션](#)에는 SAML Single Logout을 전송하지 않습니다.

세션 관리 모범 사례

효과적인 세션 관리에는 신중한 구성 및 모니터링이 필요합니다. 조직은 일반적으로 민감한 애플리케이션 및 환경에 더 짧은 기간을 사용하여 보안 요구 사항에 적합한 세션 기간을 구성해야 합니다.

사용자가 역할을 변경하거나 조직을 떠날 때 세션을 종료하는 프로세스를 구현하는 것은 보안 경계를 유지하는 데 필수적입니다. 비정상적인 액세스 패턴, 예상치 못한 로그인 시간 또는 위치, 정상 직무 이외의 리소스에 대한 액세스 등 보안 문제를 나타낼 수 있는 비정상적인 동작을 탐지하려면 활성 세션에 대한 정기적인 검토를 보안 모니터링 사례에 통합해야 합니다.

IAM Identity Center에서 세션 지속 시간 구성

작업 인력 사용자가 Kiro를 포함하여 IAM Identity Center에서 작동하는 AWS 액세스 포털 및 애플리케이션을 사용할 때 작업 인력 사용자의 세션 기간을 구성할 수 있습니다. IAM Identity Center는 사용자 대화형 세션, 사용자 백그라운드 세션, Kiro용 확장 세션 등의 세션 유형을 제공합니다.

주제

- [사용자 대화형 세션](#)
- [사용자 백그라운드 세션](#)
- [Kiro에 대한 확장 세션](#)
- [직원 사용자의 활성 세션 보기 및 종료](#)
- [자격 증명 소스, AWS CLI 및 AWS SDKs 사용에 대한 세션 기간 고려 사항](#)

사용자 대화형 세션

사용자 대화형 세션은 AWS 액세스 포털에 대한 사용자의 로그인 또는 [AWS 관리형 애플리케이션에](#) 대한 액세스와 연결된 세션입니다. AWS 액세스 포털 및 애플리케이션에 대한 세션 인증 기간은 사용자가 재인증 없이 로그인할 수 있는 최대 시간입니다. 활성 AWS 액세스 포털 세션을 종료하면 이러한 관리형 애플리케이션에 대한 모든 세션도 종료됩니다.

사용자 대화형 세션의 기본 세션 지속 시간은 8시간입니다. 최소 15분에서 최대 90일까지 다른 지속 시간을 지정할 수 있습니다. 사용자 지정 지속 시간 값은 분 단위로 입력해야 하며 15분~129,600분(90일) 사이여야 합니다. 자세한 내용은 [IAM Identity Center의 인증 세션 이해](#) 단원을 참조하십시오.

IAM Identity Center 자격 증명 소스가 사용자 대화형 세션 기간에 미치는 영향과 같은 고려 사항은 [섹션을 참조하세요](#) [the section called “자격 증명 소스, AWS CLI 및 AWS SDKs에 대한 고려 사항”](#).

사용자 대화형 세션의 지속 시간을 구성하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.

4. 인증에서 세션 지속 시간 옆의 구성을 선택합니다. 세션 지속 시간 구성 대화 상자가 나타납니다.
5. 세션 지속 시간 구성 대화 상자의 사용자 대화형 세션에서 드롭다운 화살표를 선택하여 사용자의 최대 세션 지속 시간을 선택합니다. 세션 길이를 선택한 다음 저장을 선택합니다.

Note

세션 지속 시간에 대한 변경은 새 세션에만 적용됩니다. 현재 세션은 원래의 지속 시간을 유지합니다.

6. 인증 탭으로 돌아갑니다. 탭 위에 녹색 알림 메시지가 표시되면서 세션 설정이 성공적으로 업데이트되었음을 나타냅니다.

사용자 백그라운드 세션

사용자 백그라운드 세션을 사용하면 사용자가 작업이 실행되는 동안 로그인 상태를 유지할 필요 없이 [Amazon SageMaker Studio](#)와 같은 AWS 관리형 애플리케이션에서 장기 실행 작업을 시작할 수 있습니다. 작업은 즉시 실행되며 IAM Identity Center의 [신뢰할 수 있는 ID 전파](#) 기능을 사용하여 작업이 백그라운드에서 실행되는 동안 사용자의 권한이 유지되도록 합니다. 사용자가 컴퓨터를 끄거나, IAM Identity Center 로그인 세션이 만료되거나, 사용자가 AWS 액세스 포털에서 로그아웃하더라도 작업은 계속 실행될 수 있습니다. 이 기능으로 데이터 과학자, 기계 학습 엔지니어 등이 사용자의 적극적인 개입 없이 백그라운드에서 실행되는 분석 및 기계 학습 워크플로를 시작할 수 있습니다.

사용자 백그라운드 세션은 Amazon SageMaker Studio와 같은 지원되는 AWS 관리형 애플리케이션에 대해 기본적으로 활성화됩니다. 그러나 이 기능을 사용하려면 도메인을 생성하거나 업데이트할 때 Amazon SageMaker Studio에서 신뢰할 수 있는 ID 전파를 활성화해야 합니다. 자세한 내용은 [Amazon SageMaker AI 도메인에서 신뢰할 수 있는 ID 전파 활성화](#)를 참조하세요.

사용자 백그라운드 세션의 기본 세션 지속 시간은 7일입니다. 최소 15분에서 최대 90일까지 다른 지속 시간을 지정할 수 있습니다. 사용자 지정 지속 시간 값은 분 단위로 입력해야 하며 15분~129,600분(90일) 사이여야 합니다.

사용자 백그라운드 세션에 대한 다음 고려 사항에 유의하세요.

- 사용자 백그라운드 세션은 사용자가 Amazon SageMaker Studio에서 작업을 수동으로 시작할 때에만 생성할 수 있습니다. 이 기능은 자동화된 예약 워크플로에는 지원되지 않습니다.
- 사용자 백그라운드 세션을 지원하는 AWS 리전 목록은 [지원되는 AWS 리전을 참조하세요](#).
- CloudTrail에서 사용자 백그라운드 세션을 볼 수 있습니다. 자세한 내용은 [사용자 백그라운드 세션 세부 정보 식별](#)을 참조하세요.

- 조직의 사용자에게 대해 활성 세션을 종료할 수도 있습니다. 자세한 내용은 [직원 사용자의 활성 세션 종료](#)를 참조하세요.

사용자 백그라운드 세션의 지속 시간을 구성하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 인증에서 세션 지속 시간 옆의 구성을 선택합니다. 세션 지속 시간 구성 대화 상자가 나타납니다.
5. 세션 지속 시간 구성 대화 상자에서 사용자 백그라운드 세션 활성화 확인란이 아직 선택되지 않았으면 확인란을 선택합니다. 사용자 백그라운드 세션을 비활성화하려면 확인란의 선택을 취소합니다.

 Note

사용자 백그라운드 세션을 비활성화해도 현재 세션은 영향을 받지 않습니다.

6. 사용자 백그라운드 세션에서 드롭다운 화살표를 선택하여 최대 세션 지속 시간을 선택합니다. 세션 길이를 선택한 다음 저장을 선택합니다.

 Note

세션 지속 시간에 대한 변경은 새 세션에만 적용됩니다. 현재 세션은 원래의 지속 시간을 유지합니다.

7. 인증 탭으로 돌아갑니다. 탭 위에 녹색 알림 메시지가 표시되면서 세션 설정이 성공적으로 업데이트되었음을 나타냅니다.

 Note

고객 관리형 애플리케이션은 사용자 백그라운드 세션을 생성할 수 없습니다.

Kiro에 대한 확장 세션

개발자가 통합 개발 환경(IDE)의 일부로 Kiro를 사용하는 경우 Kiro의 세션 기간을 90일로 설정할 수 있습니다. IAM Identity Center를 활성화한 시기에 따라 Kiro의 연장 세션 기간이 기본적으로 활성화될 수

있습니다. 이 확장 세션은 AWS 액세스 포털 또는 기타 AWS 관리형 애플리케이션의 세션 기간에 영향을 주지 않습니다.

IAM Identity Center 자격 증명 소스가 연장된 세션 기간에 미치는 영향과 같은 고려 사항은 섹션을 참조하세요 [the section called “자격 증명 소스, AWS CLI 및 AWS SDKs에 대한 고려 사항”](#).

Note

Kiro는 기본적으로 활성화된 상용으로 설정된 콘솔에서 액세스할 수 AWS 리전 있습니다. IAM Identity Center 인스턴스가 현재 Kiro에 액세스할 수 없는 리전에 있는 경우 90일 연장 세션 기간을 활성화해도 기본 설정이 재정의되지 않습니다. 즉, 90일 연장 세션 지속 시간 활성화 여부와 상관없이 세션 지속 시간은 변경 없이 유지됩니다. 자세한 내용은 [Kiro에서 지원되는 AWS 리전을 참조하세요](#).

Kiro에 대한 세션을 확장하려면

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 인증에서 세션 지속 시간 옆의 구성을 선택합니다. 세션 지속 시간 구성 대화 상자가 나타납니다.
5. 세션 기간 구성 대화 상자에서 Kiro에 대한 확장 세션 활성화 확인란을 선택합니다. Kiro에 대한 확장 세션 세션을 비활성화하려면 확인란의 선택을 취소합니다.
6. 저장을 선택하고 설정 페이지로 돌아갑니다.

직원 사용자의 활성 세션 보기 및 종료

IAM Identity Center 관리자는 직원 사용자의 활성 세션 목록을 표시하고, 필요하다면 사용자의 세션을 하나 이상 종료할 수 있습니다. 예를 들어 다음과 같은 상황에서 사용자의 세션을 종료해야 할 수 있습니다.

- 사용자에게 더 이상 세션이 필요하지 않은 경우.
- 사용자가 현재 인증 상태를 유지해서는 안 되는 경우. 이러한 상황은 퇴사 또는 권한 변경 시 일어날 수 있습니다.

IAM Identity Center 콘솔을 사용하여 이러한 세션을 보고 종료할 수 있습니다. 사용자는 AWS 액세스 포털을 사용하여 자신의 세션을 보고 종료할 수도 있습니다. 직원 사용자가 관리자의 도움 없이 세션을 보고 종료하는 방법에 대한 자세한 내용은 [활성 세션 보기 및 종료](#) 섹션을 참조하세요.

Note

IAM Identity Center 사용자의 활성 세션을 종료해도 AWS Management Console 또는에서 활성 IAM 역할 세션은 종료되지 않습니다 AWS CLI. 자세한 내용은 [IAM Identity Center의 인증 세션 이해](#) 단원을 참조하십시오.

직원 사용자의 활성 세션을 종료하려면(IAM Identity Center 콘솔)

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 옆에 있는 괄호 안의 숫자는 이 사용자의 활성 세션 수를 나타냅니다.
5. 사용자 백그라운드 세션 검색(선택 사항)

세션을 사용하는 작업의 Amazon 리소스 이름(ARN)으로 세션을 검색하려면 세션 유형 목록에서 사용자 백그라운드 세션을 선택한 다음 검색 상자에 작업 ARN을 입력합니다.

Note

로드된 활성 세션만 종료할 수 있습니다. 사용자에게 많은 세션이 있는 경우 더 많은 활성 세션 로드를 선택하여 추가 세션을 표시합니다.

6. 종료하려는 각 세션 옆의 확인란을 선택한 다음 세션 종료를 선택합니다.
7. 해당 사용자의 활성 세션을 종료할지 확인하는 대화 상자가 나타납니다. 정보를 검토하고 계속하려면 confirm을 입력한 다음 세션 종료를 선택합니다.
8. 사용자 페이지로 돌아갑니다. 선택한 세션이 성공적으로 종료되었음을 나타내는 녹색 알림 메시지가 나타납니다.

자격 증명 소스, AWS CLI 및 AWS SDKs 사용에 대한 세션 기간 고려 사항

다음은 Microsoft Active Directory(AD) 또는 외부 ID 제공업체(IdP)를 ID 소스로 사용하거나 AWS Command Line Interface AWS 소프트웨어 개발 키트(SDKs) 또는 기타 AWS 개발 도구를 사용하여 프로그래밍 방식으로 AWS 서비스에 액세스하는 경우 세션 기간을 구성하기 위한 고려 사항입니다.

Kiro용 Microsoft Active Directory, 사용자 대화형 세션 및 확장 세션

Microsoft Active Directory(AD)를 자격 증명 소스로 사용하고 Kiro의 사용자 대화형 세션 또는 확장 세션에 대한 세션 기간을 구성하는 경우 다음 사항을 고려해야 합니다.

Note

이러한 고려 사항은 사용자 백그라운드 세션에 적용되지 않습니다.

에 구성된 AWS Managed Microsoft AD 또는 AD 커넥터를 사용한 Microsoft AD에 정의된 사용자 Kerberos 티켓의 AWS Directory Service 최대 수명은 Kiro에 대한 사용자 대화형 세션 및 확장 세션의 유효 기간에 영향을 미칠 수 있습니다. 이 설정에 대한 자세한 내용은 Microsoft 웹 사이트의 [사용자 티켓의 최대 수명](#)을 참조하세요.

- AWS Managed Microsoft AD:에 AWS Managed Microsoft AD 구성원을 사용하는 경우 사용자 Kerberos 티켓 AWS Directory Service의 최대 수명은 10시간으로 고정됩니다. 따라서 사용자 대화형 세션 기간은 IAM Identity Center 설정 중 더 짧은 값과 10시간으로 설정됩니다. 예를 들어 사용자 대화형 세션 기간을 12시간으로 설정한 경우 사용자는 10시간 후에 AWS 액세스 포털에서 다시 인증해야 합니다. Kiro의 확장 세션에는 동일한 10시간 제한이 적용됩니다.
- AD 커넥터:에 구성된 AD 커넥터를 사용하는 경우 사용자 Kerberos 티켓의 AWS Directory Service 최대 수명은 AD 커넥터 뒤의 Microsoft AD에 정의됩니다. 기본값은 10시간이며 사용자 대화형 세션 및 확장 세션에 대해와 동일한 영향을 미칩니다 AWS Managed Microsoft AD. 이 제한은 Microsoft AD에서 구성할 수 있지만 IT 관리자와 협력하여 위험을 고려하는 것이 좋습니다. 특히이 설정은 다른 Microsoft AD 클라이언트 애플리케이션의 세션 기간에 영향을 미칠 수 있기 때문입니다.

Kiro에 대한 외부 자격 증명 공급자, 사용자 대화형 세션 및 확장 세션

외부 ID 제공업체(IdP)를 사용하고 Kiro에 대한 사용자 대화형 세션 또는 확장 세션의 세션 기간을 구성하는 경우 다음 사항을 고려해야 합니다.

Note

이러한 고려 사항은 사용자 백그라운드 세션에 적용되지 않습니다.

IAM Identity Center는 세션 유효 지속 시간 결정에 도움을 주기 위해 SAML 어설션의 SessionNotOnOrAfter 속성을 사용합니다.

- SessionNotOnOrAfter가 SAML 어설션에 전달되지 않은 경우 AWS 액세스 포털(사용자 대화형) 세션 및 확장 세션의 지속 시간은 외부 IdP 세션의 지속 시간에 영향을 받지 않습니다. 예를 들어 IdP 세션 기간이 24시간이고 IAM Identity Center에서 18시간 세션 기간을 설정한 경우 사용자는 18시간 후에 AWS 액세스 포털에서 다시 인증해야 합니다. 마찬가지로 Kiro에 대해 90일 연장 세션을 설정하는 경우 Kiro 사용자는 90일 후에 다시 인증해야 합니다.
- SessionNotOnOrAfter가 SAML 어설션에 전달되면 세션 기간 값이 AWS 액세스 포털(사용자 대화형) 세션 또는 연장된 세션 기간과 SAML IdP 세션 기간 중 더 짧은 값으로 설정됩니다. IAM Identity Center에서 72시간의 세션 기간을 설정하고 IdP의 세션 기간이 18시간인 경우 사용자는 IdP에 정의된 18시간 동안 AWS 리소스에 액세스할 수 있습니다. 마찬가지로 Kiro에 대해 90일 연장 세션을 설정하는 경우 Kiro 사용자는 18시간 후에 Kiro에서 다시 인증해야 합니다.
- IdP의 세션 지속 시간이 IAM Identity Center에서 설정된 시간보다 긴 경우 사용자는 여전히 유효한 IdP 로그인 세션을 기반으로 자격 증명을 다시 입력하지 않고도 새로운 IAM Identity Center 세션을 시작할 수 있습니다.

AWS CLI 및 SDK 세션

AWS CLI, AWS SDKs 또는 기타 AWS 개발 도구를 사용하여 프로그래밍 방식으로 AWS 서비스에 액세스하는 경우 액세스 AWS 포털 및 AWS 관리형 애플리케이션의 세션 기간을 설정하려면 다음 사전 조건을 충족해야 합니다.

- IAM Identity Center 콘솔에서 [AWS 액세스 포털 세션 기간을 구성](#)해야 합니다.
- 공유 AWS 구성 파일에서 Single Sign-On 설정에 대한 프로파일을 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 내용은 AWS SDK 및 도구 참조 설명서의 [SSO 토큰 공급자 구성](#)을 참조하세요.
- 사용자는 세션 관리를 지원하는 또는 AWS CLI SDK 버전을 실행해야 합니다.

세션 관리를 AWS CLI 지원하는의 최소 버전

다음은 세션 관리를 AWS CLI 지원하는의 최소 버전입니다.

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

Note

계정 액세스 사용 사례의 경우 사용자가 실행 중인 경우 IAM Identity Center 세션이 만료되도록 설정되기 직전에 권한 세트를 새로 고치고 권한 세트 기간이 12시간으로 설정된 동안 세션 기간이 20시간으로 설정된 AWS CLI 경우 AWS CLI 세션은 최대 20시간에 12시간을 더하여 총 32시간 동안 실행됩니다. IAM Identity Center CLI에 대한 자세한 내용은 [AWS CLI 명령 참조](#)를 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 SDK for Java v2(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

IAM Identity Center에서 AWS 계정 및 애플리케이션에 대한 사용자 액세스 비활성화

IAM Identity Center 디렉터리에서 사용자 액세스를 비활성화하면 사용자 세부 정보를 편집하거나, 암호를 재설정하거나, 사용자를 그룹에 추가하거나, 그룹 멤버십을 볼 수 없습니다. 사용자 액세스를 비활성화하면 AWS 액세스 포털에 로그인할 수 없으며 더 이상 할당된 AWS 계정 및 애플리케이션에 액세스할 수 없습니다. 사용자 액세스 비활성화는 나중에 액세스를 복원해야 할 때 일시적인 액세스 제거를 위해 사용합니다.

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 없습니다. 자세한 내용은 [IAM Identity Center의 인증 세션 이해](#) 단원을 참조하십시오.

IAM Identity Center에서 사용자 액세스를 비활성화하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.

Important

이 페이지의 지침은 [AWS IAM Identity Center](#)에 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 관리](#)를 참조하세요.

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

서비스 제어 정책과 함께 프라이빗 액세스 사용

IAM Identity Center 사용자의 액세스가 비활성화되거나 사용자가 삭제될 때 승인된 API 직접 호출을 할 수 있는 액세스 권한을 즉시 거부하기 위해 다음을 수행할 수 있습니다.

1. 모든 리소스에 대한 모든 작업에 명시적 Deny 효과를 추가하여 사용자에게 할당된 권한 세트의 [인라인 정책](#)을 [추가하거나 업데이트](#)합니다.
2. `aws:userid` 또는 `identitystore:userid` 조건 키를 지정합니다.

또는 [서비스 제어 정책](#)을 사용하여 조직의 모든 멤버 계정에서 사용자의 액세스를 거부할 수도 있습니다.

Example 액세스를 거부하는 예제 SCP

이 거부 정책은 다른 곳에서 부여되었을 수 있는 다른 권한과 관계없이 특정 사용자에게 대한 모든 AWS 작업을 차단합니다. 이 정책은 모든 Allow 정책을 재정의합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:UserId": "*:deleteduser@domain.com"
        }
      }
    }
  ]
}
```

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
          "StringEquals": {
            "identitystore:UserId": "DELETEDUSER_ID"
          }
        }
      }
    ]
  }
}

```

IAM Identity Center 디렉터리에서 사용자에게 대한 액세스 관리

IAM Identity Center 디렉터리에서 사용자에게 대해 암호 및 다중 인증(MFA)을 관리하는 방법을 알아봅니다. 이와 같은 보안 기능은 사용자 계정을 보호하는 데 도움이 됩니다.

Note

이러한 기능은 Active Directory 사용자 또는 외부 ID 제공업체 사용자에게 적용되지 않습니다.

관리자는 IAM Identity Center 콘솔을 통해 암호와 MFA를 모두 관리할 수 있습니다. 이러한 보안 기능은 기본 제공 Identity Center 디렉터리에서만 작동합니다.

암호 관리

암호 관리에는 다음과 같은 기능이 포함됩니다.

- 이메일 지침을 통한 암호 재설정
- 일회용 암호 생성
- API로 생성된 사용자에게 대한 자동 이메일 확인 구성

AWS는 복잡성 규칙 및 암호 재사용 제한을 포함하여 고정된 보안 요구 사항을 적용합니다.

MFA

MFA는 기본적으로 활성화되어 있으며 사용자당 최대 8개의 디바이스를 지원합니다.

지원되는 디바이스 유형:

- 인증 앱
- 보안 키
- 기본 제공 생체 인식 인증자

관리자는 사용자에게 대해 MFA 디바이스를 등록하고 관리할 수 있습니다.

주제

- [사용자 암호 설정](#)
- [Identity Center 디렉터리 사용자를 위한 MFA](#)

사용자 암호 설정

Identity Center 디렉터리에서 생성된 사용자에게 대해 관리자는 암호 정책을 관리하고, 초기 암호 없이 사용자를 처리하고, 필요한 경우 암호를 재설정할 수 있습니다. 이러한 암호 관리 기능은 기본 제공 Identity Center 디렉터리의 사용자에게만 적용됩니다. Active Directory 또는 외부 ID 제공업체를 사용하는 경우 해당 시스템에서 암호를 관리해야 합니다.

암호 관리 옵션

- 암호 요구 사항 - 암호를 설정하거나 변경할 때 사용자가 충족해야 하는 보안 요구 사항입니다. 여기에는 복잡성 규칙 및 재사용 제한이 포함됩니다.
- 일회용 암호 설정 - 초기 암호 없이 API 또는 CLI를 통해 생성된 사용자의 이메일 확인을 구성합니다. 빠르게 액세스하려면 임시 암호를 생성할 수도 있습니다.
- 암호 재설정 - 잠긴 사용자나 새 자격 증명이 필요한 사용자의 암호를 재설정합니다. 이메일을 사용하여 재설정 지침을 보내거나 일회용 암호를 생성할 수 있습니다.

주제

- [IAM Identity Center에서 ID를 관리할 때 암호 요구 사항](#)
- [API로 생성된 사용자에게 일회용 암호 이메일 전송](#)

- [IAM Identity Center 최종 사용자 암호 재설정](#)

IAM Identity Center에서 ID를 관리할 때 암호 요구 사항

Note

이러한 요구 사항은 Identity Center 디렉터리에 생성된 사용자에게만 적용됩니다. [Active Directory](#) 또는 [외부 ID 제공업체](#)와 같이 인증을 위해 IAM Identity Center 외의 ID 소스를 구성한 경우 사용자 암호 정책은 IAM Identity Center가 아닌 해당 시스템에서 정의되고 적용됩니다. 자격 증명 소스가 인 경우에 [대한 암호 정책 관리를 AWS Managed Microsoft AD](#) AWS Managed Microsoft AD참조하세요.

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.

API로 생성된 사용자에게 일회용 암호 이메일 전송

[CreateUser](#)CreateUsercreate-user API 작업을 사용하여 사용자를 생성할 때는 암호가 없습니다. 사용자를 생성할 때 사용자에게 대해 이메일을 지정한 경우 이러한 사용자가 처음 로그인을 시도한 후 사용자에게 확인 이메일을 보내도록 IAM Identity Center의 설정을 업데이트할 수 있습니다. 확인 이메일 수신 후 사용자는 로그인을 위한 암호를 설정해야 합니다.

이 설정을 활성화하지 않으면 [일회용 암호를 생성](#)하고 CreateUser API 또는 create-user CLI로 생성된 사용자와 이를 공유해야 합니다.

CreateUser API 또는 **create-user** CLI 명령으로 생성된 사용자에게 이메일 주소 확인 이메일을 보내려면

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 인증 탭을 선택합니다.
4. 표준 인증 섹션에서 구성을 선택합니다.
5. 표준 인증 구성 대화 상자에서 이메일 OTP 전송 확인란을 선택합니다. 그런 다음 저장을 선택합니다. 상태가 비활성화에서 활성화로 업데이트됩니다.

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

- Microsoft Active 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, [AWS 액세스 포털 사용자 암호 재설정](#) 섹션을 참조하세요.

IAM Identity Center 최종 사용자 암호를 재설정하려면

Important

이 페이지의 지침은 [AWS IAM Identity Center](#)에 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 관리](#)를 참조하세요.

1. [IAM Identity Center 콘솔](#)을 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 잘못되었거나 잘못 구성된 이메일 주소로 전송된 경우 악의적인 수신자가 이를 사용하여 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.

Identity Center 디렉터리 사용자를 위한 MFA

Important

현재 [외부 ID 제공업체](#)에 대해서는 IAM Identity Center의 MFA가 지원되지 않습니다.

IAM Identity Center는 모든 사용자가 사용자 이름과 암호 외에도 MFA로 로그인해야 하도록 기본적으로 다중 인증(MFA)이 설정된 상태로 사전 구성되어 있습니다. 이렇게 하면 사용자가 다음 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 유효한 MFA 챌린지가 성공적으로 완료되지 않은 한 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](#)에 대해 자세히 알아보세요.

주제

- [IAM Identity Center에서 사용 가능한 MFA 유형](#)
- [IAM Identity Center에서 MFA 구성](#)
- [사용자를 위한 MFA 디바이스를 등록합니다.](#)
- [IAM Identity Center에서 MFA 디바이스 이름 바꾸기 및 삭제](#)

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 소유하는 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. 모든 MFA 유형은 브라우저 기반 콘솔 액세스뿐만 아니라 IAM Identity Center에서 AWS CLI v2를 사용할 수 있습니다.

- [FIDO2 인증자](#)(내장형 인증자와 보안 키가 포함)
- [가상 인증 앱](#)
- 를 통해 연결된 자체 [RADIUS MFA](#) 구현 AWS Managed Microsoft AD

사용자는 하나의 AWS 계정에 최대 2개의 가상 인증 앱과 6개의 FIDO 인증자를 포함하여 최대 8개의 MFA 디바이스를 등록할 수 있습니다. 새 디바이스 또는 브라우저에서 로그인할 때마다 또는 알 수 없는 IP 주소에서 로그인할 때마다 MFA가 필요하도록 MFA 설정을 구성할 수도 있습니다. 사용자를 위해 MFA 설정을 구성하는 방법에 대한 자세한 내용은 [사용자 인증을 위한 MFA 유형 선택](#) 및 [MFA 디바이스 적용 구성](#) 섹션을 참조하세요.

FIDO2 인증자

[FIDO2](#)는 CTAP2 및 [WebAuthn](#)을 포함하는 표준이며, 공개 키 암호화를 기반으로 합니다. FIDO 보안 인증은 AWS와 같이 해당 보안 인증이 생성된 웹사이트에 고유한 것이므로 피싱 방지 기능이 있습니다.

AWS는 FIDO 인증자에 대해 가장 일반적인 두 가지 폼 팩터인 내장 인증자와 보안 키를 지원합니다. 가장 일반적인 유형의 FIDO 인증자에 대한 자세한 내용은 아래를 참조하세요.

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 제품](#)을 참조하세요.

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 지원](#)을 참조하세요.

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 회계 관리를 제공하는 업계 표준 클라이언트-서버 프로토콜입니다. MFA 솔루션을 구현한 RADIUS 서버에 연결하는 RADIUS 클라이언트가 Directory Service 포함됩니다. 자세한 내용은 [AWS Managed Microsoft AD다중 인증 활성화](#)를 참조하세요.

사용자 포털에 대한 사용자 로그인에 RADIUS MFA 또는 IAM Identity Center의 MFA 중 하나를 사용할 수 있지만 둘 다 사용할 수는 없습니다. IAM Identity Center의 MFA는 포털에 액세스하기 위해 AWS 기본 2단계 인증을 원하는 경우 RADIUS MFA의 대안입니다.

IAM Identity Center에서 MFA를 활성화하면 사용자가 AWS 액세스 포털에 로그인하려면 MFA 디바이스가 필요합니다. 이전에 RADIUS MFA를 사용한 적이 있는 경우 IAM Identity Center에서 MFA를 활성화하면 AWS 액세스 포털에 로그인하는 사용자의 RADIUS MFA가 효과적으로 재정의됩니다. 그러나

RADIUS MFA는 Amazon RDS for SQL Server Directory Service와 같이에서 작업하는 다른 모든 애플리케이션에 로그인할 때 사용자에게 계속 문제를 제기합니다.

IAM Identity Center 콘솔에서 MFA가 비활성화되어 있고를 사용하여 RADIUS MFA를 구성한 경우 Directory Service RADIUS MFA가 AWS 액세스 포털 로그인을 관리합니다. 즉, MFA를 비활성화하면 IAM Identity Center는 RADIUS MFA 구성으로 되돌아갑니다.

IAM Identity Center에서 MFA 구성

ID 소스가 IAM Identity Center의 ID 스토어 AWS Managed Microsoft AD또는 AD Connector로 구성된 경우 IAM Identity Center에서 다중 인증(MFA) 기능을 구성할 수 있습니다. 현재 [외부 ID 제공업체](#)에 대해서는 IAM Identity Center의 MFA가 지원되지 않습니다.

다음은 IAM Identity Center 설정 및 조직 기본 설정에 따른 일반적인 MFA 권장 사항입니다.

- 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 액세스 포털에 로그인해야 하는 경우 이메일로 전송된 일회용 암호를 제공해야 함 옵션을 선택하지 마세요. AWS 예를 들어 사용자는 AWS 액세스 포털Microsoft 365에서를 사용하여 이메일을 읽을 수 있습니다. 이 경우 사용자는 확인 코드를 검색할 수 없으며 AWS 액세스 포털에 로그인할 수 없습니다. 자세한 내용은 [MFA 디바이스 적용 구성](#) 단원을 참조하십시오.
- 구성한 RADIUS MFA를 이미 사용하고 있는 경우 IAM Identity Center 내에서 MFA를 활성화 Directory Service할 필요가 없습니다. IAM Identity Center의 MFA는 IAM Identity Center의 Microsoft Active Directory 사용자를 위한 RADIUS MFA의 대안입니다. 자세한 내용은 [RADIUS MFA](#) 단원을 참조하십시오.
- 다음 YouTube 비디오에서는 MFA 및 IAM Identity Center에 대한 개요를 제공합니다.

[IAM Identity Center: 새 인스턴스에 대한 다중 인증 기본값](#)

주제

- [사용자에게 MFA에 대한 메시지 표시](#)
- [사용자 인증을 위한 MFA 유형 선택](#)
- [MFA 디바이스 적용 구성](#)
- [사용자가 자신의 MFA 디바이스를 등록하도록 허용](#)

사용자에게 MFA에 대한 메시지 표시

다음 단계를 사용하여 AWS 액세스 포털에 로그인하려고 할 때마다 작업 인력 사용자에게 다중 인증 (MFA) 메시지가 표시되는 빈도를 확인할 수 있습니다. 시작하기 전에 먼저 [IAM Identity Center에서 사용 가능한 MFA 유형](#)을 이해하는 것이 좋습니다.

Important

이 섹션의 지침은 [AWS IAM Identity Center](#)에 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 비활성화](#)를 참조하세요.

Note

외부 IdP를 사용하는 경우 다중 인증 섹션을 사용할 수 없게 됩니다. 외부 IdP가 MFA 설정을 관리하는 것이 아니라 IAM Identity Center에서 관리합니다.

MFA 구성

1. [IAM Identity Center 콘솔](#)을 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.

- 로그인할 때마다(상시 접속)

이 모드(기본 설정)에서는 등록된 MFA 디바이스가 있는 사용자가 로그인할 때마다 IAM Identity Center에 메시지가 표시됩니다. 이는 가장 안전한 설정이며 AWS 액세스 포털에 로그인할 때마다 MFA를 사용하도록 요구하여 조직 또는 규정 준수 정책을 적용하도록 합니다. 예를 들어, PCI DSS는 고위험 결제 거래를 지원하는 애플리케이션에 액세스하기 위해 로그인할 때마다 MFA 사용을 강력히 권장합니다.

- 로그인 컨텍스트가 변경될 때만 (컨텍스트 인식)

이 모드에서 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 작업 공간에서 자주 로그인하지만 상시 작동 옵션보다 안전하지 않은 사용자에게 사용 편의성을 제공합니다. 로그인 컨텍스트가 변경되는 경우에만 MFA를 입력하라는 메시지가 표시됩니다.

- 사용 안 함(비활성화)

이 모드에서는 모든 사용자가 표준 사용자 이름과 비밀번호로만 로그인합니다. 이 옵션을 선택하면 IAM Identity Center MFA가 비활성화되므로 이는 권장되지 않습니다.

사용자의 Identity Center 디렉터리에 대해 MFA가 비활성화되어 있지만 사용자 세부 정보에서 MFA 디바이스를 관리할 수 없으며 Identity Center 디렉터리 사용자는 AWS 액세스 포털에서 MFA 디바이스를 관리할 수 없습니다.

 Note

이미지에서 RADIUS MFA를 사용하고 Directory Service 있고 이를 기본 MFA 유형으로 계속 사용하려는 경우 인증 모드를 비활성화된 상태로 두어 IAM Identity Center에서 MFA 기능을 우회할 수 있습니다. 비활성화 모드에서 컨텍스트 인식 또는 상시 접속 모드로 변경하면 기존 RADIUS MFA 설정이 재정의됩니다. 자세한 내용은 [RADIUS MFA](#) 단원을 참조하십시오.

6. 변경 사항 저장을 선택합니다.

관련 주제

- [사용자 인증을 위한 MFA 유형 선택](#)
- [MFA 디바이스 적용 구성](#)
- [사용자가 자신의 MFA 디바이스를 등록하도록 허용](#)

사용자 인증을 위한 MFA 유형 선택

다음 절차에 따라 AWS 액세스 포털에서 멀티 팩터 인증(MFA) 메시지가 표시될 때 사용자가 인증할 수 있는 디바이스 유형을 선택합니다.

사용자의 MFA 유형을 구성하는 방법

1. [IAM Identity Center 콘솔](#)을 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](#) 단원을 참조하십시오.
 - 보안 키 및 내장된 인증자
 - 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.

IAM의 MFA에 대한 자세한 내용은 [AWS IAM 다중 요소 인증\(MFA\)](#)을 참조하세요.

사용자의 MFA 디바이스 적용을 구성하는 방법

1. [IAM Identity Center 콘솔](#)을 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 표시되

지 않습니다. 이러한 사용자에게 메시지가 표시되도록 하려면 인증 방법을 상시 접속으로 변경합니다.

- 로그인 허용

사용자가 AWS 액세스 포털에 로그인하는 데 MFA 디바이스가 필요하지 않음을 나타내려면이 옵션을 사용합니다. MFA 디바이스를 등록한 사용자에게는 계속해서 MFA를 입력하라는 메시지가 표시됩니다.

6. 변경 사항 저장을 선택합니다.

사용자가 자신의 MFA 디바이스를 등록하도록 허용

IAM Identity Center 관리자는 사용자가 자신의 MFA 디바이스를 자체 등록할 수 있도록 허용할 수 있습니다.

사용자가 자신의 MFA 디바이스를 등록하도록 허용하려면

1. [IAM Identity Center 콘솔](#)을 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 [MFA를 위한 디바이스 등록](#) 절차에 대한 링크를 보내는 것이 좋습니다. 이 주제에서는 자신의 MFA 디바이스를 설정하는 방법을 자세히 설명합니다.

사용자를 위한 MFA 디바이스를 등록합니다.

IAM Identity Center 관리자는 IAM Identity Center 콘솔에서 특정 사용자가 액세스할 수 있도록 새 MFA 디바이스를 설정할 수 있습니다. 관리자가 사용자의 MFA 디바이스를 등록하려면 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](#) 단원을 참조하십시오.

MFA 디바이스를 등록하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 왼쪽 탐색 창에서 사용자를 선택합니다. 목록에서 사용자를 선택합니다. 이 단계에서는 사용자 옆에 있는 체크박스를 선택하지 마세요.
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 앱](#)을 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 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. Assign MFA(MFA 할당)를 선택합니다. 이제 MFA 디바이스가 일회용 암호 생성을 시작할 수 있으며 사용할 준비가 되었습니다 AWS.

• 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 따르세요. 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.

IAM Identity Center에서 MFA 디바이스 이름 바꾸기 및 삭제

IAM Identity Center 관리자는 다음 절차를 사용하여 사용자의 MFA 디바이스의 이름을 바꾸거나 삭제할 수 있습니다.

MFA 디바이스의 이름을 변경하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 왼쪽 탐색 창에서 사용자를 선택합니다. 목록에서 사용자를 선택합니다. 이 단계에서는 사용자 옆에 있는 체크박스를 선택하지 마세요.

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 콘솔](#)을 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.

애플리케이션에 대한 액세스 구성

를 사용하면 애플리케이션에 대한 Single Sign-On 액세스 권한을 가질 수 있는 사용자를 제어할 AWS IAM Identity Center 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 [고객 관리형 AWS 애플리케이션의](#) 두 가지 애플리케이션 유형을 지원합니다. AWS 관리형 애플리케이션은 관련 애플리케이션 콘솔 내에서 직접 구성되거나 애플리케이션 APIs를 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.

또한 직원에게 조직의 특정 AWS 계정 에 AWS Management Console 대한 액세스 권한을 부여할 수 있습니다. 자세한 내용은 [에 대한 액세스 구성 AWS 계정](#) 단원을 참조하십시오.

주제

- [AWS 관리형 애플리케이션](#)
- [고객 관리형 애플리케이션](#)
- [신뢰할 수 있는 ID 전파 개요](#)
- [자체 OAuth 2.0 애플리케이션 설정](#)
- [IAM Identity Center 인증서 교체](#)
- [IAM Identity Center 콘솔의 애플리케이션 속성 이해](#)
- [IAM Identity Center 콘솔에서 애플리케이션에 사용자 액세스 권한 할당](#)
- [SAML 2.0 애플리케이션에 대한 사용자 액세스 제거](#)
- [애플리케이션의 속성을 IAM Identity Center 속성에 매핑](#)

AWS 관리형 애플리케이션

AWS IAM Identity Center 는 인력 사용자를 Kiro 및 Amazon Quick과 같은 AWS 관리형 애플리케이션에 연결하는 작업을 간소화하고 간소화합니다. IAM Identity Center를 사용하면 기존 ID 제공업체를 한

번 연결하고 디렉터리에서 사용자와 그룹을 동기화하거나 IAM Identity Center에서 직접 사용자를 생성하고 관리할 수 있습니다. IAM Identity Center는 페더레이션 포인트가 하나 이상이어서 각 애플리케이션에 대한 페더레이션 또는 사용자 및 그룹 동기화를 설정할 필요가 없고 관리 작업을 줄여줍니다. 또한 [사용자 및 그룹 할당에 대한 일반적인 보기](#)도 얻을 수 있습니다.

IAM Identity Center에서 작동하는 AWS 애플리케이션 포는 섹션을 참조하세요 [AWS IAM Identity Center와 함께 사용할 수 있는 관리형 애플리케이션](#).

AWS 관리형 애플리케이션에 대한 액세스 제어

AWS 관리형 애플리케이션에 대한 액세스는 다음 두 가지 방법으로 제어됩니다.

- 애플리케이션에 대한 초기 항목

IAM Identity Center가 애플리케이션에 대한 할당을 통해 이를 관리합니다. 기본적으로 AWS 관리형 애플리케이션에는 할당이 필요합니다. 애플리케이션 관리자인 경우 애플리케이션에 할당이 필요한지 여부를 선택할 수 있습니다.

할당이 필요한 경우 사용자가 AWS 액세스 포털에 로그인하면 애플리케이션에 직접 또는 그룹 할당을 통해 할당된 사용자만 애플리케이션 타일을 볼 수 있습니다.

할당이 필요하지 않은 경우 모든 IAM Identity Center 사용자가 애플리케이션을 사용하도록 허용할 수 있습니다. 이 경우 애플리케이션은 리소스에 대한 액세스를 관리하고 AWS 액세스 포털항목을 방문하는 모든 사용자에게 애플리케이션 타일이 표시됩니다.

Important

IAM Identity Center 관리자인 경우 IAM Identity Center 콘솔을 사용하여 AWS 관리형 애플리케이션에 대한 할당을 제거할 수 있습니다. 할당을 제거하기 전에 애플리케이션 관리자와 협의하는 것이 좋습니다. 할당이 필요한지 여부를 결정하는 설정을 수정하거나 애플리케이션 할당을 자동화하려는 경우에도 애플리케이션 관리자와 협의해야 합니다.

- 애플리케이션 리소스에 대한 액세스

애플리케이션이 제어하는 독립적인 리소스 할당을 통해 이를 관리합니다.

AWS 관리형 애플리케이션은 애플리케이션 리소스에 대한 액세스를 관리하는 데 사용할 수 있는 관리 사용자 인터페이스를 제공합니다. 예를 들어 빠른 관리자는 그룹 멤버십을 기반으로 대시보드에 액세스할 사용자를 할당할 수 있습니다. 또한 대부분의 AWS 관리형 애플리케이션은 애플리케이션에 사용

자를 할당할 수 있는 AWS Management Console 환경을 제공합니다. 이러한 애플리케이션의 콘솔 환경은 두 기능을 통합하여 사용자 할당 기능과 애플리케이션 리소스에 대한 액세스 관리 기능을 결합할 수 있습니다.

ID 정보 공유

에서 자격 증명 정보를 공유하기 위한 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 계정 또는의 모든 계정에서만 액세스를 활성화하도록 선택할 수 있습니다 AWS Organizations.
- 혹은 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.

서비스 제어 정책은의 기능입니다 AWS Organizations. SCP 연결에 대한 지침은 AWS Organizations 사용 설명서의 [서비스 제어 정책 연결 및 분리](#)를 참조하세요.

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 AWS Command Line Interface () 내에서 사용자, 로그인 자격 증명 및 그룹을 관리합니다 AWS CLI. 자세한 내용은 [Identity Center 디렉터리에서 사용자 관리](#) 단원을 참조하십시오.
- 다음 ID 소스 중 하나에서 들어오는 사용자 및 그룹을 IAM Identity Center ID 저장소에 프로비저닝(동기화)하도록 설정합니다.
 - Active Directory - 자세한 내용은 [Microsoft AD 디렉터리](#)의 내용을 참조하세요.
 - 외부 ID 제공업체 - 자세한 내용은 [외부 ID 제공업체](#)의 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 AWS 관리형 애플리케이션과 공유할 수 있습니다. 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.

AWS 관리형 애플리케이션 사용 제한

IAM Identity Center를 처음 활성화하면 AWS Organizations의 모든 계정에서 AWS 관리형 애플리케이션을 위한 ID 소스로 사용할 수 있게 됩니다. 애플리케이션을 제한하려면 서비스 제어 정책(SCP)을 구현해야 합니다. SCPs는 조직의 자격 증명(사용자 및 역할)이 가질 수 있는 AWS Organizations 있는 최대 권한을 중앙에서 제어하는 데 사용할 수 있는 기능입니다. SCP를 사용하여 IAM Identity Center 사용자 및 그룹 정보에 대한 액세스를 차단하고 지정된 계정을 제외하고는 애플리케이션이 시작되지 않도록 할 수 있습니다. 자세한 내용은 AWS Organizations 사용 설명서의 [서비스 제어 정책\(SCP\)](#)을 참조하세요.

다음 SCP 예시는 IAM Identity Center 사용자 및 그룹 정보에 대한 액세스를 차단하고 지정된 계정(111111111111 및 222222222222)을 제외하고는 애플리케이션이 시작되지 않도록 합니다.

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

}

AWS IAM Identity Center와 함께 사용할 수 있는 관리형 애플리케이션

IAM Identity Center를 사용하면 기존 ID 소스를 연결하거나 사용자를 생성할 수 있습니다. 이를 통해 애플리케이션 관리자는 별도의 페더레이션 또는 사용자 및 그룹 동기화 없이 다음 AWS 관리형 애플리케이션에 대한 액세스를 관리할 수 있습니다.

다음 표의 모든 AWS 관리형 애플리케이션은 [IAM Identity Center의 조직 인스턴스](#)와 통합됩니다. 이 표에는 지원되는 AWS 관리형 애플리케이션에 대한 다음 정보도 나와 있습니다.

- 애플리케이션이 IAM Identity Center의 계정 인스턴스와의 통합되는지 여부
- 애플리케이션이 IAM Identity Center를 통해 신뢰할 수 있는 ID 전파를 활성화할 수 있는지 여부
- 애플리케이션이 고객 관리형 KMS 키로 구성된 IAM Identity Center를 지원하는지 여부
- 애플리케이션이 IAM Identity Center의 추가 리전에서 배포를 지원하는지 여부

Note

IAM Identity Center의 추가 리전에서 배포를 지원하는 애플리케이션은 고객 관리형 KMS 키로 구성된 IAM Identity Center도 지원합니다. 여기에 나열된 모든 AWS 관리형 애플리케이션은 기본 리전에서 배포를 지원합니다. 자세한 내용은 [the section called “여러에 관리형 AWS 애플리케이션 배포 및 관리 AWS 리전”](#) 단원을 참조하십시오.

AWS IAM Identity Center와 통합되는 관리형 애플리케이션

AWS 관리형 애플리케이션	IAM Identity Center의 계정 인스턴스와 통합	IAM Identity Center를 통해 신뢰할 수 있는 ID 전파 활성화	고객 관리형 KMS 키로 구성된 IAM Identity Center 지원	IAM Identity Center의 추가 리전에서 배포 지원
Amazon Athena SQL	예	예	예	아니요
Amazon CodeCatalyst	예	아니요	예	아니요
Amazon DataZone	예	예	예	아니요

AWS 관리형 애플리케이션	IAM Identity Center의 계정 인스턴스 와 통합	IAM Identity Center를 통해 신뢰할 수 있는 ID 전파 활성화	고객 관리 형 KMS 키로 구성된 IAM Identity Center 지원	IAM Identity Center의 추가 리전 에서 배포 지원
Amazon EKS 기능	예	예	예	아니요
Amazon EMR on EC2	예	예	예	아니요
Amazon EMR on EKS	예	예	예	아니요
Amazon EMR Serverless	예	예	예	아니요
Amazon EMR Studio	예	예	예	아니요
Amazon Kendra	아니요	아니요	예	아니요
Amazon Managed Grafana	아니요	아니요	예	아니요
Amazon Monitron	아니요	아니요	아니요	아니요
Amazon OpenSearch Service	예	예	예	아니요
Amazon OpenSearch Service Serverless Service	예	예	예	아니요
Amazon Q Business	예	예	예	아니요
Amazon Quick	예	예	예	아니요
Amazon Redshift	예 ²	예	예	예
Amazon S3 Access Grants	예	예	예	예
Amazon SageMaker Studio	아니요	예	예	아니요
Amazon SageMaker Unified Studio	예	예	예	아니요
Amazon WorkMail	예	예	예	아니요

AWS 관리형 애플리케이션	IAM Identity Center의 계정 인스턴스 와 통합	IAM Identity Center를 통해 신뢰할 수 있는 ID 전파 활성화	고객 관리 형 KMS 키로 구성된 IAM Identity Center 지원	IAM Identity Center의 추가 리전 에서 배포 지원
Amazon WorkSpaces	예	아니요	예	아니요
Amazon WorkSpaces Secure Browser	아니요	아니요	예	아니요
AWS App Studio	예	아니요	아니요	아니요
AWS Deadline Cloud	예	아니요	예	예
AWS Glue	예	예	예	아니요
AWS IoT Events	아니요	아니요	아니요	아니요
AWS IoT SiteWise	아니요	아니요	아니요	아니요
AWS Lake Formation	예	예	예	예
AWS re:Post Private	예	아니요	예	아니요
AWS Supply Chain	예	아니요	예	아니요
AWS Systems Manager	아니요	아니요	예	예 - Fleet Manager 원격 데스크톱
AWS Transfer Family 웹 앱	예	예	예	아니요
AWS 변환	예	아니요	예	아니요
AWS Verified Access	아니요	아니요	예	아니요
Kiro	예 ¹	예	예	아니요
다자간 승인	아니요	예	예	아니요

AWS 관리형 애플리케이션	IAM Identity Center의 계정 인스턴스와 통합	IAM Identity Center를 통해 신뢰할 수 있는 ID 전파 활성화	고객 관리형 KMS 키 로 구성된 IAM Identity Center 지원	IAM Identity Center의 추가 리전 에서 배포 지원
OpenSearch user interface (Dashboards)	예	예	예	아니요

¹ Kiro의 경우 사용자가 AWS 웹 사이트의 전체 Kiro 기능 세트에 액세스해야 하는 경우가 아니면 IAM Identity Center의 계정 인스턴스가 지원됩니다. 자세한 내용은 [Kiro 사용 설명서의 Kiro 설정](#)을 참조하세요.

² Amazon Redshift의 경우 계정 인스턴스에서 지원되지 않는 권한 세트가 필요한 Query Editor v2와 같은 애플리케이션을 제외하고 IAM Identity Center의 계정 인스턴스가 지원됩니다.

Note

Amazon Connect 및와 같은 일부 AWS 서비스는 IAM Identity Center와 함께 사용할 수 있지만 테이블에 나열 AWS Client VPN 되지 않습니다. 이는 SAML을 단독으로 사용하여 IAM Identity Center와 통합되므로 [고객 관리형 애플리케이션](#)으로 분류되기 때문입니다.

빠른 시작: AWS 관리형 애플리케이션을 테스트하도록 IAM Identity Center 설정

관리자가 IAM Identity Center에 대한 액세스 권한을 아직 제공하지 않은 경우이 주제의 단계를 사용하여 AWS 관리형 애플리케이션을 테스트하도록 IAM Identity Center를 설정할 수 있습니다. IAM Identity Center를 활성화하고, IAM Identity Center에서 직접 사용자를 생성하고, 해당 사용자를 AWS 관리형 애플리케이션에 할당하는 방법을 알아봅니다.

이 주제에서는 다음 두 방식 중에서 IAM Identity Center를 활성화하는 방법에 대한 빠른 시작 단계를 제공합니다.

- 사용 AWS Organizations -이 옵션을 선택하면 IAM Identity Center의 조직 인스턴스가 생성됩니다.
- 특정 에서만 AWS 계정 -이 옵션을 선택하면 IAM Identity Center의 계정 인스턴스가 생성됩니다.

이들 인스턴스 유형에 대한 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 섹션을 참조하세요.

사전 조건

IAM Identity Center를 활성화하기 전에 다음 사항을 확인해야 합니다.

- 가 있는 경우 AWS 계정이 없는 경우 계정 관리 참조 안내서의 [시작하기 AWS 계정](#)를 AWS 계정참조하세요. AWS
- AWS 관리형 애플리케이션은 IAM Identity Center에서 작동합니다.의 목록을 검토하여 테스트하려는 AWS 관리형 애플리케이션이 IAM Identity Center에서 작동하는지 [AWS IAM Identity Center와 함께 사용할 수 있는 관리형 애플리케이션](#) 확인합니다.
- 리전별 고려 사항 검토 - IAM Identity Center를 활성화하는 AWS 리전 에서 테스트하려는 AWS 관리형 애플리케이션이 지원되는지 확인합니다. 자세한 내용은 AWS 관리형 애플리케이션의 설명서를 참조하세요.

Note

IAM Identity Center를 활성화하려는 리전과 동일한 리전에 AWS 관리형 애플리케이션을 배포해야 합니다.

AWS 관리형 애플리케이션을 테스트하도록 IAM Identity Center의 조직 인스턴스 설정

Note

이 주제에서는 IAM Identity Center를 활성화하는 권장 방법 AWS Organizations인를 사용하여 IAM Identity Center를 활성화하는 방법을 설명합니다.

권한 확인

에서 IAM Identity Center를 활성화하려면 다음 중 하나로 관리 콘솔에 AWS 로그인 AWS Organizations해야 합니다.

- AWS 계정 에 IAM Identity Center를 활성화할 AWS Organizations의 관리 권한 있는 사용자.
- 루트 사용자(다른 관리 사용자가 없는 경우가 아니라면 권장하지 않음).

⚠ Important

루트 사용자는 계정의 모든 AWS 서비스 및 리소스에 액세스할 수 있습니다. 보안 모범 사례로, 다른 자격 증명이 없는 한 계정의 루트 자격 증명을 사용하여 AWS 리소스에 액세스하지 마세요. 이 보안 인증은 계정 액세스에 제한이 없고 취소하기 어렵습니다.

1단계. 를 사용하여 IAM Identity Center 활성화 AWS Organizations

1. 다음 중 하나를 수행하여 AWS Management Console에 로그인합니다.
 - 신규 사용자 AWS (루트 사용자) - 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
 - 독립형 AWS 계정 (IAM 자격 증명)과 AWS 함께를 이미 사용 중 - 관리 권한이 있는 IAM 자격 증명을 사용하여 로그인합니다.
2. AWS 관리 콘솔 홈 페이지에서 IAM Identity Center 서비스를 선택하거나 [IAM Identity Center 콘솔](#)로 이동합니다.
3. 활성화를 선택하고를 사용하여 IAM Identity Center를 활성화합니다 AWS Organizations. 이렇게 하면 IAM Identity Center의 [조직 인스턴스](#)가 생성됩니다.

2단계. IAM Identity Center에서 관리 사용자 생성

이 절차는 기본으로 제공되는 Identity Center 디렉터리에서 직접 사용자를 생성하는 방법을 설명합니다. 이 디렉터리는 관리자가 인력 사용자를 관리하는 데 사용할 수 있는 다른 디렉터리에 연결되지 않습니다. IAM Identity Center에서 사용자를 생성한 후 해당 사용자에게 새 자격 증명을 지정합니다. AWS 관리형 애플리케이션을 테스트하기 위해이 사용자로 로그인하면 회사 리소스에 액세스하는 데 사용하는 기존 자격 증명이 아닌 새 자격 증명으로 로그인합니다.

i Note

이 사용자 생성 방법은 테스트 용도로만 사용하는 것이 좋습니다.

1. IAM Identity Center 콘솔의 탐색 창에서 사용자를 선택한 후 사용자 추가를 선택합니다.
2. 콘솔의 지침에 따라 사용자를 추가합니다. 암호 설정 지침이 포함된 이메일을 이 사용자에게 보냅니다. 선택하고 액세스 권한이 있는 이메일 주소를 지정했는지 확인합니다.

3. 탐색 창에서 선택하고 계정 옆의 확인란을 AWS 계정선택한 다음 사용자 또는 그룹 할당을 선택합니다.
4. 사용자 탭을 선택하고 방금 추가한 사용자 옆의 확인란을 선택한 후 다음을 선택합니다.
5. 권한 세트 생성을 선택하고 콘솔의 지침에 따라 AdministratorAccess 사전 정의된 권한 세트를 생성합니다.
6. 완료되면 새 권한 세트가 목록에 나타납니다. 브라우저 창에서 권한 세트 탭을 닫고 사용자 및 그룹 할당 탭으로 돌아가 권한 세트 생성 옆의 새로 고침 아이콘을 선택합니다.
7. 사용자 및 그룹 할당 브라우저 탭의 목록에 새 권한 세트가 나타납니다. 권한 세트 이름 옆의 확인란을 선택하고 다음을 선택한 후 제출을 선택합니다.
8. 콘솔에서 로그아웃합니다.

3단계. AWS 액세스 포털에 관리 사용자로 로그인

AWS 액세스 포털은 생성한 사용자에게 AWS 관리 콘솔에 대한 액세스 권한을 제공하는 웹 포털입니다. AWS 액세스 포털에 로그인하려면 먼저 IAM Identity Center 가입 초대를 수락하고 사용자 자격 증명을 활성화해야 합니다.

1. AWS IAM Identity Center 가입 초대라는 제목의 이메일을 확인하세요.
2. 초대 수락을 선택하고 가입 페이지의 지침에 따라 새 암호를 설정하고, 로그인한 후 사용자를 위해 MFA 디바이스를 등록합니다.
3. MFA 디바이스를 등록하면 AWS 액세스 포털이 열립니다.
4. AWS 액세스 포털에서 AWS 계정 선택하고 AdministratorAccess를 선택합니다. 그러면 AWS Management Console로 리디렉션됩니다.

4단계. IAM Identity Center를 사용하도록 AWS 관리형 애플리케이션 구성

1. AWS Management Console에 로그인한 상태에서 사용하려는 AWS 관리형 애플리케이션의 콘솔을 엽니다.
2. 콘솔의 지침에 따라 IAM Identity Center를 사용하도록 AWS 관리형 애플리케이션을 구성합니다. 이 과정 동안 생성한 사용자를 애플리케이션에 할당할 수 있습니다.

AWS 관리형 애플리케이션을 테스트하도록 IAM Identity Center의 계정 인스턴스 설정

Note

IAM Identity Center의 계정 인스턴스는 배포를 하나의 AWS 계정으로 제한합니다. 테스트하려는 AWS 애플리케이션 AWS 리전 과 동일한에서이 인스턴스를 활성화해야 합니다.

앱 확인

IAM Identity Center에서 작동하는 모든 AWS 관리형 애플리케이션은 IAM Identity Center의 조직 인스턴스와 함께 사용할 수 있습니다. 그러나 이러한 애플리케이션 중 일부만 IAM Identity Center의 계정 인스턴스에서 사용할 수 있습니다. [AWS IAM Identity Center와 함께 사용할 수 있는 관리형 애플리케이션](#) 목록을 검토합니다.

1단계. IAM Identity Center의 계정 인스턴스 활성화

1. 다음 중 하나를 수행하여 AWS Management Console에 로그인합니다.
 - 신규 사용자 AWS (루트 사용자) - 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.
 - 독립형 AWS 계정 (IAM 자격 증명)과 AWS 함께를 이미 사용 중 - 관리 권한이 있는 IAM 자격 증명을 사용하여 로그인합니다.
2. AWS 관리 콘솔 홈 페이지에서 IAM Identity Center 서비스를 선택하거나 [IAM Identity Center 콘솔](#)로 이동합니다.
3. 활성화를 선택합니다.
4. AWS Organizations에 IAM Identity Center 활성화 페이지에서 IAM Identity Center의 계정 인스턴스 활성화를 선택합니다.
5. IAM Identity Center의 계정 인스턴스 활성화 페이지에서 정보를 검토하고, 이 계정 인스턴스와 연결할 태그를 추가합니다(선택 사항). 그런 다음 활성화를 선택합니다.

2단계. IAM Identity Center에서 사용자 생성

이 절차는 기본으로 제공되는 Identity Center 디렉터리에서 직접 사용자를 생성하는 방법을 설명합니다. 이 디렉터리는 관리자가 인력 사용자를 관리하는 데 사용할 수 있는 다른 디렉터리에 연결되지 않습니다. IAM Identity Center에서 사용자를 생성한 후 해당 사용자에게 대해 새 자격 증명을 지정합니다. AWS 관리형 애플리케이션을 테스트하기 위해이 사용자로 로그인하면 새 자격 증명으로 로그인합니다. 이 새 자격 증명으로는 다른 회사 리소스에 액세스할 수 없습니다.

Note

이 사용자 생성 방법은 테스트 용도로만 사용하는 것이 좋습니다.

1. IAM Identity Center 콘솔의 탐색 창에서 사용자를 선택한 후 사용자 추가를 선택합니다.
2. 콘솔의 지침에 따라 사용자를 추가합니다. 암호 설정 지침이 포함된 이메일을 이 사용자에게 보낼 니다를 선택하고 액세스 권한이 있는 이메일 주소를 지정했는지 확인합니다.
3. 콘솔에서 로그아웃합니다.

3단계. IAM Identity Center 사용자로 AWS 액세스 포털에 로그인

AWS 액세스 포털은 생성한 사용자에게 AWS 관리 콘솔에 대한 액세스 권한을 제공하는 웹 포털입니 다. AWS 액세스 포털에 로그인하려면 먼저 IAM Identity Center 가입 초대를 수락하고 사용자 자격 증 명을 활성화해야 합니다.

1. AWS IAM Identity Center 가입 초대라는 제목의 이메일을 확인하세요.
2. 초대 수락을 선택하고 가입 페이지의 지침에 따라 새 암호를 설정하고, 로그인한 후 사용자를 위해 MFA 디바이스를 등록합니다.
3. MFA 디바이스를 등록하면 AWS 액세스 포털이 열립니다. 애플리케이션을 사용할 수 있으면 애플 리케이션 탭에서 해당 애플리케이션을 찾을 수 있습니다.

Note

AWS 계정 인스턴스를 지원하는 애플리케이션은 사용자가 추가 권한 없이 애플리케이션 에 로그인할 수 있도록 허용합니다. 따라서 계정 탭은 비어 있습니다.

4단계. IAM Identity Center를 사용하도록 AWS 관리형 애플리케이션 구성

1. AWS Management Console에 로그인한 상태에서 사용하려는 AWS 관리형 애플리케이션의 콘솔 을 엽니다.
2. 콘솔의 지침에 따라 IAM Identity Center를 사용하도록 AWS 관리형 애플리케이션을 구성합니다. 이 과정 동안 생성한 사용자를 애플리케이션에 할당할 수 있습니다.

AWS 관리형 애플리케이션에 대한 세부 정보 보기 및 변경

애플리케이션용 콘솔 또는 APIs를 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 확인하고 변경할 수 있습니다.

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 [신뢰할 수 있는 ID 전파 개요](#)의 내용을 참조하세요.

IAM Identity Center 콘솔에서 AWS 관리형 애플리케이션에 대한 정보를 보고 변경하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. [Applications]를 선택합니다.
3. AWS 관리형 탭을 선택합니다.
4. 열고 확인하려는 관리형 애플리케이션의 링크를 선택합니다.
5. AWS 관리형 애플리케이션에 대한 정보를 변경하려면 작업을 선택한 다음 세부 정보 편집을 선택합니다.
6. 애플리케이션의 표시 이름, 설명, 사용자 및 그룹 할당 방법을 변경할 수 있습니다.
 - a. 표시 이름을 변경하려면 표시 이름 필드에 원하는 이름을 입력하고 변경 사항 저장을 선택합니다.
 - b. 설명을 변경하려면 설명 필드에 원하는 설명을 입력하고 변경 사항 저장을 선택합니다.
 - c. 사용자 및 그룹 할당 방법을 변경하려면 원하는 변경을 수행하고 변경 사항 저장을 선택합니다. 자세한 내용은 [the section called “사용자, 그룹 및 프로비저닝”](#) 단원을 참조하십시오.

AWS 관리형 애플리케이션 비활성화

사용자가 AWS 관리형 애플리케이션에 인증하지 못하도록 IAM Identity Center 콘솔에서 애플리케이션을 비활성화할 수 있습니다.

AWS 관리형 애플리케이션을 비활성화하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. [Applications]를 선택합니다.

3. 애플리케이션 페이지의 AWS 관리형 애플리케이션에서 비활성화하려는 애플리케이션을 선택합니다.
4. 애플리케이션을 선택한 상태에서 작업을 선택하고 비활성화를 선택합니다.
5. 애플리케이션 비활성화 대화 상자에서 비활성화를 선택합니다.
6. AWS 관리형 애플리케이션 목록에서 애플리케이션 상태는 비활성으로 표시됩니다.

Note

AWS 관리형 애플리케이션이 비활성화된 경우 작업을 선택한 다음 활성화를 선택하여 사용자를 복원하여 애플리케이션에 인증할 수 있습니다.

ID 강화 콘솔 세션 활성화

콘솔에 대한 자격 증명 강화 세션은 사용자 경험을 개인화하기 위한 몇 가지 추가 사용자 컨텍스트를 제공하여 사용자의 AWS 콘솔 세션을 개선합니다. 이 기능은 현재 [AWS 앱 및 웹 사이트에서 Kiro의 Kiro Pro](#) 사용자에게 지원됩니다.

기존 액세스 패턴이나 콘솔로의 페더레이션을 변경하지 않고도 자격 증명 강화 AWS 콘솔 세션을 활성화할 수 있습니다. 사용자가 IAM으로 AWS 콘솔에 로그인하는 경우(예: IAM 사용자로 로그인하거나 IAM과의 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](#)
- [ID 강화 콘솔 세션을 활성화하는 방법](#)
- [ID 강화 콘솔 세션의 작동 방식](#)

필수 조건 및 고려 사항

ID 강화 콘솔 세션을 활성화하기 전에 다음 사전 조건 및 고려 사항을 검토합니다.

- 사용자가 Kiro Pro 구독을 통해 AWS 앱 및 웹 사이트에서 Kiro에 액세스하는 경우 자격 증명 강화 콘솔 세션을 활성화해야 합니다.

Note

Kiro 사용자는 자격 증명 강화 세션 없이 Kiro에 액세스할 수 있지만 Kiro Pro 구독에는 액세스할 수 없습니다.

- ID 강화 콘솔 세션에는 IAM Identity Center의 [조직 인스턴스](#)가 필요합니다.
- 옵트인에서 IAM Identity Center를 활성화하면 Kiro와의 통합이 지원되지 않습니다 AWS 리전.
- ID 강화 콘솔 세션을 활성화하려면 다음 권한이 있어야 합니다.
 - sso:CreateApplication
 - sso:GetSharedSsoConfiguration
 - sso:ListApplications
 - sso:PutApplicationAssignmentConfiguration
 - sso:PutApplicationAuthenticationMethod
 - sso:PutApplicationGrant
 - sso:PutApplicationAccessScope
 - signin:CreateTrustedIdentityPropagationApplicationForConsole
 - signin:ListTrustedIdentityPropagationApplicationsForConsole
- 사용자가 ID 강화 콘솔 세션을 사용할 수 있도록 하려면 ID 기반 정책에서 사용자에게 sts:setContext 권한을 부여해야 합니다. 자세한 내용은 [사용자에게 ID 강화 콘솔 세션을 사용하는 권한 부여](#)를 참조하세요.

ID 강화 콘솔 세션을 활성화하는 방법

Kiro 콘솔 또는 IAM Identity Center 콘솔에서 자격 증명 강화 콘솔 세션을 활성화할 수 있습니다.

Kiro 콘솔에서 자격 증명 강화 콘솔 세션 활성화

ID 강화 콘솔 세션을 활성화하기 전에 ID 소스가 연결된 IAM Identity Center의 조직 인스턴스가 있어야 합니다. IAM Identity Center를 이미 구성한 경우 3단계로 건너뛵니다.

1. IAM Identity Center 콘솔을 엽니다. IAM Identity Center 활성화를 선택한 다음 IAM Identity Center의 조직 인스턴스 생성을 선택합니다. 자세한 내용은 [IAM Identity Center 활성화](#) 단원을 참조하세요.

2. ID 소스를 IAM Identity Center에 연결하고 사용자를 IAM Identity Center에 프로비저닝합니다. 기존 ID 소스를 IAM Identity Center에 연결하거나 다른 ID 소스를 아직 사용하지 않는 경우 Identity Center 디렉터리를 사용할 수 있습니다. 자세한 내용은 [IAM Identity Center의 ID 소스 자습서](#) 단원을 참조하십시오.
3. IAM Identity Center 설정을 완료한 후 Kiro 콘솔을 열고 Kiro 사용 설명서의 [구독](#) 단계를 따릅니다. ID 강화 콘솔 세션을 활성화해야 합니다.

Note

ID 강화 콘솔 세션을 활성화할 수 있는 충분한 권한이 없는 경우 IAM Identity Center 관리자에게 IAM Identity Center 콘솔에서 이 작업을 수행할 권한을 달라고 요청해야 할 수 있습니다. 자세한 내용은 다음 절차를 참조하세요.

IAM Identity Center 콘솔에서 ID 강화 콘솔 세션 활성화

IAM Identity Center 관리자인 경우 다른 관리자에게 IAM Identity Center 콘솔에서 ID 강화 콘솔 세션을 활성화하도록 요청할 수 있습니다.

1. IAM Identity Center 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. ID 강화 인식 세션 활성화에서 활성화를 선택합니다.
4. 두 번째 메시지에서 활성화를 선택합니다.
5. ID 강화 콘솔 세션 활성화를 완료하면 설정 페이지 상단에 확인 메시지가 나타납니다.
6. 세부 정보 섹션에서 ID 강화 세션의 상태는 활성화됨입니다.

ID 강화 콘솔 세션의 작동 방식

IAM Identity Center는 활성 IAM Identity Center 사용자 ID와 IAM Identity Center 세션 ID를 포함하도록 사용자의 현재 콘솔 세션을 개선합니다.

ID 강화 콘솔 세션에는 다음 세 가지 값이 포함됩니다.

- Identity 스토어 사용자 ID([identitystore:UserId](#))-이 값은 IAM Identity Center에 연결된 ID 소스에서 사용자를 고유하게 식별하는 데 사용됩니다.
- ID 스토어 디렉터리 ARN([identitystore:IdentityStoreArn](#))-이 값은 IAM Identity Center에 연결된 ID 스토어의 ARN으로, `identitystore:UserId`에 대한 속성을 검색할 수 있습니다.

- IAM Identity Center 세션 ID-이 값은 사용자의 IAM Identity Center 세션이 여전히 유효한지 여부를 나타냅니다.

값은 동일하지만 다음과 같이 사용자가 로그인하는 방식에 따라 다양한 방식으로 획득되며 프로세스의 여러 지점에서 추가됩니다.

- IAM Identity Center(AWS 액세스 포털): 이 경우 활성 IAM Identity Center 세션에 사용자의 ID 스토어 사용자 ID 및 ARN 값이 이미 제공됩니다. IAM Identity Center는 세션 ID만 추가하여 현재 세션을 개선합니다.
- 기타 로그인 방법: 사용자가 AWS IAM 사용자, IAM 역할 또는 IAM이 있는 페더레이션 사용자로 로그인하는 경우 이러한 값은 제공되지 않습니다. IAM Identity Center는 ID 스토어 사용자 ID, ID 스토어 디렉터리 ARN 및 세션 ID를 추가하여 현재 세션을 개선합니다.

고객 관리형 애플리케이션

IAM Identity Center는 인력 사용자 및 그룹에 대한 중앙 ID 서비스 역할을 합니다. 이미 ID 제공업체(IdP)를 사용하는 경우 IAM Identity Center를 IdP와 통합하여 사용자 및 그룹을 IAM Identity Center에 프로비저닝하고 IdP를 인증에 사용할 수 있습니다. 단일 연결을 통해 IAM Identity Center는 여러 앞에 있는 IdP를 AWS 서비스 나타내며 OAuth 2.0 애플리케이션이 사용자를 대신하여 이러한 서비스의 데이터에 대한 액세스를 요청할 수 있습니다. IAM Identity Center를 사용하여 사용자에게 [SAML 2.0](#) 애플리케이션에 대한 액세스 권한을 할당할 수도 있습니다. 여기에는 SAML을 단독으로 사용하여 IAM Identity Center와 통합되므로 고객 관리형 애플리케이션으로 분류 AWS Client VPN되는 Amazon Connect 및와 같은 AWS 서비스가 포함됩니다.

- 애플리케이션이 JSON 웹 토큰(JWTs)을 지원하는 경우 IAM Identity Center의 신뢰할 수 있는 자격 증명 전파 기능을 사용하여 애플리케이션이 사용자를 AWS 서비스 대신하여의 데이터에 대한 액세스를 요청할 수 있습니다. 신뢰할 수 있는 ID 전파는 OAuth 2.0 권한 부여 프레임워크를 기반으로 구성되며 애플리케이션이 외부 OAuth 2.0 권한 부여 서버에서 가져온 ID 토큰을 IAM Identity Center에서 발급하고 AWS 서비스에서 인식하는 토큰으로 교환할 수 있는 옵션이 포함되어 있습니다. 자세한 내용은 [신뢰할 수 있는 ID 전파 사용 사례](#) 단원을 참조하십시오.
- 애플리케이션이 SAML 2.0을 지원하는 경우 [IAM Identity Center의 조직 인스턴스](#)에 연결할 수 있습니다. IAM Identity Center를 사용하여 SAML 2.0 애플리케이션에 대한 액세스를 할당할 수 있습니다.

Note

고객 관리형 애플리케이션을 [고객 관리형 KMS 키](#)를 사용하는 IAM Identity Center 인스턴스와 통합할 때 애플리케이션이 IAM Identity Center 서비스 APIs를 호출하여 애플리케이션에 KMS 키 권한이 필요한지 확인합니다. IAM Identity Center 사용 설명서의 [기본 KMS 키 정책에서 사용자 지정 워크플로에 KMS 키](#) 권한을 부여하는 지침을 따릅니다.

