VA 또는 CSC를 사용하여 Active Directory 통합

목차

소개

이 문서에서는 AD(Active Directory)를 Umbrella와 통합하는 두 가지 방법에 대해 설명합니다. VA(Virtual Appliance) 또는 CSC(Cisco Secure Client).

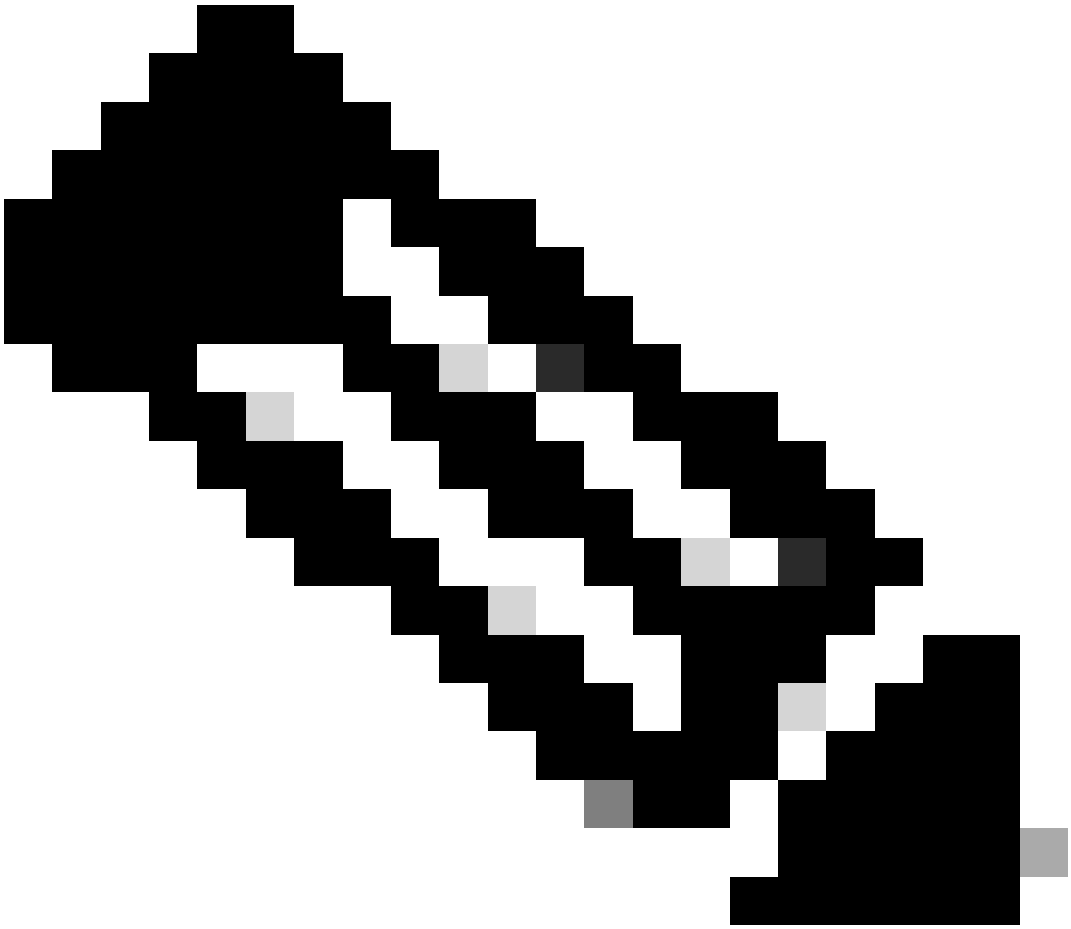
사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AD 커넥터: 단일 Active Directory 도메인의 AD 트리를 대시보드에 동기화합니다. VA 구현의 경우 동일한 Umbrella 사이트의 DC에서 VA로 로그인 이벤트를 적극적으로 동기화합니다. 조직의 AD 트리는 AD 커넥터가 Umbrella 클라우드에 동기화하여 등록된 DC에서 이 데이터를 가져옵니다. 트리 업데이트가 탐지되고 몇 시간 내에 Umbrella 클라우드가 업데이트됩니다.
- 도메인 컨트롤러(AD 서버): DC는 대시보드에서 다운로드한 대로 등록 구성 .wsf 스크립트를 통해 대시보드에 등록됩니다. 이렇게 하면 이름, 도메인 및 내부 IP가 대시보드에 추가되어 어떤 IP로 동기화를 시도할지 커넥터에 알립니다. 스크립트를 실행할 수 없는 경우 수동 등록도 가능합니다. 자세한 내용과 지원은 Umbrella Support에 문의하십시오.
- 가상 어플라이언스: Umbrella on-premise DNS 전달자입니다. 네트워크에 AD ID를 적용하고 보고서에 내부 IP를 적용합니다(선택 사항). 이렇게 하면 모든 로밍 클라이언트가 뒤에 트리거되어 DNS 보호를 사용하지 않도록 설정하고 "Behind VA protection(VA 보호 뒤)" 모드로 전환됩니다.
- Cisco Secure Client: Windows 및 macOS에 DNS 암호화 및 사용자 ID를 제공하는 Umbrella

온프레미스 소프트웨어 서비스입니다. AnyConnect 모듈로도 제공됩니다.



참고: 두 구현 간에는 사전 요구 사항이 크게 다릅니다. 전체 전제 조건은 구체적인 구현을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

이 문서에서는 Active Directory를 Umbrella Dashboard와 통합하는 두 가지 방법을 자세히 알아봅

니다. 현재 AD 사용자는 Umbrella 가상 어플라이언스 또는 Cisco Secure Client를 통해 정책 및 보고에 적용할 수 있습니다.

