Umbrella Active Directory 통합 흐름 검토

목차

소개

이 문서에서는 Cisco Umbrella Active Directory(AD) 통합의 운영 구성 요소 간 통신 흐름에 대해 설명합니다.

배경 정보

Active Directory 통신 흐름을 이해하면 문제를 해결하고 구축 전에 올바르게 구성된 환경을 확인하는 데 도움이 될 수 있습니다.

Umbrella Active Directory 구현과의 통신 흐름

AD 커넥터 스크립트가 DC(도메인 컨트롤러)에서 실행되는 경우

Windows 스크립트는 HTTPS를 사용하여 DC(Domain Controller)에서 TCP/443 포트의 클라우드로 1회 연결하여 DC를 대시보드에 등록합니다. 이 등록을 통해 커넥터는 DC를 인식할 수 있습니다. 특정 매개변수를 사용하여 **https://api.opendns.com** 로 호출됩니다. 스크립트가 DC를 성공적으로 등록하면 대시보드에 표시됩니다.

Windows의 루트 인증서 업데이트와 관련된 문제가 있을 수 있습니다. 이를 신속하게 확인하려면 Internet Explorer로 이동하여 브라우저에서 다음 작업을 수행하도록 합니다. https://api.opendns.com/v2/OnPrem.Asset. 이 작업은 If any certificate errors or warnings(인증서 오류 또는 경고가 해당 페이지에 나타나면 Microsoft의 최신 루트 인증서 업데이트가 설치되어 있는지 확인합니다)와 같은 메시지를 **1005 Missing API key**. 인쇄합니다.

AD 커넥터의 통신 방식

AD 커넥터는 다음과 같이 Umbrella Cloud 서비스 또는 Virtual Appliance와 통신합니다.

- 클라우드에 대한 커넥터

  커넥터는 변경이 발생하면 5분마다 포트 443 TCP의 HTTPS 연결을 사용하여 모든 AD(Active Directory) 데이터를 업로드합니다. 그룹, 사용자 및 컴퓨터에 대한 정보만 업로드됩니다. 비밀번호는 업로드되지 않으며 모든 사용자 정보가 로컬로 해시되어 데이터가 고유하게 됩니다.

- 가상 어플라이언스에 대한 커넥터

  커넥터는 포트 443 TCP(암호화되지 않음)를 사용하여 가상 어플라이언스에 AD 이벤트를 지속적으로 전송합니다. 이는 단방향 통신입니다. 어플라이언스는 커넥터로 다시 통신하지 않습니다. 커넥터와 VA(Virtual Appliance)가 신뢰할 수 있는 네트워크를 통해 통신해야 하는 필수 전제 조건입니다.

- 도메인 컨트롤러에 대한 커넥터

  커넥터는 LDAP 동기화를 위해 포트 389 TCP 및 3268 TCP/UDP를 사용하여 동일한 사이트에 있는 모든 도메인 컨트롤러와 통신합니다. 또한 커넥터는 WMI/RPC를 사용하여 도메인 컨트롤러와 통신합니다. 포트 135 TCP는 RPC 및 WMI의 표준 포트입니다. WMI는 또한 Windows 2003 이상의 경우 1024 TCP와 65535 TCP 사이, 또는 Windows 2008 이상의 경우 49152 TCP와 65535 TCP 사이에 임의로 할당된 포트를 사용합니다. 버전 1.1.24부터 커넥터는 포트 636 TCP 및 3269 TCP를 통해 LDAPS(LDAP over SSL)를 사용하여 도메인 컨트롤러와 통신합니다.

통신 문제가 관찰되면 데이터를 차단하거나 삭제할 수 있는 모든 Layer-7 애플리케이션 프록시를 확인합니다. 일반적인 경우는 DNS, HTTP 또는 HTTPS와 같은 프로토콜에 작동하는 Cisco 디바이스의 검사 기능입니다. 자세한 내용은 Application Layer Protocol Inspection 적용에 대한 설명서를 참조하십시오.

VA(Virtual Appliances)에서 클라우드로

가상 어플라이언스는 포트 443 TCP에서 DNS 쿼리 또는 프로브에 대해 53 TCP/UDP와 **api.opendns.com**지원 터널을 설정하기 위해 22, 25, 53, 80, 443 또는 4766 TCP와 자주 통신합니다. 가상 어플라이언스는 53 UDP/TCP, 443 TCP, 123 TCP 및 80 TCP 포트를 사용하여 클라우드와 통신합니다. 포트 443 TCP(HTTPS 연결이 아님)의 커넥터에서 데이터를 수신하지만, 이에 대한 통신이 다시 필요하지 않습니다.

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.