주제

- [SAML 2.0 및 OAuth 2.0 애플리케이션에 대한 Single Sign-On 액세스](#)
- [고객 관리형 SAML 2.0 애플리케이션 설정](#)

SAML 2.0 및 OAuth 2.0 애플리케이션에 대한 Single Sign-On 액세스

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 사용자에게 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 페더레이션 Single Sign-On AWS 액세스를 제공합니다.

Note

IAM Identity Center는 SAML 애플리케이션에서 들어오는 SAML 인증 요청에 대해 서명 검증을 지원하지 않습니다.

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 및 서비스에 액세스하기 위한 임시 자격 증명을 검색할 수 있습니다. 퍼블릭 클라이언트는 일반적으로 로컬에서 애플리케이션을 실행하는 데 사용되는 데스크톱, 노트북 또는 기타 모바일 디바이스입니다. 퍼블릭 클라이언트에서 실행되는 애플리케이션의 예로는 AWS AWS Command Line Interface (AWS CLI), AWS Toolkit 및 AWS 소프트웨어 개발 키트(SDKs). 이러한 애플리케이션이 자격 증명을 획득할 수 있도록 IAM Identity Center는 다음 OAuth 2.0 흐름의 일부를 지원합니다.

- 코드 교환용 증명 키가 포함된 권한 부여 코드 부여(PKCE)([RFC 6749](#) 및 [RFC 7636](#))
- 디바이스 인증 권한 허용([RFC 8628](#))

Note

이러한 권한 부여 유형은 이 기능을 AWS 서비스 지원하는에서만 사용할 수 있습니다. 이러한 서비스는 모든 AWS 리전에서 이러한 권한 부여 유형을 지원하지 않을 수 있습니다. 리전별 차이점 AWS 서비스 과 관련된 설명서를 참조하세요.

OpenID Connect(OIDC)는 OAuth 2.0 프레임워크를 기반으로 하는 인증 프로토콜입니다. OIDC는 인증에 OAuth 2.0을 사용하는 방식을 지정합니다. [IAM Identity Center OIDC 서비스 API](#)를 통해 애플리케이션은 OAuth 2.0 클라이언트를 등록하고 이러한 흐름 중 하나를 사용하여 IAM Identity Center 보호 API에 대한 권한을 제공하는 액세스 토큰을 획득합니다. 애플리케이션은 의도한 API 사용자를 선언할 [액세스 범위](#)를 지정합니다. IAM Identity Center 관리자로서 ID 소스를 구성한 후 애플리케이션 최종 사용자가 아직 로그인하지 않은 경우 해당 최종 사용자가 로그인 프로세스를 완료해야 합니다. 그런 다음 최종 사용자는 애플리케이션이 API를 호출하도록 허용하는 데 동의해야 합니다. 이러한 API 호출은 사용자의 권한을 사용하여 수행됩니다. 이에 대한 응답으로 IAM Identity Center는 사용자가 동의한 액세스 범위가 포함된 액세스 토큰을 애플리케이션에 반환합니다.

OAuth 2.0 권한 부여 흐름 사용

OAuth 2.0 권한 부여 흐름은 흐름을 지원하는 AWS 관리형 애플리케이션을 통해서만 사용할 수 있습니다. OAuth 2.0 흐름을 사용하려면 IAM Identity Center의 인스턴스와 사용하는 지원되는 AWS 관리형 애플리케이션을 단일 배포해야 합니다. AWS 리전, AWS 관리형 애플리케이션의 리전별 가용성과 사용하려는 IAM Identity Center의 인스턴스를 AWS 서비스 확인하려면 각에 대한 설명서를 참조하세요.

OAuth 2.0 흐름을 사용하는 애플리케이션을 사용하려면 최종 사용자가 애플리케이션이 연결될 URL을 입력하고 IAM Identity Center 인스턴스를 등록해야 합니다. 애플리케이션에 따라 관리자는 사용자에게 IAM Identity Center 인스턴스의 AWS 액세스 포털 URL 또는 발급자 URL을 제공해야 합니다. [IAM Identity Center 콘솔](#) 설정 페이지에서 이러한 두 가지 설정을 찾을 수 있습니다. 클라이언트 애플리케이션 구성에 대한 자세한 내용은 해당 애플리케이션의 문서를 참조하세요.

애플리케이션에 로그인하고 동의를 제공하기 위한 최종 사용자 경험은 애플리케이션이 [PKCE를 통한 권한 부여 코드 허용](#)과 [디바이스 인증 권한 허용](#) 중 어떤 것을 사용하는지에 따라 달라집니다.

PKCE를 통한 권한 부여 코드 허용

이 흐름은 브라우저가 있는 디바이스에서 실행되는 애플리케이션에서 사용됩니다.

1. 브라우저 창이 열립니다.
2. 사용자가 인증하지 않은 경우 브라우저는 사용자 인증을 완료하도록 리디렉션합니다.
3. 인증 후 동의 화면이 표시되며 해당 화면에는 다음 정보가 표시됩니다.
 - 애플리케이션 이름
 - 애플리케이션이 사용에 대한 동의를 요청하는 액세스 범위
4. 사용자는 동의 프로세스를 취소하거나 동의를 제공할 수 있으며 애플리케이션은 사용자의 권한에 따라 액세스를 진행합니다.

디바이스 인증 권한 허용

이 흐름은 브라우저가 있거나 없는 디바이스에서 실행되는 애플리케이션에서 사용할 수 있습니다. 애플리케이션이 흐름을 시작하면 애플리케이션이 흐름의 뒷부분에서 사용자가 확인해야 하는 URL과 사용자 코드를 제공합니다. 흐름을 시작하는 애플리케이션이 사용자가 동의한 디바이스와 다른 디바이스에서 실행 중일 수 있으므로 사용자 코드가 필요합니다. 코드는 사용자가 다른 디바이스에서 시작한 흐름에 동의하는지 확인합니다.

Note

device.sso.**region**.amazonaws.com를 사용하는 클라이언트가 있는 경우 PKCE(Proof Key for Code Exchange)를 사용하도록 권한 부여 흐름을 업데이트해야 합니다. 자세한 내용은 AWS Command Line Interface 사용 설명서에서 [AWS CLI를 사용하여 IAM Identity Center 인증 구성](#)을 참조하세요.

1. 브라우저가 있는 디바이스에서 흐름이 시작되면 브라우저 창이 열립니다. 브라우저가 없는 디바이스에서 흐름이 시작되면 사용자는 다른 디바이스에서 브라우저를 열고 애플리케이션이 제공한 URL로 이동해야 합니다.
2. 어느 경우든 사용자가 인증하지 않은 경우 브라우저는 사용자 인증을 완료하도록 리디렉션합니다.
3. 인증 후 동의 화면이 표시되며 해당 화면에는 다음 정보가 표시됩니다.
 - 애플리케이션 이름
 - 애플리케이션이 사용에 대한 동의를 요청하는 액세스 범위
 - 애플리케이션이 사용자에게 제공한 사용자 코드
4. 사용자는 동의 프로세스를 취소하거나 동의를 제공할 수 있으며 애플리케이션은 사용자의 권한에 따라 액세스를 진행합니다.

액세스 범위

범위는 OAuth 2.0 흐름을 통해 액세스할 수 있는 서비스에 대한 액세스를 정의합니다. 범위는 서비스를 위한 방식으로, 리소스 서버가 작업 및 서비스 리소스와 관련된 권한을 그룹화하는 방법이라고도 부르며, OAuth 2.0 클라이언트가 요청할 수 있는 세부적인 작업을 지정합니다. OAuth 2.0 클라이언트가 [IAM Identity Center OIDC 서비스](#)에 등록하면 클라이언트는 사용자가 동의를 제공해야 하는 의도한 작업을 선언할 범위를 지정합니다.

OAuth 2.0 클라이언트는 [OAuth 2.0\(RFC 6749\)의 섹션 3.3](#)에 정의된 scope 값을 사용하여 액세스 토큰에 대해 요청되는 액세스 권한을 지정합니다. 클라이언트는 액세스 토큰을 요청할 때 최대 25개의 범위를 지정할 수 있습니다. 사용자가 PKCE 또는 디바이스 권한 부여 흐름으로 권한 부여 코드 부여 중에 동의를 제공하는 경우 IAM Identity Center는 범위를 반환하는 액세스 토큰으로 인코딩합니다.

AWS 는 지원되는에 대한 범위를 IAM Identity Center에 추가합니다 AWS 서비스. 다음 표에는 퍼블릭 클라이언트를 등록할 때 IAM Identity Center OIDC 서비스가 지원하는 범위가 나열되어 있습니다.

퍼블릭 클라이언트를 등록할 때 IAM Identity Center OIDC 서비스에서 지원하는 액세스 범위는 다음과 같습니다.

Scope	설명	지원되는 서비스
sso:account:access	IAM Identity Center 관리 계정 및 권한 세트에 액세스합니다.	IAM Identity Center
codewhisperer:analysis	Kiro 코드 분석에 대한 액세스를 활성화합니다.	AWS Builder ID 및 IAM Identity Center
codewhisperer:completions	Kiro 인라인 코드 제안에 대한 액세스를 활성화합니다.	AWS Builder ID 및 IAM Identity Center
codewhisperer:conversations	Kiro 채팅에 대한 액세스를 활성화합니다.	AWS Builder ID 및 IAM Identity Center
codewhisperer:taskassist	소프트웨어 개발을 위해 Kiro Agent에 대한 액세스를 활성화합니다.	AWS Builder ID 및 IAM Identity Center
codewhisperer:transformations	코드 변환을 위해 Kiro Agent에 대한 액세스를 활성화합니다.	AWS Builder ID 및 IAM Identity Center
codecatalyst:read_write	Amazon CodeCatalyst 리소스를 읽고 쓸 수 있으므로 모든 기존 리소스에 액세스할 수 있습니다.	AWS Builder ID 및 IAM Identity Center
verified_access:application:connect	활성화 AWS Verified Access	AWS Verified Access
redshift:connect	Amazon Redshift에 연결	Amazon Redshift

Scope	설명	지원되는 서비스
datazone: domain:access	DataZone 도메인 실행 역할에 액세스	Amazon DataZone
nosqlwork bench:dat amodeladviser	데이터 모델 생성 및 읽기	NoSQL Workbench
transform :read_write	코드 변환을 위해 AWS Transform Agent에 대한 액세스 활성화	AWS 변환

고객 관리형 SAML 2.0 애플리케이션 설정

[SAML 2.0](#)을 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 액세스해야 하는 경우 신뢰할 수 있는 자격 증명 전파를 사용할 AWS 서비스 수 있습니다. 신뢰할 수 있는 ID 전파를 통해 사용자는 애플리케이션에 로그인할 수 있고, 해당 애플리케이션은 AWS 서비스의 데이터에 액세스하기 위한 요청에 사용자의 ID를 전달할 수 있습니다.

주제

- [IAM Identity Center 애플리케이션 카탈로그에서 애플리케이션 설정](#)
- [자체 SAML 2.0 애플리케이션 설정](#)

IAM Identity Center 애플리케이션 카탈로그에서 애플리케이션 설정

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.

IAM Identity Center와 애플리케이션의 서비스 공급자 간에 SAML 2.0 신뢰 관계를 설정해야 하는 경우 이 절차를 사용합니다.

이 절차를 시작하기 전에 더 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 콘솔](#)을 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 내용은 [IAM Identity Center 콘솔의 애플리케이션 속성 이해](#) 섹션을 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 제공하세요.
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 콘솔](#)을 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 내용은 [IAM Identity Center 콘솔의 애플리케이션 속성 이해](#) 섹션을 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.

신뢰할 수 있는 ID 전파 개요

신뢰할 수 있는 ID 전파는 AWS 서비스의 관리자가 그룹 연결과 같이 사용자 속성을 기반으로 권한을 부여할 수 있는 IAM Identity Center의 기능입니다. 신뢰할 수 있는 자격 증명 전파를 통해 자격 증명 컨텍스트가 IAM 역할에 추가되어 AWS 리소스에 대한 액세스를 요청하는 사용자를 식별합니다. 이 컨텍스트는 다른 데 전파됩니다 AWS 서비스.

자격 증명 컨텍스트는 액세스 요청을 수신할 때 권한 부여 결정을 내리는 데 AWS 서비스 사용하는 정보로 구성됩니다. 이 정보에는 요청자(예: IAM Identity Center 사용자), 액세스가 요청 AWS 서비스 되는 (예: Amazon Redshift) 및 액세스 범위(예: 읽기 전용 액세스)를 식별하는 메타데이터가 포함됩니다. 수신되는 이 컨텍스트와 사용자에게 할당된 모든 권한을 AWS 서비스 사용하여 리소스에 대한 액세스를 승인합니다.

신뢰할 수 있는 ID 전파의 이점

신뢰할 수 있는 자격 증명 전파를 통해의 관리자는 작업 인력의 기업 자격 증명을 사용하여 데이터와 같은 리소스에 권한을 AWS 서비스 부여할 수 있습니다. 또한 서비스 로그 또는를 확인하여 누가 어떤 데이터에 액세스했는지 감사할 수 있습니다 AWS CloudTrail. IAM Identity Center 관리자의 경우 다른 AWS 서비스 관리자로부터 신뢰할 수 있는 ID 전파를 활성화하라는 요청을 받을 수 있습니다.

신뢰할 수 있는 ID 전파 활성화

신뢰할 수 있는 ID 전파를 활성화하는 과정은 다음 두 단계로 이루어집니다.

1. IAM Identity Center를 활성화하고 기존 자격 증명 소스를 IAM Identity Center에 연결 - 기존 자격 증명 소스에서 인력 자격 증명을 계속 관리할 수 있습니다. IAM Identity Center에 연결하면 사용 사례 AWS 서비스 의 모든 사용자가 공유할 수 있는 인력에 대한 참조가 생성됩니다. 또한 데이터 소유자가 향후 사용 사례에서 사용할 수 있습니다.
2. 사용 사례 AWS 서비스 의를 IAM Identity Center에 연결 - 신뢰할 수 있는 자격 증명 전파 사용 사례의 각 AWS 서비스 의 관리자는 해당 서비스 설명서의 지침에 따라 서비스를 IAM Identity Center에 연결합니다.

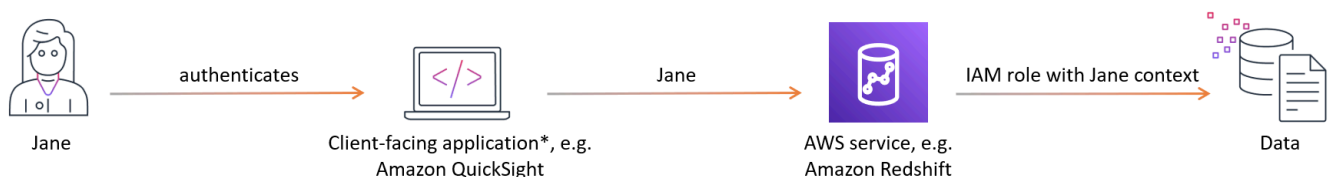
Note

사용 사례에 타사 또는 고객이 개발한 애플리케이션이 포함된 경우 애플리케이션 사용자를 인증하는 ID 제공업체와 IAM Identity Center 간의 신뢰 관계를 구성하여 신뢰할 수 있는 ID 전파를 직접 활성화합니다. 이렇게 하면 애플리케이션이 앞서 설명한 신뢰할 수 있는 ID 전파 흐름을 활용할 수 있습니다.

자세한 내용은 [신뢰할 수 있는 토큰 발급자를 사용하여 애플리케이션 사용](#) 단원을 참조하십시오.

신뢰할 수 있는 ID 전파의 작동 방식

다음 다이어그램은 신뢰할 수 있는 ID 전파의 상위 수준 워크플로를 보여줍니다.



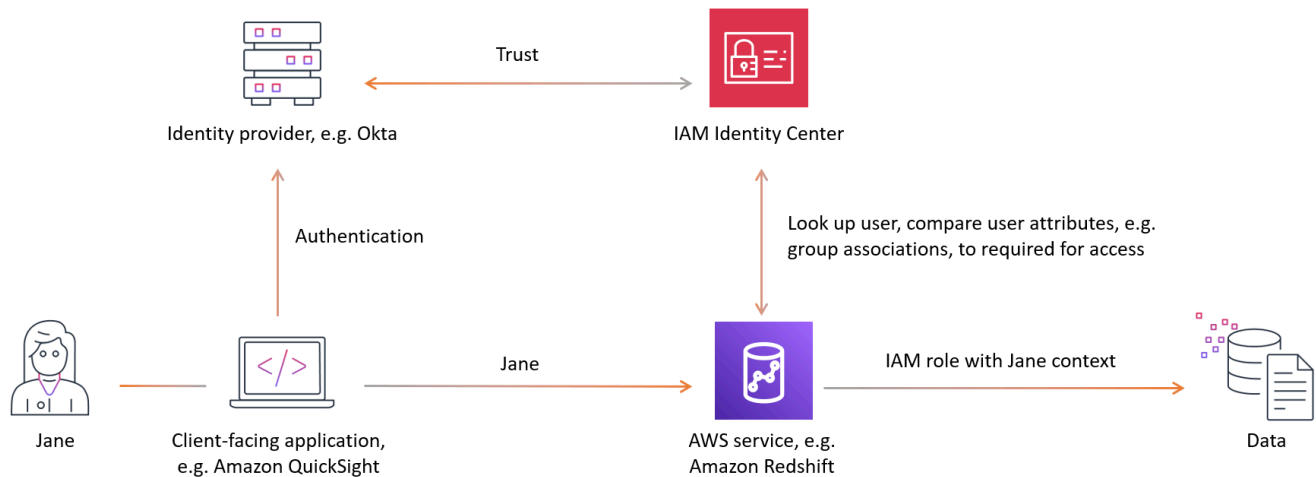
1. 사용자는 Quick과 같은 클라이언트 대상 애플리케이션으로 인증합니다.
2. 클라이언트 대상 애플리케이션은 사용하여 데이터를 쿼리 AWS 서비스 할 수 있는 액세스를 요청하고 사용자에게 대한 정보를 포함합니다.

Note

신뢰할 수 있는 일부 자격 증명 전파 사용 사례에는 서비스 드라이버를 AWS 서비스 사용하여와 상호 작용하는 도구가 포함됩니다. [사용 사례 지침](#)에서 이것이 사용 사례에 적용되는지 여부를 확인할 수 있습니다.

3. 는 IAM Identity Center를 통해 사용자 자격 증명을 AWS 서비스 확인하고 그룹 연결과 같은 사용자 속성을 액세스에 필요한 속성과 비교합니다. 는 사용자 또는 해당 그룹에 필요한 권한이 있는 한 액세스 권한을 AWS 서비스 부여합니다.
4. AWS 서비스 는 AWS CloudTrail 및 서비스 로그에 사용자 식별자를 기록할 수 있습니다. 자세한 내용은 서비스 문서를 확인하세요.

다음 이미지는 앞서 설명한 신뢰할 수 있는 ID 전파 워크플로의 단계들에 대한 개요를 보여줍니다.



주제

- [필수 조건 및 고려 사항](#)
- [신뢰할 수 있는 ID 전파 사용 사례](#)
- [권한 부여 서비스](#)

필수 조건 및 고려 사항

신뢰할 수 있는 ID 전파를 설정하기 전에 다음 사전 조건 및 고려 사항을 검토합니다.

주제

- [사전 조건](#)
- [고려 사항](#)
- [고객 관리형 애플리케이션에 대한 고려 사항](#)

사전 조건

신뢰할 수 있는 ID 전파를 사용하려면 환경에서 다음 사전 조건이 충족되어야 합니다.

- IAM Identity Center 활성화 및 프로비저닝
 - 신뢰할 수 있는 자격 증명 전파를 사용하려면 사용자가 액세스할 AWS 애플리케이션 및 서비스가 활성화된 AWS 리전 동일한에서 IAM Identity Center를 활성화해야 합니다. 자세한 내용은 [IAM Identity Center 활성화](#) 단원을 참조하세요.
 - IAM Identity Center 조직 인스턴스 권장 - AWS Organizations의 관리 계정에서 활성화한 IAM Identity Center의 [조직 인스턴스](#)를 사용하는 것이 좋습니다. IAM Identity Center의 조직 인스턴스 [관리를 멤버 계정에 위임](#)할 수 있습니다. IAM Identity Center의 [계정 인스턴스](#)를 선택하면 사용자가 신뢰할 수 있는 ID 전파로 액세스하길 원하는 모든 AWS 서비스가 IAM Identity Center를 활성화한 곳과 동일한 AWS 계정에 있어야 합니다. 자세한 내용은 [IAM Identity Center의 계정 인스턴스](#) 단원을 참조하십시오.
 - 기존 ID 제공업체를 IAM Identity Center에 연결하고 사용자 및 그룹을 IAM Identity Center에 프로비저닝합니다. 자세한 내용은 [IAM Identity Center의 ID 소스 자습서](#) 단원을 참조하십시오.
- 신뢰할 수 있는 ID 전파 사용 사례의 AWS 관리형 애플리케이션 및 서비스를 IAM Identity Center에 연결합니다. 신뢰할 수 있는 자격 증명 전파를 사용하려면 AWS 관리형 애플리케이션을 IAM Identity Center에 연결해야 합니다.

고려 사항

신뢰할 수 있는 ID 전파를 구성하고 사용할 때 다음 고려 사항에 유의해야 합니다.

- IAM Identity Center의 조직 및 계정 인스턴스의 차이점
 - IAM Identity Center의 [조직 인스턴스](#)는 여러 AWS 계정, 사용자, AWS 서비스로 사용 사례를 확장할 수 있는 가장 높은 수준의 제어와 유연성을 제공합니다. 조직 인스턴스를 사용할 수 없는 경우

IAM Identity Center의 계정 인스턴스를 통해 사용 사례가 지원될 수 있습니다. 사용 사례에서 어떤 AWS 서비스 가 IAM Identity Center의 계정 인스턴스를 지원하는지 알아보려면 [AWS IAM Identity Center와 함께 사용할 수 있는 관리형 애플리케이션](#) 섹션을 참조하세요.

- 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.

고객 관리형 애플리케이션에 대한 고려 사항

사용자가 AWSTableau 또는 사용자 지정 개발 애플리케이션에서 관리하지 않는 클라이언트 대상 애플리케이션과 상호 작용하더라도 신뢰할 수 있는 자격 증명 전파를 통해 작업 인력의 이점을 누릴 수 있습니다. 이러한 애플리케이션의 사용자는 IAM Identity Center에서 프로비저닝되지 않을 수 있습니다. AWS 리소스에 대한 사용자 액세스를 원활하게 인식하고 권한을 부여할 수 있도록 IAM Identity Center를 사용하면 사용자를 인증하는 ID 제공업체와 IAM Identity Center 간에 신뢰할 수 있는 관계를 구성할 수 있습니다. 자세한 내용은 [신뢰할 수 있는 토큰 발급자를 사용하여 애플리케이션 사용](#) 단원을 참조하십시오.

또한 애플리케이션에 대해 신뢰할 수 있는 ID 전파를 구성하려면 다음이 필요합니다.

- 애플리케이션이 인증에 OAuth 2.0 프레임워크를 사용해야 합니다. 신뢰할 수 있는 ID 전파는 SAML 2.0 통합을 지원하지 않습니다.
- IAM Identity Center가 애플리케이션을 인식해야 합니다. 해당 [사용 사례](#)에 맞는 지침을 따르세요.

신뢰할 수 있는 ID 전파 사용 사례

IAM Identity Center 관리자는 사용자 대상 애플리케이션에서 AWS 서비스로의 신뢰할 수 있는 ID 전파를 구성하는 데 도움을 달라는 요청을 받을 수 있습니다. 이 요청을 지원하려면 다음 정보가 필요합니다.

- 사용자가 어떤 클라이언트 대상 애플리케이션과 인터페이스할 것인가?
- 데이터를 쿼리하고 데이터에 대한 액세스를 승인하는 데 사용되는 AWS 서비스 것은 무엇입니까?
- 데이터에 대한 액세스 권한을 AWS 서비스 부여하는 것은 무엇입니까?

타사 애플리케이션 또는 맞춤형 개발 애플리케이션과 관련이 없는 신뢰할 수 있는 ID 전파 사용 사례를 활성화하는 데 있어 관리자의 역할은 다음과 같습니다.

1. [IAM Identity Center를 활성화합니다.](#)
2. [기존 ID 소스를 IAM Identity Center에 연결합니다.](#)

이러한 사용 사례에 대해 신뢰할 수 있는 자격 증명 구성의 나머지 단계는 연결된 AWS 서비스 및 애플리케이션 내에서 수행됩니다. 연결된 AWS 서비스 또는 애플리케이션의 관리자는 포괄적인 서비스별 지침은 해당 사용 설명서를 참조해야 합니다.

타사 애플리케이션 또는 맞춤형 개발 애플리케이션과 관련된 신뢰할 수 있는 ID 전파 사용 사례를 활성화하는 데 있어 관리자의 역할에는 [IAM Identity Center 활성화](#)의 단계 및 [ID 소스 연결](#)과 다음이 포함됩니다.

1. ID 제공업체(IdP)와 타사 또는 맞춤형 개발 애플리케이션의 연결을 구성합니다.
2. IAM Identity Center가 타사 또는 맞춤형 개발 애플리케이션을 인식할 수 있도록 합니다.
3. IAM Identity Center에서 IdP를 신뢰할 수 있는 토큰 발급자로 구성합니다. 자세한 내용은 [신뢰할 수 있는 토큰 발급자를 사용하여 애플리케이션 사용](#) 단원을 참조하십시오.

연결된 애플리케이션의 관리자 및는 포괄적인 서비스별 지침은 해당 사용 설명서를 참조 AWS 서비스 해야 합니다.

분석, 데이터 레이크하우스, 기계 학습 사용 사례

다음 분석 및 기계 학습 서비스에 신뢰할 수 있는 전파 사용 사례를 활성화할 수 있습니다.

- Amazon Redshift - 지침은 [Amazon Redshift를 사용한 신뢰할 수 있는 ID 전파](#) 섹션을 참조하세요.
- Amazon EMR - 지침은 [Amazon EMR을 사용한 신뢰할 수 있는 ID 전파](#) 섹션을 참조하세요.
- Amazon Athena - 지침은 [Amazon Athena를 사용한 신뢰할 수 있는 ID 전파](#) 섹션을 참조하세요.
- SageMaker Studio - 지침은 [Amazon SageMaker Studio를 사용한 신뢰할 수 있는 ID 전파](#) 섹션을 참조하세요.

추가 사용 사례

다음과 같은 추가 AWS 서비스에 IAM Identity Center 및 신뢰할 수 있는 ID 전파를 활성화할 수 있습니다.

- Amazon Q Business - 지침은 다음을 참조하세요.
 - [IAM Identity Center를 사용한 앱 관리 워크플로.](#)

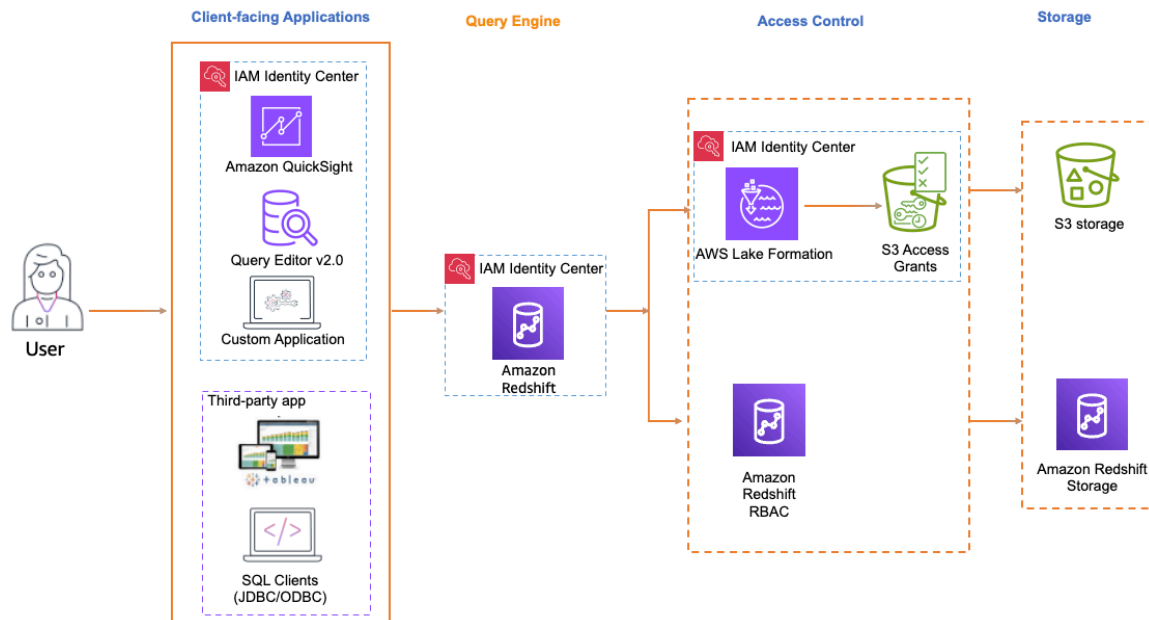
- [IAM Identity Center를 사용한 Amazon Q Business 애플리케이션 구성.](#)
- [IAM Identity Center의 신뢰할 수 있는 ID 전파를 사용한 Amazon Q Business 구성.](#)
- Amazon OpenSearch Service - 지침은 다음을 참조하세요.
 - [Amazon OpenSearch Service를 위한 IAM Identity Center의 신뢰할 수 있는 ID 전파 지원.](#)
 - [Amazon OpenSearch Service를 사용하는 중앙 집중식 OpenSearch 사용자 인터페이스\(대시보드\).](#)
- AWS Transfer Family - 지침은 다음을 참조하세요.
 - [Transfer Family 웹 앱.](#)

주제

- [Amazon Redshift를 사용한 신뢰할 수 있는 ID 전파](#)
- [Amazon EMR을 사용한 신뢰할 수 있는 ID 전파](#)
- [Amazon Athena를 사용한 신뢰할 수 있는 ID 전파](#)
- [Amazon SageMaker Studio를 사용한 신뢰할 수 있는 ID 전파](#)

Amazon Redshift를 사용한 신뢰할 수 있는 ID 전파

신뢰할 수 있는 자격 증명 전파를 활성화하는 단계는 사용자가 AWS 관리형 애플리케이션과 상호 작용하는지 아니면 고객 관리형 애플리케이션과 상호 작용하는지에 따라 달라집니다. 다음 다이어그램은 Amazon Redshift 또는 또는 Amazon AWS Lake Formation Amazon S3와 같은 권한 부여 서비스에서 제공하는 액세스 제어를 사용하여 Amazon Redshift 데이터를 쿼리 AWS 하는 AWS 관리형 또는 외부 클라이언트 대상 애플리케이션에 대한 신뢰할 수 있는 자격 증명 전파 구성을 보여줍니다Access Grants.



Amazon Redshift로의 신뢰할 수 있는 ID 전파를 활성화하면 Redshift 관리자는 IAM Identity Center에 대한 역할을 ID 제공업체로 자동 생성하고, Redshift 역할을 IAM Identity Center의 그룹에 매핑하고, Redshift 역할 기반 액세스 제어를 사용하여 액세스 권한을 부여하도록 Redshift를 구성할 수 있습니다.

지원되는 클라이언트 대상 애플리케이션

AWS 관리형 애플리케이션

다음 AWS 관리형 클라이언트 대상 애플리케이션은 Amazon Redshift로의 신뢰할 수 있는 ID 전파를 지원합니다.

- [Amazon Redshift Query Editor V2](#)
- [빠른](#)

Note

Amazon Redshift Spectrum을 사용하여 AWS Glue Data Catalog의 외부 데이터베이스 또는 테이블에 액세스하는 경우 세분화된 액세스 제어를 제공하도록 [Lake Formation](#) 및 [Amazon S3Access Grants](#)를 설정하는 것이 좋습니다.

고객 관리형 애플리케이션

다음 고객 관리형 애플리케이션은 Amazon Redshift로의 신뢰할 수 있는 ID 전파를 지원합니다.

- Tableau(Tableau Desktop, Tableau Server, Tableau Prep 포함)
 - Tableau 사용자에게 대해 신뢰할 수 있는 ID 전파를 활성화하려면 AWS 빅 데이터 블로그의 [IAM Identity Center를 사용하여 Tableau 및 Okta 항목을 Amazon Redshift와 통합](#)을 참조하세요.
- SQL 클라이언트(DBBeaver 및 DBVisualizer)
 - SQL 클라이언트(DBBeaver 및 DBVisualizer) 사용자에게 대해 신뢰할 수 있는 ID 전파를 활성화하려면 AWS 빅 데이터 블로그에서 [원활한 Single Sign-On을 위해 IAM Identity Center를 사용하여 Amazon Redshift Query Editor V2 및 SQL 클라이언트와 ID 제공업체\(IdP\) 통합](#)을 참조하세요.

Amazon Redshift Query Editor V2를 사용한 신뢰할 수 있는 ID 전파 설정

다음 절차에서는 Amazon Redshift Query Editor V2에서 Amazon Redshift로 신뢰할 수 있는 ID 전파를 달성하는 방법을 안내합니다.

사전 조건

이 자습서를 시작하려면 먼저 다음을 설정해야 합니다.

1. [IAM Identity Center를 활성화합니다. 조직 인스턴스](#)를 권장합니다. 자세한 내용은 [필수 조건 및 고려 사항](#) 단원을 참조하십시오.
2. [ID 소스의 사용자 및 그룹을 IAM Identity Center로 프로비저닝합니다.](#)

신뢰할 수 있는 ID 전파를 활성화하는 데에는 IAM Identity Center 콘솔에서 IAM Identity Center 관리자가 수행하는 작업과, Amazon Redshift 콘솔에서 Amazon Redshift 관리자가 수행하는 작업이 있습니다.

IAM Identity Center 관리자가 수행하는 작업

IAM Identity Center 관리자가 완료해야 할 작업은 다음과 같습니다.

1. 다음 권한 정책을 사용하여 Amazon Redshift 클러스터 또는 Serverless 인스턴스가 있는 계정에 [IAM 역할](#)을 생성합니다. 자세한 내용은 [IAM 역할 생성](#)을 참조하세요.
 - 다음 정책 예시에는 이 자습서를 완료하는 데 필요한 권한이 포함되어 있습니다. 이 정책을 사용하려면 정책 예제의 `#### ## ### ###`를 본인의 정보로 대체합니다. 추가 지침은 [정책 생성](#) 또는 [정책 편집](#)을 참조하세요.

권한 정책:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshiftApplication",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowIDCPermissions",
      "Effect": "Allow",
      "Action": [
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
      "Resource": [
        "arn:aws:sso::instance/Your-IAM-Identity-Center-Instance-ID",
        "arn:aws:sso::111122223333:application/Your-IAM-Identity-Center-Instance-ID/*"
      ]
    }
  ]
}
```

신뢰 정책:

JSON

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

```

    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": [
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com"
          ]
        },
        "Action": [
          "sts:AssumeRole",
          "sts:SetContext"
        ]
      }
    ]
  }
}

```

2. IAM Identity Center가 활성화된 AWS Organizations 관리 계정에서 권한 세트를 생성합니다. 다음 단계에서 이를 사용하여 페더레이션 사용자가 Redshift Query Editor V2에 액세스할 수 있도록 합니다.
 - a. IAM Identity Center 콘솔의 다중 계정 권한으로 이동하여 권한 세트를 선택합니다.
 - b. 권한 집합 생성을 선택합니다.
 - c. 사용자 지정 권한 세트를 선택한 후 다음을 선택합니다.
 - d. AWS 관리형 정책에서 **AmazonRedshiftQueryEditorV2ReadSharing**을 선택합니다.
 - e. 인라인 정책에서 다음 정책을 추가합니다.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ]
    }
  ]
}

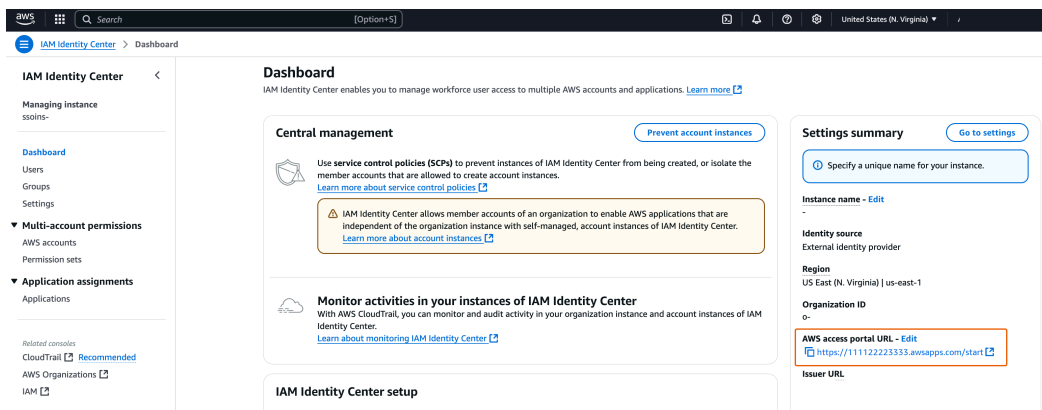
```

```

    ],
    "Resource": "*"
  }
}

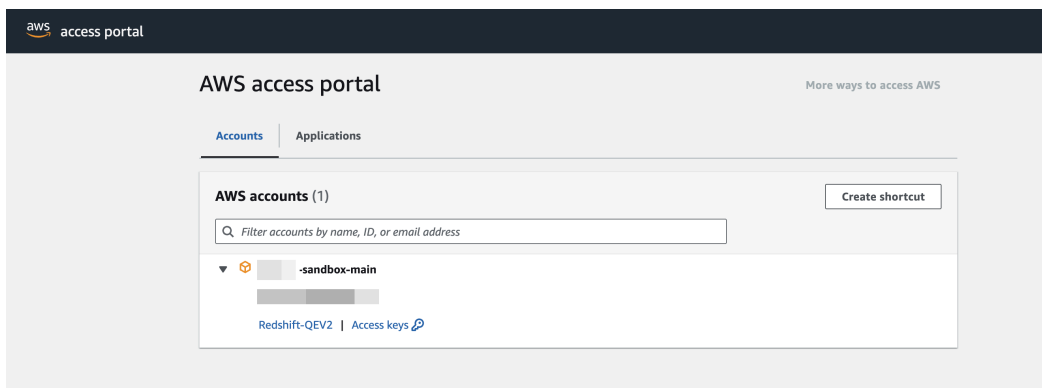
```

- f. 다음을 선택한 후 권한 세트 이름에 이름을 입력합니다. 예를 들어 **Redshift-Query-Editor-V2**입니다.
- g. 릴레이 상태 - 선택 사항에서 <https://your-region.console.aws.amazon.com/sqlworkbench/home> 형식으로 기본 릴레이 상태를 Query Editor V2 URL로 설정합니다.
- h. 설정을 검토하고 생성을 선택합니다.
- i. IAM Identity Center 대시보드로 이동하여 설정 요약 섹션에서 AWS 액세스 포털 URL을 복사합니다.



- j. 새 Incognito 브라우저 창을 열고 URL을 붙여 넣습니다.

그러면 AWS 액세스 포털로 이동하여 IAM Identity Center 사용자로 로그인합니다.



권한 세트에 대한 자세한 내용은 [권한 세트 AWS 계정 로 관리](#) 섹션을 참조하세요.

3. Redshift Query Editor V2에 대한 페더레이션 사용자 액세스를 활성화합니다.

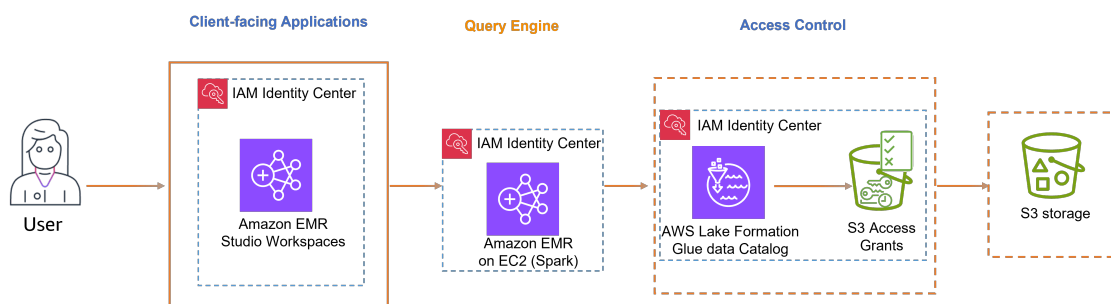
- AWS Organizations 관리 계정에서 IAM Identity Center 콘솔을 엽니다.
- 탐색 창의 다중 계정 권한에서 AWS 계정을 선택합니다.
- 페이지에서 액세스 권한을 할당할 AWS 계정 를 AWS 계정 선택합니다.
- 사용자 또는 그룹 할당을 선택합니다.
- 사용자 및 그룹 할당 페이지에서 권한 세트를 생성하려는 사용자 및/또는 그룹을 선택합니다. 그리고 다음을 선택합니다.
- 권한 세트 할당 페이지에서 이전 단계에서 생성한 권한 세트를 선택합니다. 그리고 다음을 선택합니다.
- 할당 검토 및 제출 페이지에서 선택 내용을 검토하고 제출을 선택합니다.

Amazon Redshift 관리자가 수행하는 작업

Amazon Redshift로의 신뢰할 수 있는 ID 전파를 활성화하려면 Amazon Redshift 클러스터 관리자 또는 Amazon Redshift Serverless 관리자가 Amazon Redshift 콘솔에서 몇 가지 작업을 수행해야 합니다. 자세한 내용은 AWS 빅 데이터 블로그에서 [원활한 Single Sign-On을 위해 IAM Identity Center를 사용하여 Amazon Redshift Query Editor V2 및 SQL 클라이언트와 ID 제공업체\(IdP\) 통합](#)을 참조하세요.

Amazon EMR을 사용한 신뢰할 수 있는 ID 전파

다음 다이어그램은 AWS Lake Formation 및 Amazon S3에서 제공하는 액세스 제어와 함께 Amazon EMR on Amazon EC2를 사용하는 Amazon EMR Studio에 대한 신뢰할 수 있는 자격 증명 전파 구성을 보여줍니다Access Grants.



지원되는 클라이언트 대상 애플리케이션

- Amazon EMR Studio

신뢰할 수 있는 ID 전파를 활성화하려면 다음 단계를 따릅니다.

- Amazon EMR 클러스터를 위한 클라이언트 대상 애플리케이션으로 [Amazon EMR Studio](#)를 설정합니다.
- [Apache Spark](#)를 사용하여 Amazon EC2에서 Amazon EMR 클러스터를 설정합니다.
- 권장 사항: [AWS Lake Formation](#) 및 [Amazon S3Access Grants](#)는 S3의 AWS Glue Data Catalog 및 기본 데이터 위치에 대한 세분화된 액세스 제어를 제공합니다.

Amazon EMR Studio를 사용한 신뢰할 수 있는 ID 전파 설정

다음 절차에서는 Apache Spark를 실행하는 Amazon Athena 작업 그룹 또는 Amazon EMR 클러스터에 대한 쿼리에서 신뢰할 수 있는 ID 전파를 위해 Amazon EMR Studio를 설정하는 방법을 안내합니다.

사전 조건

이 자습서를 시작하려면 먼저 다음을 설정해야 합니다.

1. [IAM Identity Center](#)를 활성화합니다. [조직 인스턴스](#)를 권장합니다. 자세한 내용은 [필수 조건 및 고려 사항](#) 단원을 참조하십시오.
2. [ID 소스의 사용자 및 그룹을 IAM Identity Center로 프로비저닝](#)합니다.

Amazon EMR Studio에서 신뢰할 수 있는 ID 전파 설정을 완료하려면 EMR Studio 관리자가 다음 단계를 수행해야 합니다.

1단계. EMR Studio에 필요한 IAM 역할 생성

이 단계에서 Amazon EMR Studio 관리자는 EMR Studio에 대한 IAM 서비스 역할과 IAM 사용자 역할을 생성합니다.

1. [EMR Studio 서비스 역할 생성](#) - EMR Studio는 이 IAM 역할을 수입하여 워크스페이스와 노트북을 안전하게 관리하고, 클러스터에 연결하고, 데이터 상호 작용을 처리합니다.
 - a. IAM 콘솔(<https://console.aws.amazon.com/iam/>)로 이동하여 IAM 역할을 생성합니다.
 - b. AWS 서비스를 신뢰할 수 있는 엔터티로 선택한 다음 Amazon EMR을 선택합니다. 다음 정책을 연결하여 역할의 권한 및 신뢰 관계를 정의합니다.

이러한 정책을 사용하려면 정책 예제의 **#### ## ### ###**를 본인의 정보로 대체합니다. 추가 지침은 [정책 생성](#) 또는 [정책 편집](#)을 참조하세요.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectActions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    },
    {
      "Sid": "BucketActions",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    }
  ]
}
```


모든 서비스 역할 권한에 대한 참조는 [EMR Studio 서비스 역할 권한](#)을 참조하세요.

2. [IAM Identity Center 인증을 위해 EMR Studio 사용자 역할 생성](#) - 사용자가 IAM Identity Center를 통해 로그인하여 워크스페이스, EMR 클러스터, 작업, git 리포지토리를 관리할 때 EMR Studio가 이 역할을 수입합니다. 이 역할은 신뢰할 수 있는 ID 전파 워크플로를 시작하는 데 사용됩니다.

Note

EMR Studio 사용자 역할에는 AWS Glue Catalog에 있는 테이블의 Amazon S3 위치에 액세스할 수 있는 권한이 포함되지 않아도 됩니다. AWS Lake Formation 권한 및 등록된 레이크 위치는 임시 권한을 받는 데 사용됩니다.

다음 예제 정책은 EMR Studio의 사용자가 Athena 작업 그룹을 사용하여 쿼리를 실행하도록 허용하는 역할에서 사용할 수 있습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
        }
      }
    },
    {
      "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
      "Effect": "Allow",
```

```

        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:*:*:security-group/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
                "ec2:CreateAction": "CreateSecurityGroup"
            }
        },
        {
            "Sid": "AllowSecretManagerListSecrets",
            "Action": [
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
            "Effect": "Allow",
            "Action": "secretsmanager:CreateSecret",
            "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
                }
            }
        },
        {
            "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
            "Effect": "Allow",
            "Action": "secretsmanager:TagResource",
            "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
        },
        {
            "Sid": "AllowPassingServiceRoleForWorkspaceCreation",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
            ]
        }
    ]
}

```

```

    ],
    "Effect": "Allow"
  },
  {
    "Sid": "AllowS3ListAndLocationPermissions",
    "Action": [
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Sid": "AllowS3ReadOnlyAccessToLogs",
    "Action": [
      "s3:GetObject"
    ],
    "Resource": [
      "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
    ],
    "Effect": "Allow"
  },
  {
    "Sid": "AllowAthenaQueryExecutions",
    "Effect": "Allow",
    "Action": [
      "athena:StartQueryExecution",
      "athena:GetQueryExecution",
      "athena:GetQueryResults",
      "athena:StopQueryExecution",
      "athena:ListQueryExecutions",
      "athena:GetQueryResultsStream",
      "athena:ListWorkGroups",
      "athena:GetWorkGroup",
      "athena:CreatePreparedStatement",
      "athena:GetPreparedStatement",
      "athena>DeletePreparedStatement"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowGlueSchemaManipulations",

```

```

        "Effect": "Allow",
        "Action": [
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:GetTable",
            "glue:GetTables",
            "glue:GetPartition",
            "glue:GetPartitions"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowQueryEditorToAccessWorkGroup",
        "Effect": "Allow",
        "Action": "athena:GetWorkGroup",
        "Resource": "arn:aws:athena:*:111122223333:workgroup*"
    },
    {
        "Sid": "AllowConfigurationForWorkspaceCollaboration",
        "Action": [
            "elasticmapreduce:UpdateEditor",
            "elasticmapreduce:PutWorkspaceAccess",
            "elasticmapreduce>DeleteWorkspaceAccess",
            "elasticmapreduce:ListWorkspaceAccessIdentities"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
            "StringEquals": {
                "elasticmapreduce:ResourceTag/creatorUserId":
"${aws:userId}"
            }
        }
    },
    {
        "Sid": "DescribeNetwork",
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups"
        ],
        "Resource": "*"
    },

```

```

    {
      "Sid": "ListIAMRoles",
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AssumeRole",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "*"
    }
  ]
}

```

다음 신뢰 정책은 EMR Studio가 역할을 수입하도록 허용합니다.

Note

EMR Studio Workspace 및 EMR 노트북을 활용하려면 추가 권한이 필요합니다. 자세한 내용은 [EMR Studio 사용자를 위한 권한 정책 생성](#)을 참조하세요.

다음 링크를 통해 자세한 내용을 확인할 수 있습니다.

- [고객 관리형 정책으로 사용자 지정 IAM 권한 정의](#)
- [EMR Studio 서비스 역할 권한](#)

2단계. EMR Studio 생성 및 구성

이 단계에서는 EMR Studio 콘솔에서 Amazon EMR Studio를 생성하고 [1단계. EMR Studio에 필요한 IAM 역할 생성](#)에서 생성한 IAM 역할을 사용합니다.

1. EMR Studio 콘솔로 이동하여 Studio 생성 및 사용자 지정 설정 옵션을 선택합니다. 새 S3 버킷을 생성하거나 기존 버킷을 사용할 수 있습니다. 자체 KMS 키로 워크스페이스 파일 암호화 확인란을 선택할 수 있습니다. 자세한 내용은 [AWS Key Management Service](#) 단원을 참조하십시오.

Create a Studio Info

Setup options Info

☐ Interactive workloads ☐ Batch jobs ☒ Custom

Studio settings Info

Studio name

Studio_1

Use up to 256 characters (alphanumeric, hyphens, or underscores).

Description - optional

The description below will be visible to your studio teams.

Describe the Studio

256 characters maximum

S3 location for Workspace storage

Specify an Amazon S3 location where Workspace work will be saved.

☒ Create new bucket ☐ Select existing location

We'll create a new bucket and use the location `s3://aws-emr-studio-225989353012-us-east-1/1735848818523`.

☐ Encrypt Workspace files with your own AWS KMS key

EMR Studio automatically uses the S3 location's encryption configuration. Choose this option if you want to override the S3 location's encryption configuration with your own AWS KMS key. This key information will not be editable past Studio creation.

2. Studio가 리소스에 액세스할 수 있도록 하는 서비스 역할의 메뉴에서 [1단계. EMR Studio에 필요한 IAM 역할 생성](#)에서 생성된 서비스 역할을 선택합니다.
3. 인증에서 IAM Identity Center를 선택합니다. [1단계. EMR Studio에 필요한 IAM 역할 생성](#)에서 생성된 사용자 역할을 선택합니다.

Service role to let Studio access your AWS resources

AmazonEMRStudio_

[View permission details](#)

Authentication Info

Choose an authentication method for your Studio.

☐ AWS Identity and Access Management (IAM)

Authenticate with single sign-on using IAM Identity federation or IAM credentials.

☒ IAM Identity Center (AWS Single Sign-On)

Authenticate with single sign-on using IAM Identity Center (recommended to centrally manage access permissions for multiple AWS accounts).

User role

Each Studio will have a default set of user roles. You can further refine user permissions once you have created a Studio. To create an additional set of permission use [AWS IAM](#)

emrstudio-userrole-idx

[Create IAM role](#)

Connect EMR Studio to IAM Identity Center

Instance of IAM Identity Center

Manage access to EMR Studio by assigning users and groups from your Identity Center directory.

arn:aws:sso::instance/ssolns-

4. 신뢰할 수 있는 ID 전파 상자를 선택합니다. 애플리케이션 액세스 섹션에서 할당된 사용자 및 그룹만을 선택합니다. 그러면 권한이 부여된 사용자 및 그룹만이 스튜디오에 액세스할 수 있습니다.
5. (선택 사항) - EMR 클러스터와 함께 이 Studio를 사용하는 경우 VPC 및 서브넷을 구성할 수 있습니다.

Trusted identity propagation [Info](#)
Control and log the access that a user has across connected applications.

☒ **Enable trusted identity propagation**
When users make requests to applications that are connected through Identity Center, share their user identity information from EMR Studio. This setting applies for the lifetime of the Studio. You can't turn it off later.

Application access [Info](#)
Choose who can access your application
Specify whether only assigned users and groups can access your application.

☒ **Only assigned users and groups**
Only the users and groups that you specify from your Identity Center directory can access this application.

☐ **All users and groups**
Any user or group from your IAM Identity Center directory can access this application.

▼ Networking and security - optional

VPC [Info](#)
Select a VPC for your Studio to use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag the VPC with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

Select a VPC

Subnets [Info](#)
Select the subnets that your Studio can use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag each subnet with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

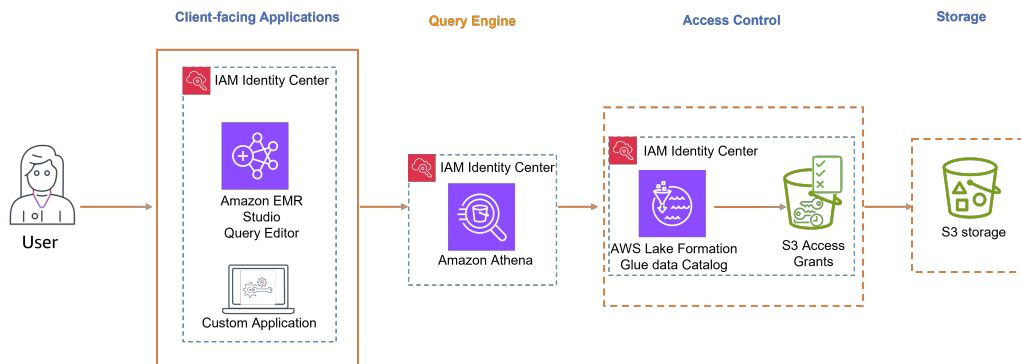
6. 모든 세부 정보를 검토하고 Studio 생성을 선택합니다.
7. Athena WorkGroup 또는 EMR 클러스터를 구성한 후 Studio의 URL에 로그인하여 다음을 수행합니다.
 - a. 쿼리 편집기로 Athena 쿼리를 실행합니다.
 - b. Jupyter 노트북을 사용하여 워크스페이스에서 Spark 작업을 실행합니다.

Amazon Athena를 사용한 신뢰할 수 있는 ID 전파

신뢰할 수 있는 자격 증명 전파를 활성화하는 단계는 사용자가 AWS 관리형 애플리케이션과 상호 작용하는지 아니면 고객 관리형 애플리케이션과 상호 작용하는지에 따라 달라집니다. 다음 다이어그램은 Amazon Athena를 사용하여 AWS Lake Formation 및 Amazon S3에서 제공하는 액세스 제어를 사용하여 Amazon S3 데이터를 쿼리 AWS 하는 AWS 관리형 또는 외부 클라이언트 대상 애플리케이션에 대한 신뢰할 수 있는 자격 증명 전파 구성을 보여줍니다 Amazon S3Access Grants.

Note

- Amazon Athena를 사용한 신뢰할 수 있는 ID 전파에는 Trino를 사용해야 합니다.
- ODBC 및 JDBC 드라이버를 통해 Amazon Athena에 연결된 Apache Spark 및 SQL 클라이언트는 지원되지 않습니다.



AWS 관리형 애플리케이션

다음 AWS 관리형 클라이언트 연결 애플리케이션은 Athena와의 신뢰할 수 있는 ID 전파를 지원합니다.

- Amazon EMR Studio

신뢰할 수 있는 ID 전파를 활성화하려면 다음 단계를 따릅니다.

- Athena를 위한 클라이언트 대상 애플리케이션으로 [Amazon EMR Studio를 설정합니다](#). 신뢰할 수 있는 ID 전파가 활성화되면 Athena 쿼리를 실행하기 위해 EMR Studio의 쿼리 편집기가 필요합니다.
- [Athena 작업 그룹을 설정합니다](#).
- IAM Identity Center의 사용자 또는 그룹을 기반으로 AWS Glue 테이블에 대한 세분화된 액세스 제어를 활성화하도록 [설정합니다 AWS Lake Formation](#).
- [Amazon S3 Access Grants를 설정](#)하여 S3의 기본 데이터 위치에 대한 임시 액세스를 활성화합니다.

Note

Lake Formation과 Amazon S3 Access Grants 모두 Amazon S3의 Athena 쿼리 결과에 대한 액세스 제어 AWS Glue Data Catalog 에 필요합니다.

고객 관리형 애플리케이션

사용자 지정 개발 애플리케이션의 사용자에게 대해 신뢰할 수 있는 자격 증명 전파를 활성화하려면 AWS 보안 블로그의 신뢰할 수 있는 [자격 증명 전파를 사용하여 AWS 서비스 프로그래밍 방식으로 액세스를 참조](#)하세요.

Amazon Athena 작업 그룹을 사용한 신뢰할 수 있는 ID 전파 설정

다음 절차는 신뢰할 수 있는 ID 전파를 위해 Amazon Athena 작업 그룹을 설정하는 방법을 안내합니다.

사전 조건

이 자습서를 시작하려면 먼저 다음을 설정해야 합니다.

1. [IAM Identity Center를 활성화합니다](#). [조직 인스턴스](#)를 권장합니다. 자세한 내용은 [필수 조건 및 고려 사항](#) 단원을 참조하십시오.
2. [ID 소스의 사용자 및 그룹을 IAM Identity Center로 프로비저닝합니다](#).
3. 이 구성에는 [Amazon EMR Studio](#), [AWS Lake Formation](#), [Amazon S3 Access Grants](#)가 필요합니다.

Athena를 사용한 신뢰할 수 있는 ID 전파 설정

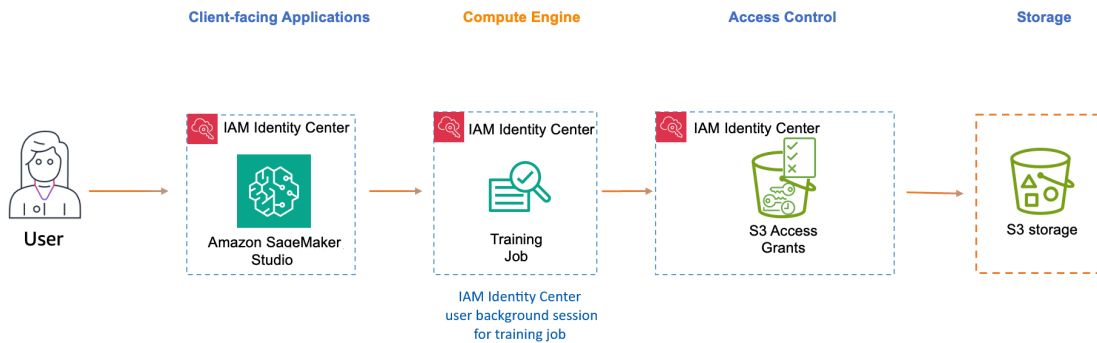
Athena를 사용하여 신뢰할 수 있는 ID 전파를 설정하려면 Athena 관리자는 다음을 수행해야 합니다.

1. [IAM Identity Center 지원 Athena 작업 그룹 사용 시 고려 사항 및 제한 사항](#)을 검토합니다.
2. [IAM Identity Center 지원 Athena 작업 그룹을 생성합니다](#).

Amazon SageMaker Studio를 사용한 신뢰할 수 있는 ID 전파

[Amazon SageMaker Studio](#)는 IAM Identity Center와 통합되어 [사용자 백그라운드 세션](#) 및 신뢰할 수 있는 ID 전파를 지원합니다. 사용자 백그라운드 세션을 사용하면 사용자가 작업을 실행하는 동안 로그인 상태를 유지할 필요 없이 SageMaker Studio에서 장기 실행 작업을 시작할 수 있습니다. 작업은 작업을 시작한 사용자의 권한을 사용하여 백그라운드에서 즉시 실행됩니다. 사용자가 컴퓨터를 끄거나, IAM Identity Center 로그인 세션이 만료되거나, 사용자가 AWS 액세스 포털에서 로그아웃하더라도 작업은 계속 실행될 수 있습니다. 사용자 백그라운드 세션의 기본 세션 기간은 7일이지만 최대 90일의 기간을 지정할 수 있습니다. 신뢰할 수 있는 ID 전파는 사용자의 자격 증명 또는 그룹 멤버십을 기반으로 Amazon S3 버킷과 같은 AWS 리소스에 제공되는 세분화된 액세스를 지원합니다.

다음 다이어그램은 SageMaker Studio가 Amazon S3 버킷에 저장된 데이터에 액세스하기 위한 신뢰할 수 있는 ID 전파의 구성을 보여줍니다. 사용자 백그라운드 세션이 IAM Identity Center에 대해 활성화되어 SageMaker Studio 훈련 작업을 백그라운드에서 실행할 수 있게 해줍니다. 훈련 데이터에 대한 액세스 제어는 Amazon S3 Access Grants에서 제공합니다.



AWS 관리형 애플리케이션

다음 AWS 관리형 클라이언트 대상 애플리케이션은 신뢰할 수 있는 ID 전파를 지원합니다.

- [Amazon SageMaker Studio](#)

신뢰할 수 있는 ID 전파 및 사용자 백그라운드 세션을 활성화하려면 다음 단계를 따릅니다.

- [SageMaker Studio를 클라이언트 대상 애플리케이션으로 설정합니다.](#)
- [Amazon S3 Access Grants를 설정](#)하여 Amazon S3의 기본 데이터 위치에 대한 임시 액세스를 활성화합니다.

SageMaker Studio를 사용한 신뢰할 수 있는 ID 전파 설정

다음 절차는 신뢰할 수 있는 ID 전파 및 사용자 백그라운드 세션을 위해 SageMaker Studio를 설정하는 방법을 안내합니다.

사전 조건

이 자습서를 시작하려면 먼저 다음 작업을 완료해야 합니다.

1. [IAM Identity Center를 활성화합니다.](#) 조직 인스턴스가 필요합니다. 자세한 내용은 [필수 조건 및 고려 사항](#) 단원을 참조하십시오.
2. [ID 소스의 사용자 및 그룹을 IAM Identity Center로 프로비저닝합니다.](#)
3. IAM Identity Center 콘솔에서 [사용자 백그라운드 세션이 활성화되어 있는지 확인합니다.](#) 기본적으로 사용자 백그라운드 세션은 활성화되어 있고 세션 기간은 7일로 설정되어 있습니다. 이 기간은 변경할 수 있습니다.

SageMaker Studio에서 신뢰할 수 있는 ID 전파를 설정하려면 SageMaker Studio 관리자가 다음 단계를 수행해야 합니다.

1단계: 신규 또는 기존 SageMaker Studio 도메인에서 신뢰할 수 있는 ID 전파 활성화

SageMaker Studio는 도메인을 사용하여 사용자 프로필, 애플리케이션 및 관련 리소스를 구성합니다. 신뢰할 수 있는 ID 전파를 활성화하려면 다음 절차에 설명된 것과 같이 SageMaker Studio 도메인을 생성하거나 기존 도메인을 수정해야 합니다.

1. SageMaker AI 콘솔을 열고 도메인으로 이동한 후 다음 중 하나를 수행합니다.

- [조직용 설정](#) 사용하여 새 SageMaker Studio 도메인을 생성합니다.

조직용 설정을 선택한 후 다음을 수행합니다.

- 인증 방법으로 AWS Identity Center를 선택합니다.
- 이 도메인의 모든 사용자에게 대해 신뢰할 수 있는 ID 전파 활성화 확인란을 선택합니다.
- 기존 SageMaker Studio 도메인을 수정합니다.
- 인증에 IAM Identity Center를 사용하는 기존 도메인을 선택합니다.

Important

신뢰할 수 있는 ID 전파는 인증에 IAM Identity Center를 사용하는 SageMaker Studio 도메인에서만 지원됩니다. 도메인이 인증에 IAM을 사용하는 경우 인증 방법을 변경할 수 없으므로 신뢰할 수 있는 ID 전파를 활성화할 수 없습니다.

- [도메인 설정을 편집합니다](#). 인증 및 권한 설정을 편집하여 신뢰할 수 있는 ID 전파를 활성화합니다.

2. [2단계: 기본 도메인 실행 역할 구성](#)으로 진행합니다. 이 역할은 SageMaker Studio 도메인 사용자가 Amazon S3와 같은 다른 AWS 서비스에 액세스하는 데 필요합니다.

2단계: 기본 도메인 실행 역할 및 역할 신뢰 정책 구성

도메인 실행 역할은 SageMaker Studio 도메인이 도메인의 모든 사용자를 대신하여 수임하는 [IAM 역할](#)입니다. 이 역할에 할당하는 권한에 따라 SageMaker Studio가 수행할 수 있는 작업이 결정됩니다.

1. 도메인 실행 역할을 생성하거나 선택하려면 다음 중 하나를 수행합니다.

- [조직용 설정](#) 사용하여 역할을 생성하거나 선택합니다.

- SageMaker AI 콘솔을 열고 2단계: 역할 및 ML 활동 구성의 콘솔 지침에 따라 새 도메인 실행 역할을 생성하거나 기존 역할을 선택합니다.
 - 나머지 설정 단계를 완료하여 SageMaker Studio 도메인을 생성합니다.
 - 수동으로 실행 역할을 생성합니다.
 - IAM 콘솔을 열고 [실행 역할을 직접 생성합니다](#).
2. 두 가지 작업, 즉 [sts:AssumeRole](#) 및 [sts:SetContext](#)가 포함되도록 도메인 실행 역할에 연결된 [신뢰 정책을 업데이트](#)합니다. SageMaker Studio 도메인의 실행 역할을 찾는 방법에 대한 자세한 내용은 [도메인 실행 역할 가져오기](#)를 참조하세요.

신뢰 정책은 역할을 맡을 수 있는 ID를 지정합니다. 이 정책은 SageMaker Studio 서비스가 도메인 실행 역할을 수임하도록 허용하는 데 필요합니다. 정책에 다음과 같이 표시되도록 이 두 가지 작업을 추가합니다.

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

  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "sagemaker.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

3단계: 도메인 실행 역할에 필요한 Amazon S3 Access Grant 권한 확인

Amazon S3 Access Grants를 사용하려면 다음 권한이 포함된 권한 정책이 SageMaker Studio 도메인 실행 역할에 (인라인 정책 또는 고객 관리형 정책으로) 연결되어 있어야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
    }
  ]
}
```

이러한 권한이 포함된 정책이 없는 경우 AWS Identity and Access Management 사용 설명서의 [IAM 자격 증명 권한 추가 및 제거](#)의 지침을 따릅니다.

4단계: 도메인에 그룹 및 사용자 할당

[그룹 및 사용자 추가](#)의 단계에 따라 그룹 및 사용자를 SageMaker Studio 도메인에 할당합니다.

5단계: Amazon S3 Access Grants 설정

Amazon S3 Access Grants를 설정하려면 [IAM Identity Center를 통한 신뢰할 수 있는 ID 전파를 위해 Amazon S3 Access Grants 구성](#)의 단계를 따릅니다. 단계별 지침에 따라 다음 작업을 완료합니다.

1. Amazon S3 Access Grants 인스턴스를 생성합니다.
2. 해당 인스턴스에 위치를 등록합니다.
3. 권한 부여를 생성하여 특정 IAM Identity Center 사용자 또는 그룹이 해당 위치 내의 지정된 Amazon S3 위치 또는 하위 집합(예: 특정 접두사)에 액세스할 수 있도록 허용합니다.

6단계: SageMaker 훈련 작업 제출 및 사용자 백그라운드 세션 세부 정보 보기

SageMaker Studio에서 새 Jupyter Notebook을 시작하고 훈련 작업을 제출합니다. 작업이 실행되는 동안 다음 단계를 완료하여 세션 정보를 표시하고 사용자 백그라운드 세션 컨텍스트가 활성화 상태인지 확인합니다.

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 옆에 있는 괄호 안의 숫자는 이 사용자의 활성 세션 수를 나타냅니다.
5. 세션을 사용하는 작업의 Amazon 리소스 이름(ARN)으로 세션을 검색하려면 세션 유형 목록에서 사용자 백그라운드 세션을 선택한 다음 검색 상자에 작업 ARN을 입력합니다.

다음은 사용자 백그라운드 세션을 사용하는 훈련 작업이 사용자의 활성 세션 탭에 어떻게 표시되는지를 보여주는 예시입니다.

The screenshot shows the 'Active sessions (5)' page in the AWS IAM Identity Center console. At the top, there are tabs for Profile, Groups (0), AWS accounts, Applications, MFA devices (1), and Active sessions (5). Below the tabs, there's a section titled 'Active sessions (5)' with a sub-header 'You can end any of the active sessions in this list. The list shows all active sessions initiated by wei_zhang. [Learn more](#)'. There's a search bar with the placeholder 'Find sessions by client or used by' and a 'Session type' dropdown menu set to 'All'. Below the search bar, there's a table with columns: Client, Session type, Used by, and IP address. The table contains one row with the following data: Client is '-', Session type is 'User background se...', Used by is 'arn:aws:sagemaker:us-west-2:777788889999:training-job/trustedidprop-trjob-12345a6b', and IP address is '-'. There's also an 'End sessions' button in the top right corner.

7단계: CloudTrail 로그를 표시하여 CloudTrail 내 신뢰할 수 있는 ID 전파 확인

신뢰할 수 있는 ID 전파가 활성화되면 onBehalfOf 요소 아래의 CloudTrail 이벤트 로그에 작업이 나타납니다. userId는 훈련 작업을 시작한 IAM Identity Center 사용자의 ID가 나타납니다. 다음 CloudTrail 이벤트에 신뢰할 수 있는 ID 전파 프로세스가 캡처되어 있습니다.