보안 클라이언트 구현

요구 사항

- AD 커넥터 1개
- 대시보드에 DC 1개
- OpenDNS_Connector 사용자에게는 읽기 전용 도메인 컨트롤러 권한이 있어야 합니다.
- 독립형 클라이언트(AnyConnect 모듈)용 Secure Client 최소 버전:
  - 창: 2.1.0(4.5.01044)
  - OSX: 2.0.39(4.5.02033).

운영 방식

- 현재 로그인한 AD 사용자는 로컬 레지스트리를 읽는 로밍 클라이언트가 로컬 컴퓨터에서 직접 확인합니다.
- 워크스테이션에서 최대 한 명의 동시 로그인 사용자를 지원합니다.
- 두 명의 동시 사용자가 AD 사용자가 적용되지 않을 수 있습니다.
- AD 사용자 GUID 및 내부 IP는 로밍 클라이언트의 DNS 프록시 내에서 EDNS0을 통해 Umbrella 확인기로 전송되는 DNS 쿼리에 연결되어 AD 사용자를 고유하게 식별합니다.
- 모든 정책은 확인자 측에 적용됩니다.
- 활성 커넥터는 필요하지 않습니다. 그러나 AD 사용자 및 그룹 정책 애플리케이션은 가장 최근의 성공적인 AD 트리 동기화를 반영할 수 있습니다.

작동 위치

- 전 세계의 모든 네트워크.
- DNS 레이어가 로컬 VA를 지연하도록 비활성화되어 있으므로 Umbrella 가상 어플라이언스 뒤에서 작동하지 않습니다.

제한 사항

- 워크스테이션에서 활성화된 엔드포인트 에이전트가 필요합니다.
- 서버 OS를 지원하지 않습니다.
- 내부 네트워크 IP를 기반으로 정책을 적용할 수 없습니다.
- AD 컴퓨터에 정책 또는 보고를 적용할 수 없습니다(대신 로밍 호스트 이름 사용).

커넥터는 등록된 DC에서 AD 로그인 이벤트를 가져오려고 시도할 수 있습니다. 이로 인해 로밍 클라이언트 기반 AD 통합과 관련이 없는 대시보드 오류가 발생할 수 있습니다. 실제로 이벤트를 가져오지 않고 로그인 이벤트 폴링과 관련된 권한 오류를 제거하려면 여기에서 감사 명령의 반대로 로그인 이벤트 감사(사용하지 않는 경우)를 비활성화합니다.

가상 어플라이언스 구현

요구 사항

- Umbrella 사이트당 2개의 VA
- Umbrella 사이트당 AD 커넥터 1개(이중화된 두 번째, 선택 사항)
- 모든 DC(읽기 전용 DC가 아님)는 대시보드에 등록해야 합니다.
- OpenDNS_Connector 사용자에게는 전체 필수 구성 요소 권한 집합이 있어야 합니다.
- 모든 DC에 4624 보안 이벤트 로그를 기록하려면 로그인 이벤트를 활성화해야 합니다. 전체 문제 해결 팁을 참조하십시오.

운영 방식

- VA는 Windows DC의 보안 로그인 이벤트 로그를 기반으로 AD 사용자 매핑을 수신합니다.
- 각 워크스테이션 로그인은 AD 사용자 이름 또는 AD 컴퓨터 이름과 워크스테이션의 내부 IP를 사용하여 고유한 로그인 이벤트로 로그인 서버 DC의 보안 이벤트 로그에 기록됩니다.
- 커넥터는 WMI 구독을 통해 이러한 이벤트를 실시간으로 구문 분석하고, TCP 443을 통해 이러한 이벤트를 Umbrella 사이트의 각 VA에 동기화합니다.
- VA는 AD 사용자/컴퓨터의 내부 IP와 AD 사용자/컴퓨터의 사용자 이름 간에 라이브 사용자 매핑을 구축합니다.
- VA는 DNS 쿼리의 내부 소스 IP에 대한 가시성만 가지며 커넥터 동기화 이벤트에서 생성한 앞서 언급한 매핑 파일을 사용합니다. VA는 현재 시스템에 로그인한 사용자를 직접 확인할 수 없습니다. 이렇게 하면 AD 사용자 GUID와 EDNS0을 통한 내부 IP가 VA에 의해 Umbrella 리졸버로 전송된 DNS 쿼리에 추가되어 AD 사용자를 고유하게 식별합니다.
- AD 컴퓨터 해시도 같은 방식으로 적용됩니다.
- 모든 정책은 확인자 측에 적용됩니다.
- AD 사용자를 받으려면 조직에서 커넥터가 작동하고 활성화되어 있어야 하며 로그인 이벤트가 최신 상태여야 합니다.
- 사용자는 이벤트 로그에 표시된 대로 이 시스템을 인증할 마지막 AD 사용자여야 합니다.

작동 위치

모든 DNS가 사용자가 인증한 DC와 동일한 Umbrella 사이트에 속한 Umbrella 가상 어플라이언스를 가리키는 로컬 기업 네트워크입니다.

제한 사항

- 컴퓨터는 다른 AD 도메인 또는 Umbrella 사이트에 속한 VA를 가리킬 수 없습니다(여러 도메인의 대규모 구축에서는 기본 네트워크의 AD 애플리케이션을 볼 수 없음).
- 대규모 구축에서는 별도의 VA를 사용하여 Umbrella 사이트로 세분화해야 할 수 있습니다.
- 서비스 AD 사용자에 대해 AD 사용자 예외가 필요할 수 있습니다.
- 앞서 언급한 커넥터에 대한 초당 최대 로그인 이벤트 처리량이 있으며, 이로 인해 사용자 애플리케이션이 지연될 수 있습니다. 이는 네트워크 레이턴시 및 VA 수의 요인입니다.

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.