

diff IDP를 사용하여 Cisco Secure Access에서 사용자/그룹 ID 동기화 문제 해결

목차

문제

이 문서에서는 Cisco Secure Access에서 Okta, Microsoft Entra ID, IBM Cloud와 같은 다른 IdP(Identity Provider)를 사용하여 사용자 및 그룹 ID 동기화를 트러블슈팅하는 방법에 대해 설명합니다.

환경

- Cisco Secure Access — SCIM 프로비저닝 통합
- SCIM 2.0 IdP 커넥터(Okta, Azure AD)에 적용됩니다.

해결

개요

Cisco Secure Access는 SCIM 2.0 표준을 사용하여 Okta 및 Microsoft Entra ID(이전의 Azure AD)에서 직접 사용자 및 그룹 ID를 프로비저닝할 수 있도록 지원합니다. 따라서 클라우드 전용 ID 소스에 대해 온프레미스 AD(Active Directory) Connector를 배포할 필요가 없습니다. 이 문서에서는 현장 엔지니어와 관리자가 이 통합을 구축하거나 유지 관리할 때 가장 자주 발생하는 아키텍처 가정, 일반적인 장애 모드 및 문제 해결 지침을 통합합니다.

이 문서는 네 개의 섹션으로 구성되어 있습니다.

- 컨피그레이션 - 공식 설정 지침을 보려면 어디로 가야 합니까?
- 아키텍처 가정(위반할 경우 무음 또는 진단하기 어려운 장애 유발)
- 공급자별 문제(Okta 대 Entra ID)
- IdP와 상관없이 적용되는 일반 SCIM 프로토콜 문제

설정

이 문서에서는 초기 설정이 아닌 문제 해결에 중점을 둡니다. 단계별 구성을 위해 이 문서의 공식 Cisco TechNotes를 사용하십시오.

- Microsoft Entra ID(Azure AD)로 Cisco Secure Access를 구성하려면 다음 링크를 참조하십시오. Entra ID를 통한 보안 액세스를 위해 사용자 및 그룹 프로비저닝
- Cisco Secure Access with Okta를 구성하려면 다음 링크를 참조하십시오. OKTA를 통한 액세스 보안을 위해 사용자 및 그룹 프로비저닝

두 문서 모두 Secure Access에서 SCIM 토큰 및 프로비저닝 URL 생성, IdP에서 해당 애플리케이션 구성, 초기 프로비저닝 동기화 실행에 대해 다룹니다.

아키텍처 입문서

트러블슈팅을 수행하기 전에 구축이 이러한 핵심 가정과 일치하는지 확인합니다. 대부분의 동기화 실패는 이러한 가정 중 하나로 다시 추적됩니다.

한 번에 하나의 ID 소스

온프레미스 AD 커넥터 및 클라우드 IdP(Okta 또는 Entra ID)에서 동일한 사용자 또는 그룹을 동시에 프로비저닝할 수 없으므로 일관되지 않은 정책이 적용됩니다. AD 커넥터에서 클라우드 IdP로 마이그레이션하는 경우:

- 온-프레미스 AD 커넥터 서비스를 중지합니다.
- 클라우드 IdP 프로비저닝을 활성화하기 전에 잔여 동기화 작업이 실행되고 있는지 확인

합니다.

가상 어플라이언스는 예외입니다.

IdP에는 VA에 필요한 프라이빗 IP-사용자 매핑에 대한 가시성이 없으므로 Centera ID 또는 Okta는 VA(Virtual Appliance)에 대한 ID 통합을 제공할 수 없습니다. VA 구축에는 다른 구성 요소에 사용되는 것과 상관없이 온프레미스 AD 커넥터가 필요합니다.

할당 대 푸시

- 작업: 애플리케이션에 사용자 또는 그룹 할당
 - 실제로 수행하는 작업: 보안 액세스를 위해 해당 그룹의 구성원 사용자를 규정합니다.
- 작업: 그룹 푸시(Okta)
 - 실제로 수행하는 작업: 그룹 객체 자체를 프로비저닝합니다(정책 대상 지정). 사용자를 동기화하지 않습니다.