```

      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAI23456789EXAMPLE:SageMaker",
        "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAI23456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",
            "accountId": "111122223333",

```

```

      "userName": "SageMaker-ExecutionRole-20250728T125817"
    },
    "attributes": {
      "creationDate": "2025-07-29T17:17:10Z",
      "mfaAuthenticated": "false"
    }
  },
  "onBehalfOf": {
    "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",
    "identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/d-1234567890"
  }
},

```

런타임 고려 사항

관리자가 사용자 백그라운드 세션 기간보다 짧은 장기 실행 훈련 또는 처리 작업에 대해 MaxRuntimeInSeconds를 설정하면 SageMaker Studio는 MaxRuntimeInSeconds 또는 사용자 백그라운드 세션 기간 중 최소 기간 동안 작업을 실행합니다.

MaxRuntimeInSeconds에 대한 자세한 내용은 Amazon SageMaker API Reference의 CreateTrainingJob [StoppingCondition](#) 섹션을 참조하세요.

권한 부여 서비스

모든 [분석 및 데이터 레이크하우스 사용 사례](#)에서 다음을 사용하여 세분화된 액세스 제어를 달성할 수 있습니다.

- AWS Lake Formation - 지침은 [IAM Identity Center AWS Lake Formation 로 설정](#).
- Amazon S3 Access Grants - 지침은 [IAM Identity Center를 사용한 Amazon S3 Access Grants 설정](#) 섹션을 참조하세요.

IAM Identity Center AWS Lake Formation 로 설정

[AWS Lake Formation](#)은 AWS에서 데이터 레이크의 생성과 관리를 간소화해주는 관리형 서비스입니다. 데이터 수집, 카탈로그 작성 및 보안을 자동화하고, 다양한 데이터 유형을 저장하고 분석하기 위한 중앙 집중식 리포지토리를 제공합니다. Lake Formation은 세분화된 액세스 제어를 제공하고 다양한

AWS 분석 서비스와 통합되어 조직이 데이터 레이크에서 인사이트를 효율적으로 설정, 보호 및 도출할 수 있도록 합니다.

Lake Formation이 IAM Identity Center 및 신뢰할 수 있는 ID 전파를 사용하여 사용자 자격 증명을 기반으로 데이터 권한을 부여하도록 하려면 다음 단계에 따릅니다.

사전 조건

이 자습서를 시작하려면 먼저 다음을 설정해야 합니다.

- [IAM Identity Center를 활성화합니다.](#) [조직 인스턴스](#)를 권장합니다. 자세한 내용은 [필수 조건 및 고려 사항](#) 단원을 참조하십시오.

신뢰할 수 있는 ID 전파를 설정하기 위한 단계

1. [Lake Formation과 IAM Identity Center 연결](#)의 지침에 따라 IAM Identity Center를 AWS Lake Formation과 통합합니다.

Important

AWS Glue Data Catalog 테이블이 없는 경우 AWS Lake Formation 을 사용하여 IAM Identity Center 사용자 및 그룹에 액세스 권한을 부여하려면 테이블을 생성해야 합니다. 자세한 내용은 [AWS Glue Data Catalog에서 객체 생성](#)을 참조하세요.

2. 데이터 레이크 위치를 등록합니다.

Glue 테이블의 데이터가 저장되는 [S3 위치를 등록합니다](#). 이렇게 하면 Lake Formation은 테이블을 쿼리할 때 필요한 S3 위치에 대한 임시 액세스 권한을 프로비저닝하기 때문에 서비스 역할(예: WorkGroup에 구성된 Athena 서비스 역할)에 S3 권한을 포함할 필요가 없습니다.

- a. AWS Lake Formation 콘솔의 탐색 창에서 관리 섹션 아래에 있는 데이터 레이크 위치로 이동합니다. 위치 등록을 선택합니다.

이렇게 하면 Lake Formation이 S3 데이터 위치에 액세스하는 데 필요한 권한으로 임시 IAM 자격 증명을 프로비저닝할 수 있습니다.

- b. Amazon S3 경로 필드에 AWS Glue 테이블의 데이터 위치에 해당하는 S3 경로를 입력합니다.
- c. 신뢰할 수 있는 ID 전파와 함께 사용하려면 IAM 역할 섹션에서 서비스 연결 역할을 선택하지 않습니다. 다음 권한을 가진 별도의 역할을 만듭니다.

이 정책을 사용하려면 정책 예제의 ##### ##를 본인의 정보로 대체합니다. 추가 지침은 [정책 생성](#) 또는 [정책 편집](#)을 참조하세요. 권한 정책은 다음 경로에 지정된 S3 위치에 대한 액세스 권한을 부여해야 합니다.

- i. 권한 정책:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket/*"
      ]
    }
  ]
}
```

```

        "Sid":
        "LakeFormationDataAccessPermissionsForS3ListBucket",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::Your-S3-Bucket"
        ]
    },
    {
        "Sid": "LakeFormationDataAccessServiceRolePolicy",
        "Effect": "Allow",
        "Action": [
            "s3:ListAllMyBuckets"
        ],
        "Resource": [
            "arn:aws:s3:::*"
        ]
    }
]
}

```

- ii. 신뢰 관계: 여기에는 신뢰할 수 있는 ID 전파에 필요한 `sts:SectContext`가 포함되어야 합니다.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}

```

}

Note

마법사에서 생성한 IAM 역할은 서비스 연결 역할이며 sts:SetContext를 포함하지 않습니다.

- d. IAM 역할을 생성했으면 위치 등록을 선택합니다.

Lake Formation을 통한 신뢰할 수 있는 ID 전파 AWS 계정

AWS Lake Formation 는 [AWS Resource Access Manager \(RAM\)](#)를 사용하여에서 테이블을 공유할 수 있도록 지원 AWS 계정 하며 AWS Organizations, 권한 부여자 계정과 피부여자 계정이 동일한 AWS 리전에 있는 경우 신뢰할 수 있는 자격 증명 전파와 함께 작동하고 IAM Identity Center의 동일한 조직 인스턴스를 공유합니다. 자세한 내용은 [Lake Formation에서의 교차 계정 데이터 공유](#)를 참조하세요.

IAM Identity Center를 사용한 Amazon S3 Access Grants 설정

[Amazon S3 Access Grants](#)는 S3 위치에 자격 증명에 기반한 세분화된 액세스 제어를 부여할 수 있는 유연성을 제공합니다. Amazon S3 Access Grants를 사용하여 회사 사용자 및 그룹에 Amazon S3 버킷 액세스 권한을 직접 부여할 수 있습니다. IAM Identity Center를 사용해 S3 Access Grants를 활성화하고 신뢰할 수 있는 ID 전파를 달성하려면 다음 단계를 따릅니다.

사전 조건

이 자습서를 시작하려면 먼저 다음을 설정해야 합니다.

- [IAM Identity Center를 활성화합니다. 조직 인스턴스](#)를 권장합니다. 자세한 내용은 [필수 조건 및 고려 사항](#) 단원을 참조하십시오.

IAM Identity Center를 통해 신뢰할 수 있는 ID 전파를 설정하기 위한 S3 Access Grants 구성

등록된 위치가 있는 Amazon S3 Access Grants 인스턴스가 이미 있는 경우 다음 단계를 따릅니다.

1. [IAM Identity Center 인스턴스를 연결합니다.](#)
2. [권한 부여를 생성합니다.](#)

Amazon S3 Access Grants를 아직 생성하지 않은 경우 다음 단계를 따릅니다.

1. [S3 Access Grants 인스턴스 생성](#) - 당 하나의 S3 Access Grants 인스턴스를 생성할 수 있습니다 AWS 리전. S3 Access Grants 인스턴스를 생성할 때 IAM Identity Center 인스턴스 추가 확인란을 선택하고 IAM Identity Center 인스턴스의 ARN을 입력해야 합니다. 다음을 선택합니다.

다음 이미지는 Amazon S3 Access Grants 콘솔의 S3 Access Grants 인스턴스 생성 페이지를 보여줍니다.

2. 위치 등록 - 계정의에서 [Amazon S3 Access Grants 인스턴스를 생성한](#) 후 해당 인스턴스에 [S3 위치를 등록](#) AWS 리전 합니다. S3 Access Grants 위치는 기본 S3 위치(S3://), 버킷 또는 접두사를 IAM 역할에 매핑합니다. S3 Access Grants는 이 Amazon S3 역할을 맡아 해당 특정 위치에 액세스하는 피부여자에게 임시 자격 증명을 제공합니다. 액세스 권한 부여를 생성하려면 먼저 S3 Access Grants 인스턴스에 위치를 하나 이상 등록해야 합니다.

위치 범위에는 해당 리전의 모든 버킷을 포함하는 s3://를 지정합니다. 이는 대부분의 사용 사례에 권장되는 위치 범위입니다. 고급 액세스 관리 사용 사례가 있는 경우 위치 범위를 특정 버킷 s3://*bucket* 또는 버킷 s3://*bucket/prefix-with-path* 내의 접두사로 설정할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [위치 등록](#)을 참조하세요.

Note

액세스 권한을 부여하려는 AWS Glue 테이블의 S3 위치가이 경로에 포함되어 있는지 확인합니다.

이 절차를 수행하려면 위치에 대해 IAM 역할을 구성해야 합니다. 이 역할에는 위치 범위에 액세스할 수 있는 권한이 포함되어야 합니다. S3 콘솔 마법사를 사용하여 이 역할을 생성할 수 있습니다.

이 IAM 역할의 정책에 S3 Access Grants 인스턴스 ARN을 지정해야 합니다. S3 Access Grants 인스턴스 ARN의 기본값은 `arn:aws:s3:Your-Region:Your-AWS-Account-ID:access-grants/default`입니다.

다음 예시 권한 정책은 생성한 IAM 역할에 Amazon S3 권한을 부여합니다. 그리고 그 뒤의 예시 신뢰 정책은 S3 Access Grants 서비스 위탁자가 IAM 역할을 맡을 수 있도록 허용합니다.

a. 권한 정책

이 정책을 사용하려면 정책 예제의 `#####` `#####` `###`를 본인의 정보로 대체합니다. 추가 지침은 [정책 생성](#) 또는 [정책 편집](#)을 참조하세요.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": [
        "arn:aws:s3::*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "ArnEquals": {
          "s3:AccessGrantsInstanceArn": [
            "arn:aws:s3:::access-grants/instance-id"
          ]
        }
      }
    }
  ],
  {
```

```

        "Sid": "ObjectLevelWritePermissions",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:PutObjectVersionAcl",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:AbortMultipartUpload"
        ],
        "Resource": [
            "arn:aws:s3:::*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceAccount": "111122223333"
            },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                ]
            }
        }
    },
    {
        "Sid": "BucketLevelReadPermissions",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceAccount": "111122223333"
            },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                ]
            }
        }
    }
},

```

```

    {
      "Sid": "OptionalKMSPermissionsForSSEEncryption",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

b. 신뢰 정책

IAM 역할 신뢰 정책에서 S3 Access Grants 서비스(access-grants.s3.amazonaws.com) 보안 주체에 생성한 IAM 역할에 대한 액세스 권한을 부여합니다. 이를 위해 다음 문이 포함된 JSON 파일을 생성할 수 있습니다. 계정에 신뢰 정책을 추가하려면 [사용자 지정 신뢰 정책을 사용하여 역할 생성](#)을 참조하세요.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-ARN"
        }
      }
    }
  ],
}

```

```

    {
      "Sid": "Stmt1234567891012",
      "Effect": "Allow",
      "Action": "sts:SetContext",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
        },
        "ForAllValues:ArnEquals": {
          "sts:RequestContextProviders":
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
        }
      }
    }
  ]
}

```

Amazon S3 액세스 권한 부여 생성

등록된 위치가 있는 Amazon S3 Access Grants 인스턴스가 있고 IAM Identity Center 인스턴스를 이와 연결한 경우 [권한 부여를 생성](#)할 수 있습니다. S3 콘솔 권한 생성 페이지에서 다음을 완료합니다.

권한 부여 생성

1. 이전 단계에서 생성한 위치를 선택합니다. 하위 접두사를 추가하여 권한 부여 범위를 줄일 수 있습니다. 하위 접두사는 버킷의 bucket, bucket/prefix 또는 객체일 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [하위 접두사](#)를 참조하세요.
2. 권한 및 액세스에서 필요에 따라 읽기 및 쓰기를 선택합니다.
3. 권한 부여자 유형에서 디렉터리 자격 증명 양식 IAM Identity Center를 선택합니다.
4. IAM Identity Center 사용자 또는 그룹 ID를 입력합니다. IAM Identity Center 콘솔의 [사용자 및 그룹 섹션](#)에서 사용자 및 그룹 ID를 찾을 수 있습니다. 다음을 선택합니다.
5. 검토 및 완료 페이지에서 S3 Access Grant에 대한 설정을 검토한 다음 권한 부여 생성을 선택합니다.

다음 이미지는 Amazon S3 Access Grants 콘솔의 권한 부여 생성 페이지를 보여줍니다.

Create Grant

Grant
Grant a user or role a specific level of access to your S3 data.

Grant scope
The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

Location
s3://
[Browse locations](#) [Register location](#)

Subprefix - optional
Further scope the grant to a bucket, prefix, or an individual object.
bucket-name/prefix/*
Don't include any part of the grant already specified in the location.
Format for bucket: <bucket>/*
Format for prefix: <bucket>/prefix-with-paths/*
Format for object: <bucket>/prefix-with-paths/subject/*

Grant scope
s3://
☐ The grant scope is an object

Permissions and access
Grant a user or role a specific level of access to your S3 data.
⚠ The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

Permissions
☒ Read
☐ Write

Grantee type
☒ Directory identity from IAM Identity Center
☐ IAM principal

Directory identity type
☐ User
☒ Group

IAM Identity Center group ID
The group that you want to grant this level of access to. You can find the ID in the [IAM Identity Center console](#).
Enter group ID: arn:aws:iam::123456789012:group/MyGroup

자체 OAuth 2.0 애플리케이션 설정

신뢰할 수 있는 자격 증명 전파를 통해 고객 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 수행한 작업 및 기타 이벤트는 서비스별 로그 및 CloudTrail 이벤트에 기록됩니다.

신뢰할 수 있는 ID 전파를 통해 사용자는 고객 관리형 애플리케이션에 로그인할 수 있고, 해당 애플리케이션은 AWS 서비스의 데이터에 액세스하기 위한 요청에 사용자의 ID를 전달할 수 있습니다.

⚠ Important

에 액세스하려면 AWS 서비스고객 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 토큰은에 대한 액세스 요청을 시작하는 애플리케이션 AWS 서비스 (애플리케이션 수신)에 권한을 부여합니다. 자세한 내용은 [신뢰할 수 있는 토큰 발급자를 사용하여 애플리케이션 사용](#) 단원을 참조하십시오.

주제

- [신뢰할 수 있는 ID 전파에 대해 고객 관리형 OAuth 2.0 애플리케이션 설정](#)
- [신뢰할 수 있는 애플리케이션 지정](#)

- [신뢰할 수 있는 토큰 발급자를 사용하여 애플리케이션 사용](#)

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 콘솔](#)을 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.

애플리케이션 타일 가시성 - 애플리케이션에 직접 또는 그룹 할당을 통해 할당된 사용자만 AWS 액세스 포털의 애플리케이션 가시성이 표시로 설정된 경우 AWS 액세스 포털에서 애플리케이션 타일을 볼 수 있습니다.

- 할당 불필요 - 모든 권한 부여된 IAM Identity Center 사용자 및 그룹이 이 애플리케이션에 액세스할 수 있도록 허용합니다.

애플리케이션 타일 가시성 - 애플리케이션 타일은 AWS 액세스 포털에 로그인하는 모든 사용자에게 표시됩니다. 단, AWS 액세스 포털의 애플리케이션 가시성이 표시되지 않음으로 설정된 경우는 예외입니다.

3. AWS 액세스 포털에서 사용자가 애플리케이션에 액세스할 수 있는 URL을 입력하고 애플리케이션 타일이 AWS 액세스 포털에 표시되는지 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 리소스 태그 지정](#) 섹션을 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 관리형 애플리케이션(수신 애플리케이션)에 대한 액세스 요청을 시작하는 애플리케이션(요청 애플리케이션)에 권한을 부여합니다.

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 방법](#)에서 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 내용은 [aud 클레임](#) 섹션을 참조하세요.
3. 사용자가 이 애플리케이션을 사용할 때 다시 인증할 필요가 없도록 하려면 새로 고침 토큰 권한 부여 활성화를 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 [CreateTokenWithIAM](#) API 작업이 필요합니다. 이 정책에 대한 자세한 내용과 해당 환경에 맞게 필요한 대로 조정하는 예시는 [IAM Identity Center에 대한 리소스 기반 정책 예시](#) 섹션을 참조하세요.

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 ARN](#)을 참조하세요.

- 정책을 수동으로 편집하려면(비AWS 자격 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 검증](#)을 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 자격 증명 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 내용은 [신뢰할 수 있는 애플리케이션 지정](#) 섹션을 참조하세요.

신뢰할 수 있는 애플리케이션 지정

[고객 관리형 애플리케이션을 설정한](#) 후에는 자격 증명 전파를 위해 하나 이상의 신뢰할 수 있는 AWS 서비스 또는 신뢰할 수 있는 애플리케이션을 지정해야 합니다. 고객 관리형 애플리케이션의 사용자가 액세스해야 하는 데이터가 있는 AWS 서비스를 지정합니다. 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 콘솔](#)을 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 애플리케이션에서 신뢰할 수 있는 자격 증명 전파를 사용할 수 있습니다 AWS. 신뢰할 수 있는 토큰 발급자를 사용하면 이러한 애플리케이션이

사용자를 대신하여 AWS 관리형 애플리케이션에 액세스하도록 요청할 수 있는 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](#)
- [ID 강화 IAM 역할 세션](#)

신뢰할 수 있는 토큰 발급자 개요

신뢰할 수 있는 자격 증명 전파는 외부에서 인증하는 애플리케이션이 신뢰할 수 있는 토큰 발급자를 사용하여 사용자를 대신하여 요청을 AWS 할 수 있도록 하는 메커니즘을 제공합니다. 신뢰할 수 있는 토큰 발급자는 서명된 토큰을 생성하는 OAuth 2.0 권한 부여 서버입니다. 이러한 토큰은에 대한 액세스 요청(애플리케이션 요청)을 시작하는 애플리케이션 AWS 서비스(애플리케이션 수신)에 권한을 부여합니다. 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 서비스 요청을 수신하는 Identity Center 디렉터리에 표시된 사용자 및 그룹 멤버십을 기반으로 리소스에 대한 세분화된 권한 부여를 관리합니다.는 외부 토큰 발급자의 토큰을 직접 사용할 AWS 서비스 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 권한 부여 서버(신뢰할 수 있는 토큰 발급자)를 구성해야 합니다. 신뢰할 수 있는 토큰 발급자는 일반적으로 IAM Identity Center의 ID 소스로 사용하는 ID 제공업체이지만 반드시 그럴 필요는 없습니다. 신뢰할 수 있는 토큰 발급자를 설정하는 방법에 대한 자세한 내용은 관련 ID 제공업체 설명서를 참조하세요.

i 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 내용은 [OIDC 검색 엔드포인트 URL\(발급자 URL\)](#) 섹션을 참조하세요.
- 신뢰할 수 있는 토큰 발급자가 발급한 토큰

신뢰할 수 있는 토큰 발급자의 토큰은 다음 요구 사항을 충족해야 합니다.

- 토큰은 서명되고 RS256 알고리즘을 사용한 [JSON 웹 토큰\(JWT\)](#) 형식이어야 합니다.
- 토큰에는 다음 클레임이 포함되어야 합니다.

- **발급자(iss)**-토큰을 발급한 엔터티입니다. 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 수신자입니다. 이 서비스는 토큰을 IAM Identity Center의 토큰으로 교환한 후 액세스할 수 있는 AWS 서비스입니다. 자세한 내용은 [aud 클레임](#) 단원을 참조하십시오.
- **만료 시간(exp)**-토큰이 만료된 이후의 시간입니다.
- 토큰은 ID 토큰 또는 액세스 토큰일 수 있습니다.
- 토큰에는 IAM Identity Center 사용자 한 명에게 고유하게 매핑될 수 있는 속성이 있어야 합니다.

Note

Microsoft Entra ID에서 발급한 JWT에 사용자 지정 서명 키를 사용하는 것은 지원되지 않습니다. 신뢰할 수 있는 토큰 발급자와 함께 Microsoft Entra ID에서 발급한 토큰을 사용하기 위해서는 사용자 지정 서명 키를 사용할 수 없습니다.

• 선택적 클레임

IAM Identity Center는 RFC 7523에 정의된 모든 선택적 클레임을 지원합니다. 자세한 내용은 이 RFC의 [섹션 3: JWT 형식 및 처리 요구 사항](#)을 참조하세요.

예를 들어 토큰에는 [JTI\(JWT ID\) 클레임](#)이 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 정보](#)의 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 사용자에게 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.

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 *.well-known/openid-configuration*까지, 없이 붙여 넣기해야 합니다. *.well-known/openid-configuration* 항목이 URL에 포함된 경우 신뢰할 수 있는 토큰 발급자 구성이 작동하지 않습니다. IAM Identity Center는 이 URL을 검증하지 않으므로 URL이 올바르게 구성되지 않으면 알림 없이 신뢰할 수 있는 토큰 발급자 설정이 실패합니다.

OIDC 검색 엔드포인트 URL은 포트 80 및 443을 통해서만 연결할 수 있어야 합니다.

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()에 대한 요청을 시작하도록 승인합니다 AWS 서비스.

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 신뢰할 수 있는 토큰 발급자를 설정하고 이를 사용하도록 AWS 서비스를 구성하는 방법을 설명합니다.

Note

애플리케이션은 IAM Identity Center와 통합되고 신뢰할 수 있는 자격 증명 전파를 지원하는 모든 AWS 서비스일 수 있습니다.

자세한 내용은 [신뢰할 수 있는 토큰 발급자 설정 작업](#) 단원을 참조하십시오.

Role	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 Center 관리자 AWS 서비스 관리자

Role	다음 작업 수행	협력 당사자
	IAM Identity Center와 외부 IdP 간에 올바른 속성 매핑을 설정하는 데 도움을 줍니다. AWS 서비스 관리자에게 대상 이름 (Aud 클레임)을 제공합니다.	
AWS 서비스 관리자	AWS 서비스 콘솔에서 신뢰할 수 있는 토큰 발급자를 확인합니다. IAM Identity Center 관리자가 IAM Identity Center 콘솔에 추가하면 신뢰할 수 있는 토큰 발급자가 AWS 서비스 콘솔에 표시됩니다. 신뢰할 수 있는 토큰 발급자를 사용하여 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 자격 증명 전파를 지원하는 모든 AWS 서비스일 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 이름입니다.
 - OIDC 검색 엔드포인트 URL(IAM Identity Center 콘솔에서 이 URL은 발급자 URL이라고 함). 검색 엔드포인트는 포트 80 및 443을 통해서만 연결할 수 있어야 합니다.

- 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. IAM Identity Center에 AWS 서비스 연결 - AWS 서비스 관리자는 애플리케이션용 콘솔 또는 애플리케이션 APIs를 사용하여 애플리케이션을 IAM Identity Center에 연결해야 합니다.

신뢰할 수 있는 토큰 발급자가 IAM Identity Center 콘솔에 추가되면 AWS 서비스 콘솔에도 표시되며 AWS 서비스 관리자가 선택할 수 있습니다.

3. 토큰 교환 사용 구성 - AWS 서비스 콘솔에서 AWS 서비스 관리자는 신뢰할 수 있는 토큰 발급자가 발급한 토큰을 수락하도록 AWS 서비스를 구성합니다. 이러한 토큰은 IAM Identity Center에서 생성한 토큰으로 교환됩니다. 이를 위해서는 1단계에서 신뢰할 수 있는 토큰 발급자의 이름과 AWS 서비스에 해당하는 Aud 클레임 값을 지정해야 합니다.

신뢰할 수 있는 토큰 발급자는 발급된 토큰에 Aud 클레임 값을 배치하여 토큰이 AWS 서비스에서 사용하기 위한 것임을 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 콘솔](#)을 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 위해 토큰을 발급할 외부 IdP의 [OIDC 검색 URL](#)을 지정합니다. 검색 엔드포인트의 URL을 `.well-known/openid-configuration`까지 (제외) 지정해야 합니다. 외부 IdP 관리자가 이 URL을 제공할 수 있습니다.

Note

참고로 이 URL은 신뢰할 수 있는 ID 전파를 위해 발급된 토큰의 발급자(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 리소스 태그 지정](#) 섹션을 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.

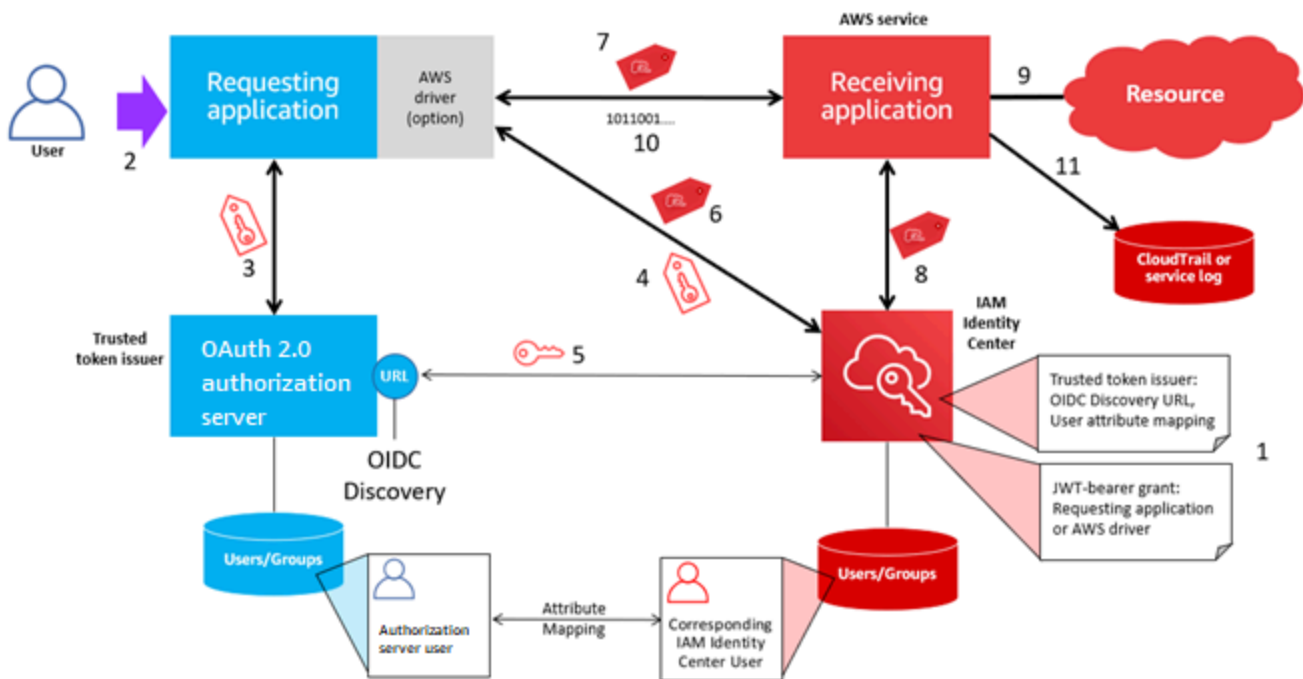
IAM Identity Center 콘솔에서 신뢰할 수 있는 토큰 발급자 설정 보기 또는 편집

1. [IAM Identity Center 콘솔](#)을 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 저장을 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. 신뢰할 수 있는 토큰 발급자를 사용하도록 IAM Identity Center 및 수신 AWS 관리형 애플리케이션을 설정합니다. 자세한 내용은 [신뢰할 수 있는 토큰 발급자 설정 작업](#) 단원을 참조하세요.
2. 요청 흐름은 사용자가 요청 애플리케이션을 열 때 시작됩니다.

3. 요청 애플리케이션은 수신 AWS 관리형 애플리케이션에 대한 요청을 시작하기 위해 신뢰할 수 있는 토큰 발급자로부터 토큰을 요청합니다. 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. 요청 애플리케이션 또는 사용하는 AWS 드라이버는 토큰을 IAM Identity Center에 전달하고 토큰을 IAM Identity Center에서 생성한 토큰으로 교환하도록 요청합니다. AWS 드라이버를 사용하는 경우 이 사용 사례에 맞춰 드라이버를 구성해야 할 수 있습니다. 자세한 내용은 관련 AWS 관리형 애플리케이션에 대한 설명서를 참조하세요.
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. AWS 관리형 애플리케이션이 사용자 및 그룹에 할당해야 하도록 구성된 경우 사용자에게 애플리케이션에 대한 직접 또는 그룹 기반 할당이 있어야 합니다. 그렇지 않으면 요청이 거부됩니다. AWS 관리형 애플리케이션이 사용자 및 그룹 할당이 필요하지 않도록 구성된 경우 처리가 계속됩니다.

 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 애플리케이션이 수신 AWS 관리형 애플리케이션에 유효한 범위를 사용하도록 구성되어 있는지 확인합니다.
6. 이전 확인 단계가 성공적이면 IAM Identity Center에서 새 토큰을 생성합니다. 새 토큰은 IAM Identity Center에서 해당 사용자의 자격 증명, 수신 AWS 관리형 애플리케이션의 대상(Aud) 및 요청 애플리케이션이 수신 AWS 관리형 애플리케이션에 요청할 때 사용할 수 있는 범위를 포함하는 불투명한(암호화된) 토큰입니다.

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 수행한 작업 및 기타 이벤트는 수신 애플리케이션 로그 및 CloudTrail 이벤트에 기록됩니다. 이 정보가 로깅되는 구체적인 방법은 애플리케이션에 따라 다릅니다.

ID 강화 IAM 역할 세션

[AWS Security Token Service\(STS\)](#)를 사용하면 애플리케이션이 ID 강화 IAM 역할 세션을 획득할 수 있습니다. 자격 증명 강화 역할 세션에는 호출하는 데 사용자 식별자를 전달하는 자격 증명 컨텍스트 AWS 서비스 가 추가되었습니다. AWS 서비스 는 IAM Identity Center에서 사용자의 그룹 멤버십 및 속성을 조회하고 이를 사용하여 리소스에 대한 사용자의 액세스 권한을 부여할 수 있습니다.

AWS 애플리케이션은 AWS STS [AssumeRole](#) API 작업을 요청하고 요청의 ProvidedContexts 파라미터에서 사용자의 식별자(userId)를 사용하여 컨텍스트 어설션에 전달하여 자격 증명 강화 역할 세션을 얻습니다. AssumeRole. 컨텍스트 어설션은 SSO OIDC에 [CreateTokenWithIAM](#)을 요청할 때 응답으로 수신된 idToken 클레임에서 획득합니다. AWS 애플리케이션이 자격 증명 강화 역할 세션을 사용하여 리소스에 액세스하는 경우 CloudTrail은 userId, 시작 세션 및 수행된 작업을 로깅합니다. 자세한 내용은 [ID 강화 IAM 역할 세션 로그](#) 단원을 참조하십시오.

주제

- [ID 강화 IAM 역할 세션의 유형](#)
- [ID 강화 IAM 역할 세션 로그](#)

ID 강화 IAM 역할 세션의 유형

AWS STS 는 AssumeRole 요청에 제공된 컨텍스트 어설션에 따라 두 가지 유형의 자격 증명 강화 IAM 역할 세션을 생성할 수 있습니다. IAM Identity Center에서 ID 토큰을 획득한 애플리케이션은 IAM 역할 세션에 sts:identiy_context(권장) 또는 sts:audit_context(이전 버전과의 호환성 지원)

를 추가할 수 있습니다. ID 강화 IAM 역할 세션에는 이러한 컨텍스트 어설션 중 하나만 있을 수 있으며 둘 다 있을 수는 없습니다.

sts:identity_context로 생성된 ID 강화 IAM 역할 세션

ID 강화 역할 세션에 sts:identity_context가 포함되어 있으면 직접적으로 호출된 AWS 서비스는 리소스 권한 부여가 역할 세션에 나타난 사용자를 기반으로 할지, 아니면 역할을 기반으로 할지를 결정합니다. 사용자 기반 권한 부여를 지원하는 AWS 서비스는 애플리케이션의 관리자에게 사용자 또는 사용자가 멤버인 그룹에 액세스 권한을 할당할 수 있는 제어권을 제공합니다.

AWS 서비스 사용자 기반 권한 부여를 지원하지 않는 것을 무시합니다 sts:identity_context. CloudTrail 로그는 역할이 수행한 모든 작업과 함께 IAM Identity Center 사용자의 userId를 기록합니다. 자세한 내용은 [ID 강화 IAM 역할 세션 로그](#) 단원을 참조하십시오.

이러한 유형의 자격 증명 강화 역할 세션을 얻기 위해 AWS STS 애플리케이션은 요청 파라미터를 사용하여 [AssumeRole](#) ProvidedContexts 요청에 sts:identity_context 필드 값을 제공합니다. arn:aws:iam::aws:contextProvider/IdentityCenter를 ProviderArn의 값으로 사용합니다.

권한 부여의 작동 방식에 대한 자세한 내용은 수신 설명서를 참조하세요 AWS 서비스.

sts:audit_context로 생성된 ID 강화 IAM 역할 세션

과거에는 sts:audit_context가 권한 부여 결정을 내리는 데 사용하지 않고 사용자 자격 증명을 AWS 서비스 로깅할 수 있도록 했습니다. 이제 AWS 서비스는 단일 컨텍스트 - sts:identity_context를 사용하여 이를 달성하고 권한 부여 결정을 내릴 수 있습니다. 신뢰할 수 있는 ID 전파의 모든 새 배포에서 sts:identity_context를 사용하는 것이 좋습니다.

ID 강화 IAM 역할 세션 로그

자격 증명 강화 IAM 역할 세션을 AWS 서비스 사용하여 요청을 하면 사용자의 IAM Identity Center userId가 OnBehalfOf 요소의 CloudTrail에 로깅됩니다. 이벤트가 CloudTrail에 기록되는 방식은 AWS 서비스에 따라 다릅니다. 모든 AWS 서비스 항목이 onBehalfOf 요소를 기록하지는 않습니다.

다음은 ID 강화 역할 세션을 사용하여 AWS 서비스에 대한 요청이 CloudTrail에 기록되는 방법의 예입니다.

```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROEXAMPLE:MyRole",
  "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
```

```

    "accountId": "111111111111",
    "accessKeyId": "ASIAEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLE",
        "arn": "arn:aws:iam::111111111111:role/MyRole",
        "accountId": "111111111111",
        "userName": "MyRole"
      },
      "attributes": {
        "creationDate": "2023-12-12T13:55:22Z",
        "mfaAuthenticated": "false"
      }
    },
    "onBehalfOf": {
      "userId": "11111111-1111-1111-1111-111111111111",
      "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/d-1111111111"
    }
  }
}

```

IAM Identity Center 인증서 교체

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.

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 교체](#)에 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 인증서 생성

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 크기](#)를 참조하세요.
- 알고리즘 - SAML 어설션/응답에 서명할 때 IAM Identity Center에서 사용하는 알고리즘을 지정합니다. 서비스 공급자가 SHA-1을 요구하지 않는 한 가능하면 SHA-256을 사용하여 이 값을 SHA-1 또는 SHA-256. AWS recommends로 설정할 수 있습니다. SHA-256 암호화 알고리즘의 작동 방식에 대한 일반 정보는 [공개 키 암호화](#)를 참조하세요.

1. [IAM Identity Center 콘솔](#)을 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 사이트 업데이트

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 콘솔](#)에서 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 설정

애플리케이션에는 인증서를 최대 2개까지 할당할 수 있습니다. IAM Identity Center에서는 활성으로 설정된 인증서를 사용하여 모든 SAML 어설션을 서명합니다.

1. [IAM Identity Center 콘솔](#)을 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 인증서 삭제

다음 절차를 사용하여 애플리케이션의 인증서 교체 프로세스를 완료합니다. 비활성 상태인 인증서만 삭제할 수 있습니다.

1. [IAM Identity Center 콘솔](#)을 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

IAM Identity Center 콘솔의 애플리케이션 페이지에는 각 애플리케이션의 속성에 상태 표시기 아이콘이 표시됩니다. 이러한 아이콘은 목록의 각 인증서 옆에 있는 만료 날짜 옆에 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.

인증서의 현재 상태 확인 방법

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. [Applications]를 선택합니다.
3. 애플리케이션 목록에서 만료 날짜 옆에 표시된 대로 목록에 있는 인증서 상태를 검토하세요.

IAM Identity Center 콘솔의 애플리케이션 속성 이해

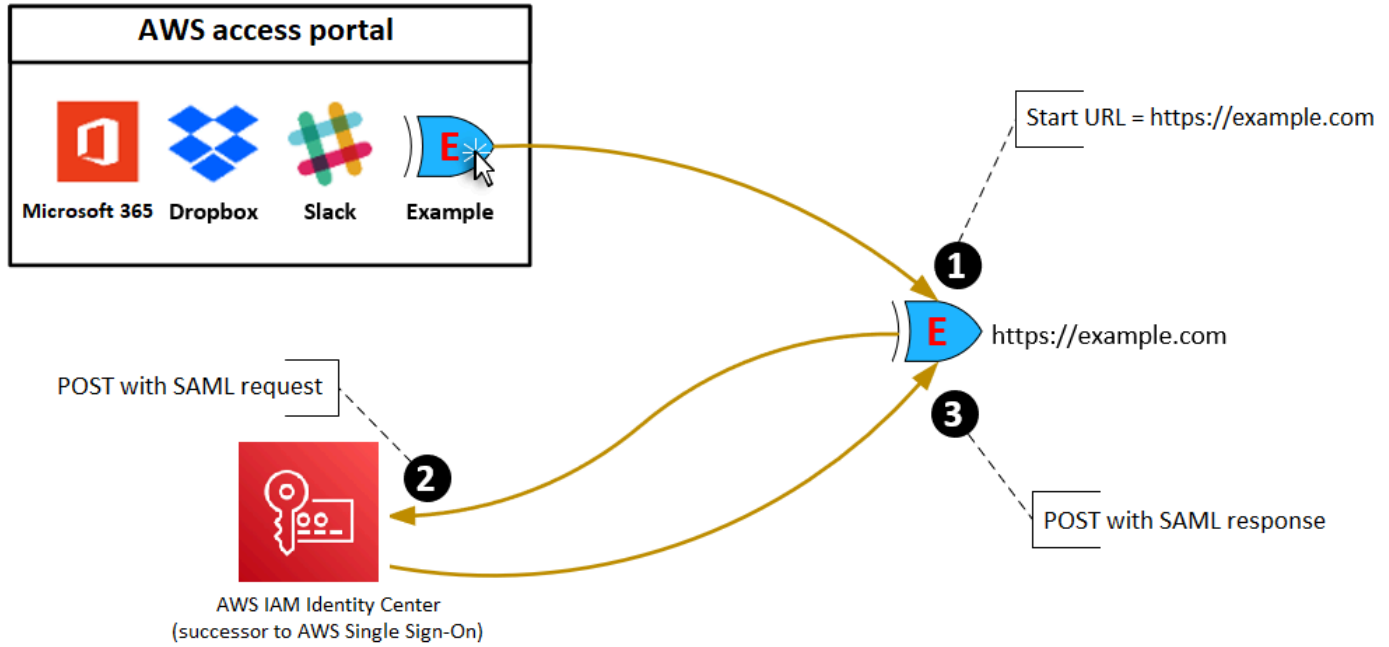
IAM Identity Center에서 애플리케이션 시작 URL, 릴레이 상태 및 세션 기간을 구성하여 사용자 경험을 최적화할 수 있습니다.

애플리케이션 시작 URL

애플리케이션 시작 URL을 사용하여 애플리케이션과의 페더레이션 프로세스를 시작합니다. 일반적으로 SP(서비스 제공업체) 초기 바인딩만 지원하는 애플리케이션에 사용됩니다.

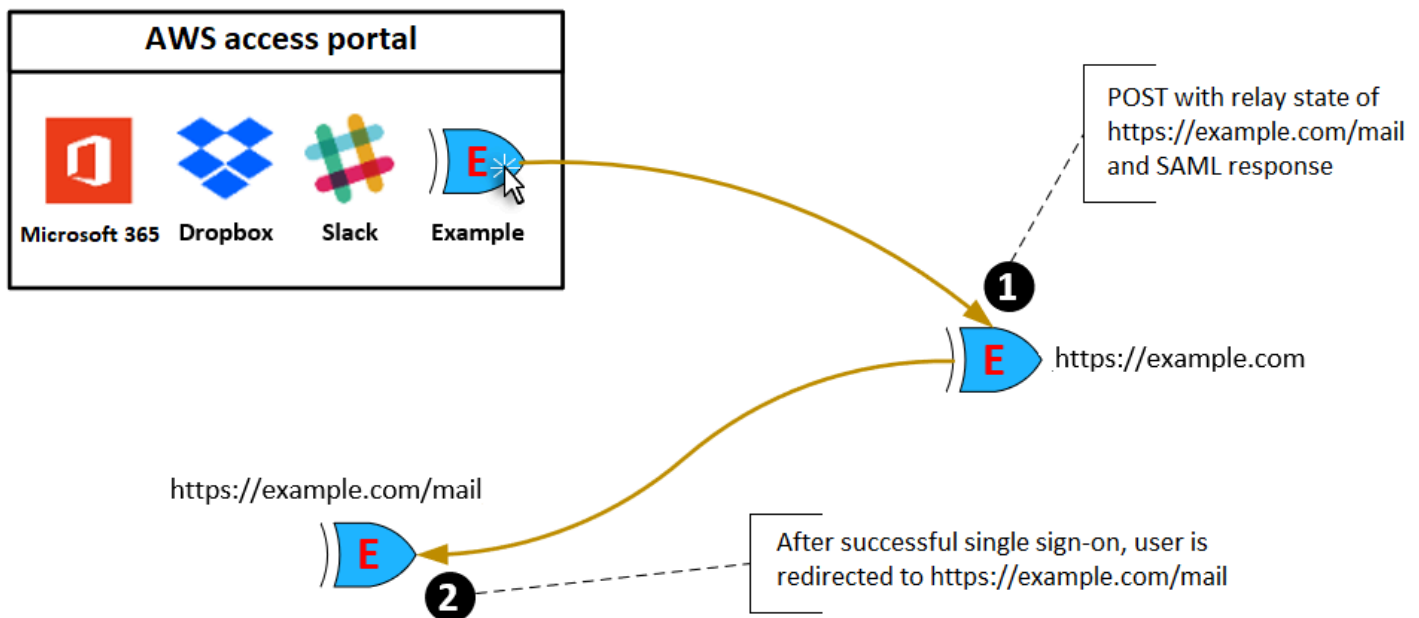
다음 단계와 다이어그램은 사용자가 AWS 액세스 포털에서 애플리케이션을 선택할 때의 애플리케이션 시작 URL 인증 워크플로를 보여줍니다.

1. 사용자 브라우저는 애플리케이션 시작 URL(이 경우 <https://example.com>)의 값을 사용하여 인증 요청을 리디렉션합니다.
2. 애플리케이션은 SAMLRequest와 함께 IAM Identity Center로 HTML POST를 전송합니다.
3. 그런 다음 IAM Identity Center는 SAMLResponse와 함께 애플리케이션으로 HTML POST를 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 수도 있습니다. 사용자가 구성원으로 속해 있는 직속 그룹을 대상으로 할당해야 합니다.

애플리케이션에 사용자 또는 액세스 할당

Important

AWS 관리형 애플리케이션의 경우 관련 애플리케이션 콘솔 내에서 직접 또는 APIs.

1. [IAM Identity Center 콘솔](#)을 엽니다.

Note

에서 사용자를 관리하는 경우 다음 단계를 수행하기 전에 IAM Identity Center 콘솔이 AWS Managed Microsoft AD 디렉터리가 위치한 AWS 리전을 사용하고 있는지 AWS Managed Microsoft AD 확인합니다.

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 표시 이름 또는 그룹 이름을 입력합니다. 검색 결과에 나타나는 해당 계정을 선택하여 여러 사용자 또는 그룹을 지정할 수 있습니다.
6. 사용자 배정을 선택합니다.

SAML 2.0 애플리케이션에 대한 사용자 액세스 제거

이 절차를 사용하여 애플리케이션 카탈로그의 SAML 2.0 애플리케이션 또는 사용자 지정 SAML 2.0 애플리케이션에 대한 사용자 액세스를 제거합니다. 인증 세션 및 기간에 대한 자세한 내용은 [IAM Identity Center의 인증 세션 이해](#) 섹션을 참조하세요.

애플리케이션에서 사용자 액세스 제거

1. [IAM Identity Center 콘솔](#)을 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 콘솔](#)을 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 [IAM Identity Center와 외부 ID 제공업체 디렉터리 간의 속성 매핑](#)의 표를 참조하세요.
8. 표의 세 번째 열에 있는 메뉴에서 속성에 적합한 형식을 선택합니다.

9. 변경 사항 저장를 선택합니다.

에 대한 액세스 구성 AWS 계정

AWS IAM Identity Center 는와 통합되어 AWS Organizations 각 계정을 수동으로 구성 AWS 계정 하지 않고도 여러에서 권한을 중앙에서 관리할 수 있습니다. 권한을 정의하고 작업 인력 사용자에게 이러한 권한을 할당하여 IAM Identity Center의 [조직 인스턴스](#)를 AWS 계정 사용하여 특정에 대한 액세스를 제어할 수 있습니다. IAM Identity Center의 [계정 인스턴스](#)는 계정 액세스를 지원하지 않습니다.

AWS 계정 유형

에는 두 가지 유형의가 AWS 계정 있습니다 AWS Organizations.

- 관리 계정 - 조직을 생성하는 데 AWS 계정 사용되는 입니다.
- 멤버 계정 - 조직에 AWS 계정 속한 나머지 입니다.

AWS 계정 유형에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [AWS Organizations 용어 및 개념을 참조하세요](#).

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](#) 섹션을 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
사용자 액세스 활성화 또는 비활성화	☒ 아니요	☑ 예	☑ 예

IAM Identity Center 관리 작업	멤버 계정	위임된 관리자 계정	관리 계정
수신 속성을 활성화, 비활성화 또는 관리합니다.	⊗ 아니요	✔ 예	✔ 예
ID 소스 변경 또는 관리	⊗ 아니요	✔ 예	✔ 예
고객 관리형 애플리케이션 생성, 편집 또는 삭제	⊗ 아니요	✔ 예	✔ 예
AWS 관리형 애플리케이션 생성, 편집 또는 삭제	✔ 예	✔ 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 활성화	⊗ 아니요	⊗ 아니요	✔ 예
IAM Identity Center 구성 삭제	⊗ 아니요	⊗ 아니요	✔ 예
관리 계정에서 사용자 액세스를 활성화 또는 비활성화합니다.	⊗ 아니요	⊗ 아니요	✔ 예

IAM Identity Center 관리 작업	멤버 계정	위임된 관리자 계정	관리 계정
위임된 관리자로 멤버 계정 등록 또는 등록 해지	⊗ 아니요	⊗ 아니요	⊙ 예

*관리 계정에 대한 사용자 및 그룹 할당과 관련한 위임된 관리 모범 사례를 참조하세요.

AWS 계정 액세스 할당

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 세트를 생성하여 조직 AWS 계정 내 여러에 할당할 수 있습니다. 동일한 사용자에게 여러 권한 집합을 할당할 수도 있습니다.

권한에 대한 자세한 내용은 [권한 세트 생성, 관리 및 삭제](#) 섹션을 참조하세요.

Note

사용자에게 애플리케이션에 대한 Single Sign-On 액세스 권한을 할당할 수도 있습니다. 자세한 내용은 [애플리케이션에 대한 액세스 구성](#) 섹션을 참조하세요.

최종 사용자 경험

AWS 액세스 포털은 IAM Identity Center 사용자에게 웹 포털을 통해 할당된 모든 AWS 계정 및 애플리케이션에 대한 Single Sign-On 액세스를 제공합니다. AWS 액세스 포털은 AWS 리소스 관리를 위한 서비스 콘솔 모음 [AWS Management Console](#)인과 다릅니다.

권한 세트를 생성하면 권한 세트에 대해 지정한 이름이 AWS 액세스 포털에 사용 가능한 역할로 표시됩니다. 사용자는 AWS 액세스 포털에 로그인하여를 선택한 AWS 계정다음 역할을 선택합니다. 역할을 선택한 후를 사용하여 AWS 서비스에 액세스 AWS Management Console 하거나 임시 자격 증명을 검색하여 프로그래밍 방식으로 AWS 서비스에 액세스할 수 있습니다.

를 열 AWS Management Console 거나 프로그래밍 방식으로에 액세스할 AWS 수 있는 임시 자격 증명을 검색하려면 사용자는 다음 단계를 완료합니다.

1. 사용자는 브라우저 창을 열고 사용자가 제공한 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 액세스 권한이 AWS 계정 있는 목록을 표시합니다.
4. 그런 다음 사용자는 사용하려는 AWS 계정 를 선택합니다.
5. 의 이름 아래 사용자가 할당된 AWS 계정모든 권한 세트가 사용 가능한 역할로 표시됩니다. 예를 들어 PowerUser 권한 세트john_styles에 사용자를 할당한 경우 AWS 액세스 포털에 역할이 표시됩니다PowerUser/john_styles. 여러 권한 집합이 할당된 사용자는 사용할 역할을 선택합니다. 사용자는 자신의 역할을 선택하여 AWS Management Console에 액세스할 수 있습니다.
6. 역할 외에도 AWS 액세스 포털 사용자는 액세스 키를 선택하여 명령줄 또는 프로그래밍 방식의 액세스에 대한 임시 자격 증명을 검색할 수 있습니다.

직원 사용자에게 제공할 수 있는 단계별 지침은 [AWS 액세스 포털 설정 및 사용](#) 및 [AWS CLI AWS SDKs에 대한 IAM Identity Center 사용자 자격 증명 가져오기](#) 섹션을 참조하세요.

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 AWS 서비스에 직접 연결된 일종의 IAM 역할입니다. IAM Identity Center를 활성화한 후 IAM Identity Center는 조직의 각에 서비스 연결 역할을 생성할 수 AWS 계정 있습니다. 이 역할은 IAM Identity Center가 조직의 특징에 대한 Single Sign-On 액세스 권한이 있는 사용자를 위임하고 적용할 AWS 계정 수 있는 사전 정의된 권한을 제공합니다 AWS Organizations. 이 역할을 사용하려면 계정에 대한 액세스 권한을 가진 한 명 이상의 사용자를 할당해야 합니다. 자세한 내용은 [IAM Identity Center 서비스 연결 역할 파악](#) 및 [IAM Identity Center 서비스 연결 역할 사용](#) 섹션을 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 승인 참조의 [AWS IAM](#)

[Identity Center 디렉터리에 사용되는 작업, 리소스 및 조건 키](#)와 [AWS Identity Store에 사용되는 작업, 리소스 및 조건 키](#)를 참조하세요.

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

AWS 관리형 애플리케이션이 IAM Identity Center와 잘 작동하도록 하려면 해당 애플리케이션을 배포 AWS 계정 한에이 SCP를 적용하지 않아야 합니다. 또한 위임된 관리를 사용하는 경우 위임된 관리 계정에 이 SCP를 적용하지 않아야 합니다. 자세한 내용은 [모범 사례](#) 단원을 참조하십시오.

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 Identity Center를 활성화하면 AWS Organizations 기본적 으로의 관리 계정에 IAM Identity Center 인스턴스가 생성됩니다. 이는 원래 IAM Identity Center가 조직의 모든 멤버 계정에서 역할을 프로비저닝, 프로비저닝 해제 및 업데이트할 수 있도록 이러한 방식으로 설계되었습니다. IAM Identity Center 인스턴스는 항상 관리 계정에 있어야 하지만의 멤버 계정에 IAM Identity Center 관리를 위임하여 관리 계정 외부에서 IAM Identity Center를 관리하는 기능을 AWS Organizations 확장할 수 있습니다.

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 섹션을 [AWS Organizations참조하세요](#)에 대한 [액세스 구성 AWS 계정](#). 추가 정보를 확인하고 위임 관리를 구성하는 방법을 보여주는 예제 회사 시나리오를 검토하려면 AWS 보안 블로그의 [IAM Identity Center 위임 관리 시작하기](#)를 참조하세요.

주제

- [모범 사례](#)
- [사전 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. 필요한 경우에만 [임시 승격 액세스](#)를 사용하여 이 액세스 권한을 부여하는 것을 고려할 수도 있습니다.
- 관리 계정에 대한 전용 권한 세트 - 관리 계정에 대한 전용 권한 세트를 사용합니다. 보안상의 이유로 관리 계정에 액세스하는 데 사용되는 권한 세트는 관리 계정의 IAM Identity Center 관리자만 수정할 수 있습니다. 위임된 관리자는 관리 계정에 프로비저닝된 권한 세트를 변경할 수 없습니다.
- 관리 계정의 권한 세트에 사용자만 할당(그룹 아님) - 관리 계정에는 특별한 권한이 있으므로 콘솔 또는 AWS Command Line Interface (CLI)에서이 계정에 대한 액세스를 할당할 때 주의해야 합니다. 관리 계정에 액세스할 수 있는 권한 세트에 그룹을 할당하면 해당 그룹의 멤버십을 수정할 수 있는 권한이 있는 모든 이가 해당 그룹에 사용자를 추가/제거하여 관리 계정에 액세스할 수 있는 사용자에게 영향을 미칠 수 있습니다. 이는 ID 제공업체(IdP) 관리자, Microsoft Active Directory 도메인 서비스(AD DS) 관리자 또는 IAM Identity Center 관리자를 포함해 ID 소스를 제어할 수 있는 모든 그룹 관리자입니다. 따라서 관리 계정에서 액세스 권한을 부여하는 권한 세트에 사용자를 직접 할당하고 그룹은 할당하지 않아야 합니다. 그룹을 사용하여 관리 계정에 대한 액세스를 관리하는 경우 IdP에 적절한 제어 수단이 마련되어 있어서 이러한 그룹을 수정할 수 있는 자를 제한하고 필요에 따라 해당 그룹에 대한 변경 사항(또는 관리 계정 내 사용자의 자격 증명에 대한 변경 사항)을 로깅하고 검토해야 합니다.
- 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 멤버 계정(있는 경우)에 있어야 합니다. Active Directory가 관리 계정에 있도록 하려면 위임된 관리자에게 이를 완료하는 데 필요한 권한이 없으므로 관리 계정에서 설정을 수행해야 합니다.

외부 ID 소스를 사용하여 위임된 관리 계정의 IAM Identity Center 자격 증명 스토어 작업 제한

IdP 또는와 같은 외부 ID 소스를 사용하는 경우 IAM Identity Center 관리자가 위임된 관리 계정 내에서 수행할 수 있는 ID 스토어 작업을 제한하는 정책을 구현 Directory Service해야 합니다. 쓰기 및 삭제 작업은 신중하게 고려해야 합니다. 일반적으로 외부 ID 소스는 사용자와 그 속성, 그리고 그룹 멤버십에 대한 신뢰할 수 있는 소스입니다. 자격 증명 스토어 API 또는 콘솔을 사용하여 이를 수정하면 일반 동기화 주기 중에 변경 사항을 덮어씁니다. 이러한 작업은 신뢰할 수 있는 ID 소스에서 전적으로 제어하도록 하는 것이 가장 좋습니다. 이렇게 하면 IAM Identity Center 관리자가 그룹 멤버십 제어 권한을 IdP 관리자에게 두지 않고 그룹 멤버십을 수정하여 그룹에 할당된 권한 세트 또는 애플리케이션에 대한 액세스 권한을 임의로 부여하는 것도 방지됩니다. 또한 위임된 관리 계정에서 SCIM 보유자 토큰을 생성할 수 있는 자도 제한해야 하는데, 그 이유는 멤버 계정 관리자가 SCIM 클라이언트를 통해 그룹 및 사용자를 수정할 수 있기 때문입니다.

위임된 관리자 계정에서 쓰기 또는 삭제 작업이 적절한 경우가 있을 수 있습니다. 예를 들어 멤버를 추가하지 않고 그룹을 생성한 다음 IdP 관리자가 그룹을 생성할 때까지 기다릴 필요 없이 권한 세트에 할당할 수 있습니다. IdP 관리자가 그룹을 프로비저닝하고 IdP 동기화 프로세스가 그룹 멤버를 설정할 때까지는 아무도 해당 할당에 액세스할 수 없습니다. IdP 동기화 프로세스로 사용자 또는 그룹의 액세스가 제거될 때까지 기다릴 수 없는 상황이라면 사용자 또는 그룹을 삭제하여 로그인 또는 권한 부여를 방지하는 것이 적절할 수도 있습니다. 그러나 이 권한을 오용하면 사용자에게 방해가 될 수 있습니다. 자격 증명 스토어 권한을 할당할 때는 최소 권한 원칙을 적용해야 합니다. 서비스 제어 정책(SCP)을 사용하면 위임된 관리 계정 관리자가 허용할 자격 증명 스토어 작업을 제어할 수 있습니다.

아래 예제 SCP는 Identity Store API 및를 통해 그룹에 사용자를 할당하는 것을 방지하며 AWS Management Console, 이는 ID 소스가 외부일 때 권장됩니다. 이는 외부 IdP(SCIM을 통해)와의 사용자 동기화 Directory Service 에는 영향을 주지 않습니다.

Note

외부 ID 소스를 사용하더라도 조직은 사용자 및 그룹을 프로비저닝하기 위해 자격 증명 스토어 API에 전적으로 또는 부분적으로 의존할 수 있습니다. 따라서 이 SCP를 활성화하기 전에 사용자 프로비저닝 프로세스가 이 자격 증명 스토어 API 작업을 사용하지 않는지 확인해야 합니다.

그룹 멤버십 관리를 특정 그룹으로 제한하는 방법에 대한 자세한 내용은 다음 섹션을 참조하세요.

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

관리 계정에 액세스 권한을 부여하는 그룹에게만 사용자를 추가하지 못하게 하려면 그룹 ARN을 사용하여 `arn:${Partition}:identitystore:::group/${GroupId}` 형식으로 해당 특정 그룹을 참조할 수 있습니다. Identity Store에서 사용할 수 있는 이 리소스 유형과 기타 리소스 유형은 서비스 승인 참조의 [AWS Identity Store에서 정의한 리소스 유형에](#) 문서화되어 있습니다. SCP에 추가 자격 증명 스토어 API를 포함하는 것도 고려할 수 있습니다. 자세한 내용은 자격 증명 스토어 API 참조의 [작업](#)을 참조하세요.

SCP에 다음 정책 문을 추가하면 위임된 관리자가 SCIM 보유자 토큰을 생성하지 못하도록 할 수 있습니다. 이는 두 외부 ID 소스 모두에 적용할 수 있습니다.

Note

위임된 관리자가 SCIM으로 사용자 프로비저닝을 설정해야 하거나 정기적인 SCIM 보유자 토큰 교환을 수행해야 하는 경우 위임된 관리자가 해당 작업을 완료할 수 있도록 이 API에 대한 액세스를 일시적으로 허용해야 합니다.

```
{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}
```

로컬에서 관리되는 사용자에게 대한 위임된 관리 계정에서 IAM Identity Center 작업 증명 스토어 작업 제한

외부 IdP를 사용하는 대신 IAM Identity Center에서 직접 사용자 및 그룹을 생성하는 경우 사용자를 생성하고 Directory Service, 암호를 재설정하고, 그룹 멤버십을 제어할 수 있는 사용자에게 대한 예방 조치를 취해야 합니다. 이러한 작업은 로그인할 수 있는 자와 그룹의 멤버십을 통해 액세스 권한을 가질 수 있는 자에 대해 관리자에게 큰 권한을 부여합니다. 이러한 정책은 SCP가 아닌 IAM Identity Center 관리자에게 사용하는 권한 세트 내에서 인라인 정책으로 구현하는 것이 가장 좋습니다. 다음 예시 인라인 정책에는 두 가지 목표가 있습니다. 첫째, 특정 그룹에 사용자를 추가하지 못하도록 하는 것입니다. 이를 통해 위임된 관리자가 관리 계정에 대한 액세스 권한을 부여하는 그룹에 사용자를 추가하지 못하도록 할 수 있습니다. 둘째, SCIM 보유자 토큰의 발급을 방지하는 것입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ arn:${Partition}:identitystore::group/${GroupId1},
                    arn:${Partition}:identitystore::group/${GroupId2}
                  ]
    },
    { "Effect": "Deny",
      "Action": ["sso-directory:CreateBearerToken"],
      "Resource": [ "*" ] }
  ]
}
```

PermissionSet 관리에서 IAM Identity Center 구성 관리 분리

관리 계정에서 별도의 관리자 권한 세트를 생성하여 외부 ID 소스 수정, SCIM 토큰 관리, 세션 제한 시간 구성을 포함한 관리 작업과 권한 세트를 생성, 수정, 할당하는 작업을 분리합니다.

SCIM 보유자 토큰 발급 제한

SCIM 보유자 토큰을 사용하면 IAM Identity Center의 ID 소스가 Okta 또는 Entra ID와 같은 외부 IdP일 때 외부 ID 소스가 SCIM 프로토콜을 통해 사용자, 그룹, 그룹 멤버십을 프로비저닝할 수 있습니다. 위임된 관리자가 SCIM 보유자 토큰을 생성하지 못하도록 다음 SCP를 설정할 수 있습니다. 위임된 관리자가 SCIM으로 사용자 프로비저닝을 설정하거나 주기적으로 SCIM 보유자 토큰 교체를 수행해야 하

는 경우에는 위임된 관리자가 그러한 작업을 완료할 수 있도록 이 API에 대한 액세스 권한을 일시적으로 허용해야 합니다.

