Active Directory 및 Microsoft EntraID와 Cisco Secure Access ID 동기화

목차

문제

사용자는 Cisco Secure Access에서 동일한 도메인 이름을 가진 두 ID 소스의 사용자와 그룹을 프로비저닝하려고 시도할 때 문제가 발생했습니다. 특정 시나리오에는 온프레미스 Active Directory와 Microsoft EntraID(이전의 Azure AD)의 ID를 동기화하는 작업이 포함되었습니다. 두 소스에서 모두 동일한 도메인 이름(예: domain.com)을 사용했습니다.

주요 관심사는 다음과 같습니다.

- 동일한 사용자 및 그룹이 두 ID 소스에 있을 때 ID 소유권 및 그룹 구성원 매핑 작동 방식 이해
- 온프레미스 및 클라우드 리소스에 액세스하는 하이브리드 사용자를 위해 일관된 보안 액세스 정책 적용 보장
- 이 하이브리드 ID 컨피그레이션의 사용자에 대한 내부 IP 가시성 유지
- 두 소스의 동시 동기화가 운영 환경에 문제를 일으키는지 확인

설명서에는 "Cisco AD Connector 및 Cisco User Management for Secure Access 앱에서 동일한 사용자 및 그룹을 동시에 동기화하는 것은 지원되지 않으며 일관되지 않은 액세스 규칙 시행으로 이어집니다."라고 명시되어 있습니다.

환경

- AD 커넥터 및 EntraID 통합을 통한 Cisco Secure Access
- 도메인 이름이 EntraID 도메인과 일치하는 온-프레미스 Active Directory
- 온-프레미스 AD와 도메인 이름이 같은 Microsoft EntraID(Azure AD)

- ID 페더레이션을 위한 SAML SSO 컨피그레이션
- 정책 시행을 위한 SWG(Secure Web Gateway) 모듈
- 온프레미스 및 클라우드 리소스에 모두 액세스해야 하는 하이브리드 환경

해결

Active Directory 및 EntraID 소스 모두에서 동시 동기화를 위해 다음 동작이 확인되었습니다.

그룹 동기화 동작

두 소스에서 이름이 같은 그룹을 동기화하는 경우:

- Cisco Secure Access에서 두 개의 개별 그룹 객체가 생성되며 각 소스에서 하나씩 생성됩니다.
- 그룹은 액세스 정책에서 소스 접두사로 구분할 수 있습니다
- 온-프레미스 AD 그룹은 다음과 같이 표시됩니다. AD-도메인/그룹 이름
- ID 그룹은 다음과 같이 표시됩니다. 그룹 이름

랩 확인에서 "성공"이라는 메시지와 성공적으로 동기화되었습니다. <<<< Synced" - 여러 EntraID 도메인의 그룹

사용자 동기화 동작

두 소스에서 동일한 사용자 ID로 사용자를 동기화하는 경우:

- 동기화 중에 사용자 ID를 덮어씁니다.
- Secure Access에서는 고유한 사용자 ID가 하나만 표시됩니다.
- 최종 동기화 원본은 사용자의 특성 및 그룹 멤버십을 결정합니다

- ENTRAID 동기화는 일반적으로 둘 다 구성된 경우 온프레미스 AD보다 우선합니다

액세스 정책 컨피그레이션

액세스 정책에서 두 그룹 유형을 모두 사용할 수 있습니다.

- 전체 경로를 사용하여 온-프레미스 AD 그룹 참조: AD-도메인/그룹 이름
- 간단한 이름을 사용하여 EntraID 그룹을 참조합니다. 그룹 이름
- 정책은 그룹 멤버십 소스에 따라 사용자를 구분할 수 있습니다.

Following Set up은 많은 고객에게 적합합니다.

```
1    Only provision identities from on-prem AD - for VA DNS protection
2    Use Azure entra for SSO/user authentication (no identities to be provisioned from Azure) - for SWG
```

원인

테스트 중에 사용자가 온프레미스 AD 커넥터에서 동기화될 때마다 Umbrella 대시보드에서 ID를 효과적으로 "클레임"하는 것을 확인했습니다. 동일한 사용자가 Azure AD 동기화를 통해 이미 존재하는 경우 온-프레미스 동기화가 기존 EntraID 사용자 데이터를 덮어씁니다.

이러한 동작은 문서화된 제한입니다. Cisco의 공식 기술 문서에 따르면: https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

"Umbrella AD Connector 및 Cisco Umbrella Azure AD 앱에서 동일한 사용자 및 그룹 ID의 동시 동기화는 지원되지 않으며 일관되지 않은 정책 시행으로 이어집니다."

결론: 원하는 설정(Azure 및 On-Prem 모두에 존재하는 사용자의 VA 가시성)이 지원되지 않는 구성인 것으로 확인되었습니다.ID를 일관성 있게 적용하려면 로밍 클라이언트를 사용해야 합니다.

관련 콘텐츠

- Azure AD에서 ID 프로비저닝 - Cisco Umbrella 설명서
- Cisco 기술 지원 및 다운로드

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.