참고: 사용자 프로비저닝을 위해 애플리케이션에도 할당된 그룹을 푸시하지 마십시오. 이렇게 하면 그룹 상태가 중복되거나 충돌할 수 있습니다.

그룹 및 사용자 제한

두 IdP 중 하나에서 프로비저닝된 사용자의 수에는 하드 제한이 없습니다.

그룹에 제한이 있습니다. 이전에는 조직당 Okta 또는 Entra ID의 200개 그룹이 사용되었습니다. 일부 최신 문서에서는 특히 Okta에 대해 더 높은 한도(최대 1,000개)를 보여줍니다. 정확한 번호는 환경에 따라 달라지므로 Cisco TAC(Technical Assistance Center) 또는 현재 Cisco 문서에 문의하십시오. Cap을 초과하는 그룹은 자동으로 프로비저닝되지 않으며 오류가 표시되지 않습니다.

더 폭넓은 커버리지가 필요한 경우, 모든 그룹을 개별적으로 푸시하는 대신 동적 "모든 사용자"(Entra ID) 또는 "모든 사용자"(Okta) 그룹을 사용합니다.

SCIM 토큰 수명 주기

Cisco Secure Access에서 Connect(연결) > Users, Groups and Endpoint Devices(사용자, 그룹 및 엔드포인트 디바이스) > Configuration Management(컨피그레이션 관리) > Integrate Directory(디렉토리 통합)를 선택하면 토큰이 생성됩니다. 토큰은 생성 시 한 번만 표시됩니다.

토큰을 재생성하면 Microsoft Entra ID 또는 Okta의 프로비저닝 컨피그레이션에 새 토큰이 입력될 때까지 IdP 측에서 프로비저닝이 즉시 중단됩니다. 유예 기간이 없으며 IdP 측 오류는 토큰 만료 메시지가 아니라 일반(인증 실패)인 경우가 많습니다.

보안 위생을 위해 토큰을 주기적으로 새로 고치고 순환 직후 IdP 측에서 연결을 테스트합니다.

Okta 관련 문제

- 증상: 보안 액세스에 그룹이 표시되지 않음
 - 근본 원인: 그룹을 푸시하면 그룹 객체만 프로비저닝됩니다. 멤버를 동기화하지 않습니다.
 - 해결: 관련 그룹 멤버가 Assignments(할당) 아래의 애플리케이션에 별도로 할당되어 있는지 확인합니다.
- 증상: 프로비저닝되었지만 특성이 누락되었거나 잘못된 사용자
 - 근본 원인: 보안 액세스 전용 서피스 표시 이름 및 사용자 이름; 지정된 이름과 패밀리 이름이 나열되지 않습니다.
 - 해결: 동기화에 필요한 특성이 명시적으로 선택되었는지 확인합니다. 모든 Okta 프로파일 필드가 전파된다고 가정하지 마십시오.
- 증상: 자동 프로비저닝은 아무 작업도 하지 않음
 - 근본 원인: 사용자 생성, 사용자 속성 업데이트 또는 사용자 비활성화 토글을 사용할 수 없습니다.
 - 해결: Okta 관리자 콘솔의 Provisioning(프로비저닝) > To App(앱으로)에서 세 가지 모두 선택되어 있는지 확인합니다.
- 증상: objectGUID 또는 사용자 지정 특성이 동기화되지 않음
 - 근본 원인: 특성은 사용자 프로필 매핑을 통해 추가되고 매핑되지 않습니다.
 - 해결: objectGUID 특성을 추가하고 이 식별자가 필요한 경우 해당 프로필 매핑을 만듭니

다.