```
{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}
```

권한 세트 태그 및 계정 목록을 사용하여 특정 계정의 관리 위임

IAM Identity Center 관리자에게 할당하는 권한 세트를 생성하여 누가 권한 세트를 생성할 수 있는지와 누가 어떤 계정에 어떤 권한 세트를 할당할 수 있는지를 위임할 수 있습니다. 이는 권한 세트에 태그를 지정하고 관리자에게 할당하는 권한 세트 내에서 정책 조건을 사용하는 방식으로 수행됩니다. 예를 들어 특정 방식으로 태그가 지정되면 사용자가 권한 세트를 생성할 수 있는 권한 세트를 생성할 수 있습니다. 또한 관리자가 특정 계정에서 특정 태그가 있는 권한 세트를 할당할 수 있도록 하는 정책을 생성할 수도 있습니다. 이렇게 하면 관리자에게 위임된 관리 계정에 대한 액세스 및 권한을 수정할 권한을 부여하지 않은 상태로 계정에 대한 관리를 위임할 수 있습니다. 예를 들어 위임된 관리 계정에서만 사용하는 권한 세트에 태그를 지정하면 특정인에게만 위임된 관리 계정에 영향을 미치는 권한 세트 및 할당을 수정할 수 있는 권한을 부여하는 정책을 지정할 수 있습니다. 다른 사람에게 위임된 관리 계정 밖의 계정 목록을 관리할 수 있는 권한을 부여할 수도 있습니다. 자세히 알아보려면 AWS 보안 블로그의 [AWS IAM Identity Center에서 권한 세트 관리 및 계정 할당 위임](#)을 참조하세요.

사전 조건

계정을 위임된 관리자로 등록하려면 먼저 다음 환경을 배포해야 합니다.

- AWS Organizations 는 기본 관리 계정 외에도 하나 이상의 멤버 계정으로 활성화 및 구성되어야 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](#) 섹션을 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 멤버 계정을 위임된 관리자로 등록하여 IAM Identity Center에 대한 관리 액세스 권한을 부여합니다.

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 Organizations. [RegisterDelegatedAdministrator](#) 관리자 API를 실행하려면 관리 계정 자격 증명이 필요합니다.
2. IAM Identity Center가 활성화된 리전을 선택한 다음 [IAM Identity Center 콘솔](#)을 엽니다.
3. 설정을 선택한 다음 관리 탭을 선택합니다.
4. 위임된 관리자 섹션에서 계정 등록을 선택합니다.
5. 위임된 관리자 등록 페이지에서 등록할을 선택한 다음 계정 등록 AWS 계정을 선택합니다.

멤버 계정 해지

관리 계정의 자격 증명으로 로그인한 경우에만 멤버 계정을 등록 취소할 수 있습니다.

다음 절차에 따라 이전에 위임된 관리자로 지정된 AWS 조직의 멤버 계정을 등록 취소하여 IAM Identity Center에서 관리 액세스를 제거합니다.

⚠ Important

계정 등록을 취소하면 사실상 모든 관리자가 해당 계정에서 IAM Identity Center를 관리할 수 있는 기능이 제거됩니다. 따라서 이 계정으로서는 더 이상 IAM Identity Center ID, 액세스 관리, 인증 또는 애플리케이션 액세스를 관리할 수 없습니다. 이 작업은 IAM Identity Center에 구성된 권한 또는 할당에 영향을 주지 않으므로 최종 사용자가 앱에 계속 액세스하고 AWS 액세스 포털 AWS 계정 내에서 액세스할 수 있으므로 최종 사용자에게는 영향을 주지 않습니다.

멤버 계정을 해지하려면

1. 에서 관리 계정의 자격 증명을 AWS Management Console 사용하여 로그인합니다 AWS Organizations. [DeregisterDelegatedAdministrator](#) 관리자 API를 실행하려면 관리 계정 자격 증명 이 필요합니다.
2. IAM Identity Center가 활성화된 리전을 선택한 다음 [IAM Identity Center 콘솔](#)을 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 이 해했는지 확인합니다.
6. 계정 등록 취소를 선택합니다.

위임된 관리자로 등록된 멤버 계정을 볼 수 있습니다.

다음 절차에 따라 IAM Identity Center의 위임된 관리자로 AWS Organizations 구성원의 멤버 계정을 찾습니다.

등록된 멤버 계정을 보려면

1. [IAM Identity Center 콘솔](#)을 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.

에 대한 임시 승격 액세스 AWS 계정

에 대한 모든 액세스 AWS 계정에는 일정 수준의 권한이 포함됩니다. 프로덕션 환경의 구성을 변경하는 것과 같은 민감한 작업에는 범위와 잠재적 영향을 고려하여 특별한 처리가 필요합니다. 임시 승격 액세스(저스트 인 타임 액세스라고도 함)는 지정된 시간 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.

Note

비즈니스 연속성을 보장하려면 [AWS Management Console에 대한 긴급 액세스를 설정](#)하는 것이 좋습니다.

고객의 다양한 요구 사항을 해결하기 위해서는 AWS Security Competency 파트너의 솔루션과 AWS IAM Identity Center 통합합니다. 이러한 솔루션이 일반적인 임시 액세스 증가 요구 사항을 충족하는지 AWS 확인합니다. 비즈니스, 클라우드 환경의 아키텍처, 예산 등 특별한 요구 사항과 선호도에 가장 적합한 솔루션을 선택하기 전에 각 파트너 솔루션을 주의 깊게 검토하는 것이 좋습니다.

검증된 솔루션에는 [Apono Access Management Platform](#), [CyberArk Secure Cloud Access](#), [Okta Access Requests](#), [Tenable](#)(이전 Ermetic)이 있습니다.

파트너는 파트너 센터에서 AWS 보안 역량 애플리케이션을 사용하여 솔루션을 추천할 수 있습니다. 자세한 내용은 [AWS Security Competency 파트너](#)를 참조하세요.

Note

리소스 기반, Amazon Elastic Kubernetes Service 또는를 사용하는 경우 just-in-time 솔루션을 선택하기 전에 [리소스 정책](#), [Amazon EKS 클러스터 구성 맵](#) 및 [AWS KMS 키 정책의 권한 세트 참조](#)를 AWS Key Management Service참조하세요.

에 대한 Single Sign-On 액세스 AWS 계정

연결된 디렉터리의 사용자에게 [일반적인 직무를](#) AWS Organizations 기반으로 조직의 관리 계정 또는 멤버 계정에 권한을 할당할 수 있습니다. 또는 사용자 지정 권한을 사용하여 특정 보안 요구 사항을 충족할 수 있습니다. 예를 들어 데이터베이스 관리자에게 개발 계정에서는 Amazon RDS에 광범위

한 권한을 부여하지만 프로덕션 계정에서는 권한을 제한할 수 있습니다. IAM Identity Center는 AWS 계정에서 필요한 모든 사용자 권한을 자동으로 구성합니다.

Note

사용자 또는 그룹에 AWS Organizations 관리 계정에서 작업할 수 있는 권한을 부여해야 할 수 있습니다. 권한이 높은 계정이므로 추가 보안 제한을 적용하려면 먼저 [IAMFullAccess](#) 정책 또는 이에 상응하는 권한이 있어야 이 계정을 설정할 수 있습니다. 이러한 추가 보안 제한은 AWS 조직의 멤버 계정에 필요하지 않습니다.

주제

- [에 사용자 또는 그룹 액세스 할당 AWS 계정](#)
- [에 대한 사용자 및 그룹 액세스 제거 AWS 계정](#)
- [권한 세트로 생성된 활성 IAM 역할 세션 취소](#)
- [관리 계정의 사용자 및 그룹에 Single Sign-On 액세스 권한을 할당할 수 있는 사람을 위임합니다.](#)

에 사용자 또는 그룹 액세스 할당 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 [권한 세트 보기 및 변경](#) 섹션을 참조하세요.

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.

에 사용자 또는 그룹 액세스 권한을 할당하려면 AWS 계정

1. [IAM Identity Center 콘솔](#)을 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 나타납니다. 액세스를 할당 AWS 계정 하려는 옆의 확인란을 선택합니다. IAM Identity Center에 대한 관리 액세스를 설정하는 경우 관리 계정 옆의 확인란을 선택합니다.

Note

사용자 및 그룹에 Single Sign-On 액세스 권한을 할당할 때 권한 세트당 AWS 계정 한 번에 최대 10개를 선택할 수 있습니다. 동일한 사용자 및 그룹 집합 AWS 계정 에 10개 이상을 할당하려면 추가 계정에 대해 필요에 따라이 절차를 반복합니다. 메시지가 표시되면 동일한 사용자, 그룹 및 권한 집합을 선택합니다.

4. 사용자 또는 그룹 할당을 선택합니다.
5. 1단계: 사용자 및 그룹 선택을 위해 '**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 세트 선택을 위해 '**AWS-account-name**'에 권한 세트 할당 페이지에서 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 계정으로 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 제출을 위해 '**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.

고려 사항

- 사용자 및 그룹 할당 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 프로세스가 성공적으로 완료될 때까지 이 페이지를 열어둡니다.

Note

사용자 또는 그룹에 AWS Organizations 관리 계정에서 작업할 수 있는 권한을 부여해야 할 수 있습니다. 권한이 높은 계정이므로 추가 보안 제한을 적용하려면 먼저 [IAMFullAccess](#) 정책 또는 이에 상응하는 권한이 있어야 이 계정을 설정할 수 있습니다. 이러한 추가 보안 제한은 AWS 조직의 멤버 계정에 필요하지 않습니다.

8. 다음 중 하나에 해당하는 경우, IAM Identity Center 다중 인증(MFA)을 활성화하기 위해 [사용자에게 MFA에 대한 메시지 표시](#)에서 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 있으며 RADIUS MFA를와 함께 사용하지 않습니다 AWS Directory Service.

Note

외부 ID 제공업체를 사용하는 경우, IAM Identity Center가 아닌 외부 ID 제공업체가 MFA 설정을 관리한다는 점에 유의하세요. IAM Identity Center의 MFA는 외부 ID 제공업체가 사용할 수 없습니다.

관리 사용자에게 대한 계정 액세스를 설정하면 IAM Identity Center에서 해당 IAM 역할을 생성합니다. IAM Identity Center에서 제어하는 이 역할은 관련에서 생성 AWS 계정되며 권한 세트에 지정된 정책은 역할에 연결됩니다.

또는 [AWS CloudFormation](#)를 사용하여 권한 세트를 생성 및 할당하고 해당 권한 세트에 사용자를 할당할 수 있습니다. 그러면 사용자는 [AWS 액세스 포털에 로그인](#)하거나 [AWS Command Line Interface \(AWS CLI\)](#) 명령을 사용할 수 있습니다.

에 대한 사용자 및 그룹 액세스 제거 AWS 계정

이 절차를 사용하여 연결된 디렉터리에 있는 하나 이상의 사용자 및 그룹에 AWS 계정 대해에 대한 Single Sign-On 액세스를 제거합니다. 또는 [delete-account-assignment](#) AWS CLI를 사용할 수 있습니다.

Note

IAM Identity Center 사용자 또는 그룹의 프로비저닝을 해제해야 할 때는 사용자 및 그룹을 삭제하기 전에 먼저 사용자 및 그룹에서 [권한 세트 할당을 제거](#)해야 합니다.

에 대한 사용자 및 그룹 액세스를 제거하려면 AWS 계정

1. [IAM Identity Center 콘솔](#)을 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 포함된의 이름을 선택합니다.
4. 개요 페이지의 AWS 계정할당된 사용자 및 그룹에서 하나 이상의 사용자 또는 그룹의 이름을 선택하고 액세스 제거를 선택합니다.
5. 액세스 제거 대화 상자에서 사용자 또는 그룹 이름이 올바른지 확인하고 액세스 제거를 선택합니다.

권한 세트로 생성된 활성 IAM 역할 세션 취소

다음은 IAM Identity Center 사용자의 활성 권한 세트 세션을 취소하는 일반적인 절차입니다. 이 절차에서는 자격 증명이 손상된 사용자 또는 시스템에 있는 악의적인 작업자의 모든 액세스를 제거하려는 것으로 가정합니다. 사전 조건은 [권한 세트에서 생성된 활성 IAM 역할 세션을 취소하기 위한 준비](#)의 지침을 따르는 것입니다. 모든 거부 정책은 서비스 제어 정책(SCP)에 나와 있다고 가정합니다.

Note

AWS에서는 콘솔 전용 작업을 제외한 모든 단계를 처리하도록 자동화를 구축할 것을 권장합니다.

1. 액세스를 취소해야 하는 사람의 사용자 ID를 가져옵니다. ID 스토어 API를 사용하여 사용자 이름으로 사용자를 찾을 수 있습니다.
2. 서비스 제어 정책(SCP)의 1단계에서 사용자 ID를 추가하도록 거부 정책을 업데이트합니다. 이 단계를 완료하면 대상 사용자는 액세스 권한을 상실하고 정책이 영향을 미치는 역할에 대해 작업을 수행할 수 없습니다.
3. 사용자의 모든 권한 세트 할당을 제거합니다. 그룹 멤버십을 통해 액세스가 할당된 경우 모든 그룹 및 모든 직접 권한 세트 할당에서 사용자를 제거합니다. 이 단계에서는 사용자가 추가 IAM 역할을 수임하지 못하도록 합니다. 사용자에게 활성 AWS 액세스 포털 세션이 있고 사용자를 비활성화한 경우 액세스를 제거할 때까지 새 역할을 계속 수임할 수 있습니다.
4. ID 제공업체(idP) 또는 Microsoft Active Directory를 ID 원본으로 사용하는 경우 ID 원본에서 사용자를 비활성화합니다. 사용자를 비활성화하면 추가 AWS 액세스 포털 세션이 생성되지 않습니다. IdP 또는 Microsoft Active Directory API 설명서를 사용하여 이 단계를 자동화하는 방법을 알아봅니다. IAM Identity Center 디렉터리를 ID 원본으로 사용하는 경우 아직 사용자 액세스를 비활성화하지 마세요. 6단계에서 사용자 액세스를 비활성화하게 됩니다.
5. IAM Identity Center 콘솔에서 사용자를 찾고 활성 세션을 삭제합니다.
 - a. 사용자를 선택하세요.
 - b. 삭제하려는 활성 세션의 사용자를 선택합니다.
 - c. 사용자 상세 페이지에서 활성 세션 탭을 선택합니다.
 - d. 삭제하고 싶은 세션 옆의 체크박스를 선택하고 세션 삭제를 선택합니다.

사용자 세션을 삭제하면 사용자는 AWS 액세스 포털에 대한 액세스 권한을 즉시 잃게 됩니다. [세션 기간](#)에 대해 알아봅니다.

6. IAM Identity Center 콘솔에서 사용자 액세스를 제거합니다.
 - a. 사용자를 선택하세요.
 - b. 액세스를 비활성화할 사용자를 선택합니다.
 - c. 사용자 세부 정보 페이지에서 일반 정보를 확장하고 사용자 액세스 비활성화 버튼을 선택하여 사용자의 추가 로그인을 방지합니다.

7. 거부 정책은 최소 12시간 동안 그대로 둡니다. 그렇지 않으면 활성 IAM 역할 세션이 있는 사용자는 IAM 역할로 복원된 작업을 갖게 됩니다. 12시간을 기다리면 활성 세션이 만료되고 사용자는 IAM 역할에 다시 액세스할 수 없습니다.

Important

사용자 세션을 중지하기 전에 사용자의 액세스를 비활성화하는 경우(5단계를 완료하지 않고 6 단계를 완료함) IAM Identity Center 콘솔을 통해 더 이상 사용자 세션을 중지할 수 없습니다. 사용자 세션을 중지하기 전에 사용자 액세스를 실수로 비활성화한 경우 사용자를 다시 활성화하고 세션을 중지한 다음 액세스를 다시 비활성화할 수 있습니다.

이제 암호가 손상된 경우 사용자의 자격 증명을 변경하고 [해당 사용자의 할당을 복원](#)할 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 AWS 계정 루트 사용자 또는 AWSSSOMasterAccountAdministrator 및 IAMFullAccess AWS 관리형 정책이 연결된 사용자만 관리 계정에 Single Sign-On 액세스 권한을 할당할 수 있습니다. AWSSSOMasterAccountAdministrator 및 IAMFullAccess 정책은 AWS Organizations 조직 내 관리 계정에 대한 Single Sign-On 액세스를 관리합니다.

또는 AWS CLI 를 사용하여 권한 세트를 생성, 정책 연결 및 할당할 수 있습니다. 다음은 각 단계의 명령을 나열한 것입니다.

- 권한 세트 생성: [create-permission-set](#)
- 권한 세트에 연결 AWS Managed Policy하려면: [attach-managed-policy-to-permission-set](#)
- 고객 관리형 정책을 권한 세트에 연결하려면: [attach-customer-managed-policy-to-permission-set](#)
- 권한 세트를 위탁자에 할당: [create-account-assignment](#)

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. 예제:

<https://console.aws.amazon.com/ec2/>

자세한 내용은 [에 빠르게 액세스할 수 있도록 릴레이 상태 설정 AWS Management Console](#) 섹션을 참조하세요.

3. 권한 집합에 포함하려는 정책은 무엇인가요?, AWS 관리형 정책 연결 확인란을 선택합니다.
4. IAM 정책 목록에서 AWSSSOMasterAccountAdministrator 및 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 리소스 태그 지정](#) 섹션을 참조하세요.
7. 선택 사항을 검토한 후 생성을 선택합니다.
3. [에 사용자 또는 그룹 액세스 할당 AWS 계정](#)의 단계에 따라 방금 만든 권한 집합에 적절한 사용자와 그룹을 할당합니다.
4. 할당된 사용자에게 다음 사항을 알립니다. 사용자가 AWS 액세스 포털에 로그인하고 계정 탭을 선택하면 방금 위임한 권한으로 인증받을 적절한 역할 이름을 선택해야 합니다.

권한 세트 AWS 계정 로 관리

권한 세트는 하나 이상의 [IAM 정책](#) 컬렉션을 정의하는 템플릿으로, 생성 및 유지 관리하는 템플릿입니다. 권한 세트는 조직의 사용자 및 그룹에 대한 AWS 계정 액세스 할당을 간소화합니다. 예를 들어

AWS RDS, DynamoDB 및 Aurora 서비스를 관리하기 위한 정책이 포함된 데이터베이스 관리자 권한 세트를 생성하고 이 단일 권한 세트를 사용하여 데이터베이스 관리자의 [AWS 조직](#) AWS 계정 내 대상 목록에 대한 액세스 권한을 부여할 수 있습니다.

IAM Identity Center는 권한 세트가 AWS 계정 있는 하나 이상의 사용자 또는 그룹에 액세스 권한을 할당합니다. 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 IAM Identity Center 사용자 포털 또는 AWS CLI를 사용하여 역할을 관리하고 정의한 권한 있는 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 대한 AWS 관리형 정책](#)을 추가할 수 있습니다. AWS 관리형 정책 또는 고객 관리형 정책을 [권한 경계](#)로 할당할 수도 있습니다.

권한 세트를 생성하려면 [권한 세트 생성, 관리 및 삭제](#)을 참조하세요.

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 모니터링할 수 있습니다. 사용 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 항상 관리 권한을 사용하는 대신 필요한 권한 AWS 계정으로만 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 세트와 달리, PowerUserAccess 권한 세트는 IAM 사용자와 그룹을 관리할 수 없습니다. AWS 액세스 포털에 로그인하여 AWS 계정에 액세스할 때 PowerUserAccess가 아닌 AdministratorAccess를 선택하여 계정에서 개발 작업을 수행할 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](#) 세트를 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 정책](#)을 참조하세요.

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

사용자에게 페더레이션 AWS 계정 하고 AWS 관리 콘솔 또는 AWS 명령줄 인터페이스(AWS CLI)를 사용하는 경우 IAM Identity Center는 권한 세트의 세션 기간 설정을 사용하여 세션 기간을 제어합니다. 기본적으로 사용자가 세션에서 로그아웃하기 전에 로그인할 수 있는 시간을 결정하는 세션 기간 값은 1시간으로 설정됩니다. AWS 계정 AWS 최대 12시간까지 값을 지정할 수 있습니다. 자세한 내용은 [에 대한 세션 기간 설정 AWS 계정](#) 단원을 참조하십시오.

- AWS 액세스 포털 세션 기간을 구성하여 작업 인력 사용자가 포털에 로그인하는 시간을 제어할 수도 있습니다.

기본적으로 작업 인력 사용자가 다시 인증해야 하기 전에 AWS 액세스 포털에 로그인할 수 있는 시간을 결정하는 최대 세션 기간의 값은 8시간입니다. 최대 90일까지 값을 지정할 수 있습니다. 자세한 내용은 [IAM Identity Center에서 세션 지속 시간 구성](#) 단원을 참조하십시오.

- AWS 액세스 포털에 로그인할 때 최소 권한 권한을 제공하는 역할을 선택합니다.

생성하여 사용자에게 할당하는 각 권한 세트는 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 AdministratorAccess를 선택하세요.

- IAM Identity Center에 다른 사용자를 추가하고 해당 사용자에게 기존 또는 새 권한 세트를 할당할 수 있습니다.

자세한 내용은 [에 사용자 또는 그룹 액세스 할당 AWS 계정](#)의 내용을 참조하세요.

주제

- [AWS 관리형 정책에 대해 미리 정의된 권한](#)
- [AWS 관리형 및 고객 관리형 정책에 대한 사용자 지정 권한](#)
- [권한 세트 생성, 관리 및 삭제](#)
- [권한 집합 속성을 구성합니다.](#)

AWS 관리형 정책에 대해 미리 정의된 권한

AWS 관리형 정책을 사용하여 사전 정의된 권한 세트를 생성할 수 있습니다.

사전 정의된 권한으로 권한 세트를 생성할 때 AWS 관리형 정책 목록에서 하나의 정책을 선택합니다. 사용 가능한 정책 내에서 일반 권한 정책 및 직무 정책 중에서 선택할 수 있습니다.

일반 권한 정책

전체의 리소스에 액세스할 수 있도록 하는 AWS 관리형 정책 목록에서 선택합니다 AWS 계정. 다음 정책 중 한 가지를 추가할 수 있습니다.

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

직무 정책

조직 내 작업과 관련이 있을 수 있는 리소스에 액세스할 수 AWS 계정 있도록 하는 AWS 관리형 정책 목록에서 선택합니다. 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 대한 AWS 관리형 정책](#)을 참조하세요.

권한 세트를 생성하는 방법에 대한 지침은 [권한 세트 생성, 관리 및 삭제](#)을 참조하세요.

AWS 관리형 및 고객 관리형 정책에 대한 사용자 지정 권한

AWS Identity and Access Management (IAM)에 있는 AWS 관리형 및 고객 관리형 정책과 인라인 정책을 결합하여 사용자 지정 권한으로 권한 세트를 생성할 수 있습니다. 권한 경계를 포함하여 다른 정책이 권한 세트 사용자에게 부여할 수 있는 가능한 최대 권한을 설정할 수도 있습니다.

권한 세트를 생성하는 방법에 대한 지침은 [권한 세트 생성, 관리 및 삭제](#)를 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 생성기](#)를 사용하여 IAM 정책을 생성할 수도 있습니다.

인라인 정책을 사용하여 권한 세트를 배포하면 IAM Identity Center는 권한 세트를 할당 AWS 계정 하는에 IAM 정책을 생성합니다. IAM Identity Center는 계정에 권한 세트를 할당할 때 정책을 생성합니다. 그러면 정책이 사용자가 수임 AWS 계정 하는의 IAM 역할에 연결됩니다.

인라인 정책을 생성하고 권한 세트를 할당하면 IAM Identity Center가 AWS 계정 에서 정책을 구성합니다. 를 사용하여 권한 세트를 빌드 [고객 관리형 정책](#)할 때는 권한 세트를 할당하기 전에 AWS 계정 직접 정책을 생성해야 합니다.

AWS 관리형 정책

권한 세트에 AWS 관리형 정책을 연결할 수 있습니다. AWS 관리형 정책은 AWS 유지하는 IAM 정책입니다. 반대로 계정에서 생성 및 유지 관리하는 [고객 관리형 정책](#) IAM 정책 AWS 이의 일반적인 최소 권한 사용 사례를 다루고 있습니까 AWS 계정? AWS 관리형 정책을 IAM Identity Center가 생성하는 역할에 대한 권한 또는 [권한 경계](#)로 할당할 수 있습니다.

AWS 는 AWS 리소스 [AWS 에 작업별 액세스 권한을 할당하는 직무에 대한 관리형 정책](#)을 유지합니다. 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.

에는 특정 AWS 서비스 및 조합에 대한 많은 AWS 관리형 IAM 정책 AWS 계정 도 포함되어 있습니다 AWS 서비스. 사용자 지정 권한으로 권한 세트를 생성할 때 여러 추가 AWS 관리형 정책 중에서 선택하여 권한 세트에 할당할 수 있습니다.

AWS 는 모든를 AWS 관리형 정책 AWS 계정 으로 채웁니다. AWS 관리형 정책이 포함된 권한 세트를 배포하려면 먼저에서 정책을 생성할 필요가 없습니다 AWS 계정. 를 사용하여 권한 세트를 빌드 [고객 관리형 정책](#)할 때는 권한 세트를 할당하기 전에 AWS 계정 직접 정책을 생성해야 합니다.

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

고객 관리형 정책

권한 세트에 고객 관리형 정책을 추가할 수 있습니다. 고객 관리형 정책은 자신의 계정에서 생성 및 관리하는 IAM 정책입니다. 반대로 [AWS 관리형 정책](#)는 계정에서 AWS 유지하는 IAM 정책입니다. IAM Identity Center에서 생성한 역할에 대한 권한으로 고객 관리형 정책을 할당하거나 [권한 경계](#)로 할당할 수 있습니다.

고객 관리형 정책으로 권한 세트를 생성할 때는 IAM Identity Center가 권한 세트를 할당 AWS 계정 하는 각에서 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 경로](#)를 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 내용은 [권한 집합에서 IAM 정책 사용](#) 단원을 참조하십시오.

Note

고객 관리형 정책이 권한 세트에 연결된 경우 정책의 이름은 대/소문자를 구분하지 않습니다.

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

권한 경계

권한 세트에 권한 경계를 추가할 수 있습니다. 권한 경계는 자격 증명 기반 정책이 IAM 보안 주체에게 부여할 수 있는 최대 권한을 설정하는 AWS 관리형 또는 고객 관리형 IAM 정책입니다. 권한 경계를 적용하면 [인라인 정책](#), [고객 관리형 정책](#) 및 [AWS 관리형 정책](#)에게는 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 경계](#)를 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 세트 및 IAM Identity Center에서 권한 세트를 사용하는 방법에 대한 자세한 내용은 [권한 세트 AWS 계정 로 관리](#) 섹션을 참조하세요.

Note

IAM Identity Center 콘솔에서 이름으로 권한 세트를 검색하고 정렬할 수 있습니다.

권한 세트를 생성할 때 고려할 사항:

- 조직 인스턴스

권한 세트를 사용하려면 IAM Identity Center의 조직 인스턴스를 사용해야 합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

- 사전 정의된 권한 세트로 시작

사전 정의된 권한을 사용하는 [사전 정의된 권한](#) 세트를 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 정책](#)을 참조하세요. 사용 데이터를 수집한 후 권한 세트를 더 제한적으로 조정할 수 있습니다.

- 관리 세션 지속 시간을 합리적인 작업 기간으로 제한

사용자에게 페더레이션 AWS 계정 하고 AWS Management Console 또는 AWS 명령줄 인터페이스(AWS CLI)를 사용하는 경우 IAM Identity Center는 권한 세트의 세션 기간 설정을 사용하여 세션 기간을 제어합니다. 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 내용은 [에 대한 세션 기간 설정 AWS 계정](#) 섹션을 참조하세요.

- 직원 사용자 포털 세션 지속 시간 제한

직원 사용자는 포털 세션을 사용하여 역할을 선택하고 애플리케이션에 액세스합니다. 기본적으로 작업 인력 사용자가 다시 인증해야 하기 전에 AWS 액세스 포털에 로그인할 수 있는 시간을 결정하

는 최대 세션 기간 값은 8시간입니다. 최대 90일까지 값을 지정할 수 있습니다. 자세한 내용은 [IAM Identity Center에서 세션 지속 시간 구성](#) 섹션을 참조하세요.

- 최소 권한을 제공하는 역할 사용

생성하여 사용자에게 할당하는 각 권한 세트는 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 AdministratorAccess를 선택하세요. 사용자 초대를 보내기 전에 권한 세트를 테스트하여 필요한 액세스 권한을 제공하는지 확인합니다.

Note

또는 [AWS CloudFormation](#)을 사용하여 권한 세트를 생성 및 할당하고 해당 권한 세트에 사용자를 할당할 수 있습니다.

주제

- [권한 집합을 생성합니다.](#)
- [권한 세트 보기 및 변경](#)
- [권한 집합 관리 위임](#)
- [권한 집합에서 IAM 정책 사용](#)
- [IAM Identity Center에서 권한 세트 제거](#)
- [IAM Identity Center에서 권한 세트 삭제](#)

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 콘솔](#)에서 최대 10개 정책에 대한 조정을 요청할 수 있습니다. IAM Identity Center 콘솔에서 권한 집합을 생성할 수 있습니다.

Note

권한 세트를 사용하려면 IAM Identity Center의 조직 인스턴스를 사용해야 합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

권한 집합을 생성하려면

1. [IAM Identity Center 콘솔](#)을 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. 사전 정의된 정책에서 목록에서 IAM Job 함수 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 정책](#)을 참조하세요.
 2. 6단계로 이동하여 권한 세트 세부 정보 지정 페이지를 완료합니다.
 - 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 계정의 Service Quotas 콘솔에서 IAM 역할에 연결된 IAM 할당량 관리형 정책을 늘려달라고 요청합니다.
 - AWS 관리형 정책을 확장하여 AWS 구축 및 유지 관리하는 IAM의 정책을 추가합니다. 자세한 내용은 [AWS 관리형 정책](#) 단원을 참조하십시오.
 - 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 완료합니다.
 - 고객 관리형 정책을 확장하여 구축 및 유지 관리하는 IAM의 정책을 추가합니다. 자세한 내용은 [고객 관리형 정책](#) 섹션을 참조하세요.
 - a. 정책 연결을 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 세트 세부 정보 지정 페이지를 완료합니다.
- 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 내용은 [인라인 정책](#) 섹션을 참조하세요.
 - a. 대화형 편집기 내에서 원하는 작업과 리소스를 인라인 정책에 추가합니다. 새 문 추가를 사용하여 추가 문을 추가할 수 있습니다.
 - b. 다른 유형의 정책을 추가하려면 해당 컨테이너를 선택합니다. 적용하려는 정책을 모두 선택했으면 다음을 선택합니다. 6단계로 이동하여 권한 세트 세부 정보 지정 페이지를 완료합니다.
- 권한 경계를 확장하여 AWS 관리형 또는 고객 관리형 IAM 정책을 권한 세트의 다른 정책이 할당할 수 있는 최대 권한으로 추가합니다. 자세한 내용은 [권한 경계](#) 단원을 참조하십시오.
 - 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 세트 세부 정보 지정 페이지를 완료합니다.

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 세트에 대해 지정하는 이름은 AWS 액세스 포털에 사용 가능한 역할로 표시됩니다. 사용자는 AWS 액세스 포털에 로그인 AWS 계정하고를 선택한 다음 역할을 선택합니다.

Note

권한 세트 이름은 IAM Identity Center 인스턴스 내에서 고유해야 합니다.

2. (선택 사항) 또한 설명을 추가할 수도 있습니다. 설명은 AWS 액세스 포털이 아닌 IAM Identity Center 콘솔에만 표시됩니다.

3. (선택 사항) 세션 기간 값을 지정합니다. 이 값은 콘솔이 세션에서 로그아웃하기 전에 사용자가 로그인할 수 있는 시간을 결정합니다. 자세한 내용은 [에 대한 세션 기간 설정 AWS 계정](#) 섹션을 참조하세요.
4. (선택 사항) 릴레이 상태 값을 지정합니다. 이 값은 페더레이션 프로세스 중 계정 내에서 사용자를 리디렉션하는 데 사용됩니다. 자세한 내용은 [에 빠르게 액세스할 수 있도록 릴레이 상태 설정 AWS Management Console](#) 단원을 참조하십시오.

Note

릴레이 상태 URL은 AWS Management Console 범위 내에 있어야 합니다. 예제:
`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 리소스 태그 지정](#) 섹션을 참조하세요.
6. 다음을 선택합니다.
7. 검토 및 생성 페이지에서 선택한 내용을 검토한 다음 생성을 선택합니다.
8. 기본적으로 권한 세트를 생성하면 권한 세트가 프로비저닝되지 않습니다(모든에서 사용됨 AWS 계정). 에서 권한 세트를 프로비저닝하려면 계정의 사용자 및 그룹에 IAM Identity Center 액세스 권한을 할당한 다음 해당 사용자 및 그룹에 권한 세트를 적용해야 AWS 계정입니다. 자세한 내용은 [에 사용자 또는 그룹 액세스 할당 AWS 계정](#) 단원을 참조하십시오.

권한 세트 보기 및 변경

권한 세트를 사용하여 사용자에게 AWS 계정에 대한 액세스 권한을 부여할 수 있습니다. AWS IAM Identity Center 콘솔을 사용하여 권한 세트를 보고 변경할 수 있습니다. IAM Identity Center 콘솔에서 이름으로 권한 세트를 검색하고 정렬할 수 있습니다. 권한 세트 및 IAM Identity Center에서 권한 세트를 사용하는 방법에 대한 자세한 내용은 [the section called “권한 세트”](#) 섹션을 참조하세요.

애플리케이션에 대한 사용자 액세스를 관리하는 데는 권한 세트가 필요하지 않습니다.

Note

권한 세트를 사용하려면 IAM Identity Center의 조직 인스턴스를 사용해야 합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

권한 세트 할당 보기

AWS IAM Identity Center 콘솔에서 적용된 권한 세트를 보려면 다음 절차를 따릅니다.

All AWS 계정 where a permission set is provisioned

권한 세트에 대한 모든 할당을 보려면 다음 절차를 따릅니다.

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/singlesignon/> AWS IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한 아래에서 권한 집합을 선택합니다.
3. 권한 세트 페이지에서 확인하려는 권한 세트를 선택합니다.
4. 선택한 권한 세트 페이지의 계정 탭에서 권한 세트가 사용되는 계정을 볼 수 있습니다. 계정을 선택하면 계정 내에서 권한 세트가 프로비저닝되는 방식을 확인할 수 있습니다. 정책을 [삭제](#), 편집하고 권한 세트에 연결할 수 있습니다.

All permission sets for an AWS 계정

권한 세트에 대한 모든 할당을 보려면 다음 절차를 따릅니다.

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/singlesignon/> AWS IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한에서 AWS 계정을 선택합니다. 프로비저닝된 권한 세트를 표시할 계정을 선택합니다.
3. 선택한 AWS 계정 페이지의 권한 세트 탭에서 선택한에 할당된 다른 권한 세트를 볼 수 있습니다. 다 AWS 계정. 권한 세트 하이퍼링크를 선택하면 권한 세트에 대해 자세히 알아볼 수 있습니다.

All applied permission sets to users and groups

사용자 또는 그룹에 할당된 모든 권한 세트를 보려면 다음 절차를 따릅니다.

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/singlesignon/> AWS IAM Identity Center 콘솔을 엽니다.
2. 대시보드에서 사용자 또는 그룹을 선택하여 IAM Identity Center 사용자 또는 그룹을 표시합니다.

- a. 사용자 페이지에서 적용된 권한 세트를 표시할 사용자를 선택합니다. 그런 다음 AWS 계정 탭을 선택하고 AWS 계정 액세스 섹션에서 AWS 계정을 선택합니다. 선택한 사용자에게 AWS 계정 대해 적용된 권한 세트 맞을 볼 수 있습니다.
- b. 그룹 페이지에서 적용된 권한 세트를 표시할 그룹을 선택합니다. 그런 다음 AWS 계정 탭을 선택하고 AWS 계정 액세스 섹션에서 AWS 계정을 선택합니다. 선택한 그룹에 AWS 계정 대해 적용된 권한 세트 맞을 볼 수 있습니다.

권한 세트 변경

IAM Identity Center 콘솔로 [권한 세트](#)를 변경하려면 다음 절차를 따릅니다. 그룹 또는 사용자에게 대해 권한 세트를 추가하거나 제거할 수 있습니다.

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/singlesignon/> AWS IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한에서 AWS 계정을 선택합니다.
3. AWS 계정 페이지에는 조직의 트리 뷰 목록이 표시됩니다. 사용 권한 집합을 변경하려는 AWS 계정의 이름을 선택합니다.
4. AWS 계정의 개요 페이지의 할당된 사용자 및 그룹 아래에서 변경하려는 권한 세트의 사용자 이름 또는 그룹 이름을 선택합니다. 그런 다음 권한 세트 변경을 선택합니다.
5. 권한 세트를 원하는 대로 변경한 다음 변경 사항 저장을 선택합니다.
6. 권한 세트 탭으로 이동하여 최근에 변경된 권한 세트를 선택하고 업데이트를 선택합니다.
7. 권한 업데이트 페이지에서 업데이트를 선택합니다.

권한 집합 관리 위임

IAM Identity Center를 사용하면 IAM Identity Center 리소스의 [Amazon 리소스 이름\(ARN\)](#)을 참조하는 [IAM 정책](#)을 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.

Note

권한 세트를 사용하려면 IAM Identity Center의 조직 인스턴스를 사용해야 합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

다음 방법 중 하나를 사용하여 이러한 유형의 정책을 생성할 수 있습니다.

- (권장) IAM Identity Center에서 각각 다른 정책을 사용하여 [권한 집합](#)을 생성하고 이 권한 집합을 다른 사용자 또는 그룹에 할당합니다. 이렇게 하면 선택한 [IAM Identity Center ID 소스](#)를 사용하여 로그인하는 사용자의 관리자 권한을 관리할 수 있습니다.
- IAM에서 사용자 지정 정책을 생성한 다음 이를 관리자가 수입하는 IAM 역할에 연결합니다. 역할에 대한 자세한 내용은 할당된 IAM Identity Center 관리 권한을 얻기 위한 [IAM 역할](#)을 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}
Account	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 계정도 정책을 생성하지 않습니다. 대신 권한 집합을 할당하려는 각 계정에서 이러한 정책을 미리 만들어 권한 집합의 이름 및 경로 사양과 일치시켜야 합니다. 조직의 AWS 계정에 권한 세트를 할당하면 IAM Identity Center는 [AWS Identity and Access Management \(IAM\) 역할](#)을 생성하고 [IAM 정책](#)을 해당 역할에 연결합니다.

고려 사항

- 권한 세트를 사용하려면 IAM Identity Center의 조직 인스턴스를 사용해야 합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.
- IAM 정책을 사용하여 권한 집합을 할당하기 전에 먼저 멤버 계정을 준비해야 합니다. 멤버 계정의 IAM 정책 이름은 관리 계정의 정책 이름과 일치해야 합니다. 멤버 계정에 정책이 없는 경우 IAM Identity Center에서 권한 집합을 할당하지 못합니다.

Note

고객 관리형 정책이 권한 세트에 연결된 경우 정책의 이름은 대/소문자를 구분하지 않습니다.

- 정책에서 부여하는 권한이 계정 간에 정확히 일치할 필요는 없습니다.

권한 집합에 IAM 정책을 할당

1. 권한 세트를 할당 AWS 계정 하려는 각에서 IAM 정책을 생성합니다.
2. IAM 정책에 권한을 할당합니다. 계정마다 다른 권한을 할당할 수 있습니다. 일관된 경험을 위해 각 정책에서 동일한 권한을 구성하고 유지합니다. AWS CloudFormation StackSets와 같은 자동화 리소스를 사용하여 각 멤버 계정에서 동일한 이름과 권한을 가진 IAM 정책의 사본을 생성할 수 있습니다. CloudFormation StackSets에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 [AWS CloudFormation StackSets 작업을](#) 참조하세요.
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.

IAM Identity Center에서 권한 세트 제거

IAM Identity Center 콘솔에서 IAM Identity Center 사용자 및 그룹에서 권한 세트를 제거할 수 있습니다. AWS 계정에서 권한 세트를 제거할 수도 있습니다. 권한 세트 및 IAM Identity Center에서 권한 세트를 사용하는 방법에 대한 자세한 내용은 [권한 세트 AWS 계정 로 관리](#) 섹션을 참조하세요.

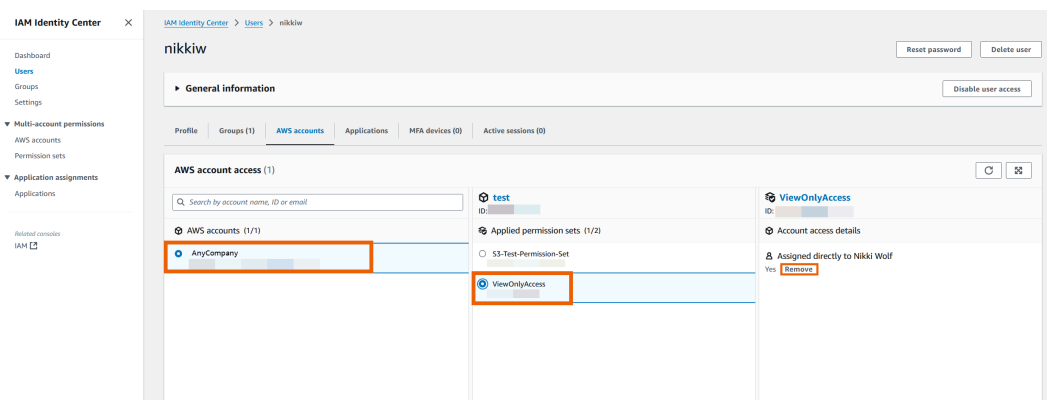
Note

권한 세트를 사용하려면 IAM Identity Center의 조직 인스턴스를 사용해야 합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

Remove permission set from a user**사용자로부터 권한 세트 제거**

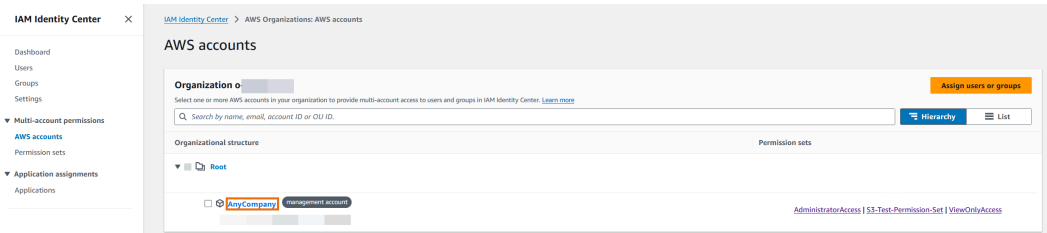
IAM Identity Center 콘솔로 사용자로부터 권한 세트를 제거하려면 이 절차를 따릅니다.

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/singlesignon/> AWS IAM Identity Center 콘솔을 엽니다.
2. IAM Identity Center에서 사용자를 선택합니다.
3. 권한 세트를 제거하려는 사용자의 사용자 이름을 선택합니다.
4. 사용자 세부 정보 페이지에서 AWS 계정 탭을 선택합니다. AWS 계정 액세스에서 AWS 계정을 선택합니다.
5. 오른쪽 창에 선택한 사용자에게 적용된 권한이 나타납니다. 제거할 권한 세트를 선택합니다. 계정 액세스 세부 정보에서 제거를 선택합니다.
6. 이 권한 세트를 제거할지 묻는 대화 상자가 나타납니다. 제거를 선택합니다.

**Remove permission set from a group****그룹에서 권한 세트 제거**

IAM Identity Center 콘솔로 그룹에서 권한 세트를 제거하려면 이 절차를 따릅니다.

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/singlesignon/> AWS IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한에서 AWS 계정을 선택합니다. 관리 계정 링크를 선택합니다.



3. 할당된 사용자 및 그룹 탭에서 권한 세트를 제거하려는 그룹을 선택한 다음 권한 세트 변경을 선택합니다.
4. 권한 세트 변경 페이지에서 제거하려는 권한 세트를 지운 다음 변경 사항 저장을 선택합니다.

Remove permission set from an AWS 계정

IAM Identity Center 콘솔로 AWS 계정 에서 권한 세트를 제거하려면 이 절차를 따릅니다.

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/singlesignon/> AWS IAM Identity Center 콘솔을 엽니다.
2. 다중 계정 권한에서 AWS 계정을 선택합니다. 권한 세트를 제거할 AWS 계정 의 이름을 선택합니다.
3. AWS 계정의 개요 페이지에서 권한 세트 탭을 선택합니다. 제거할 권한 세트를 선택합니다. 그런 다음 제거를 선택합니다.
4. 권한 집합 제거 대화 상자에서 올바른 권한 집합이 선택되었는지 확인하고, **Delete**를 입력하여 제거를 확인한 다음, 액세스 제거를 선택합니다.

IAM Identity Center에서 권한 세트 삭제

IAM Identity Center에서 권한 세트를 삭제하려면 먼저 해당 권한 세트를 사용하는 모든 AWS 계정 에서 권한 세트를 제거해야 합니다. 기존 사용자 및 그룹 액세스를 확인하려면 [권한 세트 보기 및 변경](#) 섹션을 참조하세요.

고려 사항

- 권한 세트를 사용하려면 IAM Identity Center의 조직 인스턴스를 사용해야 합니다. 자세한 내용은 [IAM Identity Center의 조직 및 계정 인스턴스](#) 단원을 참조하십시오.

- 활성 권한 세트 세션을 취소하려면 [the section called “직원 사용자의 활성 세션 종료”](#) 섹션을 참조하세요.
- 권한 세트 및 애플리케이션 할당을 삭제하려면 먼저 삭제하려는 사용자 또는 그룹에서 이를 제거해야 합니다. 그렇지 않으면 IAM Identity Center에 할당되지 않은 권한 세트와 사용되지 않은 권한 세트 및 애플리케이션이 남게 됩니다.

AWS 계정 조직의 모든에서 더 이상 사용할 수 없도록 하나 이상의 권한 세트를 삭제하려면 다음 절차를 사용합니다.

Important

이 권한 세트가 할당된 모든 사용자 및 그룹은 사용 AWS 계정 중인 항목에 관계없이 더 이상 로그인할 수 없습니다. 기존 사용자 및 그룹 액세스를 확인하려면 [권한 세트 보기 및 변경](#) 섹션을 참조하세요.

에서 권한 세트를 삭제하려면 AWS 계정

1. [IAM Identity Center 콘솔](#)을 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 관리자는 다음 구성 및 관리 작업을 완료하여 사용자 액세스 및 세션 기간을 제어할 수 있습니다.

Task	자세히 알아보기
관리자는 IAM Identity Center를 통해 AWS 리소스에 액세스할 때 사용자 세션의 최대 기간을 설정할 수 있습니다.	에 대한 세션 기간 설정 AWS 계정

Task	자세히 알아보기
관리자는 IAM Identity Center를 통해 성공적으로 인증한 후 사용자에게 표시되는 랜딩 페이지를 사용자 지정할 수 있습니다.	에 빠르게 액세스할 수 있도록 릴레이 상태 설정 AWS Management Console
권한이 취소되면 사용자가 더 이상 AWS 리소스에 액세스할 수 없도록 합니다.	거부 정책을 사용하여 활성 사용자 권한 취소

에 대한 세션 기간 설정 AWS 계정

각 [권한 집합](#)에 대해 세션 기간을 지정하여 사용자가 AWS 계정에 로그인할 수 있는 시간을 제어할 수 있습니다. 지정된 기간이 경과하면 세션에서 사용자를 AWS 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 콘솔에 페더레이션하거나 (AWS CLI)를 AWS Command Line Interface 사용하는 경우 IAM Identity Center는 권한 세트의 세션 기간 설정을 사용하여 세션 기간을 제어합니다. 기본적으로 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 콘솔](#)을 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 세트가에 프로비저닝된 경우 계정 AWS 계정 이름이 아래에 표시되어 AWS 계정 자동으로 다시 프로비저닝됩니다. 권한 세트의 세션 기간 값이 업데이트되면 권한 세트를 사용하는 모든 AWS 계정 이 다시 프로비저닝됩니다. 즉,이 설정의 새 값은 권한 세트를 AWS 계정 사용하는 모든에 적용됩니다.
7. 변경 사항 저장을 선택합니다.
8. AWS 계정 페이지 상단에 알림이 표시됩니다.
 - 권한 집합이 하나 이상 AWS 계정에 프로비저닝된 경우 해당 AWS 계정 이 성공적으로 재프로비전되었으며 업데이트된 권한 집합이 계정에 적용되었음을 알리는 알림이 표시됩니다.
 - 권한 세트가에 프로비저닝되지 않은 경우 알림 AWS 계정은 권한 세트에 대한 설정이 업데이트 되었음을 확인합니다.

에 빠르게 액세스할 수 있도록 릴레이 상태 설정 AWS Management Console

기본적으로 사용자가 AWS 액세스 포털에 로그인하고 계정을 선택한 다음 할당된 권한 세트에서가 AWS 생성하는 역할을 선택하면 IAM Identity Center는 사용자의 브라우저를 로 리디렉션합니다 AWS Management Console. 릴레이 상태를 다른 콘솔 URL로 설정하여 이 동작을 변경할 수 있습니다.

릴레이 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 AWS 리전 사용한의 콘솔 엔드포인트로 라우팅합니다. 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.

릴레이 상태 구성

다음 절차에 따라 권한 집합에 대한 릴레이 상태 URL을 구성합니다.

1. [IAM Identity Center 콘솔](#)을 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 세트 설정 편집 페이지의 릴레이 상태에서 AWS 서비스에 대한 콘솔 URL을 입력합니다. 예제:

`https://console.aws.amazon.com/ec2/`

Note

릴레이 상태 URL은 AWS Management Console범위 내에 있어야 합니다.

6. 권한 세트가에 프로비저닝된 경우 계정 AWS 계정 이름이 아래에 나타나 AWS 계정 자동으로 다시 프로비저닝됩니다. 권한 세트의 릴레이 상태 URL이 업데이트되면 권한 세트를 AWS 계정 사용하는 모든 이 다시 프로비저닝됩니다. 즉,이 설정의 새 값은 권한 세트를 AWS 계정 사용하는 모든에 적용됩니다.
7. 변경 사항 저장을 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 AWS 계정에서 프로비전되지 않은 경우 해당 권한 집합의 설정이 업데이트되었음을 알리는 알림이 표시됩니다.

Note

AWS API, AWS SDK 또는 AWS Command Line Interface()를 사용하여이 프로세스를 자동화할 수 있습니다AWS CLI. 자세한 내용은 다음을 참조하세요.

- [IAM Identity Center API 참조](#)의 CreatePermissionSet 또는 UpdatePermissionSet 작업

- AWS CLI 명령 참조의 [sso-admin](#) 섹션의 create-permission-set or update-permission-set 명령.

거부 정책을 사용하여 활성 사용자 권한 취소

사용자가 권한 세트를 적극적으로 사용하는 AWS 계정 동안에 대한 IAM Identity Center 사용자의 액세스를 취소해야 할 수 있습니다. 지정되지 않은 사용자에게 거부 정책을 미리 구현하여 활성 IAM 역할 세션을 사용할 수 있는 기능을 제거한 다음, 필요한 경우 거부 정책을 업데이트하여 액세스를 차단하려는 사용자를 지정할 수 있습니다. 이 주제에서는 거부 정책을 생성하는 방법과 정책을 배포하는 방법에 대한 고려 사항을 설명합니다.

권한 세트에서 생성된 활성 IAM 역할 세션을 취소하기 위한 준비

서비스 제어 정책을 사용하여 특정 사용자에게 대한 모든 거부 정책을 적용하여 사용자가 적극적으로 사용 중인 IAM 역할로 조치를 취하지 못하도록 할 수 있습니다. 또한 암호를 변경할 때까지 사용자가 권한 세트를 사용하지 못하도록 함으로써 도용된 자격 증명을 적극적으로 남용하는 악의적인 행위자를 제거할 수 있습니다. 액세스를 광범위하게 거부하고 사용자가 권한 세트를 다시 입력하거나 다른 권한 세트에 액세스하지 못하도록 해야 하는 경우 모든 사용자 액세스를 제거하고, 활성 AWS 액세스 포털 세션을 중지하고, 사용자 로그인을 비활성화할 수도 있습니다. 광범위한 액세스 취소를 위한 추가 작업과 거부 정책을 함께 사용하는 방법은 [the section called “직원 사용자의 활성 세션 종료”](#) 섹션을 참조하세요.

거부 정책

IAM Identity Center ID 스토어의 사용자의 UserID 항목과 일치하는 조건으로 거부 정책을 사용하여 해당 사용자가 적극적으로 사용하는 IAM 역할에 의한 추가 작업을 방지할 수 있습니다. 이 정책을 사용하면 거부 정책을 배포할 때 동일한 권한 세트를 사용할 수 있는 다른 사용자에게 영향을 미치는 일을 방지할 수 있습니다. 이 정책은 액세스를 취소하려는 사용자 ID를 업데이트할 "identitystore:userId"에 대하여 사용자 ID인 *Add user ID here* 항목을 사용합니다.

JSON

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

```

    "Action": [
        "*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "identitystore:userId": "Add user ID here"
        }
    }
}

```

“aws:userId”와 같은 다른 조건의 키를 사용할 수도 있지만, 한 명의 사람과 연결된 전세계적으로 고유한 값인 “identitystore:userId” 항목이 확실합니다. 조건에서 “aws:userId” 항목을 사용하면 사용자 속성이 ID 원본에서 동기화되는 방식에 영향을 받을 수 있으며 사용자의 사용자 이름 또는 이메일 주소가 변경됨에 따라 변경될 수 있습니다.

IAM Identity Center 콘솔에서 사용자로 이동하고, 이름으로 사용자를 검색하고, 일반 정보 섹션을 확장하고, 사용자 ID를 복사하여 사용자의 identitystore:userId 항목을 찾을 수 있습니다. 또한 사용자 ID를 검색하는 동안 동일한 섹션에서 사용자의 AWS 액세스 포털 세션을 중지하고 로그인 액세스를 비활성화하는 것이 편리합니다. ID 스토어 API에 쿼리하여 사용자의 사용자 ID를 가져옴으로써 거부 정책을 생성하는 프로세스를 자동화할 수도 있습니다.

거부 정책 배포

와 같이 유효하지 않은 자리 표시자 사용자 ID *Add user ID here*를 사용하여 AWS 계정 사용자에게 연결할 수 있는 서비스 제어 정책(SCP)을 사용하여 거부 정책을 미리 배포할 수 있습니다. 이는 편리함과 빠른 영향력을 위해 권장되는 접근 방식입니다. 거부 정책을 사용하여 사용자의 액세스를 취소하는 경우, 정책을 편집하여 자리 표시자 사용자 ID를 취소하려는 액세스 권한이 있는 사람의 사용자 ID로 교체하게 됩니다. 이 조치로 사용자가 SCP를 연결하는 모든 계정에 설정된 권한으로 작업을 수행하는 것을 방지하게 됩니다. 이 조치는 활성 AWS 액세스 포털 세션을 사용하여 다른 계정으로 이동하고 다른 역할을 맡더라도 사용자의 작업을 차단합니다. SCP에 의해 사용자의 액세스가 완전히 차단된 경우 로그인, 할당 취소 및 필요한 경우 AWS 액세스 포털 세션 중지 기능을 비활성화할 수 있습니다.

SCP를 사용하는 대신 권한 세트의 인라인 정책 및 사용자가 액세스할 수 있는 권한 세트에서 사용하는 고객 관리형 정책에 거부 정책을 포함시킬 수도 있습니다.

둘 이상의 사용자에게 대한 액세스를 취소해야 하는 경우 다음과 같은 조건 블록의 값 목록을 사용할 수 있습니다.

```

    "Condition": {
      "StringEquals": {
        "identitystore:userId": [" user1 userId", "user2 userId"...]
      }
    }
  }

```

⚠ Important

사용하는 메서드에 관계없이 다른 수정 조치를 취하고 사용자의 사용자 ID를 정책에 최소 12시간 동안 유지해야 합니다. 이 시간이 지나면 사용자가 수입한 모든 역할이 만료되며 거부 정책에서 사용자 ID를 제거할 수 있습니다.

리소스 정책, Amazon EKS 클러스터 구성 맵 및 AWS KMS 키 정책에서 권한 세트 참조

AWS 계정에 권한 세트를 할당하면 IAM Identity Center는 이름이 로 시작하는 역할을 생성합니다AWSReservedSSO_.

역할에 대한 전체 이름 및 Amazon 리소스 이름(ARN)은 다음 형식을 사용합니다.

이름	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/ <i>aws-region</i> /AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

IAM Identity Center의 ID 소스가 us-east-1에서 호스트되는 경우 ARN에는 *aws-region*이 없습니다. 역할에 대한 전체 이름 및 ARN은 다음 형식을 사용합니다.

이름	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/

이름	ARN
	AWSReservedSSO_ <i>permission-set-name-unique-suffix</i>

예를 들어 데이터베이스 관리자에게 AWS 계정 액세스 권한을 부여하는 권한 세트를 생성하면 다음 이름과 ARN으로 해당 역할이 생성됩니다.

이름	ARN
AWSReservedSSO_DatabaseAdministrator_1234567890abcdef	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef

AWS 계정에서이 권한 세트에 대한 모든 할당을 삭제하면 IAM Identity Center가 생성한 해당 역할도 삭제됩니다. 나중에 같은 권한 집합에 새 할당을 하면 IAM Identity Center에서 권한 집합에 대한 새 역할을 생성합니다. 새 역할의 이름 및 ARN에는 다른 고유한 접미사가 포함됩니다. 이 예제에서 고유한 접미사는 abcdef0123456789입니다.

이름	ARN
AWSReservedSSO_DatabaseAdministrator_ abcdef0123456789	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ abcdef0123456789

역할에 대한 새 이름 및 ARN의 접미사가 변경되면 원래 이름과 ARN을 참조하는 모든 정책이 만료되어 해당 권한 집합을 사용하는 개인의 액세스가 중단될 수 있습니다. 예를 들어, 다음 구성에서 원래 ARN을 참조하는 경우 역할에 대한 ARN이 변경되면 권한 집합의 사용자 액세스가 중단됩니다.

- 클러스터 액세스에 aws-auth ConfigMap를 사용할 때 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터의 aws-auth ConfigMap 파일.

- AWS Key Management Service (AWS KMS) 키에 대한 리소스 기반 정책. 이 정책을 키 정책이라고도 합니다.

Note

[Amazon EKS 액세스 항목](#)을 사용하여 Amazon EKS 클러스터에 대한 액세스를 관리하는 것이 좋습니다. 이를 통해 IAM 권한을 사용하여 Amazon EKS 클러스터에 액세스할 수 있는 위탁자를 관리할 수 있습니다. Amazon EKS 액세스 항목을 사용하면 Amazon EKS 권한이 있는 IAM 위탁자를 사용하여 지원에 연락하지 않고 클러스터에 대한 액세스를 다시 획득할 수 있습니다.

권한 세트에 해당하는 역할에 대한 새 ARN을 참조하도록 대부분의 AWS 서비스에 대한 리소스 기반 정책을 업데이트할 수 있지만 ARN이 변경 AWS KMS 되면 Amazon EKS용 IAM에서 생성하는 백업 역할이 있어야 합니다. Amazon EKS의 경우 백업 IAM 역할이 `aws-auth ConfigMap`에 있어야 합니다. AWS KMS의 경우 키 정책에 있어야 합니다. `aws-auth ConfigMap` 또는 AWS KMS 키 정책을 업데이트할 권한이 있는 백업 IAM 역할이 없는 경우에 문의하여 해당 리소스 지원에 다시 액세스할 수 있습니다.

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.

`aws-auth ConfigMap` Amazon EKS용에서 참조하는 역할,의 키 정책 AWS KMS또는 다른의 리소스 기반 정책이 포함된 AWS 계정에서이 할당을 유지 관리합니다 AWS 서비스.

예를 들어 `EKSAccess` 권한 세트를 생성하고 AWS 계정에서 해당 역할 ARN을 참조하는 경우 `111122223333` 해당 계정의 권한 세트에 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.

- **aws-auth ConfigMap** 및를 사용하는 Amazon EKS 클러스터의 경우 AWS KMS: IAM에서 생성된 역할을 포함합니다.

`aws-auth ConfigMap` Amazon EKS 클러스터용 또는 AWS KMS 키용 키 정책에서 권한 세트의 역할 ARNs을 참조하는 경우 IAM에서 생성한 하나 이상의 역할도 포함하는 것이 좋습니다. 역할은 Amazon EKS 클러스터에 액세스하거나 AWS KMS 키 정책을 관리할 수 있도록 허용해야 합니다.

다. 권한 집합이 이 역할을 맡을 수 있어야 합니다. 이렇게 하면 권한 세트의 역할 ARN이 변경되면 aws-auth ConfigMap 또는 AWS KMS 키 정책에서 ARN에 대한 참조를 업데이트할 수 있습니다. 다음 섹션에서는 IAM에서 생성된 역할에 대해 신뢰 정책을 생성하는 방법의 예를 제공합니다. AdministratorAccess 권한 집합으로만 역할을 수입할 수 있습니다.

사용자 지정 신뢰 정책 예

다음은 IAM에서 생성된 역할에 대한 액세스 권한이 있는 AdministratorAccess 권한 집합을 제공하는 사용자 지정 신뢰 정책의 예입니다. 다음은 이 정책의 주요 요소입니다.

- 이 신뢰 정책의 보안 주체 요소는 AWS 계정 보안 주체를 지정합니다. 이 정책에서 sts:AssumeRole 권한이 111122223333 있는 AWS 계정의 보안 주체는 IAM에서 생성된 역할을 수입할 수 있습니다.
- 이 신뢰 정책의 Condition element에는 IAM에서 생성된 역할을 수입할 수 있는 보안 주체에 대한 추가 요구 사항이 명시되어 있습니다. 이 정책에서는 다음 역할 ARN을 가진 권한 집합이 역할을 수입할 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, 권한 집합의 역할 ARN이 변경되더라도 정책에서는 권한 집합이 IAM에서 생성된 역할을 수입하도록 허용합니다.

JSON

```
{
  "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_*"
      }
    }
  }
}

```

이러한 정책에 IAM에서 생성한 역할을 포함하면 권한 세트 AWS KMS keys 또는 권한 세트에 대한 모든 할당이 실수로 삭제되고 다시 생성되는 경우 Amazon EKS 클러스터 또는 기타 AWS 리소스에 대한 긴급 액세스 권한이 제공됩니다.

속성 기반 액세스 제어

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. IAM Identity Center를 사용하면 모든 IAM Identity Center ID 소스에서 가져온 사용자 속성을 AWS 계정 사용하여 여러에서 리소스에 대한 액세스를 관리할 수 있습니다. AWS에서는 이러한 속성을 태그라고 합니다. 여기서 사용자 속성을 태그로 사용하면에서 세분화된 권한을 생성하는 프로세스를 AWS 간소화 AWS 하고 작업 인력이 일치하는 태그가 있는 AWS 리소스에만 액세스할 수 있습니다.

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 AWS 계정 IAM Identity Center는 AWS 세션에서 팀 이름 속성을 전송하므로 Bob과 Sally는 팀 이름 속성이 AWS 프로젝트 리소스의 팀 이름 태그와 일치하는 경우에만 프로젝트 리소스에 액세스할 수 있습니다. 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 세트 및 리소스 기반 정책에서 이러한 사용자 속성을 사용하여 AWS 리소스에 ABAC를 구현하고 대규모 권한 관리를 간소화할 수 있습니다.

이점

다음은 IAM Identity Center에서 ABAC를 사용할 때 얻을 수 있는 추가 이점입니다.

- ABAC는 더 적은 수의 권한 세트 필요 – 각 직무에 대해 서로 다른 정책을 생성할 필요가 없기 때문에 생성해야 하는 권한 세트 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 관리자는의 사용자 속성을 검토하여의 사용자 활동을 추적 하여 세션의 ID AWS CloudTrail 를 쉽게 확인할 수 있습니다 AWS.

IAM Identity Center 콘솔을 사용하여 ABAC를 구성하는 방법에 대한 자세한 내용은 [액세스 제어](#)를 위한 속성

섹션을 참조하세요. IAM Identity Center API를 사용하여 ABAC를 활성화하고 구성하는 방법에 대한 자세한 내용은 IAM Identity Center API 참조 가이드의 [CreateInstanceAccessControlAttributeConfiguration](#)을 참조하세요.

주제

- [체크리스트: IAM Identity Center AWS 를 사용하여에서 ABAC 구성](#)
- [액세스 제어를 위한 속성](#)

체크리스트: IAM Identity Center AWS 를 사용하여에서 ABAC 구성

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	Task	레퍼런스
1	모든 AWS 리소스에 태그를 추가하는 방법을 검토합니다. IAM Identity Center에서 ABAC를 구현하려면 먼저 ABAC를 구현하려는 모든 AWS 리소스에 태그를 추가해야 합니다.	• AWS 리소스 태그 지정
2	ID 스토어의 관련 사용자 ID 및 속성을 사용하여 IAM Identity Center에서 ID 소스를 구성하는 방법을 검토합니다. IAM Identity Center를 사용하면에서 ABAC에 대해	• ID 소스 관리

단계	Task	레퍼런스
	지원되는 모든 IAM Identity Center ID 소스의 사용자 속성을 사용할 수 있습니다 AWS.	
3	다음 기준에 따라에서 액세스 제어 결정을 내리는 데 사용할 속성을 결정 AWS 하고 IAM Identity Center로 전송합니다. - 외부 ID 제공업체(IdP)를 사용하는 경우 IdP에서 전달된 속성을 사용할지 아니면 IAM Identity Center 내에서 속성을 선택할지를 결정합니다. - IdP가 속성을 전송하도록 선택한 경우 SAML 어설션에서 속성을 전송하도록 IdP를 구성합니다. 특정 IdP에 대한 절차에서 Optional 섹션을 참조하세요. - 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. - Active Directory 또는 IAM Identity Center를 ID 소스로 사용하거나 IdP를 사용하고 IAM Identity Center에서 속성을 선택하도록 선택한 경우 구성할 수 있는 가능한 속성을 검토합니다. 그런 다음 바로 4단계로 이동하여 IAM Identity Center 콘솔을 사용하여 ABAC 속성 구성을 시작합니다.	시작하기 외부 ID 제공업체를 ID 소스로 사용할 때의 속성 선택 IAM Identity Center의 ID 소스 자습서 SCIM을 사용하여 외부 ID 제공업체의 사용자 및 그룹 프로비저닝 지원되는 외부 ID 제공업체 속성 IAM Identity Center를 ID 소스로 사용할 때의 속성 선택 를 자격 증명 소스 AWS Managed Microsoft AD 로 사용할 때 속성 선택 IAM Identity Center와 Microsoft AD 간의 기본 매핑
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. ID와 해당 속성이 IAM Identity Center에 있는 경우 액세스 제어 결정에 AWS 계정 사용할 키-값 페어(매핑)를 생성해야 합니다.	액세스 제어를 위한 속성 활성화 및 구성

단계	Task	레퍼런스
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. <code>aws:PrincipalTag/key</code> 조건을 사용하여 권한 정책의 액세스 제어 속성을 참조할 수 있습니다.	IAM Identity Center에서 ABAC에 대한 권한 정책 생성
6	다양한에서 5단계에서 생성한 권한 세트에 사용자를 AWS 계정할당합니다. 이렇게 하면 계정에 페더레이션하고 AWS 리소스에 액세스할 때 일치하는 태그를 기반으로만 액세스할 수 있습니다.	에 사용자 또는 그룹 액세스 할당 AWS 계정

이 단계를 완료하면 Single Sign-On을 AWS 계정 사용하여 페더레이션하는 사용자는 일치하는 속성을 기반으로 AWS 리소스에 액세스할 수 있습니다.

액세스 제어를 위한 속성

액세스 제어 속성은 정책에 사용하여 리소스에 대한 액세스를 제어하려는 사용자 속성을 선택하는 IAM Identity Center 콘솔의 페이지 이름입니다. 사용자 ID 소스의 기존 속성을 AWS 기반으로에서 워크로드에 사용자를 할당할 수 있습니다.

예를 들어 부서 이름을 기반으로 S3 버킷에 대한 액세스를 할당하려고 한다고 가정해 보겠습니다. 액세스 제어에 속성 페이지 있는 동안 속성 기반 액세스 제어(ABAC)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 사용자의 부서 속성을 액세스 중인 계정에 전달합니다. 그런 다음 속성을 사용하여 정책을 기반으로 액세스를 결정합니다. ABAC에 대한 자세한 내용은 [속성 기반 액세스 제어](#) 섹션을 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.

를 자격 증명 소스 AWS Managed Microsoft AD 로 사용할 때 속성 선택

를 ID 소스 AWS Managed Microsoft AD 로 사용하여 IAM Identity Center를 구성할 때 먼저 Active Directory의 속성 세트를 IAM Identity Center의 사용자 속성에 매핑합니다. 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 AWS Managed Microsoft AD 디렉터리의 사용자 속성에 대한 기본 매핑 목록은 섹션을 참조하세요 [IAM Identity Center와 Microsoft AD 간의 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. 속성에 대해 외부 IdP를 신뢰하기로 결정한 경우 사용자가 AWS 계정에 페더레이션할 때 이러한 속성이 항상 전달됩니다. 동일한 속성이 SAML과 SCIM을 통해 IAM Identity Center로 들어오는 시나리오에서는 액세스 제어 결정에서 SCIM 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 IdP에 대한 [IAM Identity Center의 ID 소스 자습서](#) 항목을 참조하세요.

- 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 IdP의 사용자 속성에 지원되는 속성의 전체 목록은 [지원되는 외부 ID 제공업체 속성](#)을 참조하세요.

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

속성 기반 액세스 제어(ABAC)를 사용하려면 먼저 IAM Identity Center 콘솔의 설정 페이지 또는 [IAM Identity Center API](#)에서 이를 활성화해야 합니다. ID 소스와 관계없이 언제든지 자격 증명 스토어에서 사용자 속성을 구성하여 ABAC에 사용할 수 있습니다. 콘솔에서 설정 페이지의 액세스 제어 속성 탭으로 이동하여 이 작업을 수행할 수 있습니다. 외부 ID 제공업체(IdP)를 ID 소스로 사용하는 경우 SAML 어설션에서 외부 IdP로부터 속성을 수신하도록 선택할 수도 있습니다. 이 경우 원하는 속성을 보내도록 외부 IdP를 구성해야 합니다. SAML 어설션의 속성이 IAM Identity Center에서 ABAC 속성으로도 정의되어 있는 경우 IAM Identity Center는 AWS 계정에 로그인 시 자격 증명 스토어의 값을 [세션 태그](#)로 보냅니다.

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 페더레이션할 때 해당 속성이 AWS 계정 로 직접 전송됩니다. 속성은 IAM Identity Center에서 매핑에 사용할 수 없습니다.

주제

- [액세스 제어에 속성 활성화](#)

- [액세스 제어를 위한 속성 선택](#)
- [액세스 제어의 속성 비활성화](#)

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 정책이 있어야 합니다. 계정에 권한 집합을 생성하지 않은 경우에는 이러한 추가 보안 제한이 필요하지 않습니다. IAM Identity Center 인스턴스가 2020년 12월 이전에 생성되었고 해당 인스턴스에서 ABAC를 활성화하려는 경우 계정에 권한 세트가 생성되었는지 여부에 관계없이 IAM Identity Center 관리 역할과 연결된 iam:UpdateAssumeRolePolicy 정책이 있어야 합니다.

액세스 제어의 속성을 활성화하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 액세스 제어 정보의 속성 정보 상자를 찾은 다음 활성화를 선택합니다. 다음 절차를 계속 진행하여 구성합니다.

액세스 제어를 위한 속성 선택

다음 절차에 따라 ABAC 구성의 속성을 설정합니다.

IAM Identity Center 콘솔을 사용하여 속성을 선택하려면

1. [IAM Identity Center 콘솔](#)을 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.

Key ⓘ	Value (optional) ⓘ	Remove
Department	<code>\${path:enterprise.department}</code>	✕
CostCenter	<code>\${path:enterprise.costCenter}</code>	✕
Add new key	Add new value	

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 CostCenter와 같이 비슷하게 일치하는 이름을 키이름으로 입력합니다. 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 [IAM Identity Center와 외부 ID 제공업체 디렉터리 간의 속성 매핑](#)에 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 저장을 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](#) 섹션을 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 콘솔](#)을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 액세스 제어용 속성 탭을 선택한 다음 속성 관리를 선택합니다.
4. 액세스 제어 속성 관리 페이지에서 비활성화를 선택합니다.
5. 액세스 제어 속성 비활성화 대화 창에서 정보를 검토하고 준비가 되면 **DISABLE**를 입력한 다음 확인을 선택합니다.

Important

이 단계를 진행하면 외부 ID 소스 제공업체의 SAML 어설션에 속성이 있는지 여부와 관계 없이 모든 속성이 삭제되고 AWS 계정 에 페더레이션할 때 액세스 제어 속성의 사용이 중지됩니다.

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 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 AWS 페더레이션할 때 세션에 비용 센터 정보를 전달합니다 AWS 계정. 따라서 조직에서 새 리소스 및 개발자를 비용 센터에 추가하면 개발자는 권한 업데이트 없이 비용 센터에 맞춰 리소스를 관리할 수 있습니다.

JSON

```
{
  "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 참조하십시오.

IAM Identity Center 서비스 연결 역할 파악

[서비스 연결 역할](#)은 사전 정의된 IAM 권한으로, 이를 통해 IAM Identity Center가 AWS Organizations에서 조직의 특정 AWS 계정에 대한 Single Sign-on 액세스 권한을 가진 사용자를 위임하고 적용할 수 있습니다. 이 서비스는 조직 AWS 계정 내 모든에서 서비스 연결 역할을 프로비저닝하여이 기능을 활성화합니다. 그런 다음이 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](#) 섹션을 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 내용은 [에 대한 액세스 구성 AWS 계정](#) 단원을 참조하십시오.

각에서 생성되는 서비스 연결 역할의 이름은 AWS 계정입니다AWSServiceRoleForSSO. 자세한 내용은 [IAM Identity Center 서비스 연결 역할 사용](#) 단원을 참조하십시오.

참고

- AWS Organizations 관리 계정에 로그인한 경우 서비스 연결 역할이 아닌 현재 로그인한 역할을 사용합니다. 이렇게 하면 권한이 에스컬레이션되는 것을 방지할 수 있습니다.
- IAM Identity Center가 AWS Organizations 관리 계정에서 IAM 작업을 수행하면 모든 작업은 IAM 보안 주체의 자격 증명을 사용하여 수행됩니다. 이렇게 하면 CloudTrail의 로그에서 누가 관리 계정의 모든 권한을 변경했는지 파악할 수 있습니다.

AWS 액세스 포털 설정 및 사용

AWS 액세스 포털은 IAM Identity Center를 통해 작업 인력을 AWS 계정 및 클라우드 애플리케이션에 연결합니다. 관리자는 포털을 구성하고 사용자 액세스를 관리하는 한편, 최종 사용자는 한 번 로그인하여 승인된 모든 리소스에 원활하게 액세스할 수 있습니다.

AWS 액세스 포털은 다음에 대한 Single Sign-On 액세스를 제공합니다.

- AWS 계정 조직의 .
- AWS Amazon Quick 및 Kiro와 같은 관리형 애플리케이션.
- Office 365, Concur, Salesforce 등과 같은 클라우드 애플리케이션.

사용자가 포털에 로그인하면 추가 로그인 없이 액세스할 수 있는 권한이 있는 AWS 계정 및 애플리케이션을 찾습니다.

AWS 액세스 포털 시작하기

관리자의 경우:

AWS 액세스 포털을 구성하고 사용자 액세스를 관리하려면 IAM Identity Center의 [조직 인스턴스](#) 또는 [계정 인스턴스](#)에 대한 관리 액세스 권한이 필요합니다.

1. 선택적으로 AWS 액세스 포털 URL을 사용자 지정합니다.
2. AWS 계정 및 애플리케이션에 대한 사용자 액세스 권한을 할당합니다. 할당된 AWS 리소스가 포털에 표시됩니다.

최종 사용자의 경우:

관리자가 AWS 액세스 포털 설정을 완료하고 포털 URL과 로그인 자격 증명을 제공해야 합니다.

1. 관리자로부터 포털 URL을 받습니다(일반적으로 `https://your-company.awsapps.com/start`).
2. 관리자가 제공한 자격 증명을 사용하여 로그인합니다.
3. 포털의 리소스에 액세스합니다.

AWS 액세스 포털 구성

관리자는 조직의 요구 사항에 맞게 AWS 액세스 포털을 사용자 지정하고 사용자가 승인된 리소스에 쉽게 액세스할 수 있도록 할 수 있습니다.

구성할 수 있는 항목

AWS 액세스 포털 활성화: 사용자 자격 증명 활성화 및 최초 로그인 프로세스를 포함하여 AWS 액세스 포털에 대한 초기 사용자 액세스를 설정합니다.

사용자 지정 AWS 액세스 포털 URL(선택 사항): 조직의 AWS 액세스 포털 URL을 기본 형식()에서 보다 인식 가능한 하위 도메인(d-xxxxxxxxx.awsapps.com/start)으로 개인화합니다your-company.awsapps.com/start.

시작하기 전 준비 사항

IAM Identity Center에 대한 관리 액세스 권한이 있는지 확인하고, IAM Identity Center가 [조직 인스턴스](#) 또는 [계정 인스턴스](#)로 설정되어 있는지 확인하고, 사용자 지정 하위 도메인 이름을 계획합니다(나중에 변경할 수 없는 일회성 구성임).

구성이 완료되면 사용자는 사용자 지정 URL을 사용하여 AWS 액세스 포털에 액세스하고 조직에 대해 설정한 활성화 프로세스를 따를 수 있습니다.

주제

- [처음 IAM Identity Center 사용자를 위한 AWS 액세스 포털 활성화](#)
- [AWS 액세스 포털 URL 사용자 지정](#)
- [사용자가 AWS 액세스 포털에 로그인할 수 있는지 확인](#)

처음 IAM Identity Center 사용자를 위한 AWS 액세스 포털 활성화

AWS 액세스 포털에 처음 로그인하는 경우 이메일에서 사용자 자격 증명을 활성화하는 방법에 대한 지침을 확인하세요.

사용자 보안 인증 정보 활성화

1. 회사로부터 받은 이메일에 따라 다음 방법 중 하나를 선택하여 AWS 액세스 포털 사용을 시작할 수 있도록 사용자 자격 증명을 활성화합니다.

- a. AWS IAM Identity Center 가입 초대라는 제목의 이메일을 받은 경우 이메일을 열어 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 암호를 제공하여 사용자 자격 증명을 활성화하면 AWS 액세스 포털에서 자동으로 로그인합니다. 이 문제가 해결되지 않으면 [AWS 액세스 포털에 로그인](#) 섹션에 나와 있는 지침에 따라 AWS 액세스 포털에 수동으로 로그인할 수 있습니다.

AWS 액세스 포털 URL 사용자 지정

기본적으로 다음 형식의 URL을 사용하여 AWS 액세스 포털에 액세스할 수 있습니다: `다d-xxxxxxxxxx.awsapps.com/start`. 다음과 같이 URL을 사용자 지정할 수 있습니다: `your_subdomain.awsapps.com/start`.

Important

AWS 액세스 포털 URL을 변경하면 나중에 편집할 수 없습니다.

URL을 사용자 지정하는 방법

1. <https://console.aws.amazon.com/singlesignon/> AWS IAM Identity Center 콘솔을 엽니다.
2. IAM Identity Center 콘솔 탐색 창에서 대시보드를 선택하고 설정 요약 섹션을 찾습니다.
3. AWS 액세스 포털 URL 아래에서 사용자 지정 버튼을 선택합니다.

Note

사용자 지정 버튼이 표시되지 않을 경우 이는 AWS 액세스 포털이 이미 사용자 지정되었음을 의미합니다. AWS 액세스 포털 URL을 사용자 지정하는 작업은 되돌릴 수 없는 일회성 작업입니다.

4. 원하는 서브도메인 이름을 입력하고 저장을 선택합니다.

이제 사용자 지정 URL을 사용하여 AWS 액세스 포털을 통해 AWS 콘솔에 로그인할 수 있습니다.

사용자가 AWS 액세스 포털에 로그인할 수 있는지 확인

다음 단계는 IAM Identity Center 관리자가 IAM Identity Center 사용자가 AWS 액세스 포털에 로그인하고 액세스할 수 있는지 확인하는 것입니다 AWS 계정.

AWS 액세스 포털에 로그인

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 사용 중 AWS (IAM 자격 증명) - IAM 자격 증명으로 로그인하고 관리자 역할을 선택합니다.
2. [IAM Identity Center 콘솔](#)을 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 자격 증명을 사용하여 로그인합니다.
 - 기본 Identity Center 디렉터리를 ID 소스로 사용하는 경우, 사용자를 생성할 때 지정한 사용자 이름과 해당 사용자에게 지정한 새 암호를 사용하여 로그인합니다.
6. 계정 탭에서를 찾아 AWS 계정 확장합니다.
7. 사용할 수 있는 역할이 표시됩니다. 예를 들어, AdministratorAccess 권한 세트와 Billing 권한 세트가 모두 할당된 경우 해당 역할은 AWS 액세스 포털에 표시됩니다. 세션에 사용할 IAM 역할 이름을 선택합니다.
8. AWS 관리 콘솔로 리디렉션되면에 대한 액세스 설정을 성공적으로 완료한 것입니다 AWS 계정.

Note

목록에 AWS 계정이 표시되지 않으면 사용자에게 해당 계정에 대한 권한 세트가 아직 할당되지 않았을 가능성이 높습니다. 권한 세트에 사용자를 할당하는 방법에 대한 지침은 [예 사용자 또는 그룹 액세스 할당 AWS 계정](#)을 참조하세요.

이제 IAM Identity Center 자격 증명을 사용하여 로그인할 수 있음을 확인했으므로에 로그인 AWS Management Console 하고 루트 사용자 또는 IAM 사용자 자격 증명에서 로그아웃하는 데 사용한 브라우저로 전환합니다.

Important

AWS 액세스 포털에 로그인할 때 IAM 사용자 또는 루트 사용자 자격 증명을 사용하는 대신 IAM Identity Center 관리 사용자의 자격 증명을 사용하여 관리 작업을 수행하는 것이 좋습니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 다른 사용자가 계정과 애플리케이션에 액세스하고 IAM Identity Center를 관리하도록 활성화하려면 IAM Identity Center로만 권한 세트를 생성하고 할당합니다.

AWS 액세스 포털 사용

포털에서 AWS 계정 또는 애플리케이션 탭을 선택하여 여러 애플리케이션을 시작할 수 있습니다. AWS 액세스 포털에 애플리케이션 아이콘이 있다는 것은 회사의 관리자가 해당 AWS 계정 또는 애플리케이션에 대한 액세스 권한을 부여했음을 의미합니다. 또한 추가 로그인 프롬프트 없이 AWS 액세스 포털에서 이러한 모든 계정 또는 애플리케이션에 액세스할 수 있습니다.

AWS 액세스 포털 사용 방법

AWS 액세스 포털을 사용하려면:

1. 관리자로부터 포털 URL을 받습니다(일반적으로 `https://your-company.awsapps.com/start`와 같음).
2. 관리자가 제공한 자격 증명을 사용하여 로그인합니다.
3. 포털에서 액세스하려는 계정과 애플리케이션을 선택합니다.

역할 및 권한에 따라 포털에 표시되는 내용은 관리자가 제어합니다. 다음과 같은 상황에서는 관리자에게 문의해 추가 액세스 권한을 요청합니다.

- 액세스해야 하는 AWS 계정 또는 애플리케이션이 표시되지 않습니다.
- 특정 계정 또는 애플리케이션에 대한 액세스 권한이 예상했던 것과 다릅니다.

주제

- [AWS 액세스 포털에 로그인](#)

- [AWS 액세스 포털 사용자 암호 재설정](#)
- [AWS CLI AWS SDKs에 대한 IAM Identity Center 사용자 자격 증명 가져오기](#)
- [AWS Management Console 대상에 대한 바로 가기 링크 생성](#)
- [MFA를 위한 디바이스 등록](#)
- [활성 세션 보기 및 종료](#)

AWS 액세스 포털에 로그인

AWS 액세스 포털은 IAM Identity Center 사용자에게 웹 포털을 통해 할당된 모든 AWS 계정 및 애플리케이션에 대한 Single Sign-On 액세스를 제공합니다. 다음은 AWS 액세스 포털에 로그인하는 방법, 로그인 팁, AWS 액세스 포털에서 로그아웃하는 방법을 간략하게 설명합니다.

사전 조건

AWS 액세스 포털을 사용하려면 IAM Identity Center를 활성화해야 합니다. 자세한 내용은 [IAM Identity Center 활성화](#) 단원을 참조하십시오.

Note

로그인한 후 AWS 액세스 포털 세션의 기본 기간은 8시간입니다. 관리자는 이 세션의 [지속 시간을 변경](#)할 수 있습니다.

AWS 액세스 포털에 로그인

AWS 액세스 포털에 로그인하려면

1. 브라우저 창에서 제공 받은 로그인 URL을 붙여넣고 Enter를 선택합니다. 이 URL은 d-xxxxxxxxxx.awsapps.com/start 또는 *your_subdomain*.awsapps.com/start와 같은 형식입니다. 나중에 빠르게 액세스할 수 있도록 지금 이 포털 링크를 북마크하는 것이 좋습니다.
2. 표준 회사 로그인 자격 증명을 사용하여 로그인합니다.

Note

소속 관리자가 이메일로 일회용 암호(OTP)를 보내왔고 이번이 처음 로그인인 경우 해당 암호를 입력하십시오. 로그인 후에는 향후 로그인에 사용할 새 암호를 만들어야 합니다.

확인 코드를 입력하라는 메시지가 표시되면 이메일을 확인한 다음 코드를 복사하여 로그인 페이지에 붙여 넣습니다.

Note

확인 코드는 보통 이메일로 전송되지만 전달 방법은 다를 수 있습니다. 자세한 내용은 관리자에게 확인하세요.

- 로그인한 후에는 포털에 표시되는 AWS 계정 모든 및 애플리케이션에 액세스할 수 있습니다.

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 포털 로그인 팁

다음은 AWS 액세스 포털 경험을 관리하는 데 도움이 되는 몇 가지 팁입니다.

- 경우에 따라 로그아웃했다가 AWS 액세스 포털에 다시 로그인해야 할 수 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 애플리케이션의 아이콘을 선택하여 포털에 나열된 애플리케이션을 열 수 있습니다. 애플리케이션 사용을 완료한 후 애플리케이션을 닫거나 AWS 액세스 포털에서 로그아웃할 수 있습니다. 애플리케이션을 닫으면 해당 애플리케이션에서만 로그아웃됩니다. AWS 액세스 포털에서 열어본 다른 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 로그인하면 역할로 전환할 수 있습니다. 역할을 전환하면 기존 사용자 권한이 일시적으로 무효화되고 역할에게 할당된 권한이 부여됩니다. 자세한 내용은 [역할\(콘솔\) 전환](#)을 참조하세요.

AWS 액세스 포털에서 로그아웃

포털에서 로그아웃하면 브라우저 세션에서 보안 인증이 완전히 제거됩니다. 자세한 내용은 AWS Sign-In 가이드의 [AWS 액세스 포털에서 로그아웃](#)을 참조하세요.

AWS 액세스 포털에서 로그아웃하려면

- AWS 액세스 포털의 탐색 모음에서 로그아웃을 선택합니다.

