Secure Access AD Connector를 레거시 인증에서 API 인증으로 마이그레이션

목차

문제

AD(Active Directory) 커넥터가 있는 Cisco Secure Access를 사용하는 조직은 Active Directory 및 가상 어플라이언스에 대해 API 인증이 권장됨을 알리는 알림을 받습니다. 레거시 인증은 2026년 5월 29일에 만료됩니다. 사용자는 만료일 전에 레거시 인증에서 API 인증으로 마이그레이션하기 위해 컨피그레이션 지원이 필요하며 마이그레이션 프로세스 동안 AD 및 가상 어플라이언스 동기화에 미칠 수 있는 영향을 알고 싶어합니다. 주 관심사는 근무 시간 동안 이 변경 사항을 구현하면 ID 및 정책 종속 작업에 영향을 줄 수 있는 AD 및 VA 동기화 작업에 장애가 발생할 수 있는지 여부입니다.

환경

- Cisco Secure Access(이전의 Cisco Umbrella)
- Active Directory Connector 구축
- 현재 사용 중인 레거시 인증 방법
- 2026년 5월 29일 이전에 필요한 API 인증 마이그레이션
- AD 전용 환경(경우에 따라 가상 어플라이언스 없음)

해결

레거시 인증에서 API 인증으로 마이그레이션하려면 Secure Access 포털에서 API 키를 생성하고 올바르게 구성해야 합니다. 이 프로세스에서는 AD 커넥터 및 가상 어플라이언스에 대한 관리 API 키와 클라이언트 API 키를 모두 생성해야 합니다.

1단계: 관리 API 키 생성

Secure Access 포털에서 Admin(관리) > API Keys(API 키)로 이동하여 새 Admin API Key(관리 API 키)와 Admin Key Secret(관리 키 암호)를 생성합니다. 클라이언트 API 키 쌍을 생성하는 데 필요한 경우 이러한 자격 증명을 안전하게 저장합니다.

2단계: 클라이언트 API 키 쌍 생성

Users and Groups(사용자 및 그룹) > Configuration Management(컨피그레이션 관리) > Advanced Settings(고급 설정)로 이동하고 API Authentication(API 인증) 섹션을 찾습니다. 1단계에서 생성한 Admin API Key 및 Admin Key Secret을 입력한 다음 Generate Client API Key Pair(클라이언트 API 키 쌍 생성)를 클릭합니다. 이렇게 하면 AD 커넥터 및 가상 어플라이언스에서 사용되는 클라이언트 API 키 및 클라이언트 암호가 생성됩니다.

3단계: 고급 설정에서 API 인증 구성

생성된 클라이언트 API 키 및 클라이언트 암호를 Secure Access 포털의 API Authentication Advanced Settings 섹션에 복사합니다. 모든 AD 커넥터 및 가상 어플라이언스 컨피그레이션에 필요한 자격 증명을 안전하게 저장합니다.

4단계: AD 커넥터 및 가상 어플라이언스 업데이트

새로 생성된 클라이언트 API 키 및 클라이언트 암호를 구축된 모든 AD 커넥터 및 가상 어플라이언스에 적용합니다. 이렇게 하면 새 API 인증 방법을 사용하여 등록 및 상태 확인을 위해 올바르게 인증할 수 있습니다.

마이그레이션이 미치는 영향 및 모범 사례

Secure Access 포털에서 API 키를 생성하는 작업은 일반적으로 중단되지 않습니다. 그러나 AD 커넥터와 가상 어플라이언스가 새 클라이언트 API 키 및 암호를 사용하도록 업데이트되는 컷오버 순간 동안 운영상의 영향이 발생합니다.

컷오버 중 예상되는 영향:

- 레거시 인증을 사용하는 구성 요소에 대해 일시적인 동기화 및 상태 확인 오류가 발생할 수 있습니다.
- 전환 기간 중에 AD/VA 동기화 지연 또는 실패
- 동기화가 실패할 경우 새로운 ID/그룹 데이터에 의존하는 정책 결정이 영향을 받을 수 있습니다.

권장 구현 접근 방식:

- 가능한 경우 근무 외 시간 또는 유지 보수 기간 동안 마이그레이션을 수행합니다.
- 근무 시간 구현의 경우 제어된 롤링 업데이트 접근 방식을 사용합니다.
- 계속 진행하기 전에 한 번에 하나의 커넥터/VA를 업데이트하고 정상 상태를 확인합니다.
- 모든 노드를 동시에 업데이트하지 마십시오.
- 롤링 업데이트를 위해 여러 커넥터/VA로 적절한 이중화를 보장합니다.

호환성 및 요구 사항:

- API 인증은 AD 전용 구축에서 작동하며 가상 어플라이언스가 필요하지 않습니다.
- 레거시 및 API 인증 방법은 모두 마이그레이션 기간 동안 활성 상태로 유지됩니다.
- AD 커넥터는 api.opendns.com을 통해 Umbrella와 동기화하고 api.umbrella.com으로 전환할 수 있어야 합니다.

원인

Cisco Secure Access는 기존 인증 방법에서 표준 인증 메커니즘인 API 인증으로 전환되고 있습니다. 레거시 인증 방법은 예약된 감가상각 날짜가 2026년 5월 29일입니다. API 인증은 결국 지원되는 유일한 인증 방법이 되며, 조직은 서비스 중단 및 복구를 위해 전체 재설치가 필요할 수 있는 잠재적인 AD/VA 동기화 실패를 방지하려면 기존 방법이 만료되기 전에 마이그레이션해야 합니다.

관련 콘텐츠

- Cisco Secure Access API 인증 설명서

- Cisco Secure Access 고급 컨피그레이션
- Cisco Secure Access 컨피그레이션 관리
- 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.