- 증상: 토큰 순환 후 동기화가 중지되었습니다.
 - 근본 원인: SCIM 또는 API 토큰은 Secure Access에서 다시 생성되지만 Okta에서는 업데이트되지 않습니다.
 - 해결: Provisioning(프로비저닝) > Configure API Integration(API 통합 구성)에서 새 토큰을 입력하고 Test API Credentials(API 자격 증명 테스트)를 다시 실행합니다.
- 증상: 특정 사용자 또는 그룹이 실패한 이유를 확인할 수 없습니다.
 - 근본 원인: 로그를 먼저 확인하지 않았습니다.
 - 해결: 에스컬레이션하기 전에 Reports(보고서) > System Log in Okta(Okta(Cisco User Management Connector 애플리케이션으로 필터링된 시스템 로그))를 선택합니다.
- 증상: 그룹 수가 한도를 초과합니다. 일부는 오류 없이 누락되었습니다.
 - 근본 원인: 조직에는 Secure Access가 지원하는 것보다 더 많은 그룹이 있습니다.
 - 해결: 정책 관련 그룹으로만 범위를 축소하거나, Cisco TAC와 협력하여 더 높은 수준의 그룹 지원을 받으십시오.

Microsoft Entra ID별 문제

- 증상: 동적 그룹 멤버십이 보안 액세스에 반영되지 않음
 - 근본 원인: 동적 그룹 규칙이 잘못 구성되었거나 그룹이 프로비저닝된 범위에 없습니다.
 - 해결: Secure Access 동기화 버그를 가정하기 전에 Entra ID에서 직접 동적 구성원 규칙을 검증합니다.
- 증상: SAML SSO가 SWG ID를 구동해야 합니다.
 - 근본 원인: AnyConnect SWG(Secure Web Gateway)는 Entra ID에 대해 SAML(Security Assertion Markup Language) 인증을 지원하지 않습니다. 온프레미스 AD와 동일한 패시브 인증 메커니즘을 사용합니다.
 - 해결: Entra ID에 대한 SAML 기반 SWG ID를 중심으로 설계하지 마십시오. 수동 인증을 사용합니다.
- 증상: 사용자가 비활성화된 상태로 잘못 표시됨
 - 근본 원인: 활성 상태로 보낸 Entra ID 사용자가 할당된 그룹 범위를 벗어났거나 활성 특성 매핑이 잘못 구성되었기 때문에 false입니다.

- 해결: 사용자가 범위가 지정된 그룹에서 제거되었는지 확인합니다. 활성 매핑을 확인합니다(일반적으로 Not([isSoftDeleted])으로 평가되어야 함).
- 증상: 애플리케이션이 격리됨, 모든 프로비저닝이 중단됨
 - 근본 원인: 대상 응용 프로그램에서 반복된 비 SCIM 규격 응답을 반환했습니다.
 - 해결: 개별 사용자 장애가 발생할 경우를 가정하기 전에 격리 플래그에 대한 엔터프라이즈 애플리케이션 프로비저닝 상태를 확인합니다.
- 증상: 초기 프로비저닝 사이클이 완전히 실패함
 - 근본 원인: 첫 번째 실행에서 일시적인 동기화 오류가 발생했습니다.
 - 해결: Overview(개요) 페이지에서 Restart Provisioning(프로비저닝 재시작)을 클릭하여 Entra ID에서 초기 동기화를 다시 시도합니다.
- 증상: 중복 사용자가 여기치 않게 병합됩니다.
 - 근본 원인: 두 소스 ID가 동일한 이메일 또는 UPN(User Principal Name)을 공유합니다.
 - 해결: 소스 디렉토리에서 이메일 및 UPN 고유성을 확인합니다. 메일 특성이 확인된 도메인에서 오는지 확인합니다.
- 증상: 스키마 변경 후 특성 업데이트 중지
 - 근본 원인: 대상 측에서 속성 유형이 변경되었지만(예: string to boolean) Entra ID 매핑이 업데이트되지 않았습니다.
 - 해결: 특성 매핑 아래의 고급 설정에서 유형을 수동으로 수정합니다.
- 증상: 관리자 참조가 채워지지 않음
 - 근본 원인: 관리자가 되기 전에 사용자가 범위에 포함되었습니다. 프로비저닝은 자동으로 백필되지 않습니다.
 - 해결: 범위에 있는 모든 사용자를 완전히 다시 평가하도록 프로비저닝을 다시 시작합니다.