Note

다른 사용자로 로그인하려면 먼저 AWS 액세스 포털에서 로그아웃해야 합니다.

AWS 액세스 포털 사용자 암호 재설정

AWS 액세스 포털은 [IAM Identity Center](#) 사용자에게 웹 포털을 통해 할당된 모든 AWS 계정 및 클라우드 애플리케이션에 대한 Single Sign-On 액세스를 제공합니다. AWS 액세스 포털은 AWS 리소스 관리를 위한 서비스 콘솔 모음 [AWS Management Console](#)인과 다릅니다.

이 절차를 사용하여 AWS 액세스 포털의 IAM Identity Center 사용자 암호를 재설정합니다. AWS Sign-In 사용 설명서에서 [사용자 유형](#)에 대해 자세히 알아보세요.

고려 사항

AWS 액세스 포털의 암호 재설정 기능은 Identity Center 디렉터리를 사용하거나 자격 증명 소스 [AWS Managed Microsoft AD](#)로 사용하는 Identity Center 인스턴스의 사용자만 사용할 수 있습니다. 사용자가 외부 ID 제공업체 또는 [AD Connector](#)에 연결된 경우 사용자 암호 재설정은 외부 ID 제공업체 또는 연결된 Active Directory에서 수행해야 합니다.

- ID 소스가 IAM Identity Center 디렉터리인 경우 [IAM Identity Center에서 ID를 관리할 때 암호 요구 사항을](#) 참조하세요.
- ID 소스가 AWS Managed Microsoft AD인 경우 [AWS Managed Microsoft AD에서 암호 재설정 시 암호 요구 사항을](#) 참조하세요.

AWS 액세스 포털로 암호를 재설정하려면

1. 웹 브라우저를 열고 AWS 액세스 포털의 로그인 페이지로 이동합니다.

AWS 액세스 포털 URL이 없는 경우 이메일을 확인하세요. AWS 액세스 포털에 대한 특정 로그인 URL이 포함된 AWS IAM Identity Center 가입 초대장을 이메일로 받으셨을 것입니다. 또는 관리자가 일회용 암호와 AWS 액세스 포털 URL을 직접 제공했을 수 있습니다. 이 정보를 찾을 수 없는 경우 관리자에게 해당 정보를 보내 달라고 요청합니다.

AWS 액세스 포털 로그인에 대한 자세한 내용은 AWS Sign-In 사용 설명서 [의 AWS 액세스 포털에 로그인](#)을 참조하세요.

2. 사용자 이름을 입력하고 다음을 선택합니다.
3. 암호에서 암호 분실을 선택합니다.

사용자 ID를 인증하고 제공된 이미지의 문자를 입력하여 로봇이 아님을 확인합니다. 그리고 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.aws로부터 암호 재설정이 요청됨이라는 제목의 이메일이 전송됩니다. 이메일에서 암호 재설정을 선택합니다.
6. 암호 재설정 페이지에서 사용자 이름을 확인하고 AWS 액세스 포털의 새 암호를 지정한 다음 새 암호 설정을 선택합니다.
7. no-reply@signin.aws로부터 암호가 업데이트됨이라는 이메일이 전송됩니다.

Note

관리자는 암호 재설정 지침이 포함된 이메일을 보내거나 일회용 암호를 생성하여 공유함으로 써 암호를 재설정할 수 있습니다. 관리자인 경우 [IAM Identity Center 최종 사용자 암호 재설정](#) 단원을 참조하십시오.

AWS CLI AWS SDKs에 대한 IAM Identity Center 사용자 자격 증명 가져오기

AWS Command Line Interface 또는 AWS 소프트웨어 개발 키트(SDKs)를 IAM Identity Center의 사용자 자격 증명과 함께 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 및 클라우드 애플리케이션에 대한 AWS 계정 Single Sign-On 액세스를 제공합니다. IAM Identity Center 사용자로 AWS 액세스 포털에 로그인하면

임시 자격 증명을 얻을 수 있습니다. 그런 다음 AWS CLI 또는 AWS SDKs에서 IAM Identity Center 사용자 자격 증명이라고도 하는 자격 증명을 사용하여 리소스에 액세스할 수 있습니다 AWS 계정.

AWS CLI 를 사용하여 프로그래밍 방식으로 AWS 서비스에 액세스하는 경우이 주제의 절차를 사용하여 액세스를 시작할 수 있습니다 AWS CLI. 에 대한 자세한 내용은 [AWS Command Line Interface 사용 설명서](#)를 AWS CLI참조하세요.

AWS SDKs를 사용하여 프로그래밍 방식으로 AWS 서비스에 액세스하는 경우이 주제의 절차에 따라 AWS SDKs에 대한 인증도 직접 설정됩니다. AWS SDKs에 대한 자세한 내용은 [AWS SDKs 및 도구 참조 안내서를 참조하세요](#).

Note

IAM Identity Center의 사용자는 [IAM 사용자](#)와 다릅니다. IAM 사용자에게는 AWS 리소스에 대한 장기 자격 증명(credential)이 부여됩니다. IAM Identity Center의 사용자에게는 임시 보안 인증(credential)이 부여됩니다. 임시 자격 증명(credential)은 로그인할 때마다 생성 AWS 계정 되므로 액세스하기 위한 보안 모범 사례로 임시 자격 증명(credential)을 사용하는 것이 좋습니다.

사전 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 Center 시작하기](#)를 참조하세요.
- 에 대한 사용자 액세스 AWS 계정 - IAM Identity Center 사용자에게 임시 자격 증명(credential)을 검색할 수 있는 권한을 부여하려면 사용자 또는 관리자가 IAM Identity Center 사용자를 [권한 세트](#)에 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 내용은 [에 사용자 또는 그룹 액세스 할당 AWS 계정](#) 단원을 참조하십시오.
- AWS CLI installed - 임시 자격 증명(credential)을 사용하려면 설치해야 합니다 AWS CLI. 설치 지침은 AWS CLI 사용 설명서의 [AWS CLI의 최신 버전 설치 또는 업데이트](#)를 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 세트로 생성된 IAM 역할은 다음과 같은 AWS Identity and Access Management 방식으로에서 생성된 IAM 역할과 다릅니다.
- IAM Identity Center는 권한 집합으로 생성된 역할을 소유하고 보호합니다. IAM Identity Center만이 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 [주체](#)에 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 사용](#)을 참조하세요.

- 권한 세트의 세션 기간 설정 가능 - AWS 액세스 포털에 로그인하면 IAM Identity Center 사용자에게 할당된 권한 세트가 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 내용은 [에 대한 세션 기간 설정 AWS 계정 단원을 참조하십시오](#).

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 모든 AWS 계정에 대해 할당된 권한 세트와 연결된 모든 역할에 자동으로 액세스할 수 있습니다.

IAM Identity Center 사용자를 위해 생성된 역할에 액세스하려면 `aws configure sso` 명령을 실행한 다음 AWS CLI 브라우저 창에서 권한을 부여합니다. 활성 AWS 액세스 포털 세션이 있는 한은 임시 자격 증명을 AWS CLI 자동으로 검색하고 자격 증명을 자동으로 새로 고칩니다.

자세한 내용은 AWS Command Line Interface 사용 설명서에서 [aws configure sso wizard를 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 보냅니다. 자세한 내용은 [로그인 사용 설명서의 AWS 액세스 포털](#)에 로그인을 참조하세요. AWS
2. 계정 탭에서 자격 증명을 검색할 AWS 계정 를 찾습니다. 계정을 선택하면 해당 계정과 연결된 계정 이름, 계정 ID 및 이메일 주소가 표시됩니다.

Note

목록에 AWS 계정이 표시되지 않으면 해당 계정에 대한 권한 세트가 아직 할당되지 않았을 가능성이 높습니다. 이 경우 관리자에게 연락하여 이 액세스 권한을 추가해 달라고 요청합니다. 자세한 내용은 [에 사용자 또는 그룹 액세스 할당 AWS 계정](#) 단원을 참조하십시오.

3. 계정 이름 아래에는 IAM Identity Center 사용자에게 할당된 권한 집합이 사용 가능한 역할로 표시됩니다. 예를 들어 IAM Identity Center 사용자가 계정에 대한 PowerUserAccess 권한 세트에 할당된 경우 AWS 액세스 포털에 역할이 PowerUserAccess로 표시됩니다.
4. 역할 이름 옆의 옵션에 따라 액세스 키를 선택하거나 명령줄 또는 프로그래밍 방식 액세스를 선택합니다.
5. 자격 증명 받기 대화 상자에서 AWS CLI를 설치한 운영 체제에 따라 macOS 및 Linux, Windows 또는 PowerShell을 선택합니다.
6. AWS IAM Identity Center 보안 인증(권장)에 SSO Start URL과 SSO Region가 표시됩니다. 이 값은 IAM Identity Center 지원 프로파일과 sso-session을 AWS CLI에 구성하는 데 필요합니다. 이 구성을 완료하려면 AWS Command Line Interface 사용 설명서의 [aws configure sso wizard로 프로필 구성](#) 지침을 따릅니다.

자격 증명만료 AWS 계정 될 때까지 필요에 AWS CLI 따라를 계속 사용합니다.

수동 보안 인증 새로 고침

수동 보안 인증 새로 고침 방법을 사용하여 특정 AWS 계정의 특정 권한 집합과 연결된 역할에 대한 임시 보안 인증을 얻을 수 있습니다. 이렇게 하려면 임시 보안 인증에 필요한 명령을 복사하여 붙여 넣습니다. 이 방법을 사용하면 임시 보안 인증을 수동으로 새로 고침해야 합니다.

임시 자격 증명만료될 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 보냅니다. 자세한 내용은 [로그인 사용 설명서의 AWS 액세스 포털](#)에 로그인을 참조하세요. AWS
2. 계정 탭에서 액세스 자격 증명을 검색할 AWS 계정 를 찾아 확장하여 IAM 역할 이름(예: 관리자)을 표시합니다. IAM 역할 이름 옆의 옵션에 따라 액세스 키를 선택하거나 명령줄 또는 프로그래밍 방식 액세스를 선택합니다.

Note

목록에 AWS 계정이 표시되지 않으면 해당 계정에 대한 권한 세트가 아직 할당되지 않았을 가능성이 높습니다. 이 경우 관리자에게 연락하여 이 액세스 권한을 추가해 달라고 요청합니다. 자세한 내용은 [에 사용자 또는 그룹 액세스 할당 AWS 계정](#) 단원을 참조하십시오.

3. 자격 증명 받기 대화 상자에서 AWS CLI를 설치한 운영 체제에 따라 macOS 및 Linux, Windows 또는 PowerShell을 선택합니다.
4. 다음 옵션 중 하나를 선택합니다.

- 옵션 1: AWS 환경 변수 설정

이 옵션을 선택하면 credentials 파일 및 config 파일의 설정을 포함하여 모든 자격 증명 설정을 재정의할 수 있습니다. 자세한 내용은 AWS CLI 사용 설명서의 [AWS CLI를 구성할 환경 변수](#)를 참조하세요.

이 옵션을 사용하려면 명령을 클립보드에 복사하고 명령을 AWS CLI 터미널 창에 붙여 넣은 다음 Enter 키를 눌러 필요한 환경 변수를 설정합니다.

- 옵션 2: 자격 AWS 증명 파일에 프로필 추가

다양한 보안 인증 집합을 사용하여 명령을 실행하려면 이 옵션을 선택합니다.

이 옵션을 사용하려면 명령을 클립보드에 복사한 다음 명령을 공유 AWS credentials 파일에 붙여 넣어 명명된 새 프로필을 설정합니다. 자세한 정보는 AWS SDK 및 도구 참조 설명서의 [공유 구성 및 자격 증명 파일](#)을 참조하세요. 이 자격 증명을 사용하려면 AWS CLI 명령에서 `--profile` 옵션을 지정합니다. 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 [AWS기반의 도구](#)를 참조하세요.

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 대상에 대한 바로 가기 링크 생성

AWS 액세스 포털에서 생성된 바로 가기 링크는 IAM Identity Center 사용자의 특정 대상 AWS Management Console, 특정 권한 세트 및의 특정 대상으로 안내합니다 AWS 계정.

바로가기 링크는 본인과 협업자의 시간을 절약합니다. AWS 액세스 포털을 포함하여 여러 페이지를 통해 AWS Management Console (예: Amazon S3 버킷 인스턴스 페이지)에서 원하는 대상 URL로 이동하는 대신 바로 가기 링크를 사용하여 동일한 대상으로 자동으로 이동할 수 있습니다.

바로가기 링크 목적지 옵션

바로가기 링크에는 다음과 같이 우선 순위에 따라 제시된 세 가지 목적지 옵션이 있습니다.

- (선택 사항) 바로 가기 링크에 AWS Management Console 지정된의 모든 대상 URL입니다. 예: Amazon S3 버킷 인스턴스 페이지.
- (선택 사항) 해당 권한 집합에 대한 관리자 구성 릴레이 상태 URL. 릴레이 상태 설정에 대한 더 자세한 내용은 [에 빠르게 액세스할 수 있도록 릴레이 상태 설정 AWS Management Console](#)을 참조하세요.
- AWS Management Console 홈. 목적지를 지정하지 않은 경우의 기본 목적지.

Note

대상에 대한 자동 탐색은 IAM Identity Center로 인증되고 AWS 계정 및 대상 URL에 필요한 권한 세트가 할당된 경우에만 성공합니다.

AWS 액세스 포털에는 공유 가능한 바로 가기 링크를 생성하는 데 도움이 되는 바로 가기 생성 버튼이 포함되어 있습니다. 목적지 URL을 지정하려는 경우(이전 목록의 첫 번째 옵션) URL을 클립보드로 복사하여 공유할 수 있습니다.

AWS 액세스 포털에서 바로 가기 링크 생성

1. AWS 액세스 포털에 로그인한 상태에서 계정 탭을 선택한 다음 바로 가기 생성 버튼을 선택합니다.
2. 대화 상자에서 다음을 수행합니다.
 - a. 계정 ID 또는 계정 이름을 AWS 계정 사용하여 선택합니다. 입력 시 드롭다운 메뉴에 이와 일치하는 액세스 가능 계정 ID와 이름이 표시됩니다. 액세스 권한이 있는 계정만 선택할 수 있습니다.
 - b. 드롭다운 목록에서 원하는 IAM 역할을 선택합니다. 이것은 선택한 계정에 대해 사용자에게 할당된 권한 집합입니다. 역할 선택을 생략하면 바로가기 링크 사용 시 선택한 계정에 대해 사용자에게 할당된 역할을 선택하라는 메시지가 표시됩니다.

Note

바로가기 링크로 새 액세스 권한을 부여할 수 없습니다. 바로가기 링크는 사용자에게 이미 할당된 권한 집합에 대해서만 작동합니다. 계정 및 목적지 URL에 대해 사용자에게 할당된 필요한 권한 세트가 없는 경우 액세스가 거부됩니다.

- c. 선택적으로 AWS 액세스 포털 대상 URL을 입력합니다. URL 입력을 생략하면 바로가기 링크 사용 시 앞서 언급한 바로가기 링크 목적지 옵션에 따라 목적지가 자동 결정됩니다.
- d. 바로가기 링크는 입력값에 따라 대화 상자 하단에 생성됩니다. URL 복사 버튼을 선택합니다. 이제 복사된 바로가기 링크로 북마크를 생성하거나 동일한 권한 집합 또는 다른 충분한 권한 집합을 가지고 동일 계정에 액세스할 수 있는 협업자와 이를 공유할 수 있습니다.

URL 인코딩을 사용하여 보안 AWS Management Console 바로 가기 링크 구성

계정 ID, 권한 집합 이름, 목적지 URL 등 URL의 모든 파라미터 값은 URL 인코딩되어야 합니다.

바로 가기 링크는 다음 경로를 사용하여 AWS 액세스 포털 URL을 확장합니다.

/#/console?

account_id=[*account_ID*]&role_name=[*permission_set_name*]&destination=[*destination*]

클래식 AWS 파티션의 전체 URL은 다음 패턴을 따릅니다.

IPv4 엔드포인트:

https://[*your_subdomain*].awsapps.com/start/#/console?

account_id=[*account_ID*]&role_name=[*permission_set_name*]&destination=[*destination*]

듀얼 스택 엔드포인트

https://[*identity_center_instance_id*].portal.[*region*].app.aws/#/console?

account_id=[*account_ID*]&role_name=[*permission_set_name*]&destination=[*destination*]

다음은 S3FullAccess 권한 집합이 있는 계정 123456789012에 로그인하고 S3 콘솔 홈페이지로 이동하는 바로가기 링크의 예입니다.

- IPv4 엔드포인트: https://example.awsapps.com/start/#/console?
account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome
- 듀얼 스택 엔드포인트: https://ssoins-1234567890abcdef.portal.us-east-1.app.aws/#/console?
account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome
- (AWS GovCloud (US) Region) IPv4 엔드포인트: 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
- (AWS GovCloud (US) Region) 듀얼 스택 엔드포인트: https://ssoins-1234567890abcdef.portal.us-gov-west-1.app.aws/#/console?
account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome

MFA를 위한 디바이스 등록

Identity Center 디렉터리의 사용자는 AWS 액세스 포털 내에서 다음 절차에 따라 새 디바이스에 다중 인증(MFA)을 등록합니다.

Important

현재 [외부 ID 제공업체](#)에 대해서는 IAM Identity Center의 MFA가 지원되지 않습니다.

시작하기 전 준비 사항

이 절차의 단계를 시작하기 전에 먼저 적절한 인증 앱을 디바이스에 다운로드하는 것이 좋습니다. MFA 디바이스에서 사용할 수 있는 앱 목록은 [가상 인증 앱](#)을 참조하세요.

디바이스 등록

MFA를 사용할 디바이스를 등록하는 방법

1. AWS 액세스 포털에 로그인합니다. 자세한 내용은 [AWS 액세스 포털에 로그인](#) 단원을 참조하십시오.
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 디바이스 상에서 수동 입력할 수 있는 보안 암호 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 앱](#)을 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 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. 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 디바이스가 일회용 암호 생성을 시작할 수 있으며 사용할 준비가 되었습니다 AWS.

• 보안 키 또는 내장된 인증자

1. 사용자 보안 키 등록 페이지에서 브라우저 또는 플랫폼에 나와 있는 지침을 따릅니다.

Note

경험은 브라우저 또는 플랫폼에 따라 달라집니다. 디바이스가 성공적으로 등록되면 친숙한 표시 이름을 새로 등록된 디바이스에 연결할 수 있습니다. 이를 변경하려면 이름 바꾸기를 선택하고 새 이름을 입력한 다음 저장을 선택합니다.

활성 세션 보기 및 종료

AWS 액세스 포털을 사용하여 활성 세션 목록을 보고 필요한 경우 하나 이상의 세션을 종료할 수 있습니다.

AWS 액세스 포털을 사용하여 활성 세션 종료

1. AWS 액세스 포털에 로그인합니다. 자세한 내용은 [AWS 액세스 포털에 로그인](#) 단원을 참조하십시오.
2. 페이지의 우측 상단 근처에서 보안을 선택합니다.
3. 보안 페이지에서 활성 세션 옆에 있는 괄호 안의 숫자는 활성 세션의 수를 나타냅니다. 종료하려는 각 세션 옆의 확인란을 선택한 다음 세션 종료를 선택합니다.

Tip

사용자 백그라운드 세션의 경우 세션을 사용하는 작업의 Amazon 리소스 이름(ARN)으로 세션을 검색할 수 있습니다. 세션 유형 목록에서 사용자 백그라운드 세션을 선택한 다음 검색 상자에 작업 ARN을 입력합니다.

로드된 활성 세션만 종료할 수 있습니다. 세션이 많은 경우 더 많은 활성 세션 로드를 선택하여 추가 세션을 표시합니다.

4. 종료하려는 각 세션 옆의 확인란을 선택한 다음 세션 종료를 선택합니다.
5. 활성 세션을 종료할지 확인하는 대화 상자가 나타납니다. 정보를 검토하고 계속하려면 confirm을 입력한 다음 세션 종료를 선택합니다.
6. 활성 세션 목록으로 돌아갑니다. 선택한 세션이 성공적으로 종료되었음을 나타내는 녹색 알림 메시지가 나타납니다.

여러에서 IAM Identity Center 사용 AWS 리전

이 주제에서는 여러 AWS IAM Identity Center 에서를 사용하는 방법을 설명합니다 AWS 리전. 서비스 중단 중에 인스턴스를 추가 리전에 복제하고, 인력 액세스 및 세션을 관리하고, 애플리케이션을 배포하고, 계정 액세스를 유지하는 방법을 알아봅니다.

IAM Identity Center의 조직 인스턴스를 활성화할 때 단일 AWS 리전 (기본 리전)을 선택합니다. 특정 사전 조건을 충족하는 AWS 리전 경우이 인스턴스들에 추가로 복제할 수 있습니다. IAM Identity Center는 기본 리전에서 선택한 추가 리전으로 인력 자격 증명, 권한 세트, 사용자 및 그룹 할당, 세션 및 기타 메타데이터를 자동으로 복제합니다.

다중 리전 지원의 이점

IAM Identity Center를 추가로 복제하면 두 가지 주요 이점 AWS 리전 이 있습니다.

- AWS 계정 액세스 복원력 향상 - IAM Identity Center 인스턴스가 기본 리전에서 서비스 중단을 겪더라도 작업 인력이 AWS 계정에 액세스할 수 있습니다. 이는 중단 전에 프로비저닝된 권한이 있는 액세스에 적용됩니다.
- AWS 관리형 애플리케이션의 배포 리전 선택 유연성 향상 - 선호하는 리전에 AWS 관리형 애플리케이션을 배포하여 애플리케이션 데이터 레지던시 요구 사항을 충족하고 사용자와의 근접성을 통해 성능을 개선할 수 있습니다. 추가 리전에 배포된 애플리케이션은 최적의 성능과 신뢰성을 위해 복제된 작업 인력 ID에 로컬로 액세스합니다.

필수 조건 및 고려 사항

IAM Identity Center 인스턴스를 복제하기 전에 다음 요구 사항을 충족하는지 확인합니다.

- 인스턴스 유형 - IAM Identity Center 인스턴스는 [조직 인스턴스](#)여야 합니다. [계정 인스턴스](#)에서는 다중 리전 지원을 사용할 수 없습니다.
- ID 소스 - IAM Identity Center 인스턴스와 같은 외부 ID 제공업체(IdP)에 연결해야 합니다 [Okta](#), [Active Directory](#) 또는 [Identity Center 디렉터리](#)를 ID 소스로 사용하는 인스턴스에서는 다중 리전 지원을 사용할 수 없습니다.
- AWS 리전 - 다중 리전 지원은에서 [기본적으로 활성화된 상용 리전](#)에서 사용할 수 있습니다 AWS 계정. 옵트인 리전은 현재 지원되지 않습니다.

- 유휴 시 암호화를 위한 KMS 키 유형 - IAM Identity Center 인스턴스는 다중 리전 [고객 관리형 KMS 키](#)로 구성해야 합니다. KMS 키는 IAM Identity Center와 동일한 AWS 계정에 있어야 합니다. 자세한 내용은 [에서 고객 관리형 KMS 키 구현 AWS IAM Identity Center](#) 단원을 참조하십시오.
- AWS 관리형 애플리케이션 호환성 -의 애플리케이션 테이블 [the section called “IAM Identity Center 와 함께 사용할 수 있는 애플리케이션”](#)을 방문하여 다음 두 가지 애플리케이션 요구 사항을 확인합니다.
 - 조직에서 사용 중인 모든 AWS 관리형 애플리케이션은 고객 관리형 KMS 키로 구성된 IAM Identity Center를 지원해야 합니다.
 - 추가 리전에 배포하려는 AWS 관리형 애플리케이션은 이러한 유형의 배포를 지원해야 합니다.
- 외부 IdP 호환성 - 다중 리전 지원을 완전히 활용하려면 외부 IdP가 여러 어설션 소비자 서비스(ACS) URLs 지원해야 합니다. , Okta, PingFederate, Microsoft Entra ID, PingOne 및 JumpCloud와 같은 IdPs에서 지원하는 SAML 기능입니다.

와 같이 여러 ACS URLs 지원하지 않는 IdP를 사용하는 경우 IdP 공급업체와 협력하여이 기능을 활성화하는 Google Workspace가 좋습니다. 여러 ACS URLs [the section called “AWS 계정 여러 ACS URLs 없이 복원력에 액세스”](#). [the section called “여러 ACS URLs 없이 AWS 관리형 애플리케이션 사용”](#)

추가 리전 선택

기본적으로 활성화된 상용 리전 중에서 추가 리전을 선택할 때는 다음 요소를 고려하세요.

- 규정 준수 요구 사항 - 규정 준수를 위해 특정 리전으로 제한된 데이터 세트에 액세스하는 관리형 애플리케이션을 실행 AWS 해야 하는 경우 데이터 세트가 있는 리전을 선택합니다.
- 성능 최적화 - 데이터 레지던시가 요인이 아닌 경우 애플리케이션 사용자와 가장 가까운 리전을 선택하여 경험을 최적화합니다.
- 애플리케이션 지원 - 선택한 리전에서 필요한 AWS 애플리케이션을 사용할 수 있는지 확인합니다.
- AWS 계정 액세스 복원력 - AWS 계정에 대한 액세스 연속성을 위해 IAM Identity Center 인스턴스의 기본 리전에서 지리적으로 멀리 떨어진 리전을 선택합니다.

Note

IAM Identity Center에는의 수에 대한 할당량이 있습니다 AWS 리전. 자세한 내용은 [the section called “추가 할당량”](#) 단원을 참조하십시오.

IAM Identity Center를 추가 리전에 복제

환경이 다중 리전 고객 관리형 KMS 키로 IAM Identity Center를 구성하는 등의 [사전 조건](#)을 충족하는 경우 다음 단계를 완료하여 IAM Identity Center 인스턴스를 추가 리전에 복제합니다. 기본 리전은 이러한 단계 도중과 이후에도 계속 정상적으로 작동합니다.

1단계: 추가 리전에서 복제본 키 생성

IAM Identity Center를 리전에 복제하기 전에 먼저 해당 리전에서 고객 관리형 KMS 키의 복제본 키를 생성하고 IAM Identity Center 운영에 필요한 권한으로 복제본 키를 구성해야 합니다. 다중 리전 복제본 키 생성에 대한 지침은 [다중 리전 복제본 키 생성](#)을 참조하세요.

KMS 키 권한에 권장되는 접근 방식은 기본 키에서 키 정책을 복사하는 것입니다. 기본 키는 기본 리전의 IAM Identity Center에 이미 설정된 것과 동일한 권한을 부여합니다. 또는 리전별 키 정책을 정의할 수 있지만이 접근 방식은 리전 간 권한 관리의 복잡성을 높이고 향후 정책을 업데이트할 때 추가 조정이 필요할 수 있습니다.

Note

AWS KMS 는 다중 리전 KMS 키의 리전 간에 KMS 키 정책을 동기화하지 않습니다. KMS 키 리전 간에 KMS 키 정책을 동기화된 상태로 유지하려면 각 리전에서 변경 사항을 개별적으로 적용해야 합니다.

2단계: IAM Identity Center에서 리전 추가

IAM Identity Center에 리전을 추가하면 IAM Identity Center 데이터가 해당 리전으로 자동 복제됩니다. 복제는 비동기식이며 최종 일관성이 유지됩니다. 다음 탭은 AWS Management Console 및에서이 작업을 수행하는 지침을 제공합니다 AWS CLI.

Console

리전을 추가하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. [Management] 탭을 선택한 후
4. IAM Identity Center의 리전 섹션에서 리전 추가를 선택합니다.

5. AWS 리전 복제에 사용 가능한 섹션에서 원하는 항목을 선택합니다 AWS 리전. 리전이 목록에 표시되지 않으면 KMS 키가 복제되지 않았기 때문에 복제할 수 없습니다. 자세한 내용은 [the section called “고객 관리형 KMS 키 구현”](#) 단원을 참조하십시오.
6. 리전 추가를 선택합니다.
7. IAM Identity Center의 리전 섹션에서 리전 상태를 모니터링합니다. 새로 고침 버튼(원형 화살표)을 사용하여 필요에 따라 최신 리전 상태를 확인합니다. 복제가 완료되면 2단계로 진행합니다.

AWS CLI

리전을 추가하려면

```
aws sso-admin add-region \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --region-name eu-west-1
```

현재 리전 상태를 확인하려면

```
aws sso-admin describe-region \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --region-name eu-west-1
```

리전 상태가 ACTIVE이면 2단계로 진행할 수 있습니다.

추가 리전으로의 초기 복제 기간은 IAM Identity Center 인스턴스의 데이터 양에 따라 달라집니다. 후속 증분 변경 사항은 대부분의 경우 몇 초 내에 복제됩니다.

3단계: 외부 IdP 설정 업데이트

다음 단계는 외부 IdP에 [ID 소스 자습서](#) 대한 자습서를 따릅니다.

3.a단계: 외부 IdP에 어설션 소비자 서비스(ACS) URLs 추가

이 단계에서는 각 추가 리전에 직접 로그인할 수 있으며 해당 리전에 배포된 AWS 관리형 애플리케이션에 로그인하고 해당 리전을 AWS 계정통해 액세스하려면 필요합니다. ACS URLs [기본 및 추가의 ACS 엔드포인트 AWS 리전](#).

3.b단계(선택 사항): 외부 IdP 포털에서 AWS 액세스 포털 사용할 수 있도록 설정

추가 리전 AWS 액세스 포털 의를 외부 IdP 포털에서 북마크 앱으로 사용할 수 있도록 합니다. 북마크 앱에는 원하는 대상에 대한 링크(URL)만 포함되며 브라우저 북마크와 유사합니다. IAM Identity Center의 리전 섹션에서 allURL 보기를 선택하여 AWS 액세스 포털 URLs 콘솔에서 URL을 찾을 수 있습니다. AWS 액세스 포털 URLs 자세한 내용은 [the section called “AWS 기본 및 추가의 포털 엔드포인트에 액세스 AWS 리전”](#) 단원을 참조하십시오.

IAM Identity Center는 각 추가 리전에서 IdP 시작 SAML SSO를 지원하지만 외부 IdPs 일반적으로 단일 ACS URL에서만 이를 지원합니다. 연속성을 위해 기본 리전의 ACS URL을 IdP 시작 SAML SSO에 사용하고 북마크 앱 및 브라우저 북마크를 사용하여 추가 리전에 액세스하는 것이 좋습니다.

4단계: 방화벽 및 게이트웨이 허용 목록 확인

방화벽 또는 게이트웨이에서 도메인 허용 목록을 검토하고 [문서화된 허용 목록에 따라 업데이트합니다](#).

5단계: 사용자에게 정보 제공

추가 리전의 AWS 액세스 포털 URL과 추가 리전 사용 방법을 포함하여 새 설정에 대한 정보를 사용자에게 제공합니다. 관련 세부 정보는 다음 섹션을 검토하세요.

- [the section called “추가 리전을 통한 인력 액세스”](#)
- [the section called “AWS 계정 액세스를 위해 추가 리전으로 장애 조치”](#)
- [the section called “여러에 애플리케이션 배포 및 관리 AWS 리전”](#)

첫 번째 리전 추가 이후 리전 변경

추가 리전을 추가 및 제거할 수 있습니다. 전체 IAM Identity Center 인스턴스를 삭제하는 것 외에는 기본 리전을 제거할 수 없습니다. 리전 제거에 대한 자세한 내용은 섹션을 참조하세요 [the section called “IAM Identity Center에서 리전 제거”](#).

추가 리전을 기본 리전으로 승격하거나 기본 리전을 추가 리전으로 강등할 수 없습니다.

복제되는 데이터는 무엇입니까?

IAM Identity Center는 다음 데이터를 복제합니다.

데이터	복제 소스 및 대상
직원 자격 증명(사용자, 그룹, 그룹 멤버십)	기본 리전에서 추가 리전으로
사용자 및 그룹에 대한 권한 세트 및 할당	기본 리전에서 추가 리전으로
구성(예: 외부 IdP SAML 설정)	기본 리전에서 추가 리전으로
사용자 및 그룹에 대한 애플리케이션 메타데이터 및 애플리케이션 할당	애플리케이션의 연결된 IAM Identity Center 리전에서 활성화된 다른 리전으로
신뢰할 수 있는 토큰 발급자	기본 리전에서 추가 리전으로
세션	세션의 발신 리전에서 활성화된 다른 리전으로

Note

IAM Identity Center는 AWS 관리형 애플리케이션에 저장된 데이터를 복제하지 않습니다. 또한 애플리케이션 배포의 리전 공간도 변경되지 않습니다. 예를 들어 미국 동부(버지니아 북부)의 에 있는 IAM Identity Center 인스턴스가 동일한 리전에 Amazon Redshift를 배포한 경우 IAM Identity Center를 미국 서부(오레곤)로 복제해도 Amazon Redshift의 배포 리전과 해당 인스턴스에 저장된 데이터에 영향을 주지 않습니다.

고려 사항:

- 활성화된 리전의 글로벌 리소스 식별자 - 사용자, 그룹, 권한 세트 및 기타 리소스는 활성화된 리전에서 동일한 식별자를 갖습니다.
- 복제는 프로비저닝된 IAM 역할에 영향을 주지 않음 - 권한 세트 할당에서 프로비저닝된 기존 IAM 역할은 활성화된 모든 리전에서 계정 로그인 중에 사용됩니다.

추가 리전을 통한 인력 액세스

이 섹션에서는 여러 리전에서 IAM Identity Center를 활성화한 경우 작업 인력 AWS 액세스 포털 AWS 계정이 및 애플리케이션에 액세스하는 방법을 설명합니다.

추가 리전의 AWS 계정에는 기본 리전 AWS 액세스 포털과 동일한 방식으로 작업 인력이 액세스할 수 있는 및 애플리케이션이 표시됩니다. 작업 인력은 리전 포털 엔드포인트에 대한 직접 링크(예: <https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com>) 또는 외부 IdP AWS 액세스 포털에서 설정한 [복마크 앱](#)을 통해 추가 리전의에 로그인할 수 있습니다.

추가 리전의 AWS 액세스 포털 엔드포인트를 사용하여 IAM Identity Center 사용자로 APIs AWS CLI에 액세스할 수 있도록에 권한을 부여할 수 있습니다. 이 기능은 기본 리전과 동일한 방식으로 작동합니다. 그러나 CLI 권한 부여는 활성화된 리전 간에 복제되지 않습니다. 따라서 각 리전에서 CLI를 개별적으로 승인해야 합니다.

여러의 사용자 세션 AWS 리전

IAM Identity Center는 원래 리전에서 다른 활성화된 리전으로 사용자 세션을 복제합니다. 한 리전의 세션 취소 및 로그아웃도 다른 리전에 복제됩니다.

IAM Identity Center 관리자의 세션 취소

IAM Identity Center 관리자는 추가 리전에서 사용자 세션을 취소할 수 있습니다. 세션이 리전 간에 복제되므로 정상적인 조건에서는 단일 리전에서 세션을 취소하고 IAM Identity Center가 변경 사항을 다른 활성화된 리전으로 복제하는 것으로 충분합니다. IAM Identity Center의 기본 리전에 중단이 있는 경우 관리자는 추가 리전에서 작업을 수행할 수 있습니다.

AWS 액세스 포털 기본 및 추가의 엔드포인트 AWS 리전

활성화된 리전의 AWS 액세스 포털 URLs을 조회해야 하는 경우 다음 단계를 따르세요.

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. [Management] 탭을 선택한 후
4. IAM Identity Center의 리전 섹션에서 모든 AWS 액세스 포털 URLs 보기를 선택합니다.

다음 표는 IAM Identity Center 인스턴스의 기본 및 추가 리전에서 AWS 액세스 포털 엔드포인트를 지정합니다.

AWS 액세스 포털 엔드포인트	기본 리전	추가 리전	URL 패턴 및 예제
클래식 IPv4 전용 ¹	예	아니요	Pattern: <code>https://[Identity Store ID].awsapps.com/start</code> 예: <code>https://d-12345678.awsapps.com/start</code>
사용자 지정 별칭 IPv4 전용 ¹	예(선택 사항)	아니요	Pattern: <code>https://[custom alias].awsapps.com/start</code> 예: <code>https://mycompany.awsapps.com/start</code>
대체 IPv4 전용 ²	예	예	Pattern: <code>https://[Identity Center instance ID].[Region].portal.amazonaws.com</code> 예: <code>https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com</code>
듀얼 스택 ²	예	예	Pattern: <code>https://[Identity Center instance ID].portal.[Region].app.aws</code> 예: <code>https://ssoins-111111h2222j33pp.portal.eu-west-1.app.aws</code>

¹ 추가 리전에서는 사용자 지정 별칭이 지원되지 않으며 `awsapps.com` 상위 도메인을 사용할 수 없습니다.

² 대체 IPv4 전용 및 듀얼 스택 포털 엔드포인트에는 URL/start에 후행이 없습니다.

기본 및 추가의 어설션 소비자 서비스(ACS) 엔드포인트 AWS 리전

ACS URLs을 조회하거나 SAML 메타데이터의 일부로 다운로드해야 하는 경우 다음 단계를 따르세요.

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 자격 증명 소스 탭을 선택합니다.
4. 작업 드롭다운 메뉴에서 인증 관리를 선택합니다.
5. 서비스 공급자 메타데이터 섹션에는 활성화된 각 리전의 AWS 액세스 포털 및 ACS URL이 표시됩니다. IPv4-only 및 듀얼 스택 URLs은 별도의 탭에 표시됩니다. IdP가 SAML 메타데이터 파일 업로드를 지원하는 경우 메타데이터 파일 다운로드를 선택하여 모든 ACS URLs. IdP가 메타데이터 파일 업로드를 지원하지 않거나 ACS URLs 개별적으로 추가하려는 경우 콘솔의 테이블에서 개별 URLs을 복사하거나 ACS URLs 보기를 선택한 다음 모든 URLs. 기본 리전에서 서비스 공급자가 시작한 SAML Single Sign-On이 계속 작동하도록 기본 리전에 대해 이미 구성된 ACS URL을 유지합니다.

다음 표는 IAM Identity Center 인스턴스의 기본 및 추가 리전에서 SAML 어설션 소비자 서비스(ACS) 엔드포인트를 지정합니다.

ACS 엔드포인트	기본 리전	추가 리전	URL 패턴 및 예제
IPv4 전용	예	예	Pattern: https://[Region].signin.aws/platform/saml/acs/ [Tenant ID] 예: https://us-west-2.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111
대체 IPv4 전용*	예	아니요	Pattern: https://[Region].signin.aws.amazon.com/platform/saml/acs/ [Tenant ID]

ACS 엔드포인트	기본 리전	추가 리전	URL 패턴 및 예제
			예: https://us-west-2.signin.aws.amazon.com/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111
이중 스택	예	예	Pattern: https://[Region].sso.signin.aws/platform/saml/acs/[Tenant ID] 예: https://us-west-2.sso.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111

* 2026년 2월 이전에 활성화된 인스턴스의 경우 서비스 공급자가 시작한 기본 리전에 대한 SAML Single Sign-On에 필요하므로 이 엔드포인트를 유지합니다. IAM Identity Center는 2026년 2월 이후에 활성화된 인스턴스에는 이 엔드포인트를 사용하지 않습니다.

여러 ACS URLs 없이 AWS 관리형 애플리케이션 사용

일부 외부 ID 제공업체(IdPs)는 IAM Identity Center 애플리케이션에서 여러 어설션 소비자 서비스(ACS) URLs을 지원하지 않습니다. 다중 ACS URLs은 다중 리전 IAM Identity Center의 특정 리전에 직접 로그인하는 데 필요한 SAML 기능입니다.

예를 들어 애플리케이션 링크를 통해 AWS 관리형 애플리케이션을 시작하면 시스템은 애플리케이션의 연결된 IAM Identity Center 리전을 통해 로그인을 트리거합니다. 그러나 해당 리전의 ACS URL이 외부 IdP에 구성되지 않은 경우 로그인이 실패합니다.

이 문제를 해결하려면 IdP 공급업체와 협력하여 여러 ACS URLs에 대한 지원을 활성화합니다. 그 동안에도 추가 리전에서 AWS 관리형 애플리케이션을 계속 사용할 수 있습니다. 먼저 외부 IdP에 ACS URL이 구성된 리전(기본 리전)에 로그인합니다. IAM Identity Center에 활성 세션이 있으면 활성화된 리전의 AWS 액세스 포털에서 또는 애플리케이션 링크를 통해 애플리케이션을 시작할 수 있습니다.

AWS 계정 액세스를 위해 추가 리전으로 장애 조치

IAM Identity Center를 통한 AWS 계정 액세스 주제에서 광범위하게 다룹니다 [AWS 계정 액세스](#). 이 섹션에서는 기본 리전 AWS 리전에서 서비스 중단이 발생할 경우 여러에서 AWS 계정 액세스를 유지하는 것과 관련된 추가 세부 정보를 제공합니다.

IAM Identity Center 인스턴스가 기본 리전에서 중단되는 경우(예: 기본 리전의 AWS 액세스 포털을 사용할 수 없음) 작업 인력은 추가 리전으로 전환하여 AWS 계정 및 영향을 받지 않는 애플리케이션에 계속 액세스할 수 있습니다. 자세한 내용은 [the section called “추가 리전을 통한 인력 액세스”](#) 단원을 참조하십시오.

에서 설정을 완료하는 즉시 추가 리전의 AWS 액세스 포털 엔드포인트와 외부 IdP 설정(예: 추가 리전의 북마크 앱)을 작업 인력에게 전달하는 것이 좋습니다 [the section called “IAM Identity Center를 추가 리전에 복제”](#). 이렇게 하면 필요한 경우 추가 리전으로 장애 조치를 수행할 준비가 됩니다.

마찬가지로 AWS CLI 사용자는 기본 리전에 대해 보유한 각 [AWS CLI 프로필](#)에 대해 추가 리전에 대한 프로필을 생성하는 것이 좋습니다. 그런 다음 기본 리전에 서비스 중단이 있는 경우 해당 프로필로 전환할 수 있습니다.

Note

또한 AWS 계정에 대한 액세스 연속성은 외부 IdP의 상태와 서비스 중단 전에 프로비저닝되고 복제되는 권한 세트 할당 및 그룹 멤버십과 같은 권한에 따라 달라집니다. 또한 외부 IdP에서 서비스 중단이 있을 때 권한이 있는 소규모 사용자 그룹에 대한 AWS 액세스를 유지하려면 조직에서 [AWS 브레이크 글래스](#) 액세스를 설정하는 것이 좋습니다. [긴급 액세스](#)는 IAM 사용자를 사용하지 않는 유사한 옵션이지만 외부 IdP에도 의존합니다.

AWS 계정 여러 ACS URLs 없이 복원력에 액세스

일부 외부 ID 제공업체(IdPs)는 IAM Identity Center 애플리케이션에서 여러 어설션 소비자 서비스(ACS) URLs을 지원하지 않습니다. 다중 ACS URLs은 다중 리전 IAM Identity Center의 특정 리전에 직접 로그인하는 데 필요한 SAML 기능입니다.

사용자가 여러 IAM Identity Center 리전을 AWS 계정 통해에 액세스할 수 있도록 하려면 외부 IdP에서 해당 리전 ACS URLs을 구성해야 합니다. 그러나 외부 IdP가 IAM Identity Center 애플리케이션에서 단일 ACS URL만 지원하는 경우 사용자는 단일 IAM Identity Center 리전에 직접 로그인할 수 있습니다.

이 문제를 해결하려면 IdP 공급업체와 협력하여 여러 ACS URLs에 대한 지원을 활성화합니다. 그 동안 추가 리전을 액세스를 위한 백업으로 사용할 수 있습니다 AWS 계정.

기본 리전에서 IAM Identity Center 서비스 중단이 발생하는 경우 외부 IdP의 ACS URL을 추가 리전의 ACS URL로 업데이트해야 합니다. 이 업데이트 후 사용자는 외부 IdP 포털의 기존 IAM Identity Center 애플리케이션을 사용하거나 공유한 직접 링크를 통해 추가 리전의 AWS 액세스 포털에 액세스할 수 있습니다.

이 설정을 주기적으로 테스트하여 필요할 때 작동하는지 확인하고이 장애 조치 프로세스를 조직에 알리는 것이 좋습니다.

Note

이 설정 AWS 계정 에서에 액세스하기 위해 추가 리전을 사용하는 경우 사용자가 기본 리전에 연결된 AWS 관리형 애플리케이션에 액세스하지 못할 수 있습니다. 따라서 이는에 대한 액세스를 유지하기 위한 임시 조치로만 사용하는 것이 좋습니다 AWS 계정.

여러 AWS 리전에 애플리케이션 배포 및 관리

IAM Identity Center를 통한 애플리케이션 액세스 주제에서 광범위하게 다룹니다 [애플리케이션 액세스](#). 이 섹션에서는 여러에서 애플리케이션의 배포 및 관리와 관련된 추가 세부 정보를 제공합니다 AWS 리전.

여러에 관리형 AWS 애플리케이션 배포 및 관리 AWS 리전

단일 리전 IAM Identity Center 인스턴스를 사용하면 인스턴스와 동일한 리전에 AWS 관리형 애플리케이션을 배포할 수 있습니다. Amazon Q Business와 같은 일부 애플리케이션은 IAM Identity Center에 대한 리전 간 연결을 지원하므로 관심 애플리케이션을 사용할 수 있는 경우 IAM Identity Center의 리전 외부에서 배포할 수 있습니다. 그러나 리전 간 호출로 인해 애플리케이션 성능이 느려질 수 있으며 대부분의 AWS 관리형 애플리케이션은 이러한 유형의 연결을 지원하지 않습니다.

다중 리전 IAM Identity Center 인스턴스를 사용하면 동일한 리전(“리전-로컬 연결”)의 IAM Identity Center에 연결하여 활성화된 모든 리전에 AWS 관리형 애플리케이션을 배포할 수 있습니다. 기본 리전에서의 배포는 모든 통합 AWS 관리형 애플리케이션에서 지원됩니다. IAM Identity Center의 추가 리전에서 배포를 지원하는 AWS 관리형 애플리케이션을 확인하려면의 애플리케이션 표를 참조하세요 [the section called “IAM Identity Center와 함께 사용할 수 있는 애플리케이션”](#). 어떤 경우든 AWS 관리형 애플리케이션은 배포하려는 리전에서 사용할 수 있어야 합니다.

IAM Identity Center에 대한 리전-로컬 연결을 통해 AWS 관리형 애플리케이션은 최적의 성능과 신뢰성을 위해 동일한 리전의 직원 ID에 액세스합니다. [사전 조건](#)이 충족될 때마다 AWS 관리형 애플리케이션을 배포할 때 리전-로컬 연결을 선택하는 것이 좋습니다.

IAM Identity Center의 추가 리전에 AWS 관리형 애플리케이션을 배포하려면 기본 리전에 배포하는 것과 동일한 방식으로 애플리케이션 콘솔 또는 API를 통해 해당 리전에서 배포를 시작합니다.

고려 사항:

- IAM Identity Center를 해당 리전에 아직 복제하지 않은 경우 애플리케이션 배포를 즉시 완료할 수 있도록 먼저 복제하는 것이 좋습니다.
- AWS 관리형 애플리케이션은 이미 IAM Identity Center를 리전에 복제한 경우 대부분의 경우 리전-로컬 연결을 자동으로 설정합니다.
- AWS 관리형 애플리케이션이 IAM Identity Center에 대한 리전 간 연결을 제공하는 경우 [사전 조건이](#) 충족되면 리전-로컬 연결을 선택하는 것이 좋습니다.
- 애플리케이션이 추가 리전에서 배포를 지원하지 않는 경우 애플리케이션을 사용할 수 있는 경우 기본 리전에 배포할 수 있습니다.

Important

IAM Identity Center 인스턴스가 다중 리전인 경우 조직에서 사용 중인 모든 AWS 관리형 애플리케이션은 애플리케이션 배포 리전에 관계없이 고객 관리형 KMS 키로 구성된 IAM Identity Center를 지원해야 합니다. 애플리케이션을 배포 [the section called “IAM Identity Center와 함께 사용할 수 있는 애플리케이션”](#)하기 전과 IAM Identity Center에서 고객 관리형 KMS 키를 구성하기 전에에서 이를 확인합니다.

애플리케이션의 관리 리전

리전-로컬 연결을 사용하여 IAM Identity Center의 추가 리전에 AWS 관리형 애플리케이션을 배포한 후 동일한 리전의 사용자 및 그룹에 대한 애플리케이션 및 할당을 관리합니다. IAM Identity Center는 사용자 및 그룹에 대한 할당을 포함하여 애플리케이션 메타데이터를 다른 활성화된 리전으로 복제하므로 작업 인력이 활성화된 모든 리전에서 애플리케이션을 시작할 수 있습니다.

AWS 관리형 애플리케이션이 IAM Identity Center에 대한 리전 간 연결을 사용하는 경우 연결된 리전의 IAM Identity Center 콘솔 및 API를 통해 이름 및 설명, 사용자 및 그룹에 대한 애플리케이션 할당과 같은 애플리케이션 세부 정보를 관리할 수 있습니다. 연결 유형에 관계없이 배포 리전의 콘솔을 통해 애플리케이션을 관리할 수 있습니다.

신뢰할 수 있는 ID 전파

IAM Identity Center 인스턴스의 활성화된 모든 리전에서 지원되는 AWS 관리형 애플리케이션에서 신뢰할 수 있는 ID 전파를 사용할 수 있습니다.

자격 증명 컨텍스트를 서로 전파하는 모든 애플리케이션은 동일한 리전에 있어야 합니다.

연결된 IAM Identity Center 리전에 대한 애플리케이션의 종속성

각 AWS 관리형 애플리케이션은 배포 중에 특정 IAM Identity Center 리전에 연결됩니다. 그런 다음 IAM Identity Center가 여러 리전에서 활성화된 경우에도 애플리케이션은 사용자 로그인을 위해 해당 리전에 따라 달라집니다. IAM Identity Center가 해당 리전에서 중단되는 경우 사용자는 리전에 연결된 AWS 관리형 애플리케이션에 액세스하지 못할 수 있습니다.

여러에 걸쳐 고객 관리형 애플리케이션 배포 및 관리 AWS 리전

IAM Identity Center는 SAML 및 OAuth2 [고객 관리형 애플리케이션을](#) 지원합니다. IAM Identity Center 인스턴스의 활성화된 모든 리전에서 생성하도록 선택할 수 있습니다. 하나를 생성한 후 동일한 리전의 사용자 및 그룹에 대한 애플리케이션 및 할당을 관리합니다.

IAM Identity Center에서 리전 제거

IAM Identity Center 인스턴스에서 추가 리전을 제거하려면 다음 단계를 따르세요.

1단계: 외부 IdP 구성 업데이트

외부 IdP에서이 리전의 ACS URL을 제거하거나 나중 에이 리전을 다시 추가하려는 경우에 대비하여 유지할 수 있습니다. 이 리전 AWS 액세스 포털 에서에 대해 생성했을 수 있는 북마크 앱을 제거하거나 숨기는 것이 좋습니다.

2단계: 리전 제거

Console

리전을 추가하려면

1. [IAM Identity Center 콘솔](#)을 엽니다.
2. 탐색 창에서 설정을 선택합니다.

3. [Management] 탭을 선택한 후
4. IAM Identity Center의 리전 섹션에서 제거할 추가 리전을 선택합니다.
5. 제거를 선택합니다.
6. 리전 제거를 선택하여 제거를 확인하기 전에 IAM Identity Center 리전에서 생성된 애플리케이션에 대한 잠재적 액세스 손실에 대한 경고에 유의하세요. 이러한 애플리케이션이 있는지 확실하지 않은 경우 탐색 창에서 애플리케이션을 선택하고 각 AWS 관리형 및 고객 관리형 애플리케이션의 에서 생성된 열에서 연결된 리전을 확인합니다.

Note

제거된 리전에 계속 연결된 AWS 관리형 애플리케이션을 배포하는 경우 이러한 애플리케이션에 대한 액세스 권한을 잃더라도 요금이 계속 발생할 수 있습니다. 이를 방지하려면 IAM Identity Center에서 리전을 제거하기 전에 애플리케이션 콘솔 또는 API를 통해 이러한 AWS 관리형 애플리케이션 배포를 제거해야 합니다. IAM Identity Center 리전을 이미 제거한 경우 리전을 다시 추가하여 애플리케이션에 대한 액세스를 복원할 수 있습니다.

7. IAM Identity Center의 리전 섹션에서 리전 상태를 모니터링합니다. 새로 고침 버튼(원형 화살표)을 사용하여 필요에 따라 최신 리전 상태를 확인합니다. 리전이 제거되면 리전 목록에 해당 리전이 더 이상 표시되지 않습니다.

AWS CLI

리전을 제거하려면

```
aws sso-admin remove-region \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --region-name eu-west-1
```

현재 리전 상태를 확인하려면

```
aws sso-admin describe-region \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --region-name eu-west-1
```

리전이 제거되면 2단계로 진행합니다.

3단계: 복제본 키 삭제

KMS 스토리지 요금이 발생하지 않도록 리전에서 복제본 키를 제거하도록 선택할 수 있습니다. 자세한 내용은 [AWS KMS 키 삭제를 참조하세요](#).

Important

이 특정 리전에서는 복제본 키만 삭제해야 합니다. 다른 IAM Identity Center 리전은 정상 작업을 위해 활성화된 다른 리전의 KMS 키에 계속 의존합니다.

추가 AWS 리전에서 지원되는 IAM Identity Center 서비스 APIs

API	추가 리전의 기능
Identity Center API	지원됨: • 애플리케이션 관리 읽기/쓰기 작업 • 인스턴스 읽기 작업 지원되지 않음: • 애플리케이션 관련 이외의 모든 쓰기 작업 • 권한 세트 및 계정 할당 읽기 작업
자격 증명 스토어 인증	읽기 작업
OIDC API	모든 작업이 지원됩니다.
포털 API 액세스	모든 작업이 지원됩니다.
SCIM API	작업이 지원되지 않음

AWS CloudTrail 기본 및 추가 리전의 IAM Identity Center 이벤트

에서는 IAM Identity Center 사용자 및 관리자가 IAM Identity Center 인스턴스 AWS 리전 의 활성화된 모든에서 수행하는 작업을 감사 AWS CloudTrail할 수 있습니다. AWS CloudTrail 이벤트는 작업이 수

행되는 리전에서 내보내지고 로깅됩니다. 자세한 내용은 [the section called “로깅 및 모니터링”](#) 단원을 참조하십시오.

기본 및 추가 리전에서 IAM Identity Center 사용 사례의 가용성

기능	리전별 가용성
사용자 포털이 있는 작업 인력 디렉터리	
포털 로그인 및 글로벌 세션을 AWS 액세스 포털 포함 한에 대한 사용자 액세스(모든 리전에 대해 하나의 로그인)	활성화된 모든 리전
할당된 모든 계정 표시	활성화된 모든 리전
할당된 모든 애플리케이션의 표시(애플리케이션이 생성된 위치에 관계없이)	활성화된 모든 리전
AWS 콘솔 또는 Identity Store APIs를 통해 사용자, 그룹 및 멤버십에 대한 읽기 액세스	활성화된 모든 리전
사용자 세션 취소	활성화된 모든 리전
SCIM API 또는 Identity Store API를 통해 외부 IdP와 같은 외부 ID 소스에서 사용자 및 그룹 자동 동기화	기본 리전만
SCIM을 사용하여 자동 자격 증명 프로비저닝 구성	기본 리전만
외부 IdP를 사용하여 SAML SSO 구성	기본 리전만 - 활성화된 모든 리전에서 콘솔을 통한 읽기 액세스
콘솔 또는 Identity Store API를 통해 사용자, 그룹 및 그룹 멤버십에 대한 작업을 Create/update/delete합니다. APIs	기본 리전: Identity Store API를 통해 사용할 수 있지만 SCIM API를 프로비저닝에 사용할 때 IAM Identity Center 콘솔에서 차단됩니다(항상 사용할 수 있는 사용자 액세스 및 삭제 비활성화/활성화 제외). 추가 리전: 사용 불가
다중 계정 액세스	

기능	리전별 가용성
AWS 액세스 포털 AWS CLI 및 바로 가기 링크를 통해 할당된 계정에 액세스	활성화된 모든 리전
콘솔 및 APIs에서 다중 계정 권한 세트 및 할당 관리(임시 승격된 액세스 포함)	기본 리전만
애플리케이션 및 AWS 서비스에 대한 액세스	
애플리케이션 콘솔 및 APIs를 통해 AWS 관리형 애플리케이션 배포	활성화된 모든 리전 - 애플리케이션의 리전 가용성 및 추가 리전에서의 배포 지원에 따라 다름
Identity Center 콘솔 및 APIs를 통해 고객 관리형 애플리케이션 생성	활성화된 모든 리전
콘솔 및 APIs에서 애플리케이션 메타데이터 및 할당 관리	애플리케이션의 연결된 IAM Identity Center 리전
에서 또는 애플리케이션 링크 AWS 액세스 포털 나 북마크를 통해 직접 애플리케이션 시작	활성화된 모든 리전
Amazon EC2 인스턴스에 대한 SSO	활성화된 모든 리전
신뢰할 수 있는 자격 증명 전파	
신뢰할 수 있는 토큰 발급자 생성	기본 리전만
AWS 관리형 애플리케이션을 통한 신뢰할 수 있는 자격 증명 전파	활성화된 모든 리전 - 자격 증명 컨텍스트를 서로 전파하는 애플리케이션은 동일한 리전에 있어야 합니다.
기타 관리 기능	
리전 관리, KMS 키 관리, 인스턴스 관리 및 세션 관리와 같은 기타 모든 관리 기능(세션 취소 제외)	기본 리전만 - 일부 데이터에 대해 활성화된 모든 리전에서 읽기 액세스 사용 가능(권한 세트 할당 제외)

복원력 설계 및 리전 동작

IAM Identity Center 서비스는 완전 관리형이며 Amazon S3 및 Amazon EC2와 같은 가용성과 내구성이 뛰어난 AWS 서비스를 사용합니다. 가용 영역 중단 시 가용성을 보장하기 위해 IAM Identity Center는 여러 가용 영역에서 작동합니다. IAM Identity Center 인스턴스를 추가 리전에 복제하여 리전 중단 시 이미 프로비저닝된 권한으로 계정 액세스를 유지할 수 있습니다. 자세한 내용은 [여러에서 IAM Identity Center 사용 AWS 리전](#) 단원을 참조하십시오.

AWS Organizations 관리 계정에서 IAM Identity Center를 활성화합니다. 이는 IAM Identity Center가 모든에서 역할을 프로비저닝, 프로비저닝 해제 및 업데이트하는 데 필요합니다 AWS 계정. IAM Identity Center를 활성화하면 "기본 리전"이라고 하는 AWS 리전 현재 선택된에 배포됩니다. 특정에 배포하려면 IAM Identity Center가 활성화된 후에는 기본 리전을 변경할 수 없으므로 IAM Identity Center를 활성화하기 전에 리전 선택을 AWS 리전변경합니다.

IAM Identity Center는 기본 리전에서만 대부분의 관리 함수를 지원합니다. 여기에는 외부 자격 증명 공급자에 대한 연결, 사용자 및 그룹 동기화, 사용자 및 그룹에 대한 권한 세트 생성 및 할당이 포함됩니다. 반대로 애플리케이션 및 할당 관리는 애플리케이션이 생성된 IAM Identity Center 리전에서 이루어져야 합니다.

Note

IAM Identity Center가 추가 리전에 복제되더라도 [AWS 휴지통 액세스](#)를 설정하는 것이 좋습니다. 이를 통해 외부 IdP의 서비스 중단과 같은 이벤트 중에 권한이 있는 소규모 사용자 그룹에 대한 AWS 액세스를 유지할 수 있습니다. [긴급 액세스](#)는 IAM 사용자 대신 외부 IdP의 자격 증명을 사용하는 또 다른 옵션이지만 외부 IdP의 중단을 방지하지는 않습니다.

IAM Identity Center는 서비스를 활성화한 리전의 액세스를 결정하지만, AWS 계정은 전역에 걸쳐 있습니다. 즉, 사용자가 IAM Identity Center에 로그인하면 IAM Identity Center를 AWS 계정 통해 액세스할 때 모든 리전에서 운영할 수 있습니다. 하지만 Amazon SageMaker AI와 같은 대부분의 AWS 관리형 애플리케이션은 사용자가 이러한 애플리케이션에 대한 액세스를 인증하고 할당할 수 있도록 IAM Identity Center 인스턴스의 리전에 설치해야 합니다. IAM Identity Center에서 애플리케이션을 사용할 때의 리전 제약 조건에 대한 자세한 내용은 애플리케이션 및 설명서를 참조하세요 [the section called “여러에 관리형 AWS 애플리케이션 배포 및 관리 AWS 리전”](#).

또한 IAM Identity Center를 사용하여 애플리케이션이 구축된 플랫폼 또는 클라우드에 관계없이 퍼블릭 URL을 통해 연결할 수 있는 SAML 기반 고객 관리형 애플리케이션에 대한 액세스를 인증하고 권한을 부여할 수 있습니다.

계정 AWS 액세스를 지원하지 않고 조직 인스턴스에 연결되지 않은 두 번째 격리된 제어 지점을 생성하기 때문에 복원력을 구현하는 [IAM Identity Center의 계정 인스턴스](#) 수단으로 사용하지 않는 것이 좋습니다.

가용성을 위한 설계

다음 표는 IAM Identity Center가 단일 AWS 리전에서 달성하도록 설계된 가용성을 제공합니다. 이 값은 서비스 수준 계약 또는 보증을 나타내는 것이 아니라 설계 목표에 대한 이해를 제공합니다. 가용성은 데이터 또는 함수에 대한 액세스를 가리키는 것으로 내구성(예: 데이터 장기 보존)을 나타내지 않습니다.

서비스 구성 요소	가용성 설계 목표
데이터 플레인(로그인 포함)	99.95%
컨트롤 플레인	99.90%

에 대한 긴급 액세스 설정 AWS Management Console

IAM Identity Center는고가용성 AWS 인프라를 기반으로 구축되었으며 가용 영역 아키텍처를 사용하여 단일 장애 지점을 제거합니다. 드물지만 IAM Identity Center 또는 AWS 리전 중단이 발생할 경우 추가 보호 계층을 위해에 대한 임시 액세스를 제공하는 데 사용할 수 있는 구성을 설정하는 것이 좋습니다 AWS Management Console.

AWS 를 사용하면 다음을 수행할 수 있습니다.

- [타사 IdP를 IAM Identity Center에 연결합니다.](#)
- SAML 2.0 기반 페더레이션을 사용하여 타사 IdP를 개별 AWS 계정 에 연결합니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

IAM Identity Center를 사용하면 이러한 기능을 사용하여 다음 섹션에 설명된 비상 액세스 구성을 생성할 수 있습니다. 이 구성을 사용하면 IAM Identity Center를 AWS 계정 액세스 메커니즘으로 사용할 수 있습니다. IAM Identity Center가 중단되면 비상 운영 사용자는 계정에 액세스하는 데 사용하는 것과 동일한 자격 증명을 사용하여 직접 페더레이션을 AWS Management Console 통해 로그인할 수 있습니다. 이 구성은 IAM Identity Center를 사용할 수 없지만 IAM 데이터 영역과 외부 ID 제공업체(idP)를 사용할 수 있는 경우에 작동합니다. 외부 IdP에 의존하지 않으려면 [AWS 브레이크 글래스 액세스](#)를 설정하는 것이 좋습니다.

⚠ 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.

주제

- [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.](#)
- [를 사용하여 직접 IAM 페더레이션 애플리케이션의 일회성 설정 ADFS](#)

비상 액세스 구성 요약

긴급 액세스를 구성하려면 다음 작업을 완료해야 합니다.

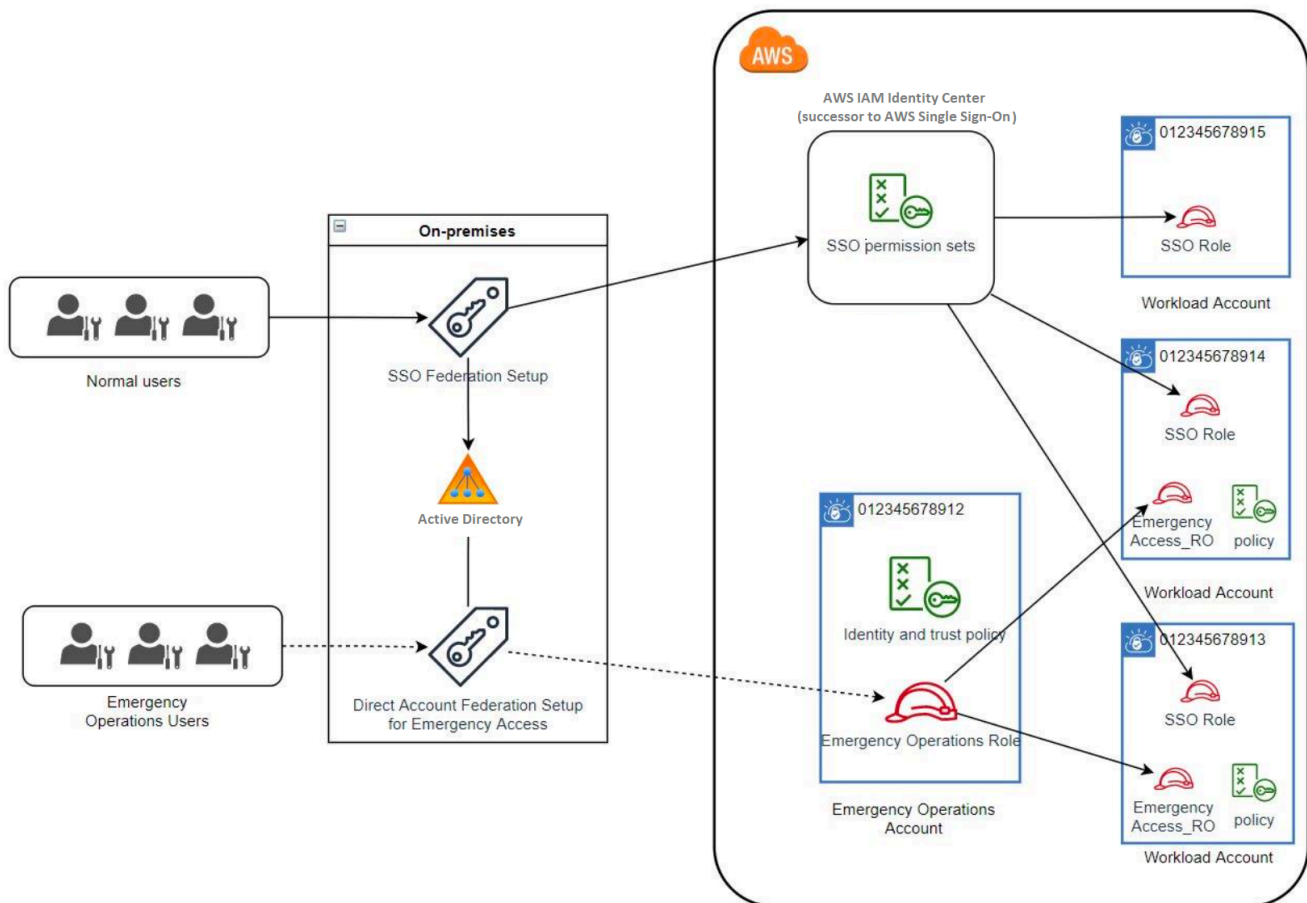
1. [AWS Organizations에서 조직의 비상 운영 계정을 계정을 만듭니다](#). 이 계정은 비상 운영 계정이 됩니다.
2. [SAML 2.0 기반 페더레이션](#)을 사용하여 IdP를 IdP를 비상 운영 계정에 연결합니다.
3. 비상 운영 계정에서 [제3자 ID 제공업체 페더레이션에 필요한 역할을 생성합니다](#). 또한 필요한 권한을 사용하여 각 워크로드 계정에서 비상 운영 역할을 생성합니다.
4. [비상 운영 계정에서 생성한 IAM 역할의 워크로드 계정에 대한 액세스 권한을 위임합니다](#). 비상 운영 계정에 대한 액세스를 승인하려면 구성원 없이 IdP에 비상 운영 그룹을 생성합니다.
5. IdP에 [AWS Management Console에 대한 SSAML 2.0 페더레이션 액세스를 활성화](#)하는 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. 그런 다음 이러한 사용자는 IdP에 로그인하고, 로 이동하고 AWS Management Console, 비상 운영 계정에서 비상 운영 역할을 수임할 수 있습니다. 여기에서 해당 사용자는 비상 운영을 수행해야 하는 워크로드 계정에서 비상 액세스 역할로 역할을 전환할 수 있습니다.

중요 운영 역할을 설계하는 방법

이 설계에서는 사용자가 중요한 운영 역할을 수임할 수 있도록 IAM을 통해 페더레이션 AWS 계정 하는 단일를 구성합니다. 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.



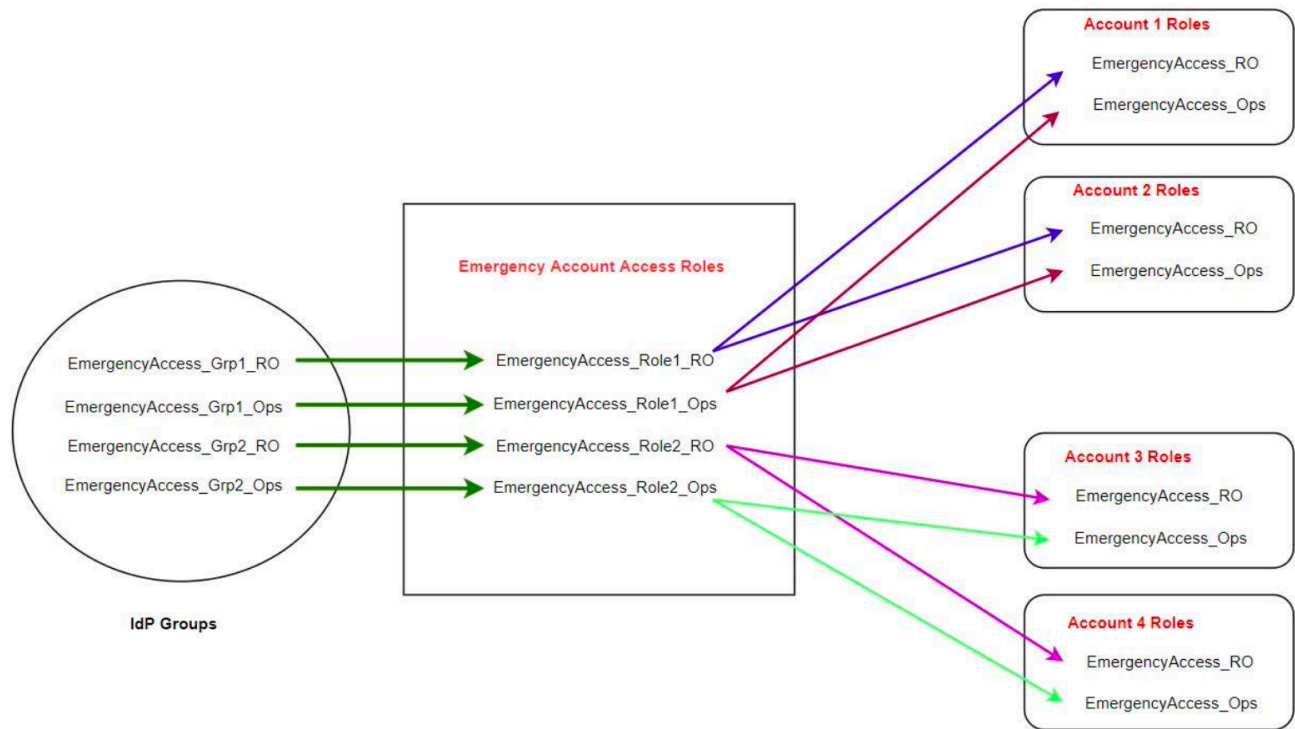
액세스 모델을 계획하는 방법

비상 액세스를 구성하기 전에 액세스 모델 작동 방식에 대한 계획을 세웁니다. 다음 프로세스를 사용하여 이 계획을 생성합니다.

1. IAM Identity Center 중단 시 AWS 계정 긴급 운영자 액세스가 필요한을 식별합니다. 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 정책](#)일 수 있습니다.

Account	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

Account	역할 생성	신뢰 정책	권한 정책
계정 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:p olicy/job-function/ SystemAdministrator
비상 액세스 계정	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	계정의 역할 리소스에 대한 AssumeRole

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. Okta 또는 기타 외부 IdPs ID 소스로 사용하는 경우 섹션을 참조하세요 [Okta에서 직접 IAM 페더레이션 애플리케이션을 한 번만 설정하면 됩니다.](#).. Active Directory를 ID 소스로 사용하는 경우 섹션을 참조하세요 [를 사용하여 직접 IAM 페더레이션 애플리케이션의 일회성 설정 ADFS.](#)
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 Management Console에 대한 긴급 액세스를 제공해야 한다고 판단되면 다음 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 대시보드](#)를 확인하여 IAM Identity Center 서비스의 상태가 복원되는 시기를 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. 계정 연동을 위해 SAML 2.0을 구성하는 방법의 단계에 따라 AWS 사용하여 직접 IAM 연동을 설정합니다. [AWS](#) 리전 장애 시나리오를 처리하려면 로그인 엔드포인트를 구성할 때 페더레이션 복원력을 개선하기 위해에서 운영하는 모든 리전에 대해 리전이 아닌 엔드포인트와 여러 리전 엔드포인트를 모두 활성화하는 것이 좋습니다. 이 긴급 액세스를 위해 ACS URL을 구성할 때는 IAM Identity Center가 배포된 리전과 다른 리전의 리전 엔드포인트를 사용하는 것이 좋습니다. 리전 [엔드포인트](#) 목록은 AWS 일반 참조의 로그인 엔드포인트를 참조하세요.
5. 로그인 옵션 탭에서 SAML 2.0을 선택하고 그룹 필터 및 역할 값 패턴 설정을 입력합니다. 사용자 디렉터리의 그룹 이름은 구성된 필터에 따라 달라집니다.

Group Filter

^aws\#\S+\#(?[role])[\w\-\+]\#(?[accountid])\d+\$

Role Value Pattern

arn:aws:iam::\${accountid}:saml-provider/Okta,arn:aws:iam::\${accountid}:role/\${role}

위 그림에서 role 변수는 비상 액세스 계정의 비상 운영 역할에 대한 변수입니다. 예를 들어에서 EmergencyAccess_Role1_R0 역할(매핑 테이블에 설명된 대로)을 생성하고 그룹 필터 설정이 위 그림과 같이 구성된 AWS 계정 123456789012 경우 그룹 이름은 여야 합니다 aws#EmergencyAccess_Role1_R0#123456789012.

6. 디렉터리(예: Active Directory의 디렉터리)에서 비상 액세스 그룹을 만들고 디렉터리 이름(예: aws#EmergencyAccess_Role1_R0#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_R0 역할에 연결된 사용자 지정 신뢰 정책에 대한 예제 설명입니다. 설명을 보려면 [비상 역할, 계정 및 그룹 매핑을 설계하는 방법](#) 아래의 다이어그램에서 긴급 계정을 참조하세요. 샘플 SAML 공급자 ARN을 긴급 액세스 계정에서 생성한 올바른 공급자 ARN으로 바꿉니다. 예제의 리전 엔드포인트를 선택한 리전으로 바꿉니다.

JSON

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

```

    "Effect": "Allow",
    "Principal": {
      "Federated": "arn:aws:iam::123456789012:saml-provider/[SAML
PROVIDER NAME]"
    },
    "Action": [
      "sts:AssumeRoleWithSAML",
      "sts:TagSession"
    ],
    "Condition": {
      "StringEquals": {
        "SAML:aud": [
          "https://signin.aws.amazon.com/saml",
          "https://us-west-2.signin.aws.amazon.com/saml",
          "https://us-west-1.signin.aws.amazon.com/saml",
          "https://us-east-2.signin.aws.amazon.com/saml"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Principal": {
      "Federated": "arn:aws:iam::123456789012:saml-provider/Okta"
    },
    "Action": "sts:SetSourceIdentity"
  }
]
}

```

8. 다음은 EmergencyAccess_Role1_R0 역할에 연결된 사용자 지정 권한 정책에 대한 예제 설명입니다. 설명을 보려면 [비상 역할, 계정 및 그룹 매핑을 설계하는 방법](#) 아래의 다이어그램에서 긴급 계정을 참조하세요.

JSON

```

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

```

```

        "Action": "sts:AssumeRole",
        "Resource": [
            "arn:aws:iam::111122223333:role/EmergencyAccess_R0",
            "arn:aws:iam::444455556666:role/EmergencyAccess_R0"
        ]
    }
]
}

```

9. 워크로드 계정에서 사용자 지정 신뢰 정책을 구성합니다. 다음은 EmergencyAccess_R0 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 참조하세요.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

Note

대부분의 IdP에서는 필요할 때까지 애플리케이션 통합을 비활성화할 수 있습니다. 비상 액세스가 필요할 때까지 IdP에서 직접 IAM 페더레이션 애플리케이션을 비활성화 상태로 유지하는 것이 좋습니다.

를 사용하여 직접 IAM 페더레이션 애플리케이션의 일회성 설정 ADFS

이 가이드에서는 IAM Identity Center를 사용할 수 없을 AWS 계정 때에 대한 긴급 액세스를 활성화 ADFS하기 위해를 사용하여 직접 IAM 페더레이션을 구성하는 일회성 설정 프로세스에 대해 설명합니다.

사전 조건

AWS 관리형 Microsoft ADADFS로를 구성하려는 경우 먼저 [다중 리전 복제를 구성](#)하고 복원력을 위해 기본 리전이 아닌 추가 리전에서 다음 단계를 계속하는 것이 좋습니다.

Active Directory 그룹 이름 지정 규칙 계획

그룹 이름과 AWS IAM 역할 간의 자동 일치를 활성화하는 특정 이름 지정 패턴을 사용하여 AD 그룹을 생성합니다.

그룹 이름 지정 형식: AWS-<AccountNumber>-<RoleName>

설명을 보려면 [비상 역할, 계정 및 그룹 매핑을 설계하는 방법](#) 아래의 다이어그램에서 긴급 계정을 참조하세요. 사용자가이 그룹에 할당되면 계정의 EmergencyAccess_Role1_R0 역할에 대한 액세스 권한이 부여됩니다123456789012. 사용자가 여러 그룹과 연결된 경우 별로 사용 가능한 역할 목록이 표시되고 수임할 역할을 선택할 AWS 계정 수 있습니다.

AWS 구성

전체 설정에는 긴급 액세스 계정 및 워크로드 계정의 구성이 포함됩니다. 전체 설정에 대한 그림은 단원을 참조하십시오[비상 역할, 계정 및 그룹 매핑을 설계하는 방법](#).

1. [SAML 자격 증명 공급자 생성](#)
2. [긴급 액세스 역할 생성](#)
3. [워크로드 계정 역할 구성](#)

SAML 자격 증명 공급자 생성

긴급 액세스 계정에서 IAM에서 SAML 자격 증명 공급자 생성의 단계에 따라 [IAM에서 SAML 자격 증명 공급자를 생성합니다](#). ADFS 서버에서 필요한 메타데이터를 다운로드합니다.

`https://<yourADFSserverFQDN>/FederationMetadata/2007-06/
FederationMetadata.xml`

긴급 액세스 역할 생성

SAML 2.0 연동을 신뢰할 수 있는 엔터티 유형으로 사용하여 긴급 계정에서 긴급 [액세스 역할을 생성합니다](#). 이전 단계에서 생성한 SAML 2.0 공급자를 선택합니다.

고려 사항:

- 운영 중인 모든 리전 포함 - 활성 워크로드가 있는 모든 리전을 선택하여 리전 중단 시 페더레이션을 계속 사용할 수 있도록 합니다.
- 단일 리전에서 운영하는 경우에도 하나 이상의 추가 리전 엔드포인트를 구성합니다. 예를 들어 에서는만 운영하는 경우 us-east-1를 보조 엔드포인트us-west-2로 추가합니다. IdP를 us-west-2 SAML 로그인 엔드포인트로 장애 조치하고의 워크로드 없이도 us-east-1 리소스에 계속 액세스할 수 있습니다us-west-2.
- 비리전 엔드포인트와 리전 엔드포인트 모두 활성화 - 비리전 엔드포인트(<https://signin.aws.amazon.com/saml>)는 가용성이 높지만 단일에서 호스팅되는 AWS 리전us-east-1반면 리전 엔드포인트(<https://<region>.signin.aws.amazon.com/saml>)는 단일 글로벌 엔드포인트에 대한 종속성을 줄여 복원력을 개선합니다.

신뢰 정책 구성

여러 로그인 리전 엔드포인트가 있는 신뢰 정책의 예는 섹션을 참조[Okta에서 직접 IAM 페더레이션 애플리케이션을 한 번만 설정하면 됩니다](#). 하세요. 샘플 리전 엔드포인트 및 SAML 공급자 ARNs 사용자 의 것으로 바꿉니다.

권한 정책 구성

긴급 액세스 역할에 연결하는 권한 정책의 [Okta에서 직접 IAM 페더레이션 애플리케이션을 한 번만 설정하면 됩니다](#). 예는 섹션을 참조하세요.

워크로드 계정 역할 구성

워크로드 계정 역할의 경우 긴급 액세스 계정의 긴급 액세스 역할이 해당 역할을 수입하도록 허용하는 사용자 지정 신뢰 정책을 구성합니다. 계정이 긴급 액세스 계정인 신뢰 정책의 [Okta에서 직접 IAM 페더레이션 애플리케이션을 한 번만 설정하면 됩니다](#). 예는 섹션을 참조123456789012하세요.

Active Directory 구성

다음 단계에서는 긴급 액세스를 위해 Active Directory 및 ADFS를 구성하는 방법을 설명합니다.

1. [그룹 생성](#)

2. [신뢰 당사자 생성](#)

3. [클레임 규칙 생성](#)

그룹 생성

앞에서 설명한 이름 지정 규칙(예:)에 따라 Active Directory에서 비상 그룹을 생성합니다. AWS-123456789012-EmergencyAccess_Role1_R0. 기존 프로비저닝 메커니즘을 통해 이러한 그룹에 사용자를 할당합니다.

신뢰 당사자 생성

ADFS 페더레이션에는 신뢰 당사자 구성이 필요합니다. 신뢰 당사자는 자격 증명 공급자 ADFS로 인증을 아웃소싱하는 AWS Security Token Service (AWS STS)입니다.

1. ADFS 관리 콘솔에서 작업 메뉴를 사용하고 신뢰 당사자 신뢰 추가를 선택합니다. 신뢰 당사자를 추가할 때 클레임 인식을 선택합니다.
2. 페더레이션 메타데이터의 경우 IAM 콘솔의 자격 증명 공급자 메타데이터 정보에서 메타데이터 URL을 입력합니다. 예제:

```
https://signin.aws.amazon.com/static/saml/SAMLSPXXXXXX/saml-metadata.xml
```

3. 신뢰 당사자(예: AWS 계정 액세스)의 표시 이름을 설정한 후 다음을 선택합니다.
4. 에 액세스할 사용자를 선택합니다 AWS. 특정 그룹을 선택하고 MFA와 같은 요구 사항을 정의할 수 있습니다.
5. 완료 페이지에서 닫기를 선택하여 신뢰 당사자 추가 신뢰 마법사를 완료합니다. AWS 가 이제 신뢰 당사자로 구성됩니다.

클레임 규칙 생성

ADFS는 클레임 규칙 언어를 사용하여 클레임 공급자와 신뢰 당사자 간에 클레임을 발행하고 변환합니다. NameId, RoleSessionName, AD 그룹 가져오기 및 AWS 액세스를 위한 역할이라는 네 가지 클레임 규칙을 생성해야 합니다.

신뢰 당사자를 마우스 오른쪽 버튼으로 클릭한 다음 클레임 발급 정책 편집을 선택합니다. 규칙 추가를 선택하여 규칙을 추가합니다.

1. NameId

- a. 수신 클레임 변환을 선택한 후 다음을 선택합니다.
- b. 다음 설정을 사용합니다.
 - 클레임 규칙 이름: NameId
 - 수신 클레임 유형: Windows Account Name
 - 발신 클레임 유형: Name ID
 - 발신 이름 ID 형식: Persistent Identifier
 - 모든 클레임 값 전달: 확인됨
- c. 확인을 선택합니다.

2. RoleSessionName

- a. 규칙 추가(Add Rule)를 선택합니다.
- b. 클레임 규칙 템플릿 목록에서 클레임으로 LDAP 속성 전송을 선택합니다.
- c. 다음 설정을 사용합니다.
 - 클레임 규칙 이름: RoleSessionName
 - 속성 저장소: Active Directory
 - LDAP 속성: E-Mail-Addresses
 - 발신 클레임 유형: <https://aws.amazon.com/SAML/Attributes/RoleSessionName>
- d. 확인을 선택합니다.

3. AD 그룹 가져오기

- a. 규칙 추가(Add Rule)를 선택합니다.
- b. 클레임 규칙 템플릿 목록에서 사용자 지정 규칙을 사용하여 클레임 전송을 선택한 후 다음을 선택합니다.
- c. 클레임 규칙 이름에 Get AD Groups를 입력한 다음 사용자 지정 규칙에 다음을 입력합니다.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
";tokenGroups;{0}", param = c.Value);
```

이 사용자 지정 규칙은 인증된 사용자가 속한 모든 그룹을 검색하여 라는 임시 클레임에 배치하는 클레임 규칙 언어의 스크립트를 사용합니다 <http://temp/variable>.

Note

예상치 못한 결과를 방지하기 위해 후행 공백이 없는지 확인합니다.

4. 역할 속성

- a. 규칙 추가(Add Rule)를 선택합니다.
- b. 클레임 규칙 템플릿 목록에서 사용자 지정 규칙을 사용하여 클레임 전송을 선택한 후 다음을 선택합니다.
- c. 클레임 규칙 이름에 Roles를 입력한 다음 사용자 지정 규칙에 다음을 입력합니다.

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([\d]{12})"]
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
  RegExReplace(c.Value, "AWS-([\d]{12})-", "arn:aws:iam::$1:saml-provider/
  <ADFS>,arn:aws:iam::$1:role/"));
```

이 사용자 지정 규칙은 정규식을 사용하여 양식의 각 그룹 멤버십을가 AWS 예상하는 IAM 역할 ARN 및 IAM 페더레이션 공급자 ARN 양식AWS-<Account Number>-<Role Name>으로 변환합니다.

Note

위의 예제 규칙 언어에서는 자격 증명 공급자 설정에서 SAML AWS 자격 증명 공급자에 지정된 논리적 이름을 ADFS 나타냅니다. ID 제공업체의 IAM 콘솔에서 선택한 논리적 이름을 기반으로 이를 변경합니다.

구성 테스트

에서 인증하여 솔루션이 작동하는지 테스트합니다<https://<yourADFSserverFQDN>/adfs/ls/IdpInitiatedSignOn.aspx>. 사이트의 드롭다운 목록에서 생성한 신뢰 당사자 이름을 선택합니다.

에서 기본 SAML 어설션 엔드포인트 업데이트 ADFS

Important

에서 신뢰 당사자 신뢰를 구성할 때 SAML 어설션 엔드포인트 ADFS는 기본적으로 글로벌 엔드포인트 `https://signin.aws.amazon.com/`가 아니며에 있습니다 `us-east-1`. 기본 엔드포인트를 IAM Identity Center가 복원력을 위해 구성된 리전 엔드포인트와 다른 리전 엔드포인트로 수정하는 것이 좋습니다. 예를 들어 IAM Identity Center가에 배포되어 `us-east-1` 있고 에서도 작업하는 경우 기본 SAML 어설션 소비자 엔드포인트를 로 `us-west-2` 변경합니다 `https://us-west-2.signin.aws.amazon.com/saml`.

1. 신뢰 당사자 신뢰에서 속성을 선택하고 모니터링 탭으로 이동합니다. 신뢰 당사자 자동 업데이트 확인란의 선택을 취소합니다.
2. 엔드포인트 탭으로 이동하여 원하는 로그인 엔드포인트를 선택하고 편집을 선택합니다.
3. 신뢰할 수 있는 URL을 기본값으로 설정 확인란을 선택합니다. 설정을 적용하려면 확인 및 적용을 선택합니다.

Note

대부분의 IdP에서는 필요할 때까지 애플리케이션 통합을 비활성화할 수 있습니다. 비상 액세스가 필요할 때까지 IdP에서 직접 IAM 페더레이션 애플리케이션을 비활성화 상태로 유지하는 것이 좋습니다.

의 보안 AWS IAM Identity Center

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

보안은 AWS와 사용자 간의 공동 책임입니다. [공동 책임 모델](#)은 이를 클라우드의 보안과 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 [AWS 규정 준수 프로그램](#)의 일환으로 보안 효과를 테스트하고 검증합니다. 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 [AWS 규정 준수 프로그램 제공 범위 내 서비스를](#) AWS IAM Identity Center 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 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 방법을 알아봅니다.

주제

- [IAM Identity Center ID 및 액세스 관리](#)
- [IAM Identity Center 콘솔 및 API 인증](#)
- [AWS STS IAM Identity Center에 사용되는 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 액세스하려면가 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 연결한 디렉터리에 의해 제어됩니다. 그러나 AWS 액세스 포털 내에서 사용자가 사용할 수 AWS 계정 있는에 대한 권한 부여는 다음 두 가지 요인으로 결정됩니다.

1. IAM Identity Center 콘솔 AWS 계정 에서 액세스 권한이 할당된 사용자입니다. 자세한 내용은 [에 대한 Single Sign-On 액세스 AWS 계정](#) 단원을 참조하십시오.
2. IAM Identity Center 콘솔의 사용자가 AWS 계정에 대한 적절한 액세스를 갖도록 허용된 권한 수준. 자세한 내용은 [권한 세트 생성, 관리 및 삭제](#) 단원을 참조하십시오.

다음 섹션에서는 관리자가 IAM Identity Center 콘솔에 대한 액세스를 제어하거나 IAM Identity Center 콘솔에서 일상적인 작업에 대한 관리 액세스를 위임하는 방법을 설명합니다.

- [Authentication](#)
- [액세스 관리](#)

Authentication

IAM 자격 증명을 AWS 사용하여 액세스하는 방법을 알아봅니다. <https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html>

액세스 관리

요청을 인증하는 데 유효한 자격 증명이 있더라도 권한이 없다면 IAM Identity Center 리소스를 생성하거나 액세스할 수 없습니다. 예를 들어 IAM Identity Center에 연결된 디렉터리를 생성할 권한이 있어야 합니다.

Note

IAM Identity Center 인스턴스가 고객 관리형 KMS 키로 구성된 경우 IAM Identity Center 관리자 및 KMS 키에 액세스해야 하는 기타 액터에게 추가 권한이 필요합니다. 자세한 내용은 [에서 고객 관리형 KMS 키 구현 AWS IAM Identity Center](#) 항목을 참조하세요.

다음 단원에서는 IAM Identity Center에 대한 권한을 관리하는 방법을 설명합니다. 먼저 개요를 읽어보면 도움이 됩니다.

- [IAM Identity Center 리소스에 대한 액세스 권한 관리 개요](#)
- [IAM Identity Center에 대한 자격 증명 기반 정책 예시](#)
- [IAM Identity Center에 대한 리소스 기반 정책 예시](#)
- [IAM Identity Center 서비스 연결 역할 사용](#)

IAM Identity Center 리소스에 대한 액세스 권한 관리 개요

모든 AWS 리소스에서는 소유하며 AWS 계정, 리소스를 생성하거나 액세스할 수 있는 권한은 권한 정책에 의해 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 사례](#)를 참조하세요.

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

리소스 소유자는 리소스를 AWS 계정 생성한 입니다. 즉, 리소스 소유자는 리소스를 생성하는 요청을 인증하는 AWS 계정 보안 주체 엔터티(계정, 사용자 또는 IAM 역할)의 입니다. 다음 예제에서는 이러한 작동 방법을 설명합니다.

- 가 애플리케이션 인스턴스 또는 권한 세트와 같은 IAM Identity Center 리소스를 AWS 계정 루트 사용자 생성하는 경우 AWS 계정 는 해당 리소스의 소유자입니다.
- AWS 계정에서 사용자를 생성하고 해당 사용자에게 IAM Identity Center 리소스를 생성할 수 있는 권한을 부여하면 사용자는 IAM Identity Center 리소스를 생성할 수 있습니다. 하지만 사용자가 속한 AWS 계정이 리소스를 소유합니다.
- AWS 계정에 IAM Identity Center 리소스를 생성할 권한이 있는 IAM 역할을 생성하는 경우 해당 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 내용은 다루지 않습니다. IAM 설명서 전체 내용은 IAM 사용 설명서의 [IAM이란 무엇입니까?](#)를 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 Center에 권한을 추가할 수 있습니다. 예를 들면, 다음을 수행할 수 있습니다.

- 의 사용자 또는 그룹에 권한 정책 연결 AWS 계정- 계정 관리자는 특정 사용자와 연결된 권한 정책을 사용하여 해당 사용자에게 새 애플리케이션과 같은 IAM Identity Center 리소스를 추가할 수 있는 권한을 부여할 수 있습니다.
- 역할에 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 List로 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.

JSON

```
{
  "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 예시](#)를 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.
- 작업 – 작업 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 암시적으로 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 reference](#)를 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 내용은 IAM 사용 설명서의 [조건](#)을 참조하십시오.

조건을 표시하려면 미리 정의된 조건 키를 사용합니다. IAM Identity Center에만 해당되는 특정한 조건 키는 없습니다. 그러나 필요에 따라 사용할 수 있는 AWS 조건 키가 있습니다. AWS 키의 전체 목록은 IAM 사용 설명서의 [사용 가능한 전역 조건 키](#)를 참조하세요.

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 내용은 [IAM Identity Center 리소스에 대한 액세스 권한 관리 개요](#) 단원을 참조하십시오.

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 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 설명서](#)의 IAM 정책 시뮬레이터로 IAM 정책 테스트를 참조하세요.

주제

- [예 1: 사용자가 IAM Identity Center를 볼 수 있도록 허용](#)
- [예제 2: 사용자가 IAM Identity Center AWS 계정 에서에 대한 권한을 관리하도록 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 Center에 대한 ViewOnlyAccess AWS 관리형 정책을 사용하는 것이 좋습니다.

JSON

```
{
  "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:ListDelegatedAdministrators",
        "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": "*"
}
]
}

```

예제 2: 사용자가 IAM Identity Center AWS 계정 에서에 대한 권한을 관리하도록 허용

다음 권한 정책은 사용자가 AWS 계정의 권한 세트를 생성, 관리 및 배포하도록 허용하는 권한을 부여합니다.

JSON

```

{
  "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": "AccessToSSOProvisionedRoles" 섹션에 나열된 추가 권한은 사용자가 AWS Organizations 관리 계정에서 할당을 생성할 수 있도록 하기 위해서만 필요합니다. 경우에 따라 이 섹션에 iam:UpdateSAMLProvider를 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 사용자가 기존 권한 세트를 사용하여 AWS 계정에 사용자 및 그룹을 할당할 수 있습니다. 사용자가 IAM Identity Center 내에서 AWS 계정 액세스를 관리해야 하고 권한 세트를 관리하는 데 필요한 권한이 필요한 경우 섹션을 참조하세요 [예제 2: 사용자가 IAM Identity Center AWS 계정 에서에 대한 권한을 관리하도록 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.

JSON

```
{
  "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.

JSON

```

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

```

```

    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "sso-directory:ListGroupForUser",
          "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 사용자에게 의도대로 작동하지 않습니다. 다음 예제는 IAM Identity Center 콘솔 내에서 오류 없이 운영하기 위해 필요할 수 있는 권한 세트를 나열합니다.

JSON

```

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

```



```

"Effect": "Allow",
"Action": [
    "sso:DescribeAccountAssignmentCreationStatus",
    "sso:DescribeAccountAssignmentDeletionStatus",
    "sso:DescribePermissionSet",
    "sso:DescribePermissionSetProvisioningStatus",
    "sso:DescribeRegisteredRegions",
    "sso:GetApplicationInstance",
    "sso:GetApplicationTemplate",
    "sso:GetInlinePolicyForPermissionSet",
    "sso:GetManagedApplicationInstance",
    "sso:GetMfaDeviceManagementForDirectory",
    "sso:GetPermissionSet",
    "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": "*"

```

```

    }
  ]
}

```

IAM Identity Center에 대한 리소스 기반 정책 예시

IAM Identity Center와 통합되어 작동하고 [OAuth 2.0](#)을 사용하는 모든 애플리케이션에는 리소스 기반 정책이 필요합니다. 애플리케이션은 고객 관리형 또는 AWS 관리형일 수 있습니다. 애플리케이션 정책(또는 API의 [ActorPolicy](#))이라고 하는 필수 리소스 기반 정책은 [CreateTokenWithIAM](#)과 같은 [IAM 인증 방법 API 작업을 직접 호출할 권한이 있는 IAM 위탁자](#)를 정의합니다. IAM 인증 방법을 사용하면 IAM 역할 또는 AWS 서비스와 같은 IAM 보안 주체가 IAM 자격 증명을 제시하여 /token?aws_iam=t 엔드포인트에서 액세스 토큰을 요청하거나 관리하여 IAM Identity Center OIDC 서비스에 인증할 수 있습니다.

애플리케이션 정책은 토큰 발급(CreateTokenWithIAM) 작업을 관리합니다. 또한 이 정책은 토큰 검증(IntrospectTokenWithIAM) 및 토큰 취소()를 위해 AWS 관리형 애플리케이션에서만 사용하는 권한 전용 작업을 관리합니다. RevokeTokenWithIAM. 고객 관리형 애플리케이션의 경우 CreateTokenWithIAM을 직접 호출할 권한이 있는 IAM 위탁자를 지정하여 이 정책을 구성합니다. 권한이 있는 위탁자가 이 API 작업을 직접 호출하면 위탁자는 애플리케이션에 대한 액세스 및 새로 고침 토큰을 받습니다.

IAM Identity Center 콘솔을 사용하여 고객 관리형 애플리케이션에 [신뢰할 수 있는 ID 전파](#)를 설정하는 경우 애플리케이션 정책을 구성하는 방법에 대한 자세한 내용은 [고객 관리형 OAuth 2.0 애플리케이션 설정](#)의 4단계를 참조하세요. 예제 정책은 이번 주제 후반부의 [예제 정책: IAM 역할이 액세스 및 새로 고침 토큰을 생성하도록 허용](#) 섹션을 참조하세요.

정책 요구 사항

정책은 다음 요구 사항을 충족해야 합니다.

- 정책은 "2012-10-17"로 설정된 Version 요소를 포함해야 합니다.
- 정책은 하나 이상의 Statement 요소를 포함해야 합니다.
- 각 정책 Statement은 Effect, Principal, Action, Resource 요소를 포함해야 합니다.

정책 요소

정책은 다음 요소를 포함해야 합니다.

버전

정책 문서 버전을 지정합니다. 버전을 2012-10-17(최신 버전)로 설정합니다.

명령

정책 Statements을 포함합니다. 정책은 하나 이상의 Statement를 포함해야 합니다.

각 정책 Statement는 다음 요소로 구성됩니다.

Effect

(필수) 정책 문서에서 권한을 허용할지 거부할지를 결정합니다. 유효한 값은 Allow 또는 Deny입니다.

Principal

(필수) [보안 주체](#)는 정책 설명에 지정된 권한을 갖는 자격 증명입니다. IAM 역할 또는 AWS 서비스 위탁자를 지정할 수 있습니다.

작업

(필수) 허용하거나 거부할 IAM Identity Center OIDC 서비스 API 작업입니다. 유효한 작업은 다음과 같습니다.

- sso-oauth:CreateTokenWithIAM: [CreateTokenWithIAM](#) API 작업에 해당하는 작업은 AWS 서비스 역할 또는 사용자와 같은 IAM 엔티티를 사용하여 인증된 승인된 클라이언트 애플리케이션에 대한 액세스 및 새로 고침 토큰을 생성하고 반환할 수 있는 권한을 부여합니다. 이러한 토큰에는 read:profile 또는 write:data와 같은 권한을 지정하는 정의된 범위가 포함될 수 있습니다.
- sso-oauth:IntrospectTokenWithIAM[권한 전용]: 연결된 범위 및 권한을 포함하여 활성 상태의 OAuth 2.0 액세스 토큰 및 새로 고침 토큰에 대한 정보를 검증하고 검색할 수 있는 권한을 부여합니다. 이 권한은 AWS 관리형 애플리케이션에서만 사용되며 IAM Identity Center OIDC API 참조에 문서화되어 있지 않습니다.
- RevokeTokenWithIAM [권한 전용]: OAuth 2.0 액세스 토큰 및 새로 고침 토큰을 철회하여 정상적인 만료 전에 무효화할 수 있는 권한을 부여합니다. 이 권한은 AWS 관리형 애플리케이션에서만 사용되며 IAM Identity Center OIDC API 참조에 문서화되어 있지 않습니다.

Resource

(필수) 이 정책에서 Resource 요소의 값은 "*"이며, 이는 "이 애플리케이션"을 의미합니다.

AWS 정책 구문에 대한 자세한 내용은 [AWS IAM 사용 설명서의 IAM 정책 참조](#)를 참조하세요.

예제 정책: IAM 역할이 액세스 및 새로 고침 토큰을 생성하도록 허용

다음 권한 정책은 워크로드가 수입하는 IAM 역할인 ExampleAppClientRole에 액세스 및 새로 고침 토큰을 생성하고 반환할 수 있는 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRoleToCreateTokens",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
      },
      "Action": "sso-oauth:CreateTokenWithIAM",
      "Resource": "*"
    }
  ]
}
```

AWS IAM Identity Center에 대한 관리형 정책

팀에 필요한 권한만 제공하는 [IAM 고객 관리형 정책을 생성](#)하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 정보는 [IAM 사용 설명서](#)에서 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 유형의 업데이트는 정책이 연결된 모든 ID(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.

또한는 여러 서비스에 걸쳐 있는 직무에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면는 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 [직무에 관한AWS 관리형 정책](#)을 참조하세요.

사용자 세션을 나열하고 삭제할 수 있는 새 작업은 새 네임스페이스 identitystore-auth에서 사용할 수 있습니다. 해당 네임스페이스의 작업에 대한 추가 권한은 이 페이지에서 업데이트됩니다. 사용

자 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 AWS IAM Identity Center 관리자의 작업 역할을 수행하는 보안 주체를 대상으로 합니다. 제공된 작업 목록은 시간이 지나면 IAM Identity Center의 기존 기능 및 관리자에게 필요한 작업에 맞게 업데이트됩니다.

AWSSSOMasterAccountAdministrator 정책을 IAM ID에 연결할 수 있습니다.

AWSSSOMasterAccountAdministrator 정책을 자격 증명에 연결할 때 관리 AWS IAM Identity Center 권한을 부여합니다. 이 정책을 사용하는 보안 주체는 AWS Organizations 관리 계정 및 모든 멤버 계정 내의 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 주체는 AWS 조직 멤버 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 정책에는 암호화에 고객 관리형 키를 사용하는 IAM Identity Center 인스턴스에 필요한 AWS Key Management Service 권한도 포함되어 있습니다.

권한 그룹화

이 정책은 제공된 권한에 따라 명령문으로 그룹화됩니다.

- AWSSSOMasterAccountAdministrator— IAM Identity Center가 AWSServiceRoleforSSO로 지정된 [서비스 역할을 IAM Identity Center에 전달](#)하여 이후에 역할을 맡고 대신 작업을 수행할 수 있도록 합니다. 이는 개인이나 애플리케이션이 IAM Identity Center를 활성화하려고 할 때 필요합니다. 자세한 내용은 [에 대한 액세스 구성 AWS 계정](#) 단원을 참조하십시오.
- AWSSSOMemberAccountAdministrator - IAM Identity Center가 다중 계정 AWS 환경에서 계정 관리자 작업을 수행할 수 있도록 허용합니다. 자세한 내용은 [AWS 관리형 정책: AWSSSOMemberAccountAdministrator](#) 단원을 참조하십시오.
- AWSSSOManageDelegatedAdministrator— IAM Identity Center에서 조직의 위임된 관리자를 등록 및 등록 취소할 수 있습니다.
- AllowKMSKeyUseViaService 및 AllowKMSKeyDiscovery - IAM Identity Center 인스턴스에서 사용하는 고객 관리형 키에 대한 AWS Key Management Service 작업을 허용합니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 [AWSSSOMasterAccountAdministrator](#)를 참조하세요.

이 정책에 대한 추가 정보입니다.

IAM Identity Center가 처음 활성화된 경우 IAM Identity Center 서비스는 AWS Organizations 관리 계정(이전 마스터 계정)에 [서비스 연결 역할을](#) 생성하여 IAM Identity Center가 계정의 리소스를 관리할 수 있도록 합니다. 필요한 작업은 iam:CreateServiceLinkedRole 및 iam:PassRole입니다.

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 ID에 연결할 수 있습니다.

AWSSSOMemberAccountAdministrator 정책을 자격 증명에 연결할 때 관리 AWS IAM Identity Center 권한을 부여합니다. 이 정책을 사용하는 보안 주체는 AWS Organizations 관리 계정 및 모든 멤버 계정 내의 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 주체는 AWS 조직 멤버 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 정책에는 암호화에 고객 관리형 키를 사용하는 IAM Identity Center 인스턴스에 필요한 AWS Key Management Service 권한도 포함되어 있습니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 [AWSSSOMemberAccountAdministrator](#)를 참조하세요.

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 관리자는 일상적인 작업을 수행하려면 다음 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 [Directory Service API 권한: 작업, 리소스 및 조건 참조](#)를 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 관리자는 일상적인 작업을 수행하려면 다음 AWS Organizations 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 관리](#)를 참조하세요. 이러한 권한을와 함께 사용하는 방법에 대한 자세한 내용은 [다른 AWS 서비스와 AWS Organizations 함께 사용](#)을 AWS Organizations참조하세요.

AWS 관리형 정책: AWSSSODirectoryAdministrator

AWSSSODirectoryAdministrator 정책을 IAM ID에 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 정책에는 암호화에 고객 관리형 키를 사용하는 IAM Identity Center 인스턴스에 필요한 AWS Key Management Service 권한도 포함되어 있습니다.

이 정책에는 다음 권한이 포함되어 있습니다.

- IAM Identity Center 디렉터리 - IAM Identity Center 디렉터리 작업에 대한 전체 관리 액세스.
- 자격 증명 스토어 - 자격 증명 스토어 작업 및 인증에 대한 전체 관리 액세스.
- IAM Identity Center - 디렉터리 연결을 나열할 수 있는 권한.
- AWS Key Management Service - IAM Identity Center 인스턴스에서 사용하는 고객 관리형 키에 대한 복호화, 키 설명, 데이터 키 생성 권한.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 [AWSSSODirectoryAdministrator](#)를 참조하세요.

AWS 관리형 정책: AWSSSOReadOnly

AWSSSOReadOnly 정책을 IAM ID에 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 보

안 주체는 IAM Identity Center에서 어떤 업데이트도 수행할 수 없습니다. 예를 들어 이러한 권한이 있는 보안 주체는 IAM Identity Center 설정을 볼 수 있지만 설정 값을 변경할 수 없습니다.

이 정책에는 암호화에 고객 관리형 키를 사용하는 IAM Identity Center 인스턴스에 필요한 AWS Key Management Service 권한도 포함되어 있습니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 [AWSSSODirectoryReadOnly](#)를 참조하세요.

AWS 관리형 정책: AWSSSODirectoryReadOnly

AWSSSODirectoryReadOnly 정책을 IAM ID에 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 위탁자는 IAM Identity Center 사용자를 볼 수 있지만 사용자 속성을 변경하거나 MFA 디바이스를 할당할 수는 없습니다.

이 정책에는 암호화에 고객 관리형 키를 사용하는 IAM Identity Center 인스턴스에 필요한 AWS Key Management Service 권한도 포함되어 있습니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 [AWSSSODirectoryReadOnly](#)를 참조하세요.

AWS 관리형 정책: AWSIdentitySyncFullAccess

AWSIdentitySyncFullAccess 정책을 IAM ID에 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 정책의 권한을 보려면 AWS 관리형 정책 참조의 [AWSIdentitySyncFullAccess](#)를 참조하세요.

AWS 관리형 정책: AWSIdentitySyncReadOnlyAccess

AWSIdentitySyncReadOnlyAccess 정책을 IAM ID에 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 위탁자는 동기화 설정을 업데이트할 수 없습니다. 예를 들어 이러한 권한이 있는 위탁자는 프로필 동기화 설정을 볼 수 있지만 프로필 또는 필터 값을 변경할 수 없습니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 [AWSIdentitySyncReadOnlyAccess](#)를 참조하세요.

AWS 관리형 정책: AWSSSOServiceRolePolicy

AWSSSOServiceRolePolicy 정책은 IAM ID에 연결할 수 없습니다.

이 정책은 IAM Identity Center가 특정에 대한 Single Sign-On 액세스 권한이 있는 사용자를 위임하고 적용할 수 있도록 서비스 연결 역할에 연결됩니다 AWS 계정 AWS Organizations. IAM을 활성화하면 조직 AWS 계정 내 모든에 서비스 연결 역할이 생성됩니다. 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. 각에서 생성되는 서비스 연결 역할의 이름은 AWS 계정입니다AWSServiceRoleForSSO. 자세한 내용은 [IAM Identity Center 서비스 연결 역할 사용](#) 단원을 참조하십시오.

AWS 관리형 정책: AWSIAMIdentityCenterAllowListForIdentityContext

IAM Identity Center 자격 증명 컨텍스트로 역할을 수입할 때 AWS Security Token Service (AWS STS)는 AWSIAMIdentityCenterAllowListForIdentityContext 정책을 역할에 자동으로 연결합니다.

이 정책은 IAM Identity Center ID 컨텍스트를 사용하여 수입한 역할에서 신뢰할 수 있는 ID 전파를 사용할 때 허용되는 작업 목록을 제공합니다. 이 컨텍스트로 호출되는 다른 모든 작업은 차단됩니다. ID 컨텍스트는 ProvidedContext로 전달됩니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 [AWSIAMIdentityCenterAllowListForIdentityContext](#)를 참조하세요.

AWS 관리형 정책: AWSIdentityCenterExternalManagementPolicy

AWSIdentityCenterExternalManagementPolicy 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 외부 공급자의 IAM Identity Center 사용자를 관리할 수 있는 액세스 권한을 제공합니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 [AWSIdentityCenterExternalManagementPolicy](#)를 참조하세요.

AWS 관리형 정책에 대한 IAM Identity Center 업데이트

다음 표에서는이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 IAM Identity Center의 AWS 관리형 정책 업데이트에 대해 설명합니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 IAM Identity Center 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경	설명	Date
AWSIdentityCenterExternalManagementPolicy	프로비저닝 테넌트의 ARN을 변경하도록 관리형 정책을 업데이트했습니다.	2025년 12월 5일
AWSIdentityCenterExternalManagementPolicy	이 정책은 외부 공급자의 IAM Identity Center 사용자를 관리할 수 있는 액세스 권한을 제공합니다.	2025년 11월 21일
AWSSSOMasterAccountAdministrator , AWSSSOMemberAccountAdministrator , AWSSSOReadOnly , AWSSSODirectoryAdministrator , AWSSSODirectoryReadOnly	암호화에 고객 관리형 키를 사용하는 IAM Identity Center 인스턴스에 필요한 AWS KMS 권한을 포함하도록 관리형 정책을 업데이트했습니다.	2025년 9월 17일
AWSSSOServiceRolePolicy	이제 이 정책에는 identity-sync:DeleteSyncProfile 을 직접 호출하는 권한이 포함됩니다.	2025년 2월 11일
AWSIAMIdentityCenterAllowListForIdentityContext	이제 이 정책에는 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 qapps:ListQAppSessionData 및 qapps:ExportQAppSessionData 작업이 포함됩니다.	2024년 10월 2일
AWSSSOMasterAccountAdministrator	IAM Identity Center는 이 정책을 사용하여 동기화 프로파일을 삭제할 수 있는 DeleteSyncProfile 권한을 부여하는 새 작업을 추가했습니다. DeleteIns	2024년 9월 26일

변경	설명	Date
	tance API와 연결된 작업입니다.	
AWSIAMIdentityCenterAllowListForIdentityContext	이제이 정책에는 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 s3:ListCallerAccessGrants 작업이 포함되어 있습니다.	2024년 9월 4일
AWSIAMIdentityCenterAllowListForIdentityContext	이제이 정책에는 aoss:APIAccessAll , es:ESHttpHead , es:ESHttpPost es:ESHttpGet , es:ESHttpPatch es:ESHttpDelete , 및 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 es:ESHttpPut 작업이 포함됩니다.	2024년 7월 12일

변경	설명	Date
AWSIAMIdentityCenterAllowListForIdentityContext	이제 이 정책에는 <code>qapps:PredictQApp</code> , , <code>qapps:ImportDocument</code> , <code>qapps:AssociateLibraryItemReview</code> <code>qapps:DissociateLibraryItemReview</code> , <code>qapps:GetQAppSession</code> , <code>qapps:UpdateQAppSession</code> , <code>qapps:GetQAppSessionMetadata</code> a <code>qapps:UpdateQAppSessionMetadata</code> , 및 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 <code>qapps:TagResource</code> 작업이 포함됩니다.	2024년 6월 27일
AWSIAMIdentityCenterAllowListForIdentityContext	이제 이 정책에는 Amazon EMR에서 신뢰할 수 있는 ID 전파를 지원하는 <code>elasticmapreduce:AddJobFlowSteps</code> , <code>elasticmapreduce:DescribeCluster</code> , <code>elasticmapreduce:CancelSteps</code> , <code>elasticmapreduce:DescribeStep</code> , 및 <code>elasticmapreduce:ListSteps</code> 작업이 포함됩니다.	2024년 5월 17일

변경	설명	Date
AWSIAMIdentityCenterAllowListForIdentityContext	이제이 정책에는 qapps:CreateQApp , qapps:PredictProblemStatementFromConversation , qapps:PredictQAppFromProblemStatement , qapps:CopyQApp , qapps:GetQApp , qapps:ListQApps , qapps:UpdateQApp , qapps:AssociateQAppWithUser , qapps>DeleteQApp qapps:ImportDocumentToQApp , qapps:ImportDocumentToQAppSession , qapps:DisassociateQAppFromUser qapps:CreateLibraryItem , qapps:GetLibraryItem , , qapps:UpdateLibraryItem , qapps:CreateLibraryItemReview , qapps:ListLibraryItems , qapps:CreateSubscriptionToken qapps:StartQAppSession , 및 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 qapps:Sto	2024년 4월 30일

변경	설명	Date
	pQAppSession 작업이 포함됩니다.	
AWSSSOMasterAccountAdministrator	이제이 정책에는 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> 및 <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> 작업이 포함됩니다.	2024년 4월 26일
AWSSSOMemberAccountAdministrator	이제이 정책에는 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> 및 <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> 작업이 포함됩니다.	2024년 4월 26일

변경	설명	Date
<u>AWSSSOReadOnly</u>	이제이 정책에는 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> 작업이 포함되어 있습니다.	2024년 4월 26일
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	이제이 정책에는 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 <code>qbusiness:PutFeedback</code> 작업이 포함되어 있습니다.	2024년 4월 26일
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	이제이 정책에는 <code>q:StartConversation</code> , <code>q:SendMessage</code> , <code>q:ListConversations</code> , <code>q:GetConversation</code> , <code>q:StartTroubleshootingAnalysis</code> , <code>q:GetTroubleshootingResults</code> , <code>q:StartTroubleshootingResolutionExplanation</code> , 및 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 <code>q:UpdateTroubleshootingCommandResult</code> 작업이 포함됩니다.	2024년 4월 24일

변경	설명	Date
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	이제이 정책에는 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 sts:SetContext 작업이 포함되어 있습니다.	2024년 4월 19일
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	이제이 정책에는 이러한 세션을 지원하는 AWS 관리형 애플리케이션에 대한 자격 증명 강화 콘솔 세션을 지원하는 qbusiness:Chat qbusiness:ListConversations , qbusiness:ChatSync , qbusiness:ListMessages , 및 qbusiness:DeleteConversation 작업이 포함됩니다.	2024년 4월 11일
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	이 정책에는 이제 s3:GetAccessGrantsInstanceForPrefix 및 s3:GetDataAccess 작업이 포함됩니다.	2023년 11월 26일
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	이 정책은 IAM Identity Center ID 컨텍스트를 사용하여 수입한 역할에서 신뢰할 수 있는 ID 전파를 사용할 때 허용되는 작업 목록을 제공합니다.	2023년 11월 15일

변경	설명	Date
<u>AWSSSODirectoryReadOnly</u>	이제 이 정책에는 사용자가 세션을 나열하고 가져올 수 있는 새로운 권한이 있는 새 네임스페이스 <code>identitystore-auth</code> 가 포함됩니다.	2023년 2월 21일
<u>AWSSSOServiceRolePolicy</u>	이제 이 정책을 통해 관리 계정에서 <u>UpdateSAMLProvider</u> 작업을 할 수 있습니다.	2022년 10월 20일
<u>AWSSSOMasterAccountAdministrator</u>	이제 이 정책에는 관리자가 세션을 나열하고 사용자의 세션을 삭제할 수 있는 새로운 권한이 있는 새 네임스페이스 <code>identitystore-auth</code> 가 포함됩니다.	2022년 10월 20일
<u>AWSSSOMemberAccountAdministrator</u>	이제 이 정책에는 관리자가 세션을 나열하고 사용자의 세션을 삭제할 수 있는 새로운 권한이 있는 새 네임스페이스 <code>identitystore-auth</code> 가 포함됩니다.	2022년 10월 20일
<u>AWSSSODirectoryAdministrator</u>	이제 이 정책에는 관리자가 세션을 나열하고 사용자의 세션을 삭제할 수 있는 새로운 권한이 있는 새 네임스페이스 <code>identitystore-auth</code> 가 포함됩니다.	2022년 10월 20일

변경	설명	Date
AWSSSOMasterAccountAdministrator	이제이 정책에 ListDelegatedAdministrators _는 호출할 수 있는 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
AWSSSOMemberAccountAdministrator	이제이 정책에 ListDelegatedAdministrators _는 호출할 수 있는 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	이제이 정책에 ListDelegatedAdministrators _는 호출할 수 있는 새 권한이 포함됩니다 AWS Organizations.	2022년 8월 11일

변경	설명	Date
AWSSSOServiceRolePolicy	이제 이 정책에는 DeleteRolePermissionsBoundary 및 PutRolePermissionsBoundary 를 호출하는 새로운 권한이 포함됩니다.	2022년 7월 14일
AWSSSOServiceRolePolicy	이제 이 정책에는 AWS Organizations에서 ListAWSServiceAccountsForOrganization and ListDelegatedAdministrators 를 호출할 수 있는 새로운 권한이 포함됩니다.	2022년 5월 11일
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

변경	설명	Date
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
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 Center가 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 8월 4일

IAM Identity Center 서비스 연결 역할 사용

AWS IAM Identity Center 는 AWS Identity and Access Management (IAM) [서비스 연결 역할](#)을 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 내용은 [IAM Identity Center 서비스 연결 역할 파악](#) 단원을 참조하십시오.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할은 IAM Identity Center를 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 서비스](#)를 참조하고 Service-Linked Role(서비스 연결 역할) 열에 Yes(예)가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

IAM Identity Center에 대한 서비스 연결 역할 권한

IAM Identity Center는 AWSServiceRoleForSSO라는 서비스 연결 역할을 사용하여 사용자를 대신하여 IAM 역할, 정책 및 SAML IdP를 포함한 AWS 리소스를 관리할 수 있는 IAM Identity Center 권한을 부여합니다.

AWSServiceRoleForSSO 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- IAM Identity Center(서비스 접두사: sso)

AWSSSOServiceRolePolicy 서비스 연결 역할 권한 정책에 따라 IAM Identity Center는 “/aws-reserved/sso.amazonaws.com/” 경로에서 이름 접두사가 “AWSReserveDsso_”인 역할에 대해 다음과 같은 작업을 수행할 수 있습니다.

- iam:AttachRolePolicy
- iam:CreateRole
- iam>DeleteRole
- iam>DeleteRolePermissionsBoundary
- iam>DeleteRolePolicy
- iam:DetachRolePolicy

- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

AWSSSOServiceRolePolicy 서비스 연결 역할 권한 정책은 IAM Identity Center가 이름 접두사가 “AWSSSO_”인 SAML 제공업체에서 다음을 완료하도록 허용합니다.

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam>DeleteSAMLProvider`

AWSSSOServiceRolePolicy 서비스 연결 역할 권한 정책은 모든 조직에서 IAM Identity Center의 다음을 완료하도록 허용합니다.

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

AWSSSOServiceRolePolicy 서비스 연결 역할 권한 정책은 모든 IAM 역할에서 IAM Identity Center의 다음을 완료하도록 허용합니다(*).

- `iam:listRoles`

AWSSSOServiceRolePolicy 서비스 연결 역할 권한 정책은 IAM Identity Center가 “arn:aws:iam: :role/AWS-ServiceRole/AWS-ServiceRoleForSSO/AWSServiceRoleForSSO”에서 다음을 완료하도록 허용합니다.

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam>DeleteServiceLinkedRole`

AWSSSOServiceRolePolicy 서비스 연결 역할 권한 정책은 IAM Identity Center가 “arn:aws:identity-sync:*:*:profile/*”에서 다음을 완료하도록 허용합니다.

- identity-sync:DeleteSyncProfile

AWSSSOServiceRolePolicy 서비스 연결 역할 권한 정책 업데이트에 대한 자세한 내용은 [AWS 관리형 정책에 대한 IAM Identity Center 업데이트](#) 섹션을 참조하세요.

JSON

```
{
  "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": "IAMSSAMLProviderCreationAction",
        "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": [
            "*"
        ]
    },
    {
        "Sid": "AllowDeleteSyncProfile",
        "Effect": "Allow",
        "Action": [
            "identity-sync:DeleteSyncProfile"
        ],
        "Resource": [
            "arn:aws:identity-sync:*:*:profile/*"
        ]
    }
]
}

```

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 권한](#)을 참조하세요.

IAM Identity Center에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. 활성화되면 IAM Identity Center는 AWS Organizations의 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.

참고

- AWS Organizations 관리 계정에 로그인한 경우 서비스 연결 역할이 아닌 현재 로그인한 역할을 사용합니다. 이렇게 하면 권한이 에스컬레이션되는 것을 방지할 수 있습니다.
- IAM Identity Center가 AWS Organizations 관리 계정에서 IAM 작업을 수행하면 모든 작업은 IAM 보안 주체의 자격 증명을 사용하여 수행됩니다. 이렇게 하면 CloudTrail의 로그에서 누가 관리 계정의 모든 권한을 변경했는지 파악할 수 있습니다.

Important

IAM Identity Center 서비스가 서비스 연결 역할을 지원하기 시작한 2017년 12월 7일 이전에 이 서비스를 사용 중이었다면 IAM Identity Center에서 사용자 계정에 AWSServiceRoleForSSO 역할을 이미 생성했습니다. 자세한 내용은 [내 IAM 계정에 표시되는 새 역할](#)을 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 Identity Center에서는 AWSServiceRoleForSSO 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 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 편집](#)을 참조하세요.

IAM Identity Center에 대한 서비스 연결 역할 삭제

AWSServiceRoleForSSO 역할을 수동으로 삭제하지 않아도 됩니다. AWS 조직에서 제거되면 IAM Identity Center AWS 계정 는 리소스를 자동으로 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.

AWSServiceRoleForSSO에서 사용하는 IAM Identity Center 리소스를 삭제하려면

1. AWS 계정에 액세스할 수 있는 모든 사용자 및 그룹용 [에 대한 사용자 및 그룹 액세스 제거 AWS 계정](#).
2. AWS 계정과 연결한 [IAM Identity Center에서 권한 세트 제거](#).

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 AWSServiceRoleForSSO 서비스 연결 역할을 삭제합니다. 자세한 내용은 [IAM 사용 설명서](#)의 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 작업](#)을 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 거부 없이 한 기존 API 작업과 새 API 작업을 모두 적용합니다. 2020년 10월 15일 이후에 생성된 인스턴스는 IAM ID 센터 콘솔에서 권한 부여를 위해 [최신 API 작업](#)을 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
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
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 Identity Center에 사용되는 조건 컨텍스트 키

[보안 주체](#)가에 [요청](#)하면는 요청을 평가하고 승인하는 데 사용되는 요청 컨텍스트에 요청 정보를 AWS 수집합니다. JSON 정책의 Condition 요소를 사용하여 요청 컨텍스트의 키를 정책에서 지정한 키 값과 비교할 수 있습니다. 요청 정보는 요청을 수행하는 보안 주체, 요청의 대상이 되는 리소스, 요청 자체에 대한 메타데이터 등 다양한 소스를 통해 제공됩니다. 서비스별 조건 키는 개별 AWS 서비스와 함께 사용하도록 정의됩니다.

IAM Identity Center에는 AWS 관리형 애플리케이션 및 타사 애플리케이션이 IAM Identity Center에서 정의한 조건 키의 값을 추가할 수 있는 AWS STS 컨텍스트 공급자가 포함되어 있습니다. 이 키들은 [IAM 역할](#)에 포함됩니다. 키 값은 애플리케이션이 토큰을 전달할 때 설정됩니다 AWS STS. 애플리케이션은 다음 방법 중 AWS STS 하나로 전달하는 토큰을 가져옵니다.

- IAM Identity Center로 인증하는 동안.
- 신뢰할 수 있는 ID 전파를 위해 [신뢰할 수 있는 토큰 발급자](#)와 토큰 교환 후. 이 경우 애플리케이션은 신뢰할 수 있는 토큰 발급자로부터 토큰을 얻고 해당 토큰을 IAM Identity Center의 토큰과 교환합니다.

이 키들은 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 UserId의 값에 따라 리소스에 대한 조건부 액세스를 제공할 수 있습니다. 이 값은 역할을 사용하는 IAM Identity Center 사용자를 나타냅니다. 예시는 SourceId를 사용하는 것과 유사합니다. 그러나 SourceId와 달리 UserId의 값은 ID 스토어의 검증되고 특정 사용자를 나타냅니다. 이 값은 애플리케이션이 얻은 다음 전달하는 토큰에 있습니다 AWS STS. 임의 값을 포함할 수 있는 범용 문자열이 아닙니다.

주제

- [identitystore:UserId](#)
- [identitystore:IdentityStoreArn](#)
- [identitycenter:ApplicationArn](#)
- [identitycenter:자격 증명Id](#)
- [identitycenter:InstanceArn](#)

identitystore:UserId

이 컨텍스트 키는 IAM Identity Center에서 발급한 컨텍스트 어설션의 주체인 IAM Identity Center 사용자의 UserId입니다. 컨텍스트 어설션이에 전달됩니다 AWS STS. 이 키를 사용하여 요청에 대한 IAM Identity Center 사용자의 UserId를 정책에 지정한 사용자의 식별자와 비교할 수 있습니다.

- 가용성 -이 키는 AWS CLI 또는 AWS STS AssumeRole API 작업에서 명령을 AWS STS assume-role 사용하여 역할을 수임할 때 IAM Identity Center에서 발급한 컨텍스트 어설션이 설정된 후 요청 컨텍스트에 포함됩니다.
- 데이터 유형 - [문자열](#)
- 값 유형-단일 값

identitystore:IdentityStoreArn

이 컨텍스트 키는 컨텍스트 어설션을 발행한 IAM Identity Center 인스턴스에 연결된 ID 스토어의 ARN입니다. 또한 identitystore:UserID에 대한 속성을 검색할 수 있는 ID 스토어이기도 합니다. 정책에서 이 키를 사용하여 이 예상 ID 스토어 ARN에서 identitystore:UserID가 오는지 여부를 확인할 수 있습니다.

- 가용성 -이 키는 AWS CLI 또는 AWS STS AssumeRole API 작업에서 명령을 AWS STS assume-role 사용하여 역할을 수임할 때 IAM Identity Center에서 발급한 컨텍스트 어설션이 설정된 후 요청 컨텍스트에 포함됩니다.
- 데이터 유형 – [ARN](#), [문자열](#)
- 값 유형-단일 값

identitycenter:ApplicationArn

이 컨텍스트 키는 IAM Identity Center가 컨텍스트 어설션을 발행한 애플리케이션의 ARN입니다. 정책에서 이 키를 사용하여 identitycenter:ApplicationArn가 예상 애플리케이션에서 왔는지 여부를 확인할 수 있습니다. 이 키를 사용하면 예상치 못한 애플리케이션에서 IAM 역할에 액세스하지 못하게 할 수 있습니다.

- 가용성 -이 키는 API 작업의 AWS STS AssumeRole 요청 컨텍스트에 포함됩니다. 요청 컨텍스트에는 IAM Identity Center에서 발급한 컨텍스트 어설션이 포함됩니다.
- 데이터 유형 – [ARN](#), [문자열](#)
- 값 유형-단일 값

identitycenter:자격 증명Id

이 컨텍스트 키는 ID 강화 역할 자격 증명의 임의 ID가며 로깅에만 사용됩니다. 이 키 값은 예측할 수 없으므로 정책의 컨텍스트 어설션에 사용하지 않는 것이 좋습니다.

- 가용성 -이 키는 API 작업의 AWS STS AssumeRole 요청 컨텍스트에 포함됩니다. 요청 컨텍스트에는 IAM Identity Center에서 발급한 컨텍스트 어설션이 포함됩니다.
- 데이터 유형 – [문자열](#)
- 값 유형-단일 값

identitycenter:InstanceArn

이 컨텍스트 키는 `identitystore:UserID`에 대한 컨텍스트 어설션을 발행한 IAM Identity Center 인스턴스의 ARN입니다. 이 키를 사용하여 `identitystore:UserID` 및 컨텍스트 어설션이 예상 IAM Identity Center 인스턴스 ARN에서 왔는지 확인할 수 있습니다.

- 가용성 -이 키는 API 작업의 AWS STS AssumeRole 요청 컨텍스트에 포함됩니다. 요청 컨텍스트에는 IAM Identity Center에서 발급한 컨텍스트 어설션이 포함됩니다.
- 데이터 유형 – [ARN](#), [문자열](#)
- 값 유형-단일 값

IAM Identity Center 로깅 및 모니터링

모범 사례는 조직에서 변경 사항이 기록되고 있는지 모니터링하는 것입니다. 모니터링은 예기치 않은 변경 사항을 조사하고 원치 않는 모든 변경 사항을 롤백할 수 있도록 도와줍니다. IAM Identity Center는 현재 조직과 조직 내에서 발생하는 활동, AWS CloudTrail 즉 Amazon EventBridge를 모니터링하는데 도움이 되는 두 가지 AWS 서비스를 지원합니다.

주제

- [를 사용하여 IAM Identity Center API 호출 로깅 AWS CloudTrail](#)
- [를 사용하여 IAM Identity Center SCIM API 호출 로깅 AWS CloudTrail](#)
- [Amazon EventBridge와 애플리케이션 구성 요소 연결](#)
- [구성 가능한 AD 동기화 오류 로깅](#)

를 사용하여 IAM Identity Center API 호출 로깅 AWS CloudTrail

AWS IAM Identity Center는 IAM Identity Center에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 IAM Identity Center에 대한 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 IAM Identity Center 콘솔로부터의 호출과 IAM Identity Center API 작업에 대한 코드 호출이 포함됩니다. [추적](#)을 생성하면 IAM Identity Center 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 IAM Identity Center에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하세요.

다음 표에는 IAM Identity Center의 CloudTrail 이벤트, CloudTrail 이벤트 소스, 일치하는 API가 요약되어 있습니다. API에 대해 자세히 알아보려면 [IAM Identity Center API 참조](#)를 참조하세요.

 Note

IAM Identity Center 사용자 AWS 로에 로그인하기 위해 AWS 내보내는 로그인이라고 하는 추가 CloudTrail 이벤트 그룹이 있습니다. 이러한 이벤트에는 일치하는 퍼블릭 API가 없으므로 API 참조에 나열되지 않습니다.

CloudTrail 이벤트	퍼블릭 API	설명	CloudTrail 이벤트 소스
IAM Identity Center	IAM Identity Center	IAM Identity Center API를 사용하면 권한 세트, 애플리케이션, 신뢰할 수 있는 토큰 발급자, 계정 및 애플리케이션 할당, IAM Identity Center 인스턴스, 태그를 관리할 수 있습니다.	sso.amazonaws.com
자격 증명 스토어	자격 증명 스토어	자격 증명 스토어 API를 사용하면 작업 인력의 사용자 및 그룹의 수명 주기와 사용자의 그룹 멤버십을 관리할 수 있습니다. 또한 사용자의 MFA 디바이스 관리를 지원합니다.	sso-directory.amazonaws.com, identitystore.amazonaws.com
OIDC	OIDC	OIDC APIs는 신뢰할 수 있는 ID 전파와 이미 인증된 IAM Identity Center 사용자로 AWS CLI 및 IDE 툴킷에 대	sso.amazonaws.com, sso-oidc.amazonaws.com

CloudTrail 이벤트	퍼블릭 API	설명	CloudTrail 이벤트 소스
		한 로그인을 지원합니다.	
AWS 액세스 포털	AWS 액세스 포털	AWS 액세스 포털 APIs는 AWS 액세스 포털 및 사용자를 통해 계정 자격 증명을 가져오는 작업을 지원합니다 AWS CLI.	sso.amazonaws.com
SCIM	SCIM	SCIM API는 SCIM 프로토콜을 통한 사용자, 그룹, 그룹 멤버십의 프로비저닝을 지원합니다. 자세한 정보는 를 사용하여 IAM Identity Center SCIM API 호출 로깅 AWS CloudTrail 을 참조하세요.	identitystore-scim.amazonaws.com
AWS Sign-In	퍼블릭 API 없음	AWS 는 사용자 인증 및 페더레이션 흐름을 위한 로그인 CloudTrail 이벤트를 IAM Identity Center로 내보냅니다.	signin.amazonaws.com

주제

- [IAM Identity Center의 CloudTrail 사용 사례](#)
- [CloudTrail의 IAM Identity Center 정보](#)

IAM Identity Center의 CloudTrail 사용 사례

IAM Identity Center에서 내보내는 CloudTrail 이벤트는 다양한 사용 사례에 유용할 수 있습니다. 조직은 이러한 이벤트 로그를 사용하여 AWS 환경 내 사용자 액세스 및 활동을 모니터링하고 감사할 수 있습니다. 이는 규정 준수 사용 사례에 도움이 될 수 있습니다. 누가 언제 어떤 리소스에 액세스하는지에 대한 세부 정보가 로그에 캡처되기 때문입니다. CloudTrail 데이터를 인시던트 조사에 사용하여 팀이 사용자 작업을 분석하고 의심스러운 동작을 추적할 수도 있습니다. 또한 이벤트 기록은 시간 경과에 따른 사용자 권한 및 구성의 변경에 대한 가시성을 제공하여 문제 해결 노력을 지원할 수 있습니다.

다음 섹션에서는 감사, 인시던트 조사, 문제 해결과 같은 워크플로에 정보를 제공하는 기본적인 사용 사례에 대해 설명합니다.

IAM Identity Center 사용자 시작 CloudTrail 이벤트에서 사용자 식별

IAM Identity Center는 IAM Identity Center에 로그인하거나 MFA 디바이스 관리를 포함하여 AWS 액세스 포털을 AWS CLI 사용하는 등 CloudTrail 이벤트 뒤에 있는 IAM Identity Center 사용자를 식별할 수 있는 두 개의 CloudTrail 필드를 내보냅니다.

- **userId** - IAM Identity Center 인스턴스의 자격 증명 스토어에 있는 고유하고 변경 불가능한 사용자 식별자.
- **identityStoreArn** - 사용자가 포함된 자격 증명 스토어의 Amazon 리소스 이름(ARN).

userId 및 **identityStoreArn** 필드는 다음 예제 CloudTrail 이벤트 로그와 같이 [userIdentity](#) 요소 내에 중첩된 **onBehalfOf** 요소에 표시됩니다. 이 이벤트 로그는 **userIdentity** 유형이 "IdentityCenterUser"인 이벤트에 대해 이 두 필드를 표시합니다. **userIdentity** 유형이 'Unknown'인 인증된 IAM Identity Center 사용자의 이벤트에서도 이러한 필드를 찾을 수 있습니다. 워크플로는 두 유형 값을 모두 수락해야 합니다.

```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"
}
```

i Tip

IAM Identity Center CloudTrail 이벤트 뒤에 있는 사용자를 식별하는 데에 `userId` 및 `identityStoreArn`을 사용하는 것이 좋습니다. `userIdentity` 요소 아래의 `userName` 및 `principalId` 필드는 더 이상 사용할 수 없습니다. 감사 또는 인시던트 대응과 같은 워크플로가 `username`에 대한 액세스 권한에 의존하는 경우 다음과 같은 두 가지 옵션이 있습니다.

- [로그인 CloudTrail 이벤트의 사용자 이름](#)에 설명된 대로 IAM Identity Center 디렉터리에서 사용자 이름을 검색합니다.
- Sign-in의 `additionalEventData` 요소에서 IAM Identity Center가 내보내는 `UserName`을 가져옵니다. 이 옵션은 IAM Identity Center 디렉터리에 액세스할 필요가 없습니다. 자세한 내용은 [로그인 CloudTrail 이벤트의 사용자 이름](#) 단원을 참조하십시오.

`username` 필드를 포함하여 사용자의 세부 정보를 검색하려면 사용자 ID와 자격 증명 스토어 ID를 파라미터로 하여 자격 증명 스토어를 쿼리합니다. [DescribeUser](#) API 요청 또는 CLI를 통해 이 작업을 수행할 수 있습니다. 다음은 예시 CLI 명령입니다. IAM Identity Center 인스턴스가 CLI 기본 리전에 있는 경우 `region` 파라미터를 생략할 수 있습니다.

```
aws identitystore describe-user \
--identity-store-id d-1234567890 \
--user-id 544894e8-80c1-707f-60e3-3ba6510dfac1 \
--region your-region-id
```

이전 예제에서 CLI 명령을 위한 자격 증명 스토어 ID 값을 확인하려면 `identityStoreArn` 값에서 자격 증명 스토어 ID를 추출하면 됩니다. 예제 ARN `arn:aws:identitystore::111122223333:identitystore/d-1234567890`에서 자격 증명 스토어 ID는 `d-1234567890`입니다. 또는 IAM Identity Center 콘솔의 설정 섹션에서 자격 증명 스토어 탭으로 이동하여 자격 증명 스토어 ID를 찾을 수도 있습니다.

IAM Identity Center 디렉터리에서 사용자 조회를 자동화한 경우 사용자 조회 빈도를 추정하고 [자격 증명 스토어 API에서 IAM Identity Center 스로틀 제한](#)을 고려하는 것이 좋습니다. 검색된 사용자 속성을 캐싱하면 스로틀 제한 이내로 유지하는 데 도움이 될 수 있습니다.

동일한 사용자 세션 내에서 사용자 이벤트 상호 연관

로그인 이벤트에서 내보낸 [AuthWorkflowID](#) 필드를 사용하면 IAM Identity Center 사용자 세션을 시작하기 전에 로그인 시퀀스와 연결된 모든 CloudTrail 이벤트를 추적할 수 있습니다.

AWS 액세스 포털 내의 사용자 작업의 경우 `credentialId` 값은 작업을 요청하는 데 사용되는 IAM Identity Center 사용자 세션의 ID로 설정됩니다. 이 값을 사용하여 AWS 액세스 포털의 동일한 인증된 IAM Identity Center 사용자 세션 내에서 시작된 CloudTrail 이벤트를 식별할 수 있습니다.

Note

AWS 액세스 포털 사용과 같은 후속 이벤트에 로그인 이벤트를 상호 연관시키는 데에는 `credentialId`를 사용할 수 없습니다. 로그인 이벤트에서 내보내는 `credentialId` 필드의 값은 내부용이므로 이에 의존하지 않는 것이 좋습니다. OIDC로 간접 호출된 [AWS 액세스 포털 이벤트](#)에 대해 내보내지는 `credentialId` 필드의 값은 액세스 토큰의 ID와 같습니다.

IAM Identity Center 사용자 시작 CloudTrail 이벤트에서 사용자 백그라운드 세션 세부 정보 식별

다음 CloudTrail 이벤트는 사용자의 대화형 세션을 나타내는 기존 액세스 토큰(`subjectToken`)이 새로 고침 토큰(`requestedTokenType`)으로 교환되는 OAuth 2.0 토큰 교환 프로세스를 캡처합니다. 새로 고침 토큰은 사용자가 로그아웃한 후에도 사용자가 시작한 장기 실행 작업을 사용자의 권한으로 계속 실행될 수 있게 해줍니다.

IAM Identity Center [사용자 백그라운드 세션](#)의 경우 CloudTrail 이벤트에는 요소에 `resource`라는 추가 `requestParameters` 요소가 포함됩니다. `resource` 파라미터에는 백그라운드에서 실행되는 작업의 Amazon 리소스 이름(ARN)이 포함됩니다. 이 요소는 CloudTrail 이벤트 레코드에만 존재하며 IAM Identity Center [CreateTokenWithIAM](#) API 또는 SDK 응답에는 포함되지 않습니다.

```
{
  "clientId": "EXAMPLE-CLIENT-ID",
  "grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
  "code": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "redirectUri": "https://example.com/callback",
  "assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
  "requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
  "resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
}
```

IAM Identity Center와 외부 디렉터리 간 사용자 상호 연관

IAM Identity Center는 디렉터리의 사용자를 외부 디렉터리의 동일한 사용자와 연관시키는 데 사용할 수 있는 두 가지 사용자 속성을 제공합니다(예: Microsoft Active Directory 및 Okta Universal Directory).

- `externalId` - IAM Identity Center 사용자의 외부 식별자. 이 식별자를 외부 디렉터리의 변경 불가능한 사용자 식별자에 매핑할 것을 권장합니다. IAM Identity Center는 CloudTrail에서 이 값을 내보내지 않습니다.
- `username` - 사용자가 일반적으로 로그인하는 고객 제공 값. 값은 변경될 수 있습니다(예: SCIM 업데이트를 통해). ID 소스가 인 경우 IAM Identity Center가 CloudTrail에서 내보내는 Directory Service 사용자 이름은 인증하기 위해 입력한 사용자 이름과 일치합니다. 사용자 이름이 IAM Identity Center 디렉터리의 사용자 이름과 정확히 일치할 필요는 없습니다.

CloudTrail 이벤트에 액세스할 수 있지만 IAM Identity Center 디렉터리에 액세스할 수 없는 경우 로그인 시 `additionalEventData` 요소에서 내보낸 사용자 이름을 사용할 수 있습니다.

`additionalEventData`의 사용자 이름에 대한 자세한 내용은 [로그인 CloudTrail 이벤트의 사용자 이름](#) 섹션을 참조하세요.

ID 소스가 Directory Service인 경우 외부 디렉터리의 해당 사용자 속성에 대한 이 두 사용자 속서의 매핑은 IAM Identity Center에서 정의됩니다. 자세한 내용은 [IAM Identity Center와 외부 ID 제공업체 디렉터리 간의 속성 매핑](#) 섹션을 참조하세요. SCIM으로 사용자를 프로비저닝하는 외부 IdP는 자체 매핑이 있습니다. IAM Identity Center 디렉터리를 ID 소스로 사용하더라도 `externalId` 속성을 사용하여 보안 위탁자를 외부 디렉터리로 상호 참조할 수 있습니다.

다음 섹션에서는 사용자의 `username` 및 `externalId`가 주어졌을 때 IAM Identity Center 사용자를 조회하는 방법을 설명합니다.

`username` 및 `externalId`로 IAM Identity Center 사용자 보기

이전 예제에서와 같이 먼저 [GetUserId](#) API 요청을 사용하여 해당 `userId`를 요청한 다음 [DescribeUser](#) API 요청을 발행하여 IAM Identity Center 디렉터리에서 알려진 사용자 이름에 대해 사용자 속성을 검색할 수 있습니다. 다음 예제는 자격 증명 스토어에서 특정 사용자 이름에 대해 `userId`를 검색하는 방법을 보여줍니다. IAM Identity Center 인스턴스가 CLI의 기본 리전에 있는 경우 `region` 파라미터를 생략할 수 있습니다.

```
aws identitystore get-user-id \
  --identity-store d-9876543210 \
  --alternate-identifier '{
    "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
    }
  }' \
  --region your-region-id
```

마찬가지로, externalId를 알고 있을 때도 동일한 메커니즘을 사용할 수 있습니다. 이전 예제의 속성 경로를 externalId 값으로 업데이트하고 속성 값을 검색하고 있는 특정 externalId로 업데이트합니다.

Microsoft Active Directory(AD)의 사용자 보안 식별자(SID) 및 externalId 보기

경우에 따라 IAM Identity Center는 AWS 액세스 포털 및 OIDC API가 내보내는 이벤트와 같은 CloudTrail 이벤트 principalId 필드에서 사용자의 SID를 내보냅니다. APIs 이러한 사례는 단계적으로 폐지되고 있습니다. AD의 고유 사용자 식별자가 필요한 경우 워크플로에서 AD 속성 objectguid를 사용하는 것이 좋습니다. 이 값은 IAM Identity Center 디렉터리의 externalId 속성에서 찾을 수 있습니다. 그러나 워크플로에서 SID를 사용해야 하는 경우 IAM Identity Center API를 통해 얻을 수 없으므로 AD에서 값을 검색합니다.

[동일한 사용자 세션 내에서 사용자 이벤트 상호 연관](#)에 externalId 및 username 필드를 사용하여 IAM Identity Center 사용자를 외부 디렉터리의 일치하는 사용자와 연관시키는 방법이 설명되어 있습니다. 기본적으로 IAM Identity Center는 externalId를 AD의 objectguid 속성에 매핑하며 이 매핑은 고정됩니다. IAM Identity Center를 통해 관리자는 AD의 userprincipalname에 대한 기본 매핑과 다르게 username를 매핑할 수 있는 유연성을 가질 수 있습니다.

IAM Identity Center 콘솔에서 이러한 매핑을 볼 수 있습니다. 설정의 ID 소스 탭으로 이동하여 작업 메뉴에서 동기화 관리를 선택합니다. 동기화 관리 섹션에서 속성 매핑 보기 버튼을 선택합니다.

IAM Identity Center에서 사용할 수 있는 고유 AD 사용자 식별자를 사용하여 AD의 사용자를 조회할 수 있지만, 변경 불가능한 식별자이므로 쿼리에 objectguid를 사용하는 것이 좋습니다. 다음 예제는 Powershell로 Microsoft AD를 쿼리하여 16809ecc-7225-4c20-ad98-30094aefdbca라는 사용자 objectguid 값으로 사용자를 검색하는 방법을 보여줍니다. 이 쿼리에 대한 성공적인 응답에 사용자의 SID가 포함됩니다.