IBM 보안 특정 문제 확인

- 증상: 사용자가 프로비저닝하지만 그룹은 Secure Access에 표시되지 않음
 - 근본 원인: 사용자 지정 SCIM 커넥터가 사용자 작업만 실행하는지 확인합니다. no POST /Groups calls are ever sent (account-provisioning capability gap, not a mapping error).

- 해결: 커넥터 추적을 캡처하고 /그룹 통화가 발생하는지 확인합니다. 없는 경우 Cisco AD Connector, CSV 가져오기 또는 Secure Access SCIM 엔드포인트에 대한 예약된 스크립트를 통해 그룹을 프로비저닝합니다.
- 증상: 그룹 구성원 업데이트가 400 또는 404로 실패
 - 근본 원인: members[].value references 사용자 생성 시 반환된 SCIM ID Secure Access 대신 내부 사용자 ID를 확인합니다.
 - 해결: Secure Access SCIM ID를 사용하도록 구성원 매핑을 수정하고 전체 동기화를 다시 실행합니다.
- 증상: 그룹이 표시되지만 비어 있습니다.
 - 근본 원인: 구성원 사용자가 Secure Access에 존재하기 전에 푸시된 그룹; 멤버 자격 패치가 알 수 없는 사용자를 참조했습니다.
 - 해결: 사용자가 존재하므로 전체 동기화를 다시 실행합니다. 동기화 순서에 따라 그룹 앞에 사용자가 생성되는지 확인합니다.
- 증상: SAML 로그인 루프 또는 반복된 리디렉션
 - 근본 원인: IdP 엔드포인트가 SWG에 의해 프록시되거나 암호 해독되었는지 확인합니다. 그러면 인증 흐름이 중단됩니다.
 - 해결: SAML 또는 암호 해독(외부 도메인 목록 또는 선택적 암호 해독)에서 Verify IdP URL을 우회합니다.
- 증상: 사용자가 SAML을 통해 인증하지만 사용자 기반 정책 일치 없음
 - 근본 원인: SAML NameID가 프로비저닝된 사용자 authName과 일치하지 않습니다.
 - 해결: Verify SAML 응용 프로그램에서 NameID > 형식을 authName 특성 매핑(대개 이메일 또는 UPN)과 맞춥니다. 다시 테스트합니다.
- 증상: 몇 주 또는 몇 개월에 걸친 안정성 유지 후 프로비저닝 중단
 - 근본 원인: SCIM 토큰이 Secure Access에서 회전되거나 만료되었지만 Verify 커넥터에서 업데이트되지 않았습니다.
 - 해결: Secure Access에서 토큰을 새로 고치고 Verify custom application(사용자 지정 애플리케이션 확인)에서 토큰을 업데이트합니다. 새로 고침 범위의 달력을 지정합니다.
- 증상: 재동기화 시 중복된 사용자가 생성됨
 - 근본 원인: 외부ID가 변경 가능 또는 고유하지 않은 특성(예: 표시 이름, 변경 가능한 이메일)에 매핑되었습니다.
 - 해결: 외부 ID를 변경할 수 없는 식별자에 매핑합니다(사용자 ID 또는 objectGUID 확인). 중복 항목을 정리하고 다시 동기화합니다.

- 증상: 비활성화 사용자가 보안 액세스에서 활성 상태를 유지하는지 확인
 - 근본 원인: Suspend 작업이 active:false에 매핑되지 않거나 커넥터에서 비활성화된 작업을 비활성화합니다.
 - 해결: 비활성화 작업을 활성화하고 suspend를 active:false로 매핑합니다. 테스트 사용자에게 확인합니다.
- 증상: Verify(확인)의 특성 변경 사항이 전파되지 않습니다.
 - 근본 원인: 사용자 또는 특성이 프로비저닝 정책 범위를 벗어나거나 업데이트 작업을 사용할 수 없습니다.
 - 해결: 애플리케이션 프로비저닝 정책 또는 자격 검토 업데이트 활성화; 수동 동기화를 트리거합니다.
- 증상: Secure Access에서 스키마 또는 501 스타일 오류가 있는 요청을 거부합니다.
 - 근본 원인: SCIM 규격이 아닌 페이로드(스키마 배열 누락, 잘못된 URN, 지원되지 않는 작업).
 - 해결: 기본 컬 테스트를 사용하여 재현합니다. 페이로드 또는 매핑 수정 커넥터에서 잘못된 형식의 요청이 발생하면 IBM으로 에스컬레이션합니다.
- 증상: SAML이 작동하지만 로밍 사용자에게 대한 SWG ID가 없습니다.
- 근본 원인: 수동 또는 에이전트 기반 ID를 사용하는 구축 모드의 ID를 구동하려면 SAML이 필요합니다.
- 해결: Secure Access 설명서에 대한 각 구축 모드의 ID 획득 방법을 확인합니다. SAML을 유일한 ID 소스로 설계하지 마십시오.