```
Install-WindowsFeature -Name RSAT-AD-PowerShell

Get-ADUser `
  -Filter {objectGUID -eq [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
  -Properties *
```

CloudTrail의 IAM Identity Center 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. IAM Identity Center에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 [CloudTrail 이벤트 기록을 사용하여 이벤트 보기](#)를 참조하세요.

Note

CloudTrail 이벤트에서 사용자 식별 및 사용자 작업 추적이 어떻게 진화하고 있는지에 대한 자세한 내용은 AWS 보안 블로그의 [IAM Identity Center의 CloudTrail 이벤트에 대한 중요 변경 사항](#)을 참조하세요.

IAM Identity Center에 대한 이벤트를 AWS 계정포함하여 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS Region에 추적이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서에서 다음 주제를 참조하세요.

- [추적 생성 개요](#)
- [CloudTrail 지원 서비스 및 통합](#)
- [CloudTrail에 대한 Amazon SNS 알림 구성](#)
- [여러 리전에서 CloudTrail 로그 파일 수신](#) 및 [여러 계정에서 CloudTrail 로그 파일 수신](#)

에서 CloudTrail 로깅이 활성화되면 IAM Identity Center 작업에 대한 AWS 계정 API 호출이 로그 파일에서 추적됩니다. IAM Identity Center 레코드는 로그 파일의 다른 AWS 서비스 레코드와 함께 작성됩니다. CloudTrail은 기간 및 파일 크기를 기준으로 새 파일을 만들고 기록하는 시점을 결정합니다.

지원되는 IAM Identity Center API의 CloudTrail 이벤트

다음 섹션에서는 IAM Identity Center가 지원하는 다음 API와 관련된 CloudTrail 이벤트에 관하여 정보를 제공합니다.

- [IAM Identity Center API](#)
- [자격 증명 스토어 인증](#)
- [OIDC API](#)
- [AWS 포털 API 액세스](#)
- [SCIM API](#)

IAM Identity Center API 작업의 CloudTrail 이벤트

다음 목록에 퍼블릭 IAM Identity Center 작업이 `sso.amazonaws.com` 이벤트 소스를 사용해 내보내는 CloudTrail 이벤트가 포함되어 있습니다. 퍼블릭 IAM Identity Center API 작업에 대한 자세한 내용은 [IAM Identity Center API 참조](#)를 참조하세요.

CloudTrail에서 콘솔이 사용하는 IAM Identity Center 콘솔 API 작업에 대한 추가 이벤트를 찾을 수 있습니다. 이러한 콘솔 API에 대한 자세한 내용은 [서비스 권한 부여 참조](#)를 참조하세요.

- [AttachCustomerManagedPolicyReferenceToPermissionSet](#)
- [AttachManagedPolicyToPermissionSet](#)
- [CreateAccountAssignment](#)
- [CreateApplication](#)
- [CreateApplicationAssignment](#)
- [CreateInstance](#)
- [CreateInstanceAccessControlAttributeConfiguration](#)
- [CreatePermissionSet](#)
- [CreateTrustedTokenIssuer](#)
- [DeleteAccountAssignment](#)
- [DeleteApplication](#)
- [DeleteApplicationAccessScope](#)
- [DeleteApplicationAssignment](#)
- [DeleteApplicationAuthenticationMethod](#)
- [DeleteApplicationGrant](#)

- [DeleteInlinePolicyFromPermissionSet](#)
- [DeleteInstance](#)
- [DeleteInstanceAccessControlAttributeConfiguration](#)
- [DeletePermissionsBoundaryFromPermissionSet](#)
- [DeletePermissionSet](#)
- [DeleteTrustedTokenIssuer](#)
- [DescribeAccountAssignmentCreationStatus](#)
[S](#)
- [DescribeAccountAssignmentDeletionStatus](#)
- [DescribeApplication](#)
- [DescribeApplicationAssignment](#)
- [DescribeApplicationProvider](#)
- [DescribeInstance](#)
- [DescribeInstanceAccessControlAttributeConfiguration](#)
- [DescribePermissionSet](#)

- [DescribePermissionSetProvisioningStatus](#)
- [DescribeTrustedTokenIssuer](#)
- [DetachCustomerManagedPolicyReferenceFromPermissionSet](#)
- [DetachManagedPolicyFromPermissionSet](#)
- [GetApplicationAccessScope](#)
- [GetApplicationAssignmentConfiguration](#)
- [GetApplicationAuthenticationMethod](#)
- [GetApplicationGrant](#)
- [GetInlinePolicyForPermissionSet](#)
- [GetPermissionsBoundaryForPermissionSet](#)
- [ListAccountAssignmentCreationStatus](#)
- [ListAccountAssignmentDeletionStatus](#)
- [ListAccountAssignments](#)
- [ListAccountAssignmentsForPrincipal](#)
- [ListAccountsForProvisionedPermissionSet](#)
-

[ListApplicationAccessScopes](#)

•

[ListApplicationAssignments](#)

•

[ListApplicationAssignmentsForPrincipal](#)

•

[ListApplicationAuthenticationMethods](#)

•

[ListApplicationGrants](#)

•

[ListApplicationProviders](#)

•

[ListApplications](#)

•

[ListCustomerManagedPolicyReferencesInPermissionSet](#)

•

[ListInstances](#)

•

[ListManagedPoliciesInPermissionSet](#)

•

[ListPermissionSetProvisioningStatus](#)

•

[ListPermissionSets](#)

•

[ListPermissionSetsProvisionedToAccount](#)

•

[ListTagsForResource](#)

•

[ListTrustedTokenIssuers](#)

•

[ProvisionPermissionSet](#)

- [PutApplicationAccessScope](#)
- [PutApplicationAssignmentConfiguration](#)
- [PutApplicationAuthenticationMethod](#)
- [PutApplicationGrant](#)
- [PutInlinePolicyToPermissionSet](#)
- [PutPermissionsBoundaryToPermissionSet](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateApplication](#)
- [UpdateInstance](#)
- [UpdateInstanceAccessControlAttributeConfiguration](#)
- [UpdatePermissionSet](#)
- [UpdateTrustedTokenIssuer](#)

자격 증명 스토어 API 작업의 CloudTrail 이벤트

다음 목록에 퍼블릭 자격 증명 스토어 작업이 `identitystore.amazonaws.com` 이벤트 소스를 사용해 내보내는 CloudTrail 이벤트가 포함되어 있습니다. 퍼블릭 자격 증명 스토어 API 작업에 대한 자세한 내용은 [자격 증명 스토어 API 참조](#)를 참조하세요.

CloudTrail에서 `sso-directory.amazonaws.com` 이벤트 소스를 사용하는 자격 증명 스토어 콘솔 API 작업에 대한 추가 이벤트를 찾을 수 있습니다. 이러한 APIs 콘솔 및 AWS 액세스 포털을 지원합니다. 그룹에 멤버를 추가하는 등 특정 작업의 발생을 감지해야 하는 경우 퍼블릭 및 콘솔 API 작업을 모두 고려하는 것이 좋습니다. 이러한 콘솔 API에 대한 자세한 내용은 [서비스 권한 부여 참조](#)를 참조하세요.

- [CreateGroup](#)
- [CreateGroupMembership](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteGroupMembership](#)
- [DeleteUser](#)
- [DescribeGroup](#)
- [DescribeGroupMembership](#)
- [DescribeUser](#)
- [GetGroupId](#)
- [GetGroupMembershipId](#)
- [GetUserId](#)
- [IsMemberInGroups](#)
- [ListGroupMemberships](#)
- [ListGroupMembershipsForMember](#)
- [ListGroups](#)
- [ListUsers](#)
- [UpdateGroup](#)
- [UpdateUser](#)

OIDC API 작업의 CloudTrail 이벤트

다음 목록에 퍼블릭 OIDC 작업이 내보내는 CloudTrail 이벤트가 포함되어 있습니다. 퍼블릭 OIDC API 작업에 대한 자세한 내용은 [OIDC API 참조](#)를 참조하세요.

- [CreateToken](#)(이벤트 소스 `sso.amazonaws.com`)
- [CreateTokenWithIAM](#)(이벤트 소스 `sso-oauth.amazonaws.com`)

AWS 액세스 포털 API 작업의 CloudTrail 이벤트

다음 목록에는 AWS 액세스 포털 API 작업이 이벤트 소스와 함께 내보내는 CloudTrail `sso.amazonaws.com` 이벤트가 포함되어 있습니다. 퍼블릭 API에서 사용할 수 없는 것으로 표시된 API 작업은 AWS 액세스 포털의 작업을 지원합니다. 를 사용하면 퍼블릭 AWS 액세스 포털 API 작업과 퍼블릭 API에서 사용할 수 없는 작업 모두에서 CloudTrail 이벤트가 방출될 수 있습니다. 퍼블릭 AWS 액세스 포털 API 작업에 대한 자세한 내용은 [AWS 액세스 포털 API 참조](#)를 참조하세요.

- `Authenticate` (퍼블릭 API에서는 사용할 수 없습니다. AWS 액세스 포털에 대한 로그인을 제공합니다.)
- `Federate`(퍼블릭 API에서는 사용할 수 없습니다. 애플리케이션에 대한 페더레이션을 제공합니다.)
- [ListAccountRoles](#)
- [ListAccounts](#)
- `ListApplications` (퍼블릭 API에서는 사용할 수 없습니다. AWS 액세스 포털에 표시할 사용자에게 할당된 리소스를 제공합니다.)
- `ListProfilesForApplication` (퍼블릭 API에서는 사용할 수 없습니다. AWS 액세스 포털에 표시할 애플리케이션 메타데이터를 제공합니다.)
- [GetRoleCredentials](#)
- [Logout](#)

SCIM API 작업의 CloudTrail 이벤트

퍼블릭 SCIM API 작업에 대한 자세한 내용은 [AWS 액세스 포털 API 참조](#)를 참조하세요.

IAM Identity Center CloudTrail 이벤트의 ID 정보

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 사용자 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자의 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에 의해 이루어졌는지 여부입니다.
- IAM Identity Center 사용자가 요청을 했는지 여부. 그렇다면 CloudTrail 이벤트에서 `userId` 및 `identityStoreArn` 필드를 사용하여 요청을 시작한 IAM Identity Center 사용자를 식별할 수 있습니다. 자세한 내용은 [IAM Identity Center 사용자 시작 CloudTrail 이벤트에서 사용자 식별](#) 단원을 참조하십시오.

자세한 내용은 [CloudTrail userIdentity 요소](#)를 참조하세요.

Note

현재 IAM Identity Center는 [OIDC API](#)를 사용하여 AWS 관리형 웹 애플리케이션(예: Amazon SageMaker AI Studio)에 사용자 로그인하기 위한 CloudTrail 이벤트를 내보내지 않습니다. 이러한 웹 애플리케이션은 더 광범위한 [the section called “AWS 관리형 애플리케이션”](#)들의 일부이며, 여기에는 Amazon Athena SQL 및 Amazon S3 Access Grants와 같은 웹 앱이 아닌 애플리케이션도 포함됩니다.

IAM Identity Center의 CloudTrail 이벤트 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 전달할 수 있게 하는 구성입니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 이벤트는 퍼블릭 API 직접 호출에 대한 순서 지정된 스택 추적이 아니기 때문에 특정 순서로 표시되지 않습니다. CloudTrail 사용 설명서에서 [CloudTrail 레코드의 콘텐츠](#)에 대해 자세히 알아보세요.

이 예제는 IAM Identity Center와 상호 작용하는 IAM 사용자(samadams)가 수행한 DescribePermissionsPolicies 작업을 캡처하는 CloudTrail 로그 항목을 보여줍니다.

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJAIENLMexample",
        "arn": "arn:aws:iam::08966example:user/samadams",
        "accountId": "111122223333",
        "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":"111122223333"
  }
]
}

```

이 예제는 AWS 액세스 포털 내에서 IAM Identity Center 사용자가 수행한 ListApplications 작업을 캡처하는 CloudTrail 로그 항목을 보여줍니다.

```

{
  "Records":[
    {
      "eventVersion":"1.05",
      "userIdentity":{
        "type":"IdentityCenterUser",
        "accountId":"111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
          "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
      },
      "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": "111122223333"
  }
]
}

```

이 예제는 IAM Identity Center OIDC 서비스로 인증하는 IAM Identity Center 사용자가 수행한 CreateToken 작업을 캡처하는 CloudTrail 로그 항목을 보여줍니다.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "accountId": "111122223333",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
  },
  "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": "111122223333",
        "type": "IdentityStoreId",
        "ARN": "d-1234567890"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }
}

```

IAM Identity Center 로그인 이벤트 이해

AWS CloudTrail 는 모든 IAM Identity Center ID 소스에 대해 성공 및 실패한 로그인 이벤트를 기록합니다. IAM Identity Center 및 Active Directory(AD Connector 및 AWS Managed Microsoft AD) 소스 자격 증명에는 사용자에게 특정 자격 증명 확인 요청의 상태 외에도 특정 자격 증명 챌린지 또는 요인을 해결하라는 메시지가 표시될 때마다 캡처되는 추가 로그인 이벤트가 포함됩니다. 사용자는 필요한 보안 인증 과정을 모두 완료한 후에만 로그인되며, 이 경우 UserAuthentication 이벤트가 기록됩니다.

다음 표에는 IAM Identity Center 로그인 CloudTrail 이벤트 이름, 목적, 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 Identity Center 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 Identity Center 사용자, AD Connector 및 AWS Managed Microsoft AD

이벤트 이름	이벤트 목적	ID 소스 적용 가능성
UserAuthentication	사용자에게 문제가 발생한 모든 인증 요구 사항이 성공적으로 완료되었으며 사용자가 성공적으로 로그인했음을 알리는데 사용됩니다. 사용자가 필수 보안 인증 과정을 성공적으로 완료하지 못하면 <i>UserAuthentication</i> 이벤트가 기록되지 않습니다.	모든 ID 소스

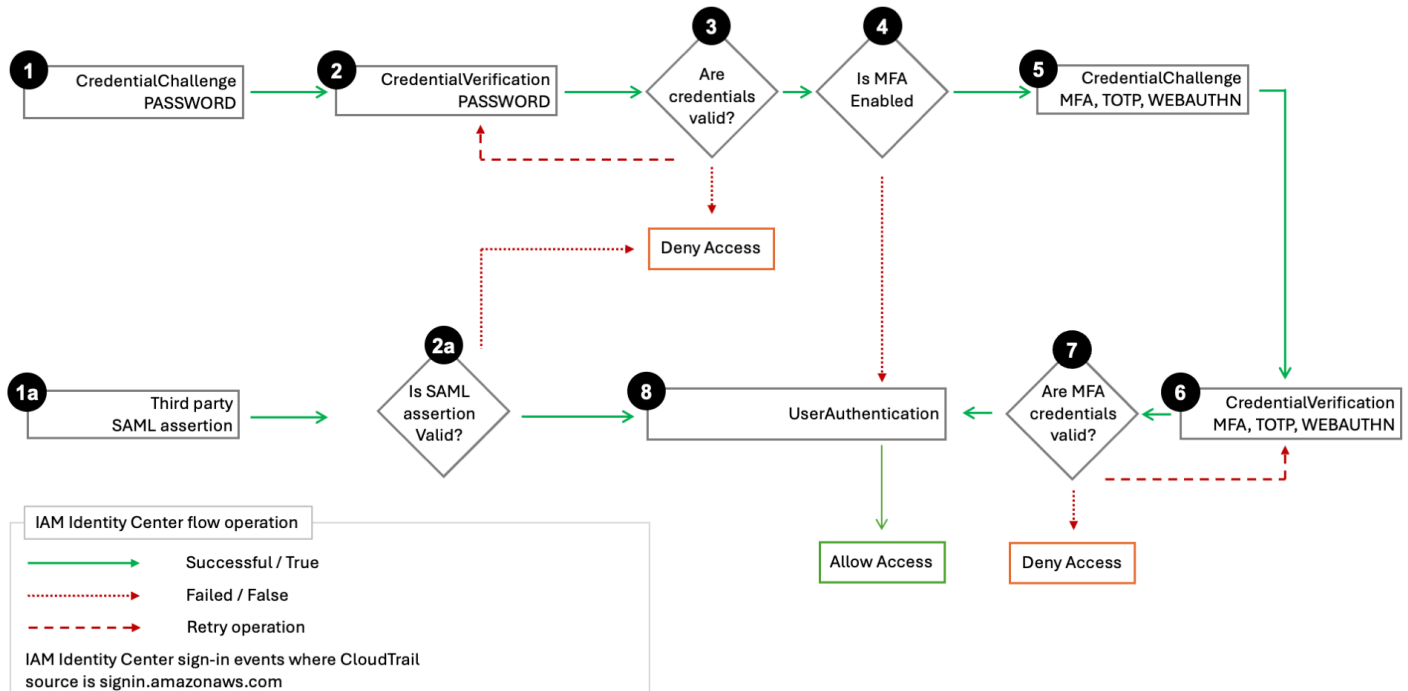
다음 표에는 특정 로그인 CloudTrail 이벤트에 포함된 유용한 추가 이벤트 데이터 필드가 나와 있습니다.

Field	이벤트 목적	로그인 이벤트 적용 가능성	예제 값
AuthWorkflowID	전체 로그인 시퀀스에서 발생하는 모든 이벤트의 상관관계를 파악하는 데 사용됩니다. IAM Identity Center는 각 사용자 로그인마다 여러 이벤트를 발생시킬 수 있습니다.	CredentialChallenge, CredentialVerification, UserAuthentication	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"
CredentialType	문제가 발생한 보안 인증 정보 또는 요소를 지정하는 데 사용됩니다. UserAuthentication 이벤트에는 사용자의 로그인 시퀀스에서 성공적으로 확인된 모든	CredentialChallenge, CredentialVerification, UserAuthentication	CredentialType": "PASSWORD" 또는 "CredentialType": "PASSWORD, TOTP" (가능한 값: PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP,

Field	이벤트 목적	로그인 이벤트 적용 가능성	예제 값
DeviceEnrollmentRequired	CredentialType 값이 포함됩니다. 사용자가 로그인할 때 MFA 디바이스를 등록해야 하고 해당 요청을 성공적으로 완료했음을 지정하는 데 사용됩니다.	UserAuthentication	RESYNC_TOTP, EMAIL_OTP) "DeviceEnrollmentRequired": "true"
LoginTo	성공적인 로그인 순서에 따라 리디렉션 위치를 지정하는 데 사용됩니다.	UserAuthentication	"LoginTo": "https://mydirectory.awsapps.com/start/....."

IAM Identity Center 로그인 흐름의 CloudTrail 이벤트

다음 다이어그램은 로그인 흐름과 로그인이 내보내는 CloudTrail 이벤트를 설명합니다.



이 다이어그램은 암호 로그인 흐름과 페더레이션 로그인 흐름을 보여줍니다.

1~8단계로 구성된 암호 로그인 흐름은 사용자 이름 및 암호 로그인 프로세스 동안 진행되는 단계를 보여줍니다. IAM Identity Center는 `userIdentity.additionalEventData.CredentialType`을 "PASSWORD"로 설정하며, IAM Identity Center는 자격 증명 문제-응답 주기를 진행하고 필요에 따라 재시도합니다.

단계의 수는 [로그인 유형과 다중 인증\(MFA\)의 존재 여부](#)에 따라 달라집니다. 인증에 성공하면 초기 프로세스에서 3개 또는 UserAuthentication 5개의 CloudTrail 이벤트가 발생하고 로 끝납니다. 암호 인증 시도가 실패하면 IAM Identity Center가 일반 인증 또는 MFA 인증(활성화된 경우)에 대한 CredentialChallenge를 다시 발급하기 때문에 추가 CloudTrail 이벤트가 발생합니다.

암호 로그인 흐름은 CreateUser API 직접 호출로 새로 생성된 IAM Identity Center 사용자가 일회용 암호(OTP)로 로그인하는 시나리오도 다릅니다. 이 시나리오의 자격 증명 유형은 "EMAIL_OTP"입니다.

1a, 2a, 8단계를 포함하는 페더레이션 로그인 흐름은 [ID 제공업체가 SAML 어설션을 제공하고](#) IAM Identity Center에서 검증한 후 성공하면 UserAuthentication을 발생시키는 페더레이션 인증 프로세스 동안의 주요 단계들을 보여줍니다. 외부 페더레이션 ID 제공업체가 모든 사용자 자격 증명 인증을 담당하기 때문에 IAM Identity Center는 3~7단계에서 내부 MFA 인증 시퀀스를 간접 호출하지 않습니다.

로그인 CloudTrail 이벤트의 사용자 이름

IAM Identity Center는 IAM Identity Center 사용자의 로그인에 성공할 때마다 한 번씩 additionalEventData 요소 아래에 UserName 필드를 내보냅니다. 다음 목록은 범위에 있는 두 가지 로그인 이벤트와 이러한 이벤트가 발생하는 조건을 설명합니다. 사용자가 로그인할 때 조건 중 하나만 true일 수 있습니다.

- CredentialChallenge
 - 이 "PASSWORD" CredentialType인 경우 - Directory Service 또는를 사용한 암호 인증에 적용됩니다 IAM Identity Center 디렉터리.
 - CredentialType가 "EMAIL_OTP"인 경우 - CreateUser API 호출 IAM Identity Center 디렉터리로 생성한 사용자가 처음으로 로그인을 시도하고 사용자가 해당 암호로 한 번 로그인할 일회용 암호를 받는 경우에만 적용됩니다.
- UserAuthentication
 - CredentialType이 "EXTERNAL_IDP"인 경우 - 외부 IdP를 통한 인증에 적용됩니다.

인증 성공 시 UserName의 값은 다음과 같습니다.

- ID 소스가 외부 IdP인 경우 이 값은 수신 SAML 어설션의 nameID 값과 같습니다. 이 값은 IAM Identity Center 디렉터리의 UserName 필드와 같습니다.
- 자격 증명 소스가 인 경우 내보낸 IAM Identity Center 디렉터리값은이 디렉터리의 UserName 필드와 같습니다.
- 자격 증명 소스가 인 경우 내보낸 Directory Service값은 사용자가 인증 중에 입력하는 사용자 이름과 같습니다. 예를 들어 사용자 이름이 anyuser@company.com인 사용자는 anyuser, anyuser@company.com 또는 company.com/anyuser로 인증할 수 있으며, 각각의 경우에 입력한 값이 각각 CloudTrail에서 내보내집니다.

잘못된 사용자 이름 시도에 대한 보안 마스킹

기록된 이벤트가 잘못된 사용자 이름 입력으로 인한 콘솔 로그인 실패인 경우 UserName 필드에는 HIDDEN_DUE_TO_SECURITY_REASONS 문자열이 포함됩니다. 이런 경우 CloudTrail은 다음 예제에 설명된 것과 같이 텍스트에 민감한 정보가 포함될 수 있으므로 내용을 기록하지 않습니다.

- 사용자가 우발적으로 사용자 이름 필드에 암호를 입력합니다.
- 사용자가 우발적으로 개인 이메일 계정의 사용자 이름, 금융 서비스 로그인 식별자, 또는 기타 프라이빗 ID를 입력합니다.

i Tip

IAM Identity Center CloudTrail 이벤트 뒤에 있는 사용자를 식별하는 데에 `userId` 및 `identityStoreArn`을 사용하는 것이 좋습니다. `userName` 필드를 사용해야 할 경우 로그인에 성공할 때마다 한 번씩 보내는 `additionalEventData` 요소 아래의 `userName`을 사용할 수 있습니다.

`UserName` 필드를 사용하는 방법에 대한 자세한 내용은 [동일한 사용자 세션 내에서 사용자 이벤트 상호 연관](#) 섹션을 참조하세요.

IAM Identity Center 로그인 시나리오의 예제 이벤트

다음 예제에서는 다양한 AWS 로그인 시나리오에서 생성된 일반적인 CloudTrail 이벤트 시퀀스를 보여줍니다. 이 예제들은 인증 로그를 해석하고, 보안 문제를 식별하고, 인증 정책이 올바르게 작동하는지 확인하는 데 도움이 되는 참조 패턴으로 활용할 수 있습니다.

주제

- [암호만으로 인증 시 로그인 성공](#)
- [외부 ID 제공업체를 통해 인증한 경우의 로그인 성공](#)
- [암호 및 시간 기반 일회용 암호\(TOTP\) 인증 앱으로 인증 시 로그인 성공](#)
- [암호 및 MFA 등록 필수 인증을 통한 로그인 성공](#)
- [잘못된 암호 인증으로 인한 로그인 실패](#)

암호만으로 인증 시 로그인 성공

다음 이벤트 시퀀스는 성공적인 암호 전용 로그인의 예제입니다.

CredentialChallenge (Password)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
```

```

    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"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",
  "UserName":"bobsmith@example.com",
  "CredentialType":"PASSWORD"
},
"requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
"eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"serviceEventDetails":{
  "CredentialChallenge":"Success"
}
}

```

Successful CredentialVerification (Password)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    }
  }
}

```

```

    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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"
  }
}

```

Successful UserAuthentication (Password Only)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  }
}

```

```

},
"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
Bsh1Ic50BAA6ftz73M6LsfLWD1f0xvi02K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx
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 로그인
인의 예제입니다.

Successful UserAuthentication (External Identity Provider)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",

```

```

    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBshIc50BAA6ftz73M6LsflWDLf0xvi02K3wet946lC30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx-east-1",
    "CredentialType": "EXTERNAL_IDP",
    "UserName": "bobsmith@example.com"
  },
  "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 시간 기반 일회용 암호(TOTP) 인증 앱으로 인증 시 로그인 성공

다음 이벤트 시퀀스는 로그인 시 다단계 인증이 필요하고 사용자가 암호와 TOTP 인증 앱을 사용하여 성공적으로 로그인한 예제입니다.

CredentialChallenge (Password)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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",
    "UserName": "bobsmith@example.com"
  },
  "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"
  }
}
```

Successful CredentialVerification (Password)


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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 (TOTP)

```
{
  "eventVersion": "1.08",
```

```

"userIdentity":{
  "type":"IdentityCenterUser",
  "arn": "",
  "accountId":"111122223333",
  "accessKeyId": "",
  "onBehalfOf": {
    "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"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"
}
}

```

Successful CredentialVerification (TOTP)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",

```

```

    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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"
  }
}

```

Successful UserAuthentication (Password + TOTP)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",

```

```

    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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-7UGIG1YUUVe31Nkzd7ihxKn6DMdnFf00108qc3RF
Sx-pjBXXG_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 시퀀스는 사용자가 로그인 프로세스를 완료하기 전에 다중 인증(MFA)을 등록하고 성공적으로 완료해야 하는 암호 인증의 성공 예시를 보여줍니다.

CredentialChallenge (Password)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },
  "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71",
  "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",
    "UserName": "bobsmith@example.com"
  },
  "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"
  }
}
```

```
}
}
```

Successful CredentialVerification (Password)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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"
  }
}
```

Successful UserAuthentication (Password + MFA Registration Required)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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_maUsZ7ABETjeQhyWfvIHyz52rgR28sYAKN1oEk2G07czrwzXvE9HL1N2K9De8LyBEV83SFeDQfrWpkwXfFJyJqkoGrt_w6rm_MpAn0uyrVq8udY_EgU3fh0L3QWvWiQuYnDPMYPmmy_qkZgR9rz__BI\u0026wdc_csrf_token\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi50YI9QSc\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"
}
}

```

잘못된 암호 인증으로 인한 로그인 실패

다음 이벤트 시퀀스는 사용자가 사용자 이름을 성공적으로 입력했지만 암호 확인 단계에 실패하여 로그인에 실패한 인증 시도를 보여줍니다.

CredentialChallenge (Password)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
  },
  "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",
    "UserName":"bobsmith@example.com"
  },
  "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"
  }
}

```

Failed CredentialVerification (Password)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": ""
  },
  "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"
  }
}

```

를 사용하여 IAM Identity Center SCIM API 호출 로깅 AWS CloudTrail

[IAM Identity Center SCIM](#)은 사용자 AWS CloudTrail, 역할 또는가 수행한 작업에 대한 레코드를 제공하는 서비스와 통합됩니다 AWS 서비스. CloudTrail은 SCIM에 대한 API 직접 호출을 이벤트로 캡처합

니다. CloudTrail에서 수집한 정보를 사용하여 요청된 작업에 대한 정보, 작업 날짜 및 시간, 요청 파라미터 등을 확인할 수 있습니다. CloudTrail에 대한 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하십시오.

Note

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. 그러나 토큰이 2024년 9월 이전에 생성된 경우 SCIM의 이벤트를 보기 위해 액세스 토큰을 교체해야 할 수 있습니다. 자세한 내용은 [액세스 토큰 교체](#) 단원을 참조하십시오.

SCIM는 다음 작업에 대한 로그를 CloudTrail의 이벤트로 기록할 수 있도록 지원합니다.

- [CreateGroup](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteUser](#)
- [GetGroup](#)
- [GetSchema](#)
- [GetUser](#)
- [ListGroups](#)
- [ListResourceTypes](#)
- [ListSchemas](#)
- [ListUsers](#)
- [PatchGroup](#)
- [PatchUser](#)
- [PutUser](#)
- [ServiceProviderConfig](#)

CloudTrail 이벤트 예시

다음 예제에서는 IAM Identity Center를 사용한 SCIM 작업 중에 생성되는 일반적인 CloudTrail 이벤트 로그를 보여줍니다. 이 예제들은 작업 성공 및 일반적인 오류 시나리오 발생 시 이벤트의 구조와 내용

을 보여줍니다. SCIM 프로비저닝 문제를 해결할 때 CloudTrail 로그를 해석하는 방법을 이해하는 데 도움이 될 것입니다.

CreateUser 작업 성공

이 CloudTrail 이벤트는 SCIM API를 통해 수행된 성공한 CreateUser 작업을 보여줍니다. 이벤트는 요청 파라미터(민감한 정보가 마스킹된 상태)와 새로 생성된 사용자의 ID를 포함한 응답 요소를 모두 캡처합니다. 이 유형의 이벤트는 ID 제공업체가 SCIM 프로토콜을 사용하여 IAM Identity Center에 새 사용자를 성공적으로 프로비저닝할 때 생성됩니다.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "schemas" : [
        "urn:ietf:params:scim:schemas:core:2.0:User"
      ],
      "name": {
        "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "active": true,
      "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": {
    "meta" : {
      "created" : "Oct 10, 2024, 1:23:45 PM",
      "lastModified" : "Oct 10, 2024, 1:23:45 PM",
      "resourceType" : "User"
    }
  }
}
```

```

    },
    "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
    "schemas" : [
        "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "name": {
        "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "active": true,
    "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
},
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

PatchGroup 작업 실패: 필수 경로 속성 누락

이 CloudTrail 이벤트는 오류 메시지 "Missing path in PATCH request"와 함께 ValidationException을 발생시킨 실패한 PatchGroup 작업을 보여줍니다. PATCH 작업에는 수정할 그룹 속성을 지정하는 경로 속성이 필요한데 이 속성이 요청에서 누락되었기 때문에 오류가 발생했습니다.

```

{
    "eventVersion": "1.10",
    "userIdentity": {
        "type": "Unknown",
        "accountId": "123456789012",
        "accessKeyId": "xxxx"
    },
    "eventTime": "xxxx",
    "eventSource": "identitystore-scim.amazonaws.com",
    "eventName": "PatchGroup",
    "awsRegion": "us-east-1",

```

```

"sourceIPAddress": "xxx.xxx.xxx.xxx",
"userAgent": "Go-http-client/2.0",
"errorCode": "ValidationException",
"errorMessage": "Missing path in PATCH request",
"requestParameters": {
  "httpBody": {
    "operations": [
      {
        "op": "REMOVE",
        "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
      }
    ],
    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ]
  },
  "tenantId": "xxxx",
  "id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

CreateGroup 작업 실패: 그룹 이름이 이미 있음

이 CloudTrail 이벤트는 오류 메시지 "Duplicate GroupDisplayName"과 함께 `ConflictException`을 발생시킨 실패한 `CreateGroup` 작업을 보여줍니다. 이 오류는 IAM Identity Center에 이미 있는 표시 이름으로 그룹을 생성하려고 할 때 발생합니다. ID 제공업체는 고유한 그룹 이름을 사용하거나 새 그룹을 생성하는 대신 기존 그룹을 업데이트해야 합니다.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",

```

```

    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ConflictException",
  "errorMessage": "Duplicate GroupDisplayName",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}

```

PatchUser 작업 실패: 여러 이메일 주소가 지원되지 않음

이 CloudTrail 이벤트는 오류 메시지 "List attribute emails exceeds allowed limit of 1"과 함께 ValidationException을 발생시킨 실패한 PatchUser 작업을 보여줍니다. IAM Identity Center는 사용자당 하나의 이메일 주소만 지원하므로 이 오류는 사용자에게 여러 이메일 주소를 할당하려고 할 때 발생합니다. ID 제공업체는 각 사용자에게 대해 하나의 이메일 주소만 보내도록 SCIM 매핑을 구성해야 합니다.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",

```

```

    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "List attribute emails exceeds allowed limit of 1",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REPLACE",
          "path": "emails",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
      "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
      ]
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}

```

IAM Identity Center의 일반적인 SCIM API 검증 오류

다음 검증 오류 메시지는 IAM Identity Center와 함께 SCIM API를 사용할 때 CloudTrail 이벤트에 흔히 나타납니다. 이러한 검증 오류는 일반적으로 사용자 및 그룹 프로비저닝 작업 중에 발생합니다.

이러한 오류를 해결하고 SCIM 프로비저닝을 적절히 구성하는 방법에 대한 자세한 지침은 이 [AWS re:Post 문서](#)를 참조하세요.

- 목록 속성 이메일이 허용 한도인 1을 초과합니다.
- 허용 한도 1의 속성 주소 나열
- 유효성 검사 오류 1건이 감지됨: '*name.familyName*'의 값이 제약 조건을 충족하지 못함: 구성원이 정규식 패턴을 충족해야 함: `[\p{L}\p{M}\p{S}\p{N}\p{P}]{1,\n\r}+`
- 검증 오류가 2건 감지됨: 'name.familyName'의 값이 제약 조건을 충족하지 못함: 구성원의 길이는 1 이상이어야 합니다. 'name.familyName'의 값이 제약 조건을 충족하지 못했습니다. 구성원은 정규식 패턴을 충족해야 합니다. `[\p{L}\p{M}\p{S}\p{N}\p{P}]{1,\n\r}+`
- 검증 오류 2건이 감지됨:
'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value'의 값이 제약 조건을 충족하지 못함: 구성원의 길이가 1 이상이어야 함;
'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value'의 값이 제약 조건을 충족하지 못함: 구성원이 정규 표현식 패턴을 충족해야 함: `[\p{L}\p{M}\p{S}\p{N}]{1,\n\r}+`,
- RequestBody의 잘못된 JSON
- 잘못된 필터 형식

Amazon EventBridge와 애플리케이션 구성 요소 연결

IAM Identity Center를 [Amazon EventBridge](#)와 통합하면 CloudTrail 이벤트에 기록된 특정 IAM Identity Center 작업에 대한 응답으로 관리 알림을 시작하거나 자동 워크플로를 간접 호출하는 이벤트를 발생시킬 수 있습니다.

예를 들어 사용자가 애플리케이션을 삭제하거나 IAM Identity Center가 새 그룹을 생성하는 순간을 감지하도록 [EventBridge 규칙](#)을 구성할 수 있습니다. 사용 사례에 따라 이러한 이벤트를 Amazon SNS 주제로 라우팅하여 관리자에게 알리거나 AWS Lambda, [Step Functions](#) 또는 기타 [EventBridge 지원 서비스](#)를 사용하여 추가 자동화를 호출할 수 있습니다.

구성 가능한 AD 동기화 오류 로깅

구성 가능한 Active Directory(AD) 동기화 구성에 대한 로깅을 활성화하여 동기화 프로세스 중에 발생할 수 있는 오류에 대한 정보가 포함된 로그를 수신할 수 있습니다. 이러한 로그를 사용하면 구성 가능한 AD 동기화에 문제가 있는지 모니터링하고 해당하는 경우 조치를 취할 수 있습니다. Amazon CloudWatch Logs 로그 그룹, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon S3 버

킷과 Firehose에 대한 교차 계정 전송이 지원되는 Amazon Data Firehose에 로그를 전송할 수 있습니다.

제한, 권한 및 벤딩된 로그에 대한 자세한 내용은 [로깅 활성화를 AWS 서비스](#) 참조하세요.

Note

로깅에 대한 요금이 부과됩니다. 자세한 내용은 [Amazon CloudWatch 요금](#)의 [판매된 로그](#)를 참조하세요.

AD 동기화 오류 로그 활성화

1. [IAM Identity Center 콘솔](#)에 로그인합니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고 작업을 선택한 다음 로그 관리를 선택합니다.
4. 로그 전송 추가와 다음 대상 유형 중 하나를 선택합니다.
 - a. Amazon CloudWatch Logs를 선택합니다. 그런 다음 대상 로그 그룹을 선택하거나 입력합니다.
 - b. Amazon S3으로 선택합니다. 그런 다음 대상 버킷을 선택하거나 입력합니다.
 - c. Firehose로 선택합니다. 그런 다음 대상 전송 스트림을 선택하거나 입력합니다.
5. 제출을 선택합니다.

AD 동기화 오류 로그 비활성화

1. [IAM Identity Center 콘솔](#)에 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.

구성 가능한 AD 동기화 오류 로그 필드

가능한 오류 로그 필드는 다음 목록을 참조하세요.

sync_profile_name

동기화 프로파일의 이름입니다.

error_code

발생한 오류 유형을 나타내는 오류 코드입니다.

error_message

발생한 오류에 대한 자세한 정보가 포함된 메시지입니다.

sync_source

동기화 소스는 엔터티가 동기화되는 곳입니다. IAM Identity Center의 경우 Directory Service에서 관리하는 Active Directory(AD)입니다. 동기화 소스에는 영향을 받는 디렉터리의 도메인과 ARN이 포함됩니다.

sync_target

동기화 대상은 엔터티가 저장되는 대상입니다. IAM Identity Center의 경우 Identity Store입니다. 동기화 대상에는 영향을 받는 Identity Store ARN이 포함됩니다.

source_entity_id

오류를 유발하는 엔터티의 고유 식별자입니다. IAM Identity Center의 경우 엔터티의 SID입니다.

source_entity_type

오류를 유발하는 엔터티 유형입니다. USER 또는 GROUP 값을 가질 수 있습니다.

eventTimestamp

오류 발생한 타임스탬프입니다.

구성 가능한 AD 동기화 오류 로그 예제

예제 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"
}

```

예제 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

타사 감사자는 여러 규정 준수 프로그램의 AWS IAM Identity Center 일환으로 AWS 서비스 의 보안 및 AWS 규정 준수를 평가합니다.

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 [AWS 서비스 규정 준수 프로그램 범위 내](#) 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 [AWS 규정 준수 프로그램](#).

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

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 AWS 서비스 결정됩니다. 사용 시 규정 준수 책임에 대한 자세한 내용은 [AWS 보안 설명서](#)를 AWS 서비스참조하세요.

지원되는 규정 준수 표준

IAM Identity Center는 다음 표준에 대한 감사를 거쳤으며 규정 준수 인증을 획득해야 하는 솔루션의 일부로 사용할 수 있습니다.



AWS 는 IAM Identity Center를 HIPAA [적격 서비스로 포함하도록 HIPAA](#)(Health Insurance Portability and Accountability Act) 규정 준수 프로그램을 확장했습니다.

AWS 는를 사용하여 상태 정보를 AWS 서비스 처리하고 저장하는 방법에 대해 자세히 알아보고자 하는 고객을 위해 [HIPAA 중심의 백서](#)를 제공합니다. 자세한 내용은 [HIPAA 규정 준수](#)를 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 리소스](#)를 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 Center에서 다음 자격 증명 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 규정 준수 패키지의 사본을 요청하는 방법을 포함하여 AWS PCI DSS에 대한 자세한 내용은 [PCI DSS 레벨 1](#)을 참조하세요.



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 - [AWS 아티팩트를 사용하여 다운로드](#)
- AWS SOC 2: 보안, 가용성 및 기밀성 보고서 - [AWS 아티팩트를 사용하여 다운로드](#)
- [AWS SOC 3: 보안, 가용성 및 기밀성 보고서](#)

IAM Identity Center는 AWS SOC 1, SOC 2 및 SOC 3 보고서의 범위에 있습니다. 자세한 내용은 [SOC 규정 준수](#)를 참조하세요.

IAM Identity Center 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 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 리전 및 가용 영역에 대한 자세한 내용은 [AWS 글로벌 인프라](#)를 참조하세요.

AWS IAM Identity Center 복원력에 대한 자세한 내용은 [섹션을 참조하세요](#) [복원력 설계 및 리전 동작](#).

IAM Identity Center의 인프라 보안

관리형 서비스인 AWS 글로벌 네트워크 보안으로 보호 AWS IAM Identity Center 됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 [AWS 클라우드 보안을](#) 참조하세요. 인프라 보안 모범 사례를 사용하여 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 [인프라 보호를](#) 참조하세요 AWS .

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 IAM Identity Center에 액세스합니다. 클라이언트는 다음을 지원해야 합니다.

- Transport Layer Security(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

IAM Identity Center에서의 데이터 보호

AWS [공동 책임 모델](#)은 AWS IAM Identity Center의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS . 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 또한 사용하는 AWS 서비스의 보안 구성 및 관리 작업에 대한 책임이 있습니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시 FAQ](#)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS Security Blog의 [AWS Shared Responsibility Model and GDPR](#) 블로그 게시물을 참조하세요.

다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- IAM Identity Center에 다중 인증(MFA)을 사용합니다..
- TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [CloudTrail 추적 작업을](#) 참조하세요.
- 서비스 내의 AWS 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그 또는 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 또는 기타 AWS 서비스에서 콘솔 AWS IAM Identity Center, API AWS CLI또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다.

전송 중 암호화

IAM Identity Center는 Transport Layer Security(TLS) 1.2 또는 TLS 1.3 암호화 프로토콜을 사용하여 모든 네트워크 간 데이터를 자동으로 암호화해 서비스를 오가는 전송 중 데이터를 보호합니다. IAM으로 인증되고 IAM Identity Center API, Identity Store API 또는 OIDC API로 전송되는 직접 HTTPS 요청은 [AWS 서명 버전 4 알고리즘](#)을 통해 서명되어 보안 연결을 설정합니다.

데이터 개인정보보호

IAM Identity Center를 사용하면 조직의 데이터에 대한 제어권을 유지할 수 있습니다. IAM Identity Center에 저장된 사용자 및 그룹 자격 증명은 IAM Identity Center에서 활성화한 경우에만 [AWS 관리형 애플리케이션](#)과 같은 다른 AWS 서비스와 공유되며 해당 서비스에서 필요한 경우에만 공유됩니다.

자세한 내용은 [AWS 데이터 개인정보 보호 FAQ](#)를 참조하세요.

데이터 보존

IAM Identity Center는 서비스에서 삭제할 때까지 사용자 및 그룹 자격 증명, 메타데이터와 같은 데이터를 저장합니다. IAM Identity Center 인스턴스를 삭제하면 해당 인스턴스에 포함된 데이터도 삭제됩니다.

저장 시 암호화

IAM Identity Center는 다음 키 유형을 사용하여 저장된 고객 데이터를 보호하기 위한 암호화를 제공합니다.

- **AWS 소유 키 (기본 키 유형)** - IAM Identity Center는 기본적으로 이러한 키를 사용하여 데이터를 자동으로 암호화합니다. 다른 목적으로는 키를 보거나, 관리하거나, 감사하거나, AWS 소유 키를 사용할 수 없습니다. IAM Identity Center는 조치를 취하지 않고도 키 관리를 완전히 처리하여 데이터를 안전하게 유지합니다. 자세한 내용은 [AWS Key Management Service 개발자 안내서](#)의 [AWS 소유 키](#)를 참조하세요.
- **고객 관리형 키** - IAM Identity Center의 조직 인스턴스에서 사용자 및 그룹 속성과 같은 인력 자격 증명 데이터에서 저장 암호화할 대칭 고객 관리형 키를 선택할 수 있습니다. 사용자는 이러한 암호화 키를 생성하고 소유 및 관리합니다. 이 암호화 계층을 완전히 제어할 수 있으므로 다음과 같은 작업을 수행할 수 있습니다.
 - 키에 대한 액세스를 IAM Identity Center 및 같은 액세스가 필요한 IAM 보안 주체와 [AWS 관리형 애플리케이션](#) 동일한 AWS Organizations 및 관리자로 제한하는 키 정책을 수립하고 유지 관리합니다.
 - 교차 계정 액세스를 포함하여 키에 액세스하기 위한 IAM 정책 설정 및 유지 관리
 - 키 정책 활성화 및 비활성화
 - 키 암호화 자료 교체
 - 키 액세스가 필요한 데이터에 대한 액세스 감사
 - 태그 추가
 - 키 별칭 만들기
 - 삭제를 위한 스케줄 키

IAM Identity Center에서 고객 관리형 KMS 키를 구현하는 방법을 알아보려면 [에서 고객 관리형 KMS 키 구현 AWS IAM Identity Center](#) 섹션을 참조하세요. 고객 관리형 키에 대한 자세한 내용은 AWS Key Management Service 개발자 가이드의 [고객 관리형 키](#)를 참조하세요.

Note

IAM Identity Center는 AWS 소유 KMS 키를 사용하여 저장 데이터 암호화를 자동으로 활성화하여 고객 데이터를 무료로 보호합니다. 그러나 고객 관리형 키를 사용할 때는 AWS KMS 요금이 적용됩니다. 요금에 대한 자세한 내용은 [AWS Key Management Service 요금](#)을 참조하십시오.

고객 관리형 키 구현 시 고려 사항:

- 전용 키: 기존 키를 재사용하는 대신 각 IAM Identity Center 인스턴스에 대해 새로운 전용 고객 관리형 KMS 키를 생성하는 것이 좋습니다. 이 접근 방식은 보다 명확한 업무 분리를 제공하고, 액세스 제어 관리를 간소화하며, 보안 감사를 보다 간단하게 만듭니다. 전용 키를 사용하면 키 변경의 영향을 단일 IAM Identity Center 인스턴스로 제한하여 위험을 줄일 수도 있습니다.
- 여러에서 IAM Identity Center 사용 AWS 리전: IAM Identity Center 인스턴스를 추가에 복제하려는 경우 유휴 시 암호화에 고객 관리형 KMS 키를 사용해야 AWS 리전합니다. 다중 리전 IAM Identity Center에서는 기본 AWS 소유 KMS 키 유형이 지원되지 않습니다. 자세한 내용은 [여러에서 IAM Identity Center 사용 AWS 리전](#) 단원을 참조하십시오.

Note

IAM Identity Center는 인력 자격 증명 데이터의 암호화에 [봉투 암호화](#)를 사용합니다. KMS 키는 실제로 데이터를 암호화하는 데 사용되는 데이터 키를 암호화하는 래핑 키의 역할을 합니다.

AWS KMS에 대한 자세한 내용은 [AWS Key Management Service란 무엇입니까?](#)를 참조하세요.

IAM Identity Center 암호화 컨텍스트

[암호화 컨텍스트](#)는 데이터에 대한 추가 컨텍스트 정보가 포함된 비밀이 아닌 키-값 페어의 선택적 집합입니다.는 암호화 컨텍스트를 추가 인증된 데이터로 AWS KMS 사용하여 인증된 암호화를 지원합니다. 데이터 암호화 요청에 암호화 컨텍스트를 포함하면는 암호화 컨텍스트를 암호화된 데이터에 AWS KMS 바인딩합니다. 요청에 동일한 암호화 컨텍스트를 포함해야 이 데이터를 해독할 수 있습니다. 암호화 컨텍스트에 대한 자세한 내용은 [AWS KMS 개발자 가이드](#)를 참조하세요.

IAM Identity Center는 aws:sso:instance-arn, aws:identitystore:identitystore-arn 및 tenant-key-id의 암호화 컨텍스트 키를 사용합니다. 예를 들어 다음 암호화 컨텍스트는 IAM Identity Center AWS KMS

API에서 호출한 API 작업에 나타날 수 있습니다. <https://docs.aws.amazon.com/singlesignon/latest/APIReference/welcome.html>

```
"encryptionContext": {
  "tenant-key-id": "ssoins-1234567890abcdef",
  "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
}
```

다음 암호화 컨텍스트는 [Identity Store](#) AWS KMS API에서 호출한 API 작업에 나타날 수 있습니다.

```
"encryptionContext": {
  "tenant-key-id": "12345678-1234-1234-1234-123456789012",
  "aws:identitystore:identitystore-arn":
    "arn:aws:identitystore:::123456789012:identitystore/d-1234567890"
}
```

암호화 컨텍스트를 사용하여 고객 관리형 키에 대한 액세스 제어

그러나 키 정책 및 IAM 정책에서 암호화 컨텍스트를 조건으로 사용하여 대칭형 고객 관리형 키에 대한 액세스를 제어할 수도 있습니다. [고급 KMS 키 정책 설명](#)의 일부 키 정책 템플릿에는 키가 특정 IAM Identity Center 인스턴스에서만 사용되도록 하기 위한 이러한 조건이 포함되어 있습니다.

IAM Identity Center에 대한 암호화 키 모니터링

고객 관리형 키를 IAM Identity Center 인스턴스와 함께 사용하면 [AWS CloudTrail](#) 또는 [Amazon CloudWatch Logs](#)를 사용하여 IAM Identity Center에서 AWS KMS로 보내는 요청을 추적할 수 있습니다. IAM Identity Center에서 호출하는 KMS API 작업은 [2단계: KMS 키 정책 설명 준비](#)에 나열되어 있습니다. 이러한 API 작업에 대한 CloudTrail 이벤트에는 암호화 컨텍스트가 포함되어 있으므로 IAM Identity Center 인스턴스에서 호출한 AWS KMS API 작업을 모니터링하여 고객 관리형 키로 암호화된 데이터에 액세스할 수 있습니다.

AWS KMS API 작업의 CloudTrail 이벤트에서 암호화 컨텍스트의 예:

```
{
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "encryptionContext": {
      "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-xxxxxxxxxxxxxxxxxx",

```

```

    "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxxx"
  }
}
}

```

AWS 관리형 애플리케이션의 IAM Identity Center ID 속성 스토리지, 암호화 및 삭제

AWS Systems Manager 및 Amazon CodeCatalyst AWS IAM Identity Center와 같이 배포하는 일부 AWS 관리형 애플리케이션은 IAM Identity Center의 특정 사용자 및 그룹 속성을 자체 데이터 스토어에 저장합니다. IAM Identity Center의 고객 관리형 KMS 키를 사용한 저장 시 암호화는 AWS 관리형 애플리케이션에 저장된 IAM Identity Center 사용자 및 그룹 속성으로 확장되지 않습니다. AWS 관리형 애플리케이션은 저장하는 데이터에 대해 다양한 암호화 방법을 지원합니다. 마지막으로 IAM Identity Center 내에서 사용자 및 그룹 속성을 삭제하면 이러한 AWS 관리형 애플리케이션은 삭제 후에도 이 정보를 IAM Identity Center에 계속 저장할 수 있습니다. 애플리케이션 내에 저장된 데이터의 암호화 및 보안은 AWS 관리형 애플리케이션의 사용 설명서를 참조하세요.

에서 고객 관리형 KMS 키 구현 AWS IAM Identity Center

고객 관리형 키는 사용자가 생성, 소유 및 관리하는 AWS Key Management Service 키입니다. AWS IAM Identity Center에서 저장 시 암호화를 위한 고객 관리형 KMS 키를 구현하려면 다음 단계를 따르세요.

Important

일부 AWS 관리형 애플리케이션은 고객 관리형 KMS 키로 구성된 AWS IAM Identity Center와 함께 사용할 수 없습니다. [AWS IAM Identity Center와 함께 사용할 수 있는 관리형 애플리케이션을\(를\)](#) 참조하세요.

1. [1단계: 조직의 사용 사례 식별](#) - KMS 키 사용에 대한 올바른 권한을 정의하려면 조직 전체에서 관련 사용 사례를 식별해야 합니다. KMS 키 권한은 적절한 IAM 위탁자가 특정 사용 사례에 KMS 키를 사용할 수 있도록 KMS 키 정책 설명과 자격 증명 기반 정책으로 구성됩니다.
2. [2단계: KMS 키 정책 설명 준비](#) - 1단계에서 식별된 사용 사례를 기반으로 관련 KMS 키 정책 설명 템플릿을 선택하고 필수 식별자와 IAM 위탁자 이름을 입력합니다. 기본 KMS 키 정책 설명으로 시작하고 보안 정책에 필요한 경우 고급 KMS 키 정책 설명에 설명된 대로 세분화합니다.
3. [3단계: 고객 관리형 키 만들기](#) - IAM Identity Center 요구 사항을 충족하는 KMS에서 AWS KMS 키를 생성하고 2단계에서 준비한 KMS 키 정책 설명을 KMS 키 정책에 추가합니다.

4. [4단계: KMS 키의 교차 계정 사용을 위한 IAM 정책 구성](#) - 1단계에서 식별된 사용 사례를 기반으로 관련 IAM 정책 설명 템플릿을 선택하고 키 ARN을 입력하여 사용할 준비를 합니다. 그런 다음 준비된 IAM 정책 설명을 위탁자의 IAM 정책에 추가하여 각 특정 사용 사례에 대한 IAM 위탁자가 계정 간에 KMS 키를 사용하도록 허용합니다.
5. [5단계: IAM Identity Center에서 KMS 키 구성](#) - IAM Identity Center 인스턴스에서 고객 관리형 KMS 키를 활성화하여 저장 암호화에 사용합니다.

1단계: 조직의 사용 사례 식별

고객 관리형 KMS 키를 생성하고 구성하기 전에 사용 사례를 식별하고 필요한 KMS 키 권한을 준비합니다. KMS 키 정책에 대한 자세한 내용은 [AWS KMS 개발자 안내서](#)를 참조하세요.

IAM Identity Center 서비스 API를 호출하는 IAM 위탁자에는 권한이 필요합니다. 예를 들어 위임된 관리자는 권한 세트 정책을 통해 이러한 API를 사용할 수 있는 권한을 부여받을 수 있습니다. IAM Identity Center가 고객 관리형 키로 구성된 경우 IAM 위탁자는 IAM Identity Center 서비스 API를 통해 KMS API를 사용할 수 있는 권한도 있어야 합니다. KMS 키 정책과 IAM 위탁자와 연결된 IAM 정책의 두 위치에서 이러한 KMS API 권한을 정의합니다.

KMS 키 권한은 다음으로 구성됩니다.

1. [3단계: 고객 관리형 키 만들기](#)에서 생성하는 동안 KMS 키에 지정하는 KMS 키 정책 설명.
2. KMS 키를 생성한 후 [4단계: KMS 키의 교차 계정 사용을 위한 IAM 정책 구성](#)에서 지정하는 IAM 위탁자에 대한 IAM 정책 설명.

다음 표에서는 KMS 키를 사용할 수 있는 권한이 필요한 관련 사용 사례 및 IAM 위탁자를 지정합니다.

사용 사례:	KMS 키를 사용할 수 있는 권한이 필요한 IAM 위탁자	필수/선택
AWS IAM Identity Center 사용	- AWS IAM Identity Center 관리자 - IAM Identity Center 서비스 및 관련 Identity Store 서비스	필수
IAM Identity Center에서 AWS 관리형 애플리케이션 사용	- AWS 관리형 애플리케이션 관리자 - AWS 관리형 애플리케이션	선택 사항

사용 사례:	KMS 키를 사용할 수 있는 권한이 필요한 IAM 위탁자	필수/선택
	AWS 관리형 애플리케이션이 IAM Identity Center 서비스 APIs를 호출하기 위해 수입하는 서비스 역할	
활성화된 AWS IAM Identity Center 인스턴스 AWS Control Tower 에서 사용	AWS Control Tower 관리자	선택 사항
AWS IAM Identity Center를 사용하여 Amazon EC2 인스턴스로 SSO	Amazon EC2 인스턴스에 대한 SSO를 수행할 권한이 있는 IAM 보안 주체	선택 사항
고객 관리형 애플리케이션, 권한 세트 프로비저닝 워크플로 또는 AWS Lambda 함수와 같은 IAM 위탁자를 통해 IAM Identity Center 서비스 API를 호출하는 기타 사용 사례	이러한 워크플로에서 IAM Identity Center 서비스 API를 호출하는 데 사용되는 IAM 위탁자	선택 사항

Note

테이블에 나열된 여러 IAM 보안 주체에는 AWS KMS API 권한이 필요합니다. 그러나 IAM Identity Center에서 사용자 및 그룹 데이터를 보호하기 위해 IAM Identity Center 및 Identity Store 서비스만 AWS KMS API를 직접 호출합니다.

2단계: KMS 키 정책 설명 준비

조직과 관련된 사용 사례를 식별한 후 해당 KMS 키 정책 설명을 준비할 수 있습니다.

- 조직의 사용 사례와 일치하는 KMS 키 정책 설명을 선택합니다. 기존 정책 템플릿으로 시작합니다. 보안 요구 사항에 따라 더 구체적인 정책이 필요한 경우 [고급 KMS 키 정책 설명](#)의 예제를 사용하여 정책 설명을 수정할 수 있습니다. 이 결정에 대한 지침은 [기존 및 고급 KMS 키 정책 설명 선택 시 고려 사항](#) 섹션을 참조하세요. 또한 [기존 KMS 키 및 IAM 정책 설명](#)의 각 기존 섹션에는 관련 고려 사항이 포함되어 있습니다.

2. 관련 정책을 편집기에 복사하고 KMS 키 정책 설명에 필요한 식별자와 IAM 위탁자 이름을 삽입합니다. 참조된 식별자의 값을 찾는 데 도움이 필요하면 [필요한 식별자를 찾을 수 있는 위치](#) 섹션을 참조하세요.

다음은 각 사용 사례에 대한 기존 정책 템플릿입니다. KMS 키를 사용하려면 AWS IAM Identity Center에 대한 첫 번째 권한 세트만 필요합니다. 사용 사례별 추가 정보는 해당 하위 섹션을 검토하는 것이 좋습니다.

- [IAM Identity Center 사용에 대한 기존 KMS 키 정책 설명\(필수\)](#)
- [AWS 관리형 애플리케이션 사용을 위한 기존 KMS 키 및 IAM 정책 설명](#)
- [사용을 위한 기존 KMS 키 문 AWS Control Tower](#)
- [IAM Identity Center를 Amazon EC2 인스턴스에 사용하기 위한 기존 KMS 키 및 IAM 정책 설명](#)
- [IAM Identity Center에서 사용자 지정 워크플로를 사용하기 위한 기존 KMS 키 및 IAM 정책 설명](#)

Important

IAM Identity Center에서 이미 사용 중인 키에 대한 KMS 키 정책을 수정할 때는 주의해야 합니다. IAM Identity Center는 KMS 키를 처음 구성할 때 암호화 및 복호화 권한을 검증하지만 후속 정책 변경을 확인할 수 없습니다. 필요한 권한을 실수로 제거하면 IAM Identity Center의 정상 작동이 중단될 수 있습니다. IAM Identity Center의 고객 관리형 키와 관련된 일반적인 오류를 해결하는 지침은 [에서 고객 관리형 키 문제 해결 AWS IAM Identity Center](#) 섹션을 참조하세요.

Note

IAM Identity Center 및 연관된 Identity Store에서 고객 관리형 KMS 키를 사용하려면 서비스 수준 권한이 필요합니다. 이 요구 사항은 서비스 자격 증명을 사용하여 IAM Identity Center 서비스 APIs를 호출하는 AWS 관리형 애플리케이션으로 확장됩니다. IAM Identity Center 서비스 API가 [전달 액세스 세션](#)과 함께 호출되는 다른 사용 사례의 경우, 시작하는 IAM 위탁자(예: 관리자)만 KMS 키 권한이 필요합니다. 특히 AWS 액세스 포털 및 AWS 관리형 애플리케이션을 사용하는 최종 사용자는 각 서비스를 통해 부여되므로 직접 KMS 키 권한이 필요하지 않습니다.

3단계: 고객 관리형 키 만들기

AWS Management Console 또는 KMS API를 사용하여 고객 관리형 AWS 키를 생성할 수 있습니다. APIs 키를 생성하는 동안 2단계에서 준비한 KMS 키 정책 설명을 KMS 키 정책에 추가합니다. 기본 KMS 키 정책에 대한 지침을 포함한 자세한 지침은 [AWS Key Management Service 개발자 안내서](#)를 참조하세요.

키는 다음 요구 사항을 충족해야 합니다.

- KMS 키는 IAM Identity Center 인스턴스와 동일한 AWS 리전에 있어야 합니다.
- 단일 리전 또는 다중 리전 키 중에서 선택할 수 있습니다. 그러나 여러 AWS 리전 에서 IAM Identity Center를 사용하려는 경우 다중 리전 KMS 키를 생성해야 합니다. 단일 리전 KMS 키를 다중 리전 KMS 키로 변환할 수 없으므로 단일 리전 KMS 키를 사용해야 하는 특정 요구 사항이 없는 한 다중 리전 KMS 키로 시작하는 것이 좋습니다.
- KMS 키는 "암호화 및 복호화" 사용에 대해 구성된 대칭 키여야 함
- KMS 키는 IAM Identity Center의 조직 인스턴스와 동일한 AWS Organizations 관리 계정에 있어야 합니다.

Note

IAM Identity Center를 복제하려는 리전에이 KMS 키를 복제하려는 경우 먼저이 섹션의 설정을 완료한 다음의 지침을 따르는 것이 좋습니다. [the section called “IAM Identity Center를 추가 리전에 복제”](#)

4단계: KMS 키의 교차 계정 사용을 위한 IAM 정책 구성

IAM Identity Center 위임된 관리자와 같이 다른 AWS 계정의 IAM Identity Center 서비스 APIs를 사용하는 모든 IAM 보안 주체에는 이러한 APIs를 통해 KMS 키를 사용할 수 있도록 허용하는 IAM 정책 설명도 필요합니다.

1단계에서 식별된 각 사용 사례의 경우:

1. 기존 KMS 키 및 IAM 정책 설명에서 관련 IAM 정책 설명 템플릿을 찾습니다.
2. 템플릿을 편집기에 복사하고 3단계에서 KMS 키를 생성한 후 사용할 수 있는 키 ARN을 입력합니다. 키 ARN을 찾는 방법에 대한 도움말은 [필요한 식별자를 찾을 수 있는 위치](#) 섹션을 참조하세요.
3. 에서 사용 사례와 연결된 IAM 보안 주체의 IAM 정책을 AWS Management Console찾습니다. 이 정책의 위치는 사용 사례와 액세스 권한 부여 방법에 따라 달라집니다.

- IAM에서 직접 부여된 액세스의 경우 IAM 콘솔에서 IAM 역할과 같은 IAM 위탁자를 찾을 수 있습니다.
- IAM Identity Center를 통해 부여된 액세스의 경우 IAM Identity Center 콘솔에서 관련 권한 세트를 찾을 수 있습니다.

4. 사용 사례별 IAM 정책 설명을 IAM 역할에 추가하고 변경 사항을 저장합니다.

Note

여기에 설명된 IAM 정책은 자격 증명 기반 정책입니다. 이러한 정책은 IAM 사용자, 그룹 및 역할에 연결할 수 있지만 가능하면 IAM 역할을 사용하는 것이 좋습니다. IAM 역할 및 IAM 사용자에 대한 자세한 내용은 IAM 사용 설명서를 참조하세요.

일부 AWS 관리형 애플리케이션의 추가 구성

일부 AWS 관리형 애플리케이션은 애플리케이션이 IAM Identity Center 서비스 APIs. 조직에서 IAM Identity Center와 함께 AWS 관리형 애플리케이션을 사용하는 경우 배포된 각 애플리케이션에 대해 다음 단계를 완료합니다.

1. IAM Identity Center에서 애플리케이션을 사용하기 위한 KMS 키 관련 권한을 포함하도록 권한이 업데이트되었는지 확인하려면 애플리케이션의 사용 설명서를 참조하세요.
2. 그런 경우 애플리케이션 사용 설명서의 지침에 따라 권한을 업데이트하여 애플리케이션 작업이 중단되지 않도록 합니다.

Note

AWS 관리형 애플리케이션이 이러한 권한을 사용하는지 확실하지 않은 경우 배포된 모든 AWS 관리형 애플리케이션의 사용 설명서를 확인하는 것이 좋습니다. 이 구성은 구성이 필요한 각 애플리케이션에 대해 한 번만 수행하면 됩니다.

5단계: IAM Identity Center에서 KMS 키 구성

Important

이 단계를 진행하기 전에:

- AWS 관리형 애플리케이션이 고객 관리형 KMS 키와 호환되는지 확인합니다. 호환되는 애플리케이션 목록은 [IAM Identity Center와 함께 사용할 수 있는 AWS 관리형 애플리케이션](#)을 참조하세요. 호환되지 않는 애플리케이션이 있는 경우 진행하지 마세요.
- KMS 키 사용에 필요한 권한을 구성합니다. 적절한 권한이 없으면 이 단계가 실패하거나 IAM Identity Center 관리, AWS 관리형 애플리케이션 사용 및 KMS 키 권한이 필요한 기타 사용 사례를 방해할 수 있습니다. 자세한 내용은 [1단계: 조직의 사용 사례 식별](#) 단원을 참조하십시오.
- IAM 역할을 가진 IAM Identity Center 서비스 APIs 호출하는 AWS 관리형 애플리케이션 및 고객 관리형 애플리케이션에 대한 권한도 IAM Identity Center 서비스 APIs를 통해 KMS 키를 사용할 수 있도록 허용하는지 확인합니다. 일부 AWS 관리형 애플리케이션은 이러한 APIs. 배포된 각 AWS 관리형 애플리케이션의 사용 설명서를 참조하여 특정 KMS 키 권한을 추가해야 하는지 확인합니다.

IAM Identity Center의 새 조직 인스턴스를 활성화할 때 KMS 키 지정

IAM Identity Center의 새 조직 인스턴스를 활성화할 때 설정 중에 고객 관리형 KMS 키를 지정할 수 있습니다. 이를 통해 인스턴스가 처음부터 저장 암호화에 키를 사용할 수 있습니다. 시작하기 전에 [고객 관리형 KMS 키 및 고급 KMS 키 정책에 대한 고려 사항](#) 섹션을 참조하세요.

1. IAM Identity Center 활성화 페이지에서 저장 암호화 섹션을 확장합니다.
2. Manage Encryption(암호화 관리)을 선택합니다.
3. 고객 관리형 키를 선택합니다.
4. KMS 키에 대해 다음 중 하나를 수행합니다.
 - a. KMS 키에서 선택을 선택하고 드롭다운 목록에서 생성한 키를 선택합니다.
 - b. KMS 키 ARN 입력을 선택하고 키의 전체 ARN을 입력합니다.
5. 저장을 선택합니다.
6. 활성화를 선택하여 설정을 완료합니다.

자세한 내용은 [IAM Identity Center 활성화](#)를 참조하세요.

IAM Identity Center의 기존 조직 인스턴스에 대한 키 구성 변경

언제든지 고객 관리형 KMS 키를 다른 키로 변경하거나 AWS 소유 키로 전환할 수 있습니다.

Console

KMS 키 구성 변경

1. <https://console.aws.amazon.com/singlesignon/> IAM Identity Center 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 추가 설정 탭으로 이동합니다.
4. 암호화 관리를 선택합니다.
5. 다음 중 하나를 선택합니다.
 - a. 고객 관리형 키 - 드롭다운에서 다른 고객 관리형 키를 선택하거나 새 키 ARN을 입력합니다.
 - b. AWS 소유 키 - 기본 암호화 옵션으로 전환합니다.
6. 저장을 선택합니다.

AWS CLI

KMS 고객 관리형 키를 사용하도록 IAM Identity Center의 기존 조직 인스턴스 변경

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration \  
    KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-  
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

AWS 소유 키를 사용하도록 IAM Identity Center의 기존 조직 인스턴스 변경

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

고객 관리형 주요 고려 사항

- IAM Identity Center 작업에 대한 KMS 키 구성을 업데이트해도 IAM Identity Center의 활성 사용자 세션에는 영향을 미치지 않습니다. 이 프로세스 중에 AWS 액세스 포털, IAM Identity Center 콘솔 및 IAM Identity Center 서비스 APIs를 계속 사용할 수 있습니다.

- 새 KMS 키로 전환할 때 IAM Identity Center는 암호화 및 복호화에 키를 성공적으로 사용할 수 있는지 확인합니다. 키 정책 또는 IAM 정책을 설정하는 동안 실수를 한 경우 콘솔에 설명 오류 메시지가 표시되고 이전 KMS 키는 계속 사용됩니다.
- 기본 연간 KMS 키 교체는 자동으로 수행됩니다. [키 교체](#), [AWS KMS 키 모니터링](#), [키 삭제에 대한 액세스 제어](#) 등의 주제에 대한 자세한 내용은 [AWS KMS 개발자 안내서](#)를 참조하세요.

⚠ Important

잘못된 KMS 키 정책으로 인해 IAM Identity Center 인스턴스에서 사용 중인 고객 관리형 KMS 키가 삭제, 비활성화 또는 액세스할 수 없는 경우 인력 사용자와 IAM Identity Center 관리자는 IAM Identity Center를 사용할 수 없습니다. 액세스 손실은 상황에 따라 일시적(키 정책을 수정할 수 있음)이거나 영구적(삭제된 키를 복원할 수 없음)일 수 있습니다. KMS 키 삭제 또는 비활성화와 같은 중요한 작업에 대한 [액세스를 제한](#)하는 것이 좋습니다. 또한 IAM Identity Center에 [AWS 액세스할 수 없는 경우 권한이 있는 사용자가 액세스할 수 있도록 조직에서 휴지통 액세스 절차를](#) 설정하는 것이 좋습니다. AWS

필요한 식별자를 찾을 수 있는 위치

고객 관리형 KMS 키에 대한 권한을 구성할 때 키 정책 및 IAM 정책 설명 템플릿을 완료하려면 특정 AWS 리소스 식별자가 필요합니다. KMS 키 정책 설명에 필수 식별자(예: 조직 ID) 및 IAM 위탁자 이름을 삽입합니다.

다음은 AWS 관리 콘솔에서 이러한 식별자를 찾기 위한 가이드입니다.

IAM Identity Center Amazon 리소스 이름(ARN) 및 Identity Store ARN

IAM Identity Center 인스턴스는 `arn:aws:sso:::instance/ssoins-1234567890abcdef`와 같은 고유한 ARN이 있는 AWS 리소스입니다. ARN은 서비스 승인 참조의 IAM Identity Center 리소스 유형 섹션에 설명된 패턴을 따릅니다.

모든 IAM Identity Center 인스턴스에는 사용자 및 그룹 자격 증명을 저장하는 연관된 Identity Store가 있습니다. Identity Store에는 Identity Store ID(예: `d-123456789a`)라는 고유 식별자가 있습니다. ARN은 [서비스 승인 참조](#)의 Identity Store 리소스 유형 섹션에 설명된 패턴을 따릅니다.

IAM Identity Center의 설정 페이지에서 ARN 및 Identity Store ID 값을 모두 찾을 수 있습니다. Identity Store ID는 자격 증명 소스 탭에 있습니다.

AWS Organizations ID

키 정책에서 조직 ID(예: o-exampleorg1)를 지정하려면 IAM Identity Center 및 Organizations 콘솔의 설정 페이지에서 해당 값을 찾을 수 있습니다. ARN은 서비스 승인 참조의 조직 리소스 유형 섹션에 설명된 패턴을 따릅니다.

KMS 키 ARN

AWS KMS 콘솔에서 KMS 키의 ARN을 찾을 수 있습니다. 왼쪽에서 고객 관리형 키를 선택하고 ARN을 조회하려는 키를 클릭하면 일반 구성 섹션에 표시됩니다. ARN은 서비스 승인 참조의 AWS KMS 리소스 유형 섹션에 설명된 패턴을 따릅니다.