일반 SCIM 문제

기본 전송이 표준 SCIM 2.0이기 때문에 Cisco에 국한되지 않지만 Secure Access 구축에서 일관되게 나타납니다.

- 격리 상태는 개별 오류를 숨깁니다. 동기화가 사용자별로 실패하는 것이 아니라 완전히 중단된 것처럼 보일 경우 개별 특성 문제를 조사하기 전에 애플리케이션 수준 격리 또는 중단 상태를 확인하십시오.
- 409 비활성화 시 충돌: IdP가 사용자를 비활성화하려고 시도하고 대상이 충돌을 발생시키는 일반적인 패턴입니다. 이는 일반적으로 활성 특성 매핑 또는 그룹 범위 문제이지 실제 시스템 오류가 아닙니다.

- 비어 있거나 지워진 필드가 항상 전파되는 것은 아닙니다. 일부 SCIM 서버 구현에서는 null이 아닌 마지막 값을 유지합니다. IdP에서 필드를 지우면 먼저 자리 표시자 값을 밀어넣어야 할 수 있습니다.
- URL 또는 컨피그레이션 변경이 자동으로 인증을 무효화합니다. SCIM 엔드포인트 URL을 변경하려면 일반적으로 베어러 토큰을 다시 제공해야 합니다. 실제 문제가 오래된 토큰인 경우에도 오류가 잘못된 URL로 표시됩니다.
- 네이티브 Webhook 또는 이벤트 스트림 없음: 사용자 또는 정책 변경에 대한 실시간 푸시 알림이 필요한 자동화는 보고 API를 폴링하거나 Cisco XDR을 통해 통합해야 합니다. Secure Access는 아웃바운드 프로비저닝 웹훅을 내보내지 않습니다.

이전 단계에서 문제가 해결되지 않을 경우 IdP 측에서 프로비저닝 로그를 사용하여 Cisco TAC로 에스컬레이션합니다. 보안 액세스 측의 백엔드 프로비저닝 로그는 일반적으로 가져오려면 TAC 액세스가 필요합니다.

원인

SCIM 프로비전 통합에서 베어러 토큰이 만료되었거나, 특성 매핑이 일치하지 않거나, 대상 그룹이 없거나, 프로비전 범위가 부족하여 하나 이상의 레코드를 푸시하지 못했습니다.

관련 콘텐츠

- Cisco: [Entra ID를 통한 보안 액세스를 위해 사용자 및 그룹 프로비저닝](#)
- Cisco: [OKTA를 통한 액세스 보안을 위해 사용자 및 그룹 프로비저닝](#)
- Microsoft Learn: SCIM 2.0 프로토콜 규정 준수와 관련된 알려진 문제 - Microsoft Entra ID
- Microsoft Learn: Microsoft Entra ID SCIM API 오류 트러블슈팅
- ID 공급자에서 SAML SSO를 구성합니다. <https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider>
- 사용자 지정(SCIM) 애플리케이션에 대한 프로비저닝: <https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications>
- 프로비저닝 및 거버넌스 개요(일반 SCIM 커넥터): <https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance>

- 온프레미스 프로비저닝 브리지(AD/LDAP 소스): <https://docs.verify.ibm.com/verify/docs/on-premises-provisioning>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.