의 키 정책 AWS KMS 및 문제 해결 AWS KMS 권한에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서를 참조하세요. IAM 정책 및 해당 JSON 표현에 대한 자세한 내용은 IAM 사용 설명서를 참조하세요.

기본 KMS 키 및 IAM 정책 설명

여기에 제공된 기본 KMS 키 및 자격 증명 기반 정책은 공통 요구 사항의 기반 역할을 합니다. 또한 특정 IAM Identity Center 인스턴스 또는 AWS 관리형 애플리케이션에서만 KMS 키에 액세스할 수 있는지 확인하는 등 보다 세분화된 액세스 제어를 제공하는 [고급 KMS 키 정책 설명](#)을 검토하는 것이 좋습니다. 고급 KMS 키 정책 설명을 사용하기 전에 [기본 및 고급 KMS 키 정책 설명 선택 시 고려 사항](#) 섹션을 검토합니다.

다음 섹션에서는 각 사용 사례에 대한 기본 정책 설명을 제공합니다. 사용 사례에 맞는 섹션을 확장하고 KMS 키 정책 설명을 복사합니다. 그런 다음 로 돌아갑니다 [2단계: KMS 키 정책 설명 준비](#).

IAM Identity Center 사용에 대한 기본 KMS 키 정책 설명(필수)

[2단계: KMS 키 정책 설명 준비](#)에서 다음 KMS 키 정책 설명 템플릿을 사용하여 IAM Identity Center, 연관된 Identity Store 및 IAM Identity Center 관리자가 KMS 키를 사용하도록 허용합니다.

- 관리자 정책 설명의 보안 주체 요소에서 "arn:aws:iam::111122223333:root" 형식을 사용하여 AWS 조직 관리 계정 및 위임된 관리 계정인 IAM Identity Center 관리 계정의 계정 보안 주체를 지정합니다 AWS .
- PrincipalArn 요소에서 예제 ARN을 IAM Identity Center 관리자의 IAM 역할로 바꿉니다.

다음 중 하나를 지정할 수 있습니다.

- 특정 IAM 역할 ARN:

```
"arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_12345678"
```

- 와일드카드 패턴(권장):

```
"arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_*
```

Identity Center는 다시 생성된 권한 세트에 대한 새 고유 식별자를 생성하므로 와일드카드(*)를 사용하면 권한 세트를 삭제하고 다시 생성할 때 액세스 손실을 방지할 수 있습니다. 구현 예제는 섹션을 참조 [사용자 지정 신뢰 정책 예](#)하세요.

- SourceAccount 요소에서 IAM Identity Center 계정 ID를 지정합니다.
- Identity Store에는 KMS 키를 사용할 수 있어야 하는 자체 서비스 위탁자 `identitystore.amazonaws.com`이 있습니다.
- 이러한 정책 설명을 통해 특정 AWS 계정의 IAM Identity Center 인스턴스가 KMS 키를 사용할 수 있습니다. 특정 IAM Identity Center 인스턴스에 대한 액세스를 제한하려면 [고급 KMS 키 정책 설명](#) 섹션을 참조하세요. 각 AWS 계정에 대해 IAM Identity Center 인스턴스를 하나만 가질 수 있습니다.

KMS 키 정책 설명

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",

```

```

        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
    ],
    },
    "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
    }
},
{
    "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
                "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
            ]
        }
    },
    "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    }
},
{
    "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
    "Effect": "Allow",
    "Principal": {

```

```

    "AWS": [
      "arn:aws:iam::111122223333:root",
      "arn:aws:iam::444455556666:root"
    ],
    "Action": "kms:DescribeKey",
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",
          "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*"
        ]
      }
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
      "Service": "sso.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  },
  {
    "Sid": "AllowIdentityStoreToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {

```

```

    "Service": "identitystore.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
},
{
  "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "identitystore.amazonaws.com",
      "sso.amazonaws.com"
    ]
  },
  "Action": "kms:DescribeKey",
  "Resource": "*"
}
]
}

```

[the section called “4단계: IAM 정책 구성”](#)에서 다음 IAM 정책 설명 템플릿을 사용하여 IAM Identity Center 관리자가 KMS 키를 사용하도록 허용합니다.

- Resource 요소의 예제 키 ARN을 실제 KMS 키 ARN으로 바꿉니다. 참조된 식별자의 값을 찾는 데 도움이 필요하면 [필요한 식별자를 찾을 수 있는 위치](#) 섹션을 참조하세요.
- 이러한 IAM 정책 문은 KMS 키에 IAM 보안 주체에 대한 액세스 권한을 부여하지만 어떤 AWS 서비스가 요청할 수 있는지는 제한하지 않습니다. KMS 키 정책은 일반적으로 이러한 서비스 제한을 제공합니다. 그러나 이 IAM 정책에 암호화 컨텍스트를 추가하여 특정 Identity Center 인스턴스로 사용을 제한할 수 있습니다. 자세한 내용은 [고급 KMS 키 정책 설명](#) 섹션을 참조하세요.

IAM Identity Center의 위임된 관리자에게 필요한 IAM 정책 설명

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToUseKMSkey",
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  {
    "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToListKeyAliases",
    "Effect": "Allow",
    "Action": "kms:ListAliases",
    "Resource": "*"
  }
]
}
```

AWS 관리형 애플리케이션 사용을 위한 기존 KMS 키 및 IAM 정책 설명

 Note

일부 AWS 관리형 애플리케이션은 고객 관리형 KMS 키로 구성된 IAM Identity Center와 함께 사용할 수 없습니다. 자세한 내용은 [IAM Identity Center에서 작동하는AWS 관리형 애플리케이션](#)을 참조하세요.

에서 다음 KMS 키 정책 설명 템플릿을 사용하여 AWS 관리형 애플리케이션과 관리자가 모두 KMS 키를 사용하도록 [2단계: KMS 키 정책 설명 준비](#) 허용합니다.

- PrincipalOrgId 및 SourceOrgId 조건에 AWS Organizations ID를 삽입합니다. 참조된 식별자의 값을 찾는 데 도움이 필요하면 [필요한 식별자를 찾을 수 있는 위치](#) 섹션을 참조하세요.
- 이러한 정책 설명을 통해 AWS 조직의 모든 AWS 관리형 애플리케이션과 모든 IAM 보안 주체(애플리케이션 관리자)는 IAM Identity Center 및 Identity Store를 사용하여 kms:Decrypt를 사용할 수 있습니다.

니다. 이러한 정책 설명을 특정 AWS 관리형 애플리케이션, 계정 또는 IAM Identity Center 인스턴스로 제한하려면 [고급 KMS 키 정책 설명](#) 섹션을 참조하세요.

*를 특정 IAM 위탁자로 대체하여 특정 애플리케이션 관리자에 대한 액세스를 제한할 수 있습니다. 권한 세트를 다시 생성할 때 IAM 역할 이름 변경을 방지하려면 [사용자 지정 신뢰 정책 예](#)의 접근 방식을 사용합니다. 자세한 내용은 [기본 및 고급 KMS 키 정책 설명 선택 시 고려 사항](#) 단원을 참조하십시오.

KMS 키 정책 설명

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-a1b2c3d4e5"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-a1b2c3d4e5"
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  }
]
}

```

[4단계: KMS 키의 교차 계정 사용을 위한 IAM 정책 구성](#)에서 다음 IAM 정책 설명 템플릿을 사용하여 AWS 관리형 애플리케이션의 관리자가 멤버 계정의 KMS 키를 사용하도록 허용합니다.

- 리소스 요소의 예제 ARN을 실제 KMS 키 ARN으로 바꿉니다. 참조된 식별자의 값을 찾는 데 도움이 필요하면 [필요한 식별자를 찾을 수 있는 위치](#) 섹션을 참조하세요.
- 일부 AWS 관리형 애플리케이션은 IAM Identity Center 서비스 APIs. IAM Identity Center에서 고객 관리형 키를 구성하기 전에 이러한 권한이 KMS 키 사용도 허용하는지 확인합니다. 특정 KMS 키 권한 요구 사항은 배포한 각 AWS 관리형 애플리케이션에 대한 설명서를 참조하세요.

AWS 관리형 애플리케이션의 관리자에게 필요한 IAM 정책 설명:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid":
    "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

사용을 위한 기준 KMS 키 문 AWS Control Tower

에서 다음 KMS 키 문 템플릿을 사용하여 AWS Control Tower 관리자가 KMS 키를 사용하도록 [2단계: KMS 키 정책 설명 준비](#) 허용합니다.

- 위탁자 요소에서 IAM Identity Center 서비스 API에 액세스하는 데 사용되는 IAM 위탁자를 지정합니다. IAM 위탁자에 대한 자세한 내용은 IAM 사용 설명서의 [위탁자 지정](#)을 참조하세요.
- 이러한 정책 설명을 통해 AWS Control Tower 관리자는 모든 IAM Identity Center 인스턴스를 통해 KMS 키를 사용할 수 있습니다. 그러나 AWS Control Tower는 동일한 조직에 있는 IAM Identity

Center의 AWS 조직 인스턴스에 대한 액세스를 제한합니다. 이러한 제한으로 인해 [고급 KMS 키 정책 설명](#)에 설명된 대로 KMS 키를 특정 IAM Identity Center 인스턴스로 추가로 제한하면 실질적인 이점이 없습니다.

- 권한 세트를 다시 생성할 때 IAM 역할 이름 변경을 방지하려면 [사용자 지정 신뢰 정책 예](#)에 설명된 접근 방식을 사용합니다.

KMS 키 정책 문:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerAdmin"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerAdmin"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}
```

}

AWS Control Tower 는 위임된 관리를 지원하지 않으므로 관리자를 위해 IAM 정책을 구성할 필요가 없습니다.

⚠ Important

앞의 정책 문은가 AWSControlTowerAdmin 역할을 AWS Control Tower 수임하는 계정의 자동 등록과 같은 AWS Control Tower 서비스 관리형 작업을 다룹니다. 그러나 Account Factory 를 통한 계정 프로비저닝 또는 직접 AWS Control Tower APIs 호출과 같이 고객이 시작한 작업의 경우는 [전달 액세스 세션\(FAS\)](#)을 AWS Control Tower 사용하고 고객의 자체 IAM 역할로 작동합니다. 즉, 이러한 작업을 시작하는 데 사용하는 IAM 역할에는 고객 관리형 KMS 키에 대한 kms:Decrypt 권한도 필요합니다.

위의 문과 함께 다음 KMS 키 정책 AWSControlTowerAdmin 문을 추가

합니다. *MyControlTowerRole*을 IAM Identity Center 권한 세트 역할(예:

AWSReservedSSO_*PermissionSetName*_*), 자동화를 위한 사용자 지정 IAM 역할 또는 AWS Control Tower 또는 AWS Service Catalog API를 호출하는 데 사용되는 기타 역할과 AWS Control Tower같이 상호 작용하는 데 사용하는 IAM 역할의 ARN으로 바꿉니다. APIs

고객 시작 AWS Control Tower 작업에 대한 KMS 키 정책 설명:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomerRoleToUseTheKMSKeyViaIdentityCenterForControlTower",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyControlTowerRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    }
  ],
}
```

```
{
  "Sid": "AllowCustomerRoleToUseTheKMSKeyViaIdentityStoreForControlTower",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/MyControlTowerRole"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "identitystore.*.amazonaws.com",
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    }
  }
}
```

IAM Identity Center를 Amazon EC2 인스턴스에 사용하기 위한 기존 KMS 키 및 IAM 정책 설명

에서 다음 KMS 키 정책 설명 템플릿을 사용하여 Amazon EC2 인스턴스에 대한 Single Sign-On(SSO) 사용자가 계정 간에 KMS 키를 사용할 수 [2단계: KMS 키 정책 설명 준비](#) 있도록 허용합니다.

- 위탁자 필드에서 IAM Identity Center에 액세스하는 데 사용되는 IAM 위탁자를 지정합니다. IAM 위탁자에 대한 자세한 내용은 IAM 사용 설명서의 [위탁자 지정](#)을 참조하세요.
- 이 정책 문은 모든 IAM Identity Center 인스턴스가 KMS 키를 사용하도록 허용합니다. 특정 IAM Identity Center 인스턴스에 대한 액세스를 제한하려면 [고급 KMS 키 정책 설명](#) 섹션을 참조하세요.
- 권한 세트를 다시 생성할 때 IAM 역할 이름 변경으로부터 보호하려면 사용자 지정 신뢰 정책 예제에 설명된 접근 방식을 사용합니다.

KMS 키 정책 설명

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
      }
    }
  ]
}
```

```

    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
]
}

```

에서 다음 IAM 정책 설명 템플릿을 사용하여 EC2 인스턴스에 대한 SSO가 KMS 키를 사용하도록 [4단계: KMS 키의 교차 계정 사용을 위한 IAM 정책 구성](#) 허용합니다.

Amazon EC2 인스턴스에 대한 SSO 액세스를 허용하는 데 사용하는 IAM Identity Center의 기존 권한 세트에 IAM 정책 설명을 연결합니다. IAM 정책 예제는 AWS Systems Manager 사용 설명서의 [원격 데스크톱 프로토콜 연결](#)을 참조하세요.

- 리소스 요소의 예제 ARN을 실제 KMS 키 ARN으로 바꿉니다. 참조된 식별자의 값을 찾는 데 도움이 필요하면 [필요한 식별자를 찾을 수 있는 위치](#) 섹션을 참조하세요.

권한 세트 IAM 정책:


```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "IAMPolicyToAllowKMSKeyUseViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

IAM Identity Center에서 사용자 지정 워크플로를 사용하기 위한 기준 KMS 키 및 IAM 정책 설명

에서 다음 KMS 키 정책 설명 템플릿을 사용하여 AWS Organizations 관리 계정 또는 위임된 관리 계정의 고객 관리형 애플리케이션과 같은 사용자 지정 워크플로가 KMS 키를 사용하도록 [2단계: KMS 키 정책 설명 준비](#) 허용합니다. 고객 관리형 애플리케이션에 대한 SAML 페더레이션에는 KMS 키 권한이 필요하지 않습니다.

- 위탁자 요소에서 IAM Identity Center 서비스 API에 액세스하는 데 사용되는 IAM 위탁자를 지정합니다. IAM 위탁자에 대한 자세한 내용은 IAM 사용 설명서의 [위탁자 지정](#)을 참조하세요.
- 이러한 정책 설명을 사용하여 워크플로는 IAM Identity Center 인스턴스를 통해 KMS 키를 사용할 수 있습니다. 특정 IAM Identity Center 인스턴스에 대한 액세스를 제한하려면 [고급 KMS 키 정책 설명](#) 섹션을 참조하세요.
- 권한 세트를 다시 생성할 때 IAM 역할 이름 변경으로부터 보호하려면 [사용자 지정 신뢰 정책 예](#)에 설명된 접근 방식을 사용합니다.

KMS 키 정책 문:

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

```

    "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
]
}

```

4단계: KMS 키의 교차 계정 사용을 위한 IAM 정책 구성에서 다음 IAM 정책 설명 템플릿을 사용하여 사용자 지정 워크플로와 연관된 IAM 위탁자가 계정 간에 KMS 키를 사용하도록 허용합니다. IAM 위탁자에 IAM 정책 설명을 추가합니다.

- 리소스 요소의 예제 ARN을 실제 KMS 키 ARN으로 바꿉니다. 참조된 식별자의 값을 찾는 데 도움이 필요하면 [필요한 식별자를 찾을 수 있는 위치](#) 섹션을 참조하세요.

IAM 정책 설명(교차 계정 사용에만 필요):

```
{
```

```

"Version": "2012-10-17",
"Statement": [{
  "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
  "Effect": "Allow",
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "Condition": {
    "StringLike": {
      "kms:ViaService": [
        "sso.*.amazonaws.com",
        "identitystore.*.amazonaws.com"
      ]
    }
  }
}]
}

```

일반적인 사용 사례에 대한 KMS 키 정책 설명의 예

위임된 관리자 및 AWS 관리형 애플리케이션이 있는 IAM Identity Center

이 섹션에는 위임된 관리자 및 AWS 관리형 애플리케이션이 있는 IAM Identity Center 인스턴스에 사용할 수 있는 예제 KMS 키 정책 설명이 포함되어 있습니다.

Important

KMS 키 정책 문은 IAM Identity Center 인스턴스가 KMS 키 권한이 필요한 다른 사용 사례에 사용되지 않는다고 가정합니다. 확인을 위해 모든 [사용 사례를](#) 검토할 수 있습니다. 또한 관리형 애플리케이션에 추가 구성이 필요한지 확인하려면 섹션을 참조하세요 AWS . [the section called “일부 AWS 관리형 애플리케이션의 추가 구성”](#)

테이블 아래에 KMS 키 정책 설명을 복사하여 KMS 키 정책에 추가합니다. 이 예제에서는 다음 예제 값을 사용합니다.

- 111122223333 - IAM Identity Center 인스턴스의 계정 ID
- 444455556666 - 위임된 관리 계정 ID
- o-a1b2c3d4e5 - AWS 조직 ID

- `arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*` - 권한 세트 `###`에서 프로비저닝된 IAM Identity Center 관리자의 IAM 역할의 와일드카드 패턴입니다. 이러한 역할에는 기본 리전(이 예제에서는 us-east-1)의 리전 코드가 포함됩니다.
- `arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*` - 권한 세트 `DelegatedAdmin`에서 프로비저닝된 IAM Identity Center 위임된 관리자의 IAM 역할의 와일드카드 패턴입니다. 이러한 역할에는 기본 리전(이 예제에서는 us-east-1)의 리전 코드가 포함됩니다.

권한 세트에서 IAM 역할이 생성되지 않은 경우 IAM 역할은와 같은 일반 역할처럼 보입니다 `arn:aws:iam::111122223333:role/idcadmin`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",
            "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*"
          ]
        }
      },
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",

```

```

        "kms:EncryptionContext:aws:sso:instance-arn": "*"
    }
},
{
    "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",
                "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*"
            ]
        }
    },
    "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    }
},
{
    "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root"
        ]
    },
    "Action": "kms:DescribeKey",

```

```

    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
          "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
        ]
      }
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
      "Service": "sso.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  },
  {
    "Sid": "AllowIdentityStoreToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
      "Service": "identitystore.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom",

```

```

    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
},
{
  "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "identitystore.amazonaws.com",
      "sso.amazonaws.com"
    ]
  },
  "Action": "kms:DescribeKey",
  "Resource": "*"
},

{
  "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalOrgID": "o-a1b2c3d4e5"
    },
    "StringLike": {
      "kms:ViaService": "sso.*.amazonaws.com",
      "kms:EncryptionContext:aws:sso:instance-arn": "*"
    }
  }
},
{
  "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",
  "Effect": "Allow",

```

```

    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      },
      "Bool": {

```



```

    "aws:PrincipalIsAWSService": "true"
  },
  "StringEquals": {
    "aws:SourceOrgID": "o-a1b2c3d4e5"
  }
}
]
}

```

고급 KMS 키 정책 설명

고급 KMS 키 정책 설명을 사용하여 고객 관리형 KMS 키에 대한 보다 세분화된 액세스 제어를 구현합니다. 이러한 정책은 암호화 컨텍스트 조건 및 서비스별 제한을 추가하여 [기존 KMS 키 및 IAM 정책 설명](#) 섹션을 기반으로 합니다. 고급 KMS 키 정책 설명을 사용할지 여부를 결정하기 전에 관련 고려 사항을 검토해야 합니다.

암호화 컨텍스트를 사용하여 액세스 제한

키 정책 설명에 암호화 컨텍스트 조건을 지정하여 KMS 키 사용을 특정 IAM Identity Center 인스턴스로 제한할 수 있습니다. 기존 키 정책 설명에는 일반 값과 함께 이 컨텍스트가 이미 포함되어 있습니다. 키가 의도한 인스턴스에서만 작동하도록 “*” 와일드카드를 특정 Identity Center 인스턴스 ARN 및 Identity Store ARN으로 바꿉니다. KMS 키의 교차 계정 사용을 위해 구성된 IAM 정책에 동일한 암호화 컨텍스트 조건을 추가할 수도 있습니다.

자격 증명 센터

```

"StringEquals": {
  "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
}

```

아이덴티티 스토어

```

"StringEquals": {
  "kms:EncryptionContext:aws:identitystore:identitystore-arn":
  "arn:aws:identitystore:::111122223333:identitystore/d-1234567890"
}

```

이러한 식별자를 찾는 데 도움이 필요한 경우 [필요한 식별자를 찾을 수 있는 위치](#) 섹션을 참조하세요.

Note

IAM Identity Center의 조직 인스턴스에서만 고객 관리형 KMS 키를 사용할 수 있습니다. 고객 관리형 키는 AWS 조직의 관리 계정에 있어야 합니다. 이렇게 하면 키를 단일 IAM Identity Center 인스턴스와 함께 사용할 수 있습니다. 그러나 암호화 컨텍스트 메커니즘은 단일 인스턴스 사용에 대한 독립적인 기술적 보호 기능을 제공합니다. Identity Center 및 Identity Store 서비스 위탁자를 위한 KMS 키 정책 설명에서 `aws:SourceArn` 조건 키를 사용할 수도 있습니다.

암호화 컨텍스트 조건 구현 시 고려 사항

암호화 컨텍스트 조건을 구현하기 전에 다음 요구 사항을 검토합니다.

- **DescribeKey 작업.** 암호화 컨텍스트는 IAM Identity Center 관리자가 사용할 수 있는 'kms:DescribeKey' 작업에 적용할 수 없습니다. KMS 키 정책을 구성할 때 IAM Identity Center 인스턴스의 적절한 작동을 보장하기 위해 이 특정 작업에 대한 암호화 컨텍스트를 제외합니다.
- **새 인스턴스 설정.** 고객 관리형 KMS 키를 사용하여 새 IAM Identity Center 인스턴스를 활성화하는 경우 [고객 관리형 KMS 키 및 고급 KMS 키 정책에 대한 고려 사항](#) 섹션을 참조하세요.
- **자격 증명 소스 변경.** 자격 증명 소스를 Active Directory로 변경하거나 Active Directory에서 변경할 때 암호화 컨텍스트에 특별한 주의가 필요합니다. [ID 소스 변경 시 고려 사항](#)(를) 참조하세요.

정책 템플릿

보안 요구 사항에 따라 이러한 고급 정책 템플릿 중에서 선택합니다. 세분화된 액세스 제어와 해당 제어가 도입하는 관리 오버헤드의 균형을 맞춥니다.

여기에서 다루는 주제는 다음과 같습니다.

- [특정 IAM Identity Center 인스턴스의 읽기 전용 사용에 대한 KMS 정책 설명](#). 이 섹션에서는 IAM Identity Center에 대한 읽기 전용 액세스에 암호화 컨텍스트를 사용하는 방법을 보여줍니다.
- [AWS 관리형 애플리케이션 사용을 위한 KMS 키 정책 설명 개선](#). 이 섹션에서는 애플리케이션 서비스 보안 주체, 애플리케이션 ARN 및 AWS 계정 ID와 같은 암호화 컨텍스트 및 애플리케이션 정보를 사용하여 AWS 관리형 애플리케이션에 대한 KMS 키 정책을 구체화하는 방법을 보여줍니다.

특정 IAM Identity Center 인스턴스의 읽기 전용 사용에 대한 KMS 정책 설명

이 정책은 IAM Identity Center에 대한 읽기 액세스 권한만 필요한 [보안 감사자](#) 및 기타 직원이 KMS 키를 사용하도록 허용합니다.

이 정책을 사용하려면 다음을 수행합니다.

1. 예제 읽기 전용 관리자 IAM 위탁자를 실제 관리자 IAM 위탁자로 바꾸기
2. 예제 IAM Identity Center 인스턴스 ARN을 실제 인스턴스 ARN으로 바꾸기
3. 예제 Identity Store ARN을 실제 Identity Store ARN으로 바꾸기
4. [위임된 관리를 사용하는 경우 4단계: KMS 키의 교차 계정 사용을 위한 IAM 정책 구성](#) 섹션을 참조하세요.

이러한 식별자의 값을 찾는 데 도움이 필요한 경우 [필요한 식별자를 찾을 수 있는 위치](#) 섹션을 참조하세요.

템플릿을 값으로 업데이트한 후 [2단계: KMS 키 정책 설명 준비](#) 섹션으로 돌아가 필요에 따라 추가 KMS 키 정책 설명을 준비합니다.

kms:Decrypt 작업만으로는 읽기 전용 작업에 대한 액세스를 제한하지 않습니다. IAM 정책은 IAM Identity Center 서비스 API에 대한 읽기 전용 액세스를 적용해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/ssoints-1234567890abcdef"
        }
      }
    }
  ]
}
```

```

    },
    {
      "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
            "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        }
      }
    }
  ]
}

```

AWS 관리형 애플리케이션 사용을 위한 KMS 키 정책 설명 개선

이러한 정책 템플릿은 KMS 키를 사용할 수 있는 AWS 관리형 애플리케이션을 보다 세밀하게 제어할 수 있습니다.

Note

일부 AWS 관리형 애플리케이션은 고객 관리형 KMS 키로 구성된 IAM Identity Center와 함께 사용할 수 없습니다. [IAM Identity Center와 함께 사용할 수 있는 AWS 관리형 애플리케이션](#)을 참조하세요.

는 동일한 AWS 조직의 모든 계정에서 AWS 관리형 애플리케이션이 KMS 키를 사용하도록 [AWS 관리형 애플리케이션 사용을 위한 기존 KMS 키 및 IAM 정책 설명](#) 허용합니다. 다음과 같이 세분화된 정책을 사용하여 액세스를 제한합니다.

- 애플리케이션 서비스 위탁자
- 애플리케이션 인스턴스 ARN
- AWS 계정 IDs
- 특정 IAM Identity Center 인스턴스의 암호화 컨텍스트

Note

서비스 보안 주체는 AWS 서비스의 고유 식별자로, 일반적으로 `servicename.amazonaws.com` 형식입니다(예: Amazon EMR의 경우 `elasticmapreduce.amazonaws.com`).

계정으로 제한

이 KMS 키 정책 설명 템플릿을 사용하면 특정 AWS 계정의 AWS 관리형 애플리케이션이 특정 IAM Identity Center 인스턴스를 사용하여 KMS 키를 사용할 수 있습니다.

이 정책을 사용하려면 다음을 수행합니다.

1. 예제 서비스 위탁자를 실제 애플리케이션 서비스 위탁자로 바꾸기
2. 예제 계정 ID를 AWS 관리형 애플리케이션이 배포된 실제 계정 ID로 바꾸기
3. 예제 Identity Store ARN을 실제 Identity Store ARN으로 바꾸기
4. 예제 IAM Identity Center 인스턴스 ARN을 실제 인스턴스 ARN으로 바꾸기

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "111122223333",
            "444455556666"
          ]
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
        }
      }
    }
  ]
}
```

```

    },
    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    }
  },
  {
    "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": [
          "111122223333",
          "444455556666"
        ]
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    }
  }
]
}

```

애플리케이션 인스턴스로 제한

이 KMS 키 정책 설명 템플릿을 사용하면 특정 AWS 관리형 애플리케이션 인스턴스가 특정 IAM Identity Center 인스턴스를 사용하여 KMS 키를 사용할 수 있습니다.

이 정책을 사용하려면 다음을 수행합니다.

1. 예제 서비스 위탁자를 실제 애플리케이션 서비스 위탁자로 바꾸기
2. 예제 애플리케이션 ARN을 실제 애플리케이션 인스턴스 ARN으로 바꾸기

3. 예제 Identity Store ARN을 실제 Identity Store ARN으로 바꾸기

4. 예제 IAM Identity Center 인스턴스 ARN을 실제 인스턴스 ARN으로 바꾸기

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/sssoins-1234567890abcdef"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    },
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-application"
        }
      }
    }
  ]
}
```

```

    "StringLike": {
      "kms:ViaService": "identitystore.*.amazonaws.com",
      "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    }
  }
}
]
}

```

고객 관리형 KMS 키 및 고급 KMS 키 정책에 대한 고려 사항

IAM Identity Center를 사용하여 고객 관리형 KMS 키를 구현할 때는 암호화 구성의 설정, 보안 및 지속적인 유지 관리에 영향을 미치는 해당 요소를 고려합니다.

기준 및 고급 KMS 키 정책 설명 선택 시 고려 사항

[고급 KMS 키 정책 설명](#) 섹션을 통해 KMS 키 권한을 보다 구체적으로 지정할지 여부를 결정할 때는 조직의 관리 오버헤드와 보안 요구 사항을 고려합니다. 보다 구체적인 정책 설명은 누가 어떤 목적으로 키를 사용할 수 있는지에 대한 보다 세분화된 제어를 제공합니다. 그러나 IAM Identity Center 구성이 발전함에 따라 지속적인 유지 관리가 필요합니다. 예를 들어 KMS 키 사용을 특정 AWS 관리형 애플리케이션 배포로 제한하는 경우 조직에서 애플리케이션을 배포하거나 배포 취소하려는 때마다 키 정책을 업데이트해야 합니다. 덜 제한적인 정책은 관리 부담을 줄이지만 보안 요구 사항에 필요한 권한보다 더 광범위한 권한을 부여할 수 있습니다.

고객 관리형 KMS 키를 사용하여 새 IAM Identity Center 인스턴스를 활성화하기 위한 고려 사항

여기에 있는 고려 사항은 [고급 KMS 키 정책 설명](#)에 설명된 암호화 컨텍스트를 통해 KMS 키 사용을 특정 IAM Identity Center 인스턴스로 제한하는 경우에 적용됩니다.

고객 관리형 KMS 키로 새 IAM Identity Center 인스턴스를 활성화하면 설정 후까지 IAM Identity Center 및 Identity Store ARN을 사용할 수 없습니다. 다음과 같은 옵션이 있습니다.

- 일반 ARN 패턴을 일시적으로 사용한 다음 인스턴스가 활성화된 후 전체 ARN으로 바꿉니다. 필요에 따라 StringEquals 연산자와 StringLike 연산자 간에 전환해야 합니다.
 - IAM Identity Center SPN의 경우: 'arn:\${Partition}:sso:::instance/*'.
 - Identity Store SPN의 경우: 'arn:\${Partition}:identitystore::\${Account}:identitystore/*'.

- ARN에서 'purpose:KEY_CONFIGURATION'을 일시적으로 사용합니다. 이는 인스턴스 활성화에만 적용되며 IAM Identity Center 인스턴스가 정상적으로 작동하려면 실제 ARN으로 교체해야 합니다. 이 접근 방식의 장점은 인스턴스가 활성화된 후 이를 대체하는 것을 잊지 않는다는 것입니다.
- IAM Identity Center SPN의 경우 'arn:\${Partition}:sso::instance/purpose:KEY_CONFIGURATION'을 사용합니다.
- Identity Store SPN의 경우 'arn:\${Partition}:identitystore::\${Account}:identitystore/purpose:KEY_CONFIGURATION'을 사용합니다.

 Important

기존 IAM Identity Center 인스턴스에서 이미 사용 중인 KMS 키에는 이 구성을 적용하지 마세요. 정상적인 작업이 중단될 수 있습니다.

- 인스턴스가 활성화된 후까지 KMS 키 정책에서 암호화 컨텍스트 조건을 생략합니다.

AWS IAM Identity Center 리소스 태그 지정

태그는 AWS 리소스를 쉽게 식별, 구성 및 검색할 수 있도록 리소스에 추가하는 사용자 지정 속성 레이블입니다. 각 태그는 두 부분으로 구성됩니다.

- 태그 키(예: CostCenter, Environment 또는 Project) 태그 키는 최대 128자이며 대/소문자를 구분합니다.
- 태그 값(예: 111122223333 또는 Production). 값은 최대 256자이며 태그 키와 같이 대/소문자를 구분합니다. 태그의 값을 빈 문자열로 설정할 수 있지만 태그의 값을 Null로 설정할 수는 없습니다. 태그 값을 생략하는 것은 빈 문자열을 사용하는 것과 같습니다.

태그는 AWS 리소스를 식별하고 구성하는 데 도움이 됩니다. 많은 AWS 서비스가 태그 지정을 지원하므로 서로 다른 서비스의 리소스에 동일한 태그를 할당하여 리소스가 관련이 있음을 나타낼 수 있습니다. 예를 들어 IAM Identity Center 인스턴스의 특정 권한 세트에 동일한 태그를 할당할 수 있습니다. 태그 지정 전략에 대한 자세한 내용은 AWS 일반 참조 가이드의 [AWS 리소스 태그 지정](#) 및 [태그 지정 모범 사례](#)를 참조하세요.

태그를 사용하여 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 방법에 대한 자세한 내용은 IAM 사용 설명서의 [태그를 사용하여 AWS 리소스에 대한 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.

태그는 권한 세트에만 적용할 수 있습니다. IAM Identity Center가 생성하는 해당 역할에는 태그를 적용할 수 없습니다 AWS 계정. IAM Identity Center 콘솔 AWS CLI 또는 IAM Identity Center APIs 사용하여 권한 세트에 대한 태그를 추가, 편집 또는 삭제할 수 있습니다.

다음 섹션에서는 IAM Identity Center의 태그에 대한 추가 정보를 제공합니다.

주제

- [태그 제한 사항](#)
- [IAM Identity Center 콘솔을 사용하여 태그 관리](#)
- [AWS CLI 예제](#)
- [IAM Identity Center API를 사용하여 태그 관리](#)

태그 제한 사항

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 콘솔](#)을 엽니다.
2. 권한 세트를 선택합니다.
3. 관리할 태그가 있는 권한 세트의 이름을 선택합니다.
4. 권한 탭의 태그에서 다음 중 하나를 수행한 후 다음 단계로 진행하세요.
 - 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) 옆에 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 콘솔](#)을 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

는 권한 세트에 할당하는 태그를 관리하는 데 사용할 수 있는 명령을 AWS CLI 제공합니다.

태그 할당

다음 명령을 사용하여 권한 세트에 태그를 할당합니다.

Example권한 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,Environment=Prod
```

```
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

태그 보기

다음 명령을 사용하여 권한 세트에 할당된 태그를 확인합니다.

Example권한 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.

Example권한 세트에 대한 untag-resource 명령

sso 명령 세트에서 [untag-resource](#)를 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.

Example태그가 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

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 Center의 통합은 로그인 프로세스를 간소화합니다. 개발자는 일반적으로 IAM Identity Center에 로그인하는 데 사용하는 것과 동일한 Active Directory 또는 IAM Identity Center 자격 증명을 AWS CLI 사용하여 직접 로그인하고 할당된 계정 및 역할에 액세스할 수 있습니다. 예를 들어 관리자가 인증에 Active Directory를 사용하도록 IAM Identity Center를 구성한 후 개발자는 Active Directory 자격 증명을 사용하여 AWS CLI 직접 로그인할 수 있습니다.

AWS CLI와 IAM Identity Center의 통합은 다음과 같은 이점을 제공합니다.

- 기업은 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 CLI를 IAM Identity Center와 통합하는 방법

IAM Identity Center와의 AWS CLI 통합을 사용하려면 AWS Command Line Interface 버전 2를 다운로드, 설치 및 구성합니다. 를 다운로드하고 IAM Identity Center AWS CLI 와 통합하는 방법에 대한 자세한 단계는 AWS Command Line Interface 사용 설명서 [의 IAM Identity Center를 사용하도록 AWS CLI 구성을](#) 참조하세요.

AWS Management Console 프라이빗 액세스 고려 사항

조직에서 AWS Management Console 프라이빗 액세스 기능을 사용하는 경우 사용자가 IAM Identity Center에 로그인하는 방법을 고려해야 합니다.

VPC 엔드포인트 정책은 관리 콘솔에 대한 로그인을 제한하므로 사용자가 액세스 권한이 없는데 로그인할 AWS 계정 수 없습니다. 자세한 내용은 AWS Management Console 시작하기 안내서의 [AWS Management Console 프라이빗 액세스](#) 섹션을 참조하세요.

VPC 엔드포인트 사용 시 IAM Identity Center에 대한 로그인 차단

VPC 엔드포인트를 사용하면 IAM Identity Center 로그인이 차단된다는 점에 유의해야 합니다. 이는 사용자가 VPC 엔드포인트를 통해 이미 관리 콘솔에 로그인한 경우 발생합니다. 사용자가 IAM Identity Center에 계속 로그인할 수 있도록 하려면 AWS 로그인 시 VPC 엔드포인트가 아닌 퍼블릭 엔드포인트를 사용해야 합니다.

IAM Identity Center의 할당량 및 제한

다음 표에서는 IAM Identity Center의 할당량에 대해 설명합니다. 할당량 증가 요청은 관리 또는 위임된 관리자 계정에서 이루어져야 합니다. 할당량을 늘리려면 [할당량 증가 요청](#)을 참조하세요.

Note

사용자 50,000명, 그룹 10,000개 또는 권한 세트가 500개 이상인 경우 AWS CLI 및 API를 사용하여 IAM Identity Center를 관리하는 것이 좋습니다. CLI에 대한 자세한 내용은 [AWS CLI와 IAM Identity Center 통합](#) 단원을 참조하세요. API에 대한 자세한 내용은 [IAM Identity Center API 참조 소개](#)를 참조하세요.

애플리케이션 할당량

Resource	기본 할당량	높일 수 있음
서비스 제공업체 SAML 인증서의 파일 크기(PEM 형식)	2KB	아니요
SAML 어설션 제한	50,000 자	아니요
IAM Identity Center에 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	3500	예

Resource	기본 할당량	높일 수 있음
당 허용되는 프로비저닝된 권한 세트 수 AWS 계정	500	예
권한 세트당 인라인 정책 수	1	아니요
권한 세트당 AWS 관리형 및 고객 관리형 정책 수	25 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 있는 IAM 역할(권한 세트) 수	1	아니요

¹AWS Identity and Access Management (IAM)은 역할당 관리형 정책 10개의 할당량을 설정합니다. 이 할당량을 활용하려면 권한 세트를 배포 AWS 계정 하려는 각에 대해 Service Quotas 콘솔에서 IAM 역할에 연결된 IAM 할당량 관리형 정책의 증가를 요청합니다.

Note

[권한 세트 AWS 계정 로 관리](#)는에서 IAM 역할 AWS 계정 로 프로비저닝되거나에서 기존 IAM 역할을 사용 AWS 계정하므로 IAM 할당량을 따릅니다. IAM 역할과 관련된 할당량에 대한 자세한 내용은 [IAM 및 STS 할당량](#)을 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	200000	예
IAM Identity Center에서 지원되는 그룹 수	100000	예
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 APIs 는 초당 트랜잭션 20개(TPS)입니다. 읽기 APIs 경우 지원 사례를 열어 한도 증가를 요청할 수 있습니다. CreateAccountAssignment 쓰기 API는 15개의 미해결 비동기 호출로 제한됩니다. 이 한도는 늘릴 수 없습니다.
Identity Store API	Identity Store APIs 는 API당 초당 트랜잭션 20개(TPS)입니다. 이 제한은 Identity Store 인스턴스당 적용됩니다. 지원 사례를 열어 한도 증가를 요청할 수 있습니다.
SCIM API	SCIM APIs 제한 한도는 쓰기 API의 경우 초당 트랜잭션 25개(TPS), 읽기 APIs 경우 40TPS입니다. 이러한 제한은 Identity Store 인스턴스당 적용됩니다. 지원 사례를 열어 한도 증가를 요청할 수 있습니다.

IAM Identity Center 인스턴스가 여러에서 활성화된 경우 AWS 리전스로틀 제한은 활성화된 각 리전에 동일하게 적용됩니다. 예를 들어 활성화된 각 리전의 Identity Store APIs에는 20TPS 스로틀 제한이 있습니다. 추가 리전에서 사용할 수 있는 API 작업에 대한 자세한 내용은 해당 [표를](#) 참조하세요.

OIDC 서비스 요청 할당량

Resource	기본값(초당 요청 수)	높일 수 있음
퍼블릭 OAuth 클라이언트를 등록하기 위한 원격 주소의 요청 속도 적용 대상: RegisterClient	20	예
OIDC 서비스에 등록된 퍼블릭 클라이언트의 요청 속도 적용 대상: CreateToken , StartDeviceAuthorization	80	예
동일한 IAM Identity Center 인스턴스에 등록된 모든 퍼블릭 클라이언트의 요청 속도 적용 대상: CreateToken	250	예
IAM Identity Center 인스턴스에 등록된 IAM Identity Center 애플리케이션의 요청 속도 적용 대상: CreateTokenWithIAM	80	예
JWT Bearer 권한 부여를 통해 동일한 IAM Identity Center 인스턴스에 등록된 모든 IAM Identity Center 애플리케이션의 토큰 생성 속도	10	AWS Support에 문의

Resource	기본값(초당 요청 수)	높일 수 있음
적용 대상: CreateTokenWithIAM		

IAM Identity Center 인스턴스가 여러에서 활성화된 경우 위의 AWS 리전요청 속도가 활성화된 각 리전에 동일하게 적용됩니다. 예를 들어 원격 주소에서 퍼블릭 OAuth 클라이언트를 등록하는 데 허용되는 요청 속도가 초당 20개의 요청인 경우이 처리량은 활성화된 각 리전에서 사용할 수 있습니다. 추가 리전에서 사용할 수 있는 API 작업에 대한 자세한 내용은 해당 [표를](#) 참조하세요.

추가 할당량

Resource	기본 할당량	높일 수 있음
구성할 수 있는 AWS 계정 총 또는 애플리케이션 수 * **	3000	예
계정당 IAM Identity Center의 총 계정 인스턴스 수	1	아니요
총 신뢰할 수 있는 토큰 발급자 수	10	아니요
AWS 계정또는 애플리케이션에 따라 권한 세트에 할당할 수 있는 총 그룹 수	100	아니요
단일 IAM Identity Center 인스턴스에 대해 AWS 리전 활성화된 총 수	3	예

* 예를 들어 2,750개의 계정과 250개의 애플리케이션을 구성하여 총 3,000개의 계정 및 애플리케이션을 구성할 수 있습니다.

** [ProvisionPermissionSet](#) API 작업은 ALL_PROVISIONED_ACCOUNTS 옵션을 사용하여 권한 세트를 최대 3,500개의 AWS 계정으로 프로비저닝할 수 있습니다. 권한 세트를 3,500개 이상의 AWS 계정으로 프로비저닝해야 하는 경우 단일 AWS 계정에서 권한 세트를 프로비저닝하

는 AWS_ACCOUNT 옵션과 함께 ProvisionPermissionSet API 작업을 사용할 수 있습니다. ProvisionPermissionSet에 대해 최대 3개의 동시 호출을 수행할 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 설정 환경을 통해 계정 인스턴스를 생성할 수 없는 경우 다음 사용 사례를 확인합니다.

- 계정 인스턴스를 생성하려는 AWS 계정 AWS 리전 의 다른를 확인합니다. AWS 계정당 IAM Identity Center 인스턴스는 1개로 제한됩니다. 애플리케이션을 활성화하려면 IAM Identity Center 인스턴스를 AWS 리전 사용하여 로 전환하거나 IAM Identity Center 인스턴스가 없는 계정으로 전환합니다.
- 2023년 9월 14일 이전 조직에서 IAM Identity Center를 활성화한 경우 관리자는 계정 인스턴스 생성을 옵트인해야 할 수도 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": "sso:ListApplicationProviders",
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "sso:ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
    ]

```

내부 API를 허용하지만 ListApplications를 거부하려면 정책에서 ListApplicationProviders만 허용해야 합니다. 명시적으로 허용되지 않는 경우 ListApplications API가 거부됩니다.

```

    "Statement": [
    {
        "Effect": "Allow",
        "Action": "sso:ListApplicationProviders",
        "Resource": "*"
    }
    ]

```

정책이 업데이트되면 지원 에 문의하여이 사전 예방 조치를 제거합니다.

IAM Identity Center에서 생성된 SAML 어설션 콘텐츠 관련 문제

IAM Identity Center는 AWS 액세스 포털에서 및 SAML 애플리케이션에 액세스할 때 이러한 어설션 내의 속성을 포함하여 IAM Identity Center에서 생성하고 전송하는 AWS 계정 SAML 어설션에 대한 웹 기반 디버그 환경을 제공합니다. IAM Identity Center에서 생성하는 SAML 어설션의 세부 정보를 보려면 다음 단계를 사용하세요.

1. AWS 액세스 포털에 로그인합니다.

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

SCIM 동기화를 사용하여 사용자를 IAM Identity Center에 프로비저닝하도록 ID 제공업체(idP)가 구성된 경우 사용자 프로비저닝 프로세스 중에 동기화 실패가 발생할 수 있습니다. 이는 IdP의 사용자 구성이 IAM Identity Center 요구 사항과 호환되지 않음을 나타내는 것일 수 있습니다. 이 경우 IAM Identity Center SCIM API는 문제의 근본 원인에 대한 이해를 제공하는 오류 메시지를 반환합니다. 이러한 오류 메시지는 IdP의 로그 또는 UI에서 찾을 수 있습니다. 또는 [AWS CloudTrail 로그](#)에서 프로비저닝 실패에 관한 보다 상세한 정보를 확인할 수 있습니다.

사용자 객체에 대한 필수적이거나 선택적인, 또는 지원되지 않는 파라미터 및 작업 사양을 포함하여 IAM Identity Center SCIM 구현에 대한 자세한 내용은 SCIM 개발자 가이드의 [IAM Identity Center SCIM 구현 개발자 지침](#)에서 확인할 수 있습니다.

이러한 오류가 발생하는 몇 가지 일반적인 이유는 다음과 같습니다.

1. IdP의 사용자 객체에 이름, 성 및/또는 표시 이름이 없습니다.

오류 메시지: "2개의 유효성 검사 오류가 감지되었습니다: '*name.givenName*'의 값이 제약 조건을 충족하지 않습니다: 구성원은 정규식 패턴 `[\p{L}\p{M}\p{S}\p{N}\p{P}]{1,\n\r}`을 충족해야 합니다; '*name.givenName*'의 값이 제약 조건을 충족하지 않습니다: 구성원의 길이는 1' 이상이어야 합니다"

- 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.

오류 메시지: "목록 속성 ###이 허용 한도 1을 초과합니다"

- 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 AWS IdP의 사용자 객체에 대한 SCIM 프로비저닝 매핑에서 해당 속성에 대한 매핑을 제거합니다.
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 username만 지정하면 됩니다.
- 해결 방법: IdP의 SCIM 구성이 IAM Identity Center의 사용자를 매칭하기 위해 단일 속성만 사용하고 있는지 확인합니다. 예를 들어, IAM Identity Center에 프로비저닝하기 위해 IdP의 username 또는 userPrincipalName를 SCIM의 userName 속성에 매핑하면 대부분의 구현에서 정확하고 충분합니다.

외부 ID 제공업체에서 사용자 또는 그룹을 프로비저닝할 때의 중복 사용자 또는 그룹 오류

외부 ID 제공업체(idP)에서 사용자 또는 그룹을 프로비저닝할 때 IAM Identity Center 동기화 문제가 발생하는 경우 이는 외부 IdP 사용자 또는 그룹에 고유한 속성 값이 없기 때문일 수 있습니다. 외부 IdP에 다음과 같은 오류 메시지가 표시될 수 있습니다.

새 중복 리소스 생성이 거부되었습니다

이러한 문제를 겪을 수 있는 시나리오는 다음과 같습니다.

- 시나리오 1
 - IAM Identity Center의 고유 속성에 대해 외부 IdP에서 사용자 지정 비고유 속성을 사용하고 있습니다. 기존 IAM Identity Center 사용자 또는 그룹이 IdP에 동기화되지 않습니다.
- 시나리오 2
 - IAM Identity Center의 고유 속성에 대해 중복 속성이 있는 사용자를 생성하려고 시도합니다.
 - 예를 들어 다음 속성을 가진 기존 IAM Identity Center 사용자를 생성하거나 이러한 사용자가 있다고 가정해 봅시다.
 - 사용자 이름: Jane Doe
 - 기본 이메일 주소: jane_doe@example.com
 - 그런 다음 다음 속성을 가진 다른 외부 IdP 사용자를 생성하려고 시도합니다.
 - 사용자 이름: Richard Doe
 - 기본 이메일 주소: jane_doe@example.com
 - 외부 IdP는 IAM Identity Center 사용자를 동기화하고 생성하려고 시도합니다. 그러나 고유해야 하는 기본 이메일 주소에 대해 두 사용자의 값이 같으므로 이 작업은 실패합니다.

외부 IdP 사용자가 IAM Identity Center로 성공적으로 동기화되려면 사용자 이름, 기본 이메일 주소, externalID가 고유해야 합니다. 마찬가지로 외부 IdP 그룹이 IAM Identity Center로 성공적으로 동기화되려면 그룹 이름이 고유해야 합니다.

이에 대한 해결 방법은 ID 소스의 속성을 검토하고 해당 속성이 고유한지 확인하는 것입니다.

사용자 이름이 UPN 형식인 경우 사용자는 로그인할 수 없습니다.

사용자는 로그인 페이지에서 사용자 이름을 입력하는 데 사용하는 형식을 기반으로 AWS 액세스 포털에 로그인하지 못할 수 있습니다. 대부분의 경우 사용자는 일반 사용자 이름, 하위 수준 로그온 이름(DOMAIN\UserName) 또는 UPN 로그온 이름(Username@Corp.Example.com)을 사용하여 사용자 포털에 로그인할 수 있습니다. 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\UserName)으로 로그인해야 합니다. 자세한 내용은 [Identity Center 디렉터리 사용자를 위한 MFA](#) 단원을 참조하십시오. Active Directory에 로그인하는 데 사용되는 사용자 이름 형식에 대한 일반적인 정보는 Microsoft 설명서 웹 사이트의 [사용자 이름 형식](#)을 참조하세요.

IAM 역할을 수정할 때 '보호된 역할에서 작업을 수행할 수 없습니다' 오류가 발생합니다.

계정의 IAM 역할을 검토할 때 'AWSReservedSSO_'로 시작하는 역할 이름을 보일 수 있습니다. 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 관리 계정에 있는 IAM Identity Center 관리자 콘솔에서만 수정할 수 있습니다 AWS Organizations. 수정한 후에는 당 변경 사항이 할당된 AWS 계정으로 푸시할 수 있습니다.

디렉터리 사용자는 비밀번호를 재설정할 수 없습니다.

AWS 액세스 포털에 로그인하는 동안 디렉터리 사용자가 암호 찾기 옵션을 사용하여 암호를 재설정하는 경우 새 암호에는 설명된 기본 암호 정책을 준수해야 합니다 [IAM Identity Center에서 ID를 관리할 때 암호 요구 사항](#).

사용자가 정책을 준수하는 암호를 입력한 다음 오류를 수신하는 경우 We couldn't update your password가 실패를 AWS CloudTrail 기록했는지 확인합니다. 이 작업은 CloudTrail의 이벤트 기록 콘솔에서 다음 필터를 사용하여 검색하면 됩니다.

```
"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 센터](#)에 문의하세요.

내 사용자는 권한 집합에서 참조할 수 있지만 할당된 계정이나 애플리케이션에 액세스할 수 없습니다.

이 문제는 외부 ID 공급업체를 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 AWS 계정()에서 이전 사용자 또는 그룹에 대한 액세스를 제거한 다음 사용자 또는 그룹에 다시 액세스 권한을 할당할 수 있습니다. 그러면 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.

또한 CloudTrail 로그에서 해당 사용자 또는 그룹의 이름을 참조하는 SCIM 동기화 이벤트를 검색하여 실패를 AWS CloudTrail 기록했는지 확인할 수 있습니다.

애플리케이션 카탈로그에서 애플리케이션을 올바르게 구성할 수 없습니다.

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 “여기치 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 일치하는 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 속성](#)가 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 로 이동하여 이벤트 이름 ExternalIdPDirectoryLogin을 AWS CloudTrail 필터링하여 외부 ID 제공업체 로그인 실패 문제를 해결할 수 있습니다.

'액세스 제어 속성을 활성화하지 못했습니다' 오류

이 오류는 ABAC를 활성화하는 사용자에게 [액세스 제어를 위한 속성](#)를 활성화하는 데 필요한 iam:UpdateAssumeRolePolicy 권한이 없는 경우 발생할 수 있습니다.

MFA에 디바이스를 등록하려고 할 때 '브라우저가 지원되지 않습니다' 메시지가 표시됩니다.

WebAuthn은 현재 Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari 웹 브라우저와 Windows 10 및 Android 플랫폼에서 지원됩니다. macOS 및 iOS 브라우저에서 플랫폼 인증 지원 등 WebAuthn 지원의 일부 구성 요소는 다양할 수 있습니다. 사용자가 지원되지 않는 브라우저 또는 플랫폼에서 WebAuthn 디바이스를 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 참조하세요. IAM Identity Center WebAuthn에 대한 자세한 내용은 [FIDO2 인증자](#)을 참조하세요.

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 또는 Microsoft Entra ID)의 계정을 사용하여 IAM Identity Center에 로그인 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 Identity Center에 로그인하려고 시도할 때 "사용자가 아닌 우리 쪽에서 문제가 발생했습니다"라는 오류가 표시됩니다.

이 오류는 IAM Identity Center 인스턴스 또는 IAM Identity Center가 ID 소스로 사용하는 외부 ID 제공 업체(idP)에 설정 문제가 있음을 나타냅니다. 다음을 확인할 것을 권장합니다.

- 로그인에 사용하는 디바이스의 날짜 및 시간 설정을 확인합니다. 날짜와 시간을 자동으로 설정할 것을 권장합니다. 그럴 수 없는 경우 날짜와 시간을 알려진 네트워크 타임 프로토콜(NTP) 서버에 동기화할 것을 권장합니다.
- IAM Identity Center에 업로드된 IdP 인증서가 IdP에서 제공한 것과 동일한지 확인합니다. 설정으로 이동하여 IAM Identity Center 콘솔의 인증서를 확인할 수 있습니다. ID 소스 탭에서 작업을 선택한 다음 인증 관리를 선택합니다. IdP와 IAM Identity Center의 인증서가 일치하지 않으면 새 인증서를 IAM Identity Center로 가져옵니다.
- ID 제공업체 메타데이터 파일의 NameID 형식이 다음과 같은지 확인합니다.
 - urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress
- 의 AD Connector를 자격 증명 공급자 AWS Directory Service 로 사용하는 경우 서비스 계정의 자격 증명이 올바르고 만료되지 않았는지 확인합니다. 자세한 내용은 [AWS Directory Service에서 AD Connector 서비스 계정 자격 증명 업데이트하기](#)를 참조하세요.

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 수신하고 이를 정크 또는 스팸으로 처리하지 않도록 구성해야 합니다.

오류: 관리 계정에 프로비저닝된 권한 세트에 대한 액세스 권한을 삭제/수정/제거/할당할 수 없습니다.

이 메시지는 [위임된 관리](#) 기능이 활성화되었으며 앞서 시도한 작업을 AWS Organizations의 관리 계정 권한이 있는 사람만이 성공적으로 수행할 수 있음을 나타냅니다. 이 문제를 해결하려면 이러한 권한이 있는 사용자로 로그인하여 작업을 다시 수행하거나 올바른 권한이 있는 사람에게 이 작업을 할당합니다. 자세한 내용은 [멤버 계정 등록](#) 단원을 참조하십시오.

오류: 세션 토큰을 찾을 수 없거나 세션 토큰이 유효하지 않습니다

이 오류는 웹 브라우저 AWS Toolkit 또는와 같은 클라이언트가 서버 측에서 취소되거나 무효화된 세션을 사용하려고 AWS CLI 할 때 발생할 수 있습니다. 이 문제를 해결하려면 메시지가 표시될 때 다시 로그인하는 것을 포함하여 클라이언트 애플리케이션 또는 웹 사이트로 돌아가 다시 시도합니다. 이로 인해 IDE AWS Toolkit 내의에서 오류 중인 연결 시도와 같은 오류 중인 요청도 취소해야 하는 경우가 있습니다.

신뢰할 수 있는 도메인의 그룹 멤버가 IAM Identity Center와 동기화되지 않음

보안 그룹이 IAM Identity Center에 성공적으로 동기화되지만 신뢰할 수 있는 온프레미스 도메인의 구성원이 IAM Identity Center에 표시되지 않는 경우, 그룹이에 AWS Managed Microsoft AD 상주하고 신뢰할 수 있는 도메인의 사용자를 나타내는 FSPs)가 포함되어 있기 때문일 수 있습니다.

문제 해결을 위해 다음 단계를 시도하세요:

- 신뢰할 수 있는 도메인에서 직접 그룹 동기화: 교차 도메인 구성원이 포함된에서 그룹을 동기화 AWS Managed Microsoft AD 하는 대신 신뢰할 수 있는 온프레미스 도메인에서 직접 그룹을 생성하고 동기화합니다. 이 접근 방식은 IAM Identity Center가 소스 도메인의 실제 사용자 객체에 액세스할 수 있기 때문에 작동합니다.
- 서비스 계정 권한 확인: IAM Identity Center 서비스 계정에 신뢰할 수 있는 도메인의 사용자 객체에 대한 필수 권한인 ReadProperties 및 ListContents 권한이 있는지 확인합니다.

에서 고객 관리형 키 문제 해결 AWS IAM Identity Center

이 주제에서는를 사용할 때 발생할 수 있는 일반적인 고객 관리형 키 관련 오류 AWS IAM Identity Center 에 대해 설명하고 이를 해결하기 위한 문제 해결 단계를 제공합니다.

액세스 거부됨: KMS 복호화 권한 문제

오류: "사용자 xxxxxxxx는 kms:Decrypt 작업을 허용하는 ID 기반 정책이 없으므로 이 사이퍼텍스트와 연결된 리소스에 대해 kms:Decrypt를 수행할 권한이 없습니다."

사용자 또는 IAM 위탁자에게 IAM 정책 또는 KMS 키 정책에 필요한 kms:Decrypt 권한이 없습니다.

다음을 사용한 문제 해결 AWS CloudTrail:

1. CloudTrail에서 kms.amazonaws.com 이벤트를 찾습니다.
2. 이벤트 이름 Decrypt를 검색합니다.
3. errorCode 및 errorMessage 필드를 검토합니다.
4. userIdentity에서 작업을 시도한 위탁자를 확인합니다.

이 문제를 해결하려면 IAM 정책 및 KMS 키 정책에서 사용자 또는 IAM 위탁자에게 kms:Decrypt 액세스 권한을 부여합니다. 자세한 내용은 [에서 고객 관리형 KMS 키 구현 AWS IAM Identity Center](#) 단원을 참조하십시오.

AWS IAM Identity Center에서 고객 관리형 KMS 키가 활성화된 관리형 애플리케이션 로그인 실패

Identity Center 사용자가 AWS 관리형 애플리케이션에 로그인할 수 없고 IAM Identity Center 인스턴스에서 고객 관리형 KMS 키가 활성화된 경우 KMS 키 정책이 AWS 관리형 애플리케이션에 고객 관리형 KMS 키를 사용할 수 있는 권한을 부여하는지 확인합니다. 자세한 내용은 [기본 KMS 키 및 IAM 정책 설명](#) 단원을 참조하십시오.

AWS IAM Identity Center에서 고객 관리형 KMS 키가 활성화된 관리형 애플리케이션 설치 및/또는 사용자 할당 실패

오류: "사용자 xxxxxxxx는 kms:Decrypt 작업을 허용하는 ID 기반 정책이 없으므로 이 사이퍼텍스트와 연결된 리소스에 대해 kms:Decrypt를 수행할 권한이 없습니다."

사용자 또는 IAM 위탁자에게 IAM 정책 또는 KMS 키 정책에 필요한 kms:Decrypt 권한이 없습니다.

CloudTrail을 통한 문제 해결:

1. 이벤트 이름 Decrypt를 검색합니다.
2. errorCode 및 errorMessage 필드를 검토합니다.
3. userIdentity에서 작업을 시도한 위탁자를 확인합니다.

이 문제를 해결하려면 IAM 정책 및 KMS 키 정책에서 사용자 또는 IAM 위탁자에게 kms:Decrypt 액세스 권한을 부여합니다. 자세한 내용은 [에서 고객 관리형 KMS 키 구현 AWS IAM Identity Center](#) 단원을 참조하십시오.

KMS 권한 문제:를 사용하여 고객 관리형 키 구성 AWS IAM Identity Center

사용자 또는 IAM 위탁자에게 고객 관리형 키를 활성화할 때 필요한 KMS 권한(`kms:Decrypt`, `kms:Encrypt`, `kms:GenerateDataKey`, `kms:DescribeKey`)이 하나 이상 없습니다.

CloudTrail을 통한 문제 해결:

1. `Decrypt`, `Encrypt`, `GenerateDataKey`, 또는 `DescribeKey` 이벤트를 검색합니다.
2. `errorCode` 및 `errorMessage` 필드를 검토합니다.
3. `userIdentity`에서 작업을 시도한 위탁자를 확인합니다.

이 문제를 해결하려면 ID 기반 정책 또는 KMS 키 정책에서 사용자 또는 IAM 위탁자에게 필요한 모든 KMS 권한을 부여합니다. 자세한 내용은 [에서 고객 관리형 KMS 키 구현 AWS IAM Identity Center](#) 단원을 참조하십시오.

AWS IAM Identity Center에서 고객 관리형 KMS 키가 활성화된 상태에서 액세스 포털 로그인 실패

오류: "오류 코드: 0001 - IdentityCenter 서비스 액세스가 차단되었습니다. 추가 단계는 IdentityCenter 관리자에게 문의하세요."

사용자가 AWS 액세스 포털에 로그인할 수 없고 IAM Identity Center 인스턴스에서 고객 관리형 KMS 키가 활성화된 경우 KMS 키 정책이 Identity Center 및 Identity Store에 필요한 권한을 부여하는지 확인합니다. 자세한 내용은 [기존 KMS 키 및 IAM 정책 설명](#) 단원을 참조하십시오.

의 다중 리전 설정 문제 해결 AWS IAM Identity Center

이 주제에서는를 사용할 때 발생할 수 있는 일반적인 다중 리전 설정 관련 오류 AWS IAM Identity Center 에 대해 설명하고 이를 해결하기 위한 문제 해결 단계를 제공합니다.

IAM Identity Center 인스턴스를 복제하려는 리전은 IAM Identity Center 콘솔에서 사용할 수 없습니다.

먼저 IAM Identity Center 인스턴스를 복제하려는 리전에서 고객 관리형 KMS 키에 대한 복제본 키를 생성해야 합니다. 복제본 키가 생성되면 복제에 사용할 수 있는 리전 목록에 리전이 표시됩니다. 자세한 내용은 [the section called “1단계: 복제본 키 생성”](#) 단원을 참조하십시오.

AWS 추가 리전의 관리형 애플리케이션 로그인 실패

IAM Identity Center에서 리전을 추가한 후 IAM Identity Center 사용자가 추가 리전의 AWS 관리형 애플리케이션에 로그인할 수 없는 경우에 설명된 대로 외부 ID 제공업체에서 추가 리전의 ACS(어설션 소비자 서비스) URL을 구성했는지 확인합니다 [the section called “3단계: 외부 IdP 설정 업데이트”](#). 또한 사용자가 리전에 연결되어 있는지 확인합니다.

문서 이력

다음 표에서는 AWS IAM Identity Center 설명서에 추가된 중요 사항에 대해 설명합니다. 사용자로부터 받은 의견을 수렴하기 위해 설명서가 자주 업데이트됩니다.

- 기본 설명서 최신 업데이트: 2025년 10월 21일

변경 사항	설명	날짜
다중 리전 지원	추가 리전으로 복제, 추가 리전의 AWS 관리형 애플리케이션 AWS 계정 액세스 및 사용을 포함한 다중 리전 지원이 추가되었습니다.	2026년 2월 2일
업데이트된 AWS 관리형 정책	테넌트 프로비저닝을 위한 ARN을 변경하도록 AWSIdentityCenterExternalManagementPolicy AWS 관리형 정책을 업데이트했습니다.	2025년 12월 5일
새로운 AWS 관리형 정책 주제	AWSIdentityCenterExternalManagementPolicy AWS 관리형 정책에 대한 세부 정보가 추가되었습니다.	2025년 11월 21일
자동 프로비저닝 감사 및 조정 지침	Identity Store APIs하고 조정하기 위한 지침이 추가되었습니다. AWS CLI	2025년 10월 17일
OIDC 서비스 요청 할당량	OAuth 클라이언트 등록, 토큰 생성 및 기타 OIDC 작업에 대한 속도 제한을 포함하여 OIDC	2025년 10월 13일

서비스 요청 할당량이 추가되었습니다.

[AWS 관리형 정책에 대한 업데이트](#)

IAM Identity Center는 암호화에 고객 관리형 키를 사용하는 IAM Identity Center 인스턴스에 필요한 AWS KMS 권한을 AWSSSODirectoryReadOnly 포함하도록 관리형 정책 AWSSSOMasterAccountAdministrator AWSSS0ReadOnly , AWSSSOMemberAccountAdministrator , AWSSS0DirectoryAdministrator , 및를 업데이트했습니다.

2025년 9월 17일

[저장 데이터 암호화에 대한 고객 관리형 키](#)

작업 인력 자격 증명 저장 데이터를 암호화하기 위한 고객 관리형 KMS 키에 대한 지원이 추가되었습니다.

2025년 9월 17일

[토큰 생성을 허용하는 리소스 기반 정책 예제](#)

승인된 클라이언트 애플리케이션에 대한 토큰 생성을 허용하는 리소스 기반 정책 예제가 추가되었습니다.

2025년 9월 16일

[사용자 백그라운드 세션 지원](#)

사용자 백그라운드 세션에 대한 콘텐츠가 추가되었습니다.

2025년 8월 11일

[자격 증명 강화 콘솔 세션](#)

자격 증명 강화 콘솔 세션(이전에는 자격 증명 인식 세션이라고 함)에 대한 용어를 업데이트했습니다.

2025년 5월 12일

재구성 시작하기	명확성과 사용자 경험을 개선하기 위해 시작하기 콘텐츠를 재구성했습니다.	2025년 5월 6일
IAM Identity Center 광고 동기화 사용 중지	더 이상 IAM Identity Center 광고 동기화를 사용하여 Active Directory 사용자를 프로비저닝할 수 없습니다. 대신 IAM Identity Center 구성 가능한 광고 동기화를 사용할 수 있습니다.	2025년 4월 17일
인증된 세션에 대한 업데이트된 콘텐츠	사용자 세션이 삭제될 때 IAM Identity Center 세션 기간을 업데이트합니다.	2025년 4월 2일
AWS 관리형 정책에 대한 업데이트	AWSSS0ServiceRolePolicy AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2025년 2월 11일
IAM Identity Center 활성화 워크플로 개선	IAM Identity Center의 조직 인스턴스 및 계정 인스턴스를 활성화하기 위한 워크플로가 업데이트되었습니다.	2025년 2월 11일
IAM Identity Center 활성화에 대한 업데이트	IAM Identity Center의 조직 인스턴스 및 계정 인스턴스를 활성화하기 위한 콘텐츠 및 절차가 업데이트되었습니다.	2024년 10월 10일
AWS 관리형 정책에 대한 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 10월 2일

AWS 관리형 정책에 대한 업데이트	AWSSSOMasterAccountAdministrator AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 9월 26일
AWS 관리형 정책에 대한 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 9월 4일
'IAM Identity Center란 무엇인가요?' 업데이트 주제	IAM Identity Center의 이점과 기능을 설명하는 콘텐츠를 업데이트했습니다.	2024년 8월 19일
AWS 관리형 정책에 대한 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 7월 12일
AWS 관리형 정책에 대한 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 6월 27일
AWS 관리형 정책에 대한 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 5월 17일
AWS 관리형 정책에 대한 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 4월 30일

AWS 관리형 정책에 대한 업데이트	AWSSS0MasterAccountAdministrator AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 4월 26일
AWS 관리형 정책에 대한 업데이트	AWSSS0MemberAccountAdministrator AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 4월 26일
AWS 관리형 정책에 대한 업데이트	AWSSS0ReadOnly AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 4월 26일
AWS 관리형 정책에 대한 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 4월 26일
AWS 관리형 정책에 대한 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 4월 24일
AWS 관리형 정책에 대한 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 4월 19일
AWS 관리형 정책에 대한 업데이트	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2024년 4월 11일

<u>AWS 관리형 정책에 대한 업데이트</u>	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2023년 11월 26일
<u>새로운 AWS 관리형 정책 주제</u>	AWSIAMIdentityCenterAllowListForIdentityContext AWS 관리형 정책에 대한 세부 정보가 추가되었습니다.	2023년 11월 15일
<u>IAM Identity Center 시작하기 에 대한 지침 개선</u>	IAM Identity Center 시작 및 관리 사용자 생성에 대한 새로운 내용이 추가되었습니다.	2022년 9월 23일
<u>Identity Center API 참조의 사 용자 및 그룹이 업데이트됨</u>	이 업데이트에는 Identity Center API 참조 가이드의 새로운 생성, 업데이트 및 API 삭제에 대한 참고 사항이 포함되어 있습니다.	2022년 8월 31일
<u>AWS Single Sign-On(AWS SSO)의 이름이 AWS IAM Identity Center로 변경되었습 니다.</u>	AWS 는를 도입합니다 AWS IAM Identity Center. IAM Identity Center는 AWS Identity and Access Management (IAM)의 기능을 확장하여 작업 인력 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 세트와 함께 AWS 관리형 및 고객 관리형 AWS Identity and Access Management (IAM) 정책을 사용하기 위한 콘텐츠가 추가되었습니다.	2022년 7월 14일
수동으로 활성화된 AWS 리전 지원	수동으로 활성화된 리전에서 IAM Identity Center 사용에 대한 내용이 추가되었습니다.	2022년 6월 15일
AWS 관리형 정책에 대한 업데이트	AWSSS0ServiceRolePolicy AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2022년 5월 11일
위임된 관리 지원	위임된 관리 기능에 대한 내용이 추가되었습니다.	2022년 5월 11일
AWS 관리형 정책에 대한 업데이트	AWSSS0MasterAccountAdministrator , AWSSS0MemberAccountAdministrator 및 AWSSS0ReadOnly AWS 관리형 정책에 대한 권한을 업데이트했습니다.	2022년 4월 28일
구성 가능한 AD 동기화 지원	구성 가능한 AD 동기화 기능에 대한 내용이 추가되었습니다.	2022년 4월 14일
새로운 AWS 관리형 정책 주제	AWSSS0MasterAccountAdministrator AWS 관리형 정책에 대한 세부 정보가 추가되었습니다.	2021년 8월 4일
할당량 업데이트	할당량 테이블 조정.	2020년 12월 21일

<u>새로운 예시 정책</u>	새로운 고객 관리형 정책 예시를 추가하고 권한 필요 섹션을 업데이트했습니다.	2020년 12월 21일
<u>속성 기반 액세스 제어(ABAC) 지원</u>	ABAC 기능에 대한 내용이 추가되었습니다.	2020년 11월 24일
<u>MFA 강제 등록 지원</u>	사용자가 로그인할 때 MFA 장치 등록을 요구하도록 업데이트되었습니다.	2020년 11월 23일
<u>WebAuthn 지원</u>	새 WebAuthn 기능에 대한 내용이 추가되었습니다.	2020년 11월 20일
<u>Ping Identity 지원</u>	지원되는 외부 ID 제공업체로 Ping Identity 제품과 통합에 대한 내용이 추가되었습니다.	2020년 10월 26일
<u>OneLogin 지원</u>	지원되는 외부 ID 제공업체로 OneLogin과 통합에 대한 내용이 추가되었습니다.	2020년 7월 31일
<u>Okta 지원</u>	지원되는 외부 ID 제공업체로 Okta와 통합에 대한 내용이 추가되었습니다.	2020년 5월 28일
<u>외부 ID 제공업체 지원</u>	디렉토리에서 ID 소스로 참조를 변경하고 외부 ID 제공업체 지원에 대한 내용이 추가되었습니다.	2019년 11월 26일
<u>새 MFA 설정</u>	2단계 인증 항목을 제거하고 그 자리에 새 MFA 항목을 추가했습니다.	2019년 10월 24일
<u>2단계 인증을 추가하기 위한 새로운 설정</u>	사용자를 위한 2단계 인증을 활성화하는 방법에 대한 내용이 추가되었습니다.	2019년 1월 16일

<u>AWS 계정의 세션 기간 지원</u>	AWS 계정의 세션 기간을 설정하는 방법에 대한 내용이 추가되었습니다.	2018년 10월 30일
<u>Identity Center 디렉터리를 사용할 수 있는 새 옵션</u>	Identity Center 디렉터리를 선택하거나 Active Directory의 기존 디렉터리에 연결하는 데 대한 내용이 추가되었습니다.	2018년 10월 17일
<u>애플리케이션의 릴레이 상태 및 세션 기간 지원</u>	애플리케이션의 릴레이 상태 및 세션 기간에 대한 내용이 추가되었습니다.	2018년 10월 10일
<u>새 애플리케이션에 대한 추가 지원</u>	4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvalnSync, 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
<u>관리 계정에 대한 다중 계정 액세스 지원</u>	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 위해 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 참조의 [AWS 용어집](#)을 참조하세요.

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