Umbrella Active Directory의 로컬 계정에 정책 적용

목차

소개

Umbrella Virtual Appliance 및 로컬 계정 ID

- Umbrella Virtual Appliance 권장 사항

Umbrella Roaming 클라이언트 및 로컬 계정 정책

- Umbrella Roaming Client 권장 사항

소개

이 문서에서는 Umbrella 온프레미스 제품을 Active Directory 및 로컬 사용자 계정과 동기화할 때의 예상 정책 동작에 대해 설명합니다.

Umbrella Virtual Appliance 및 로컬 계정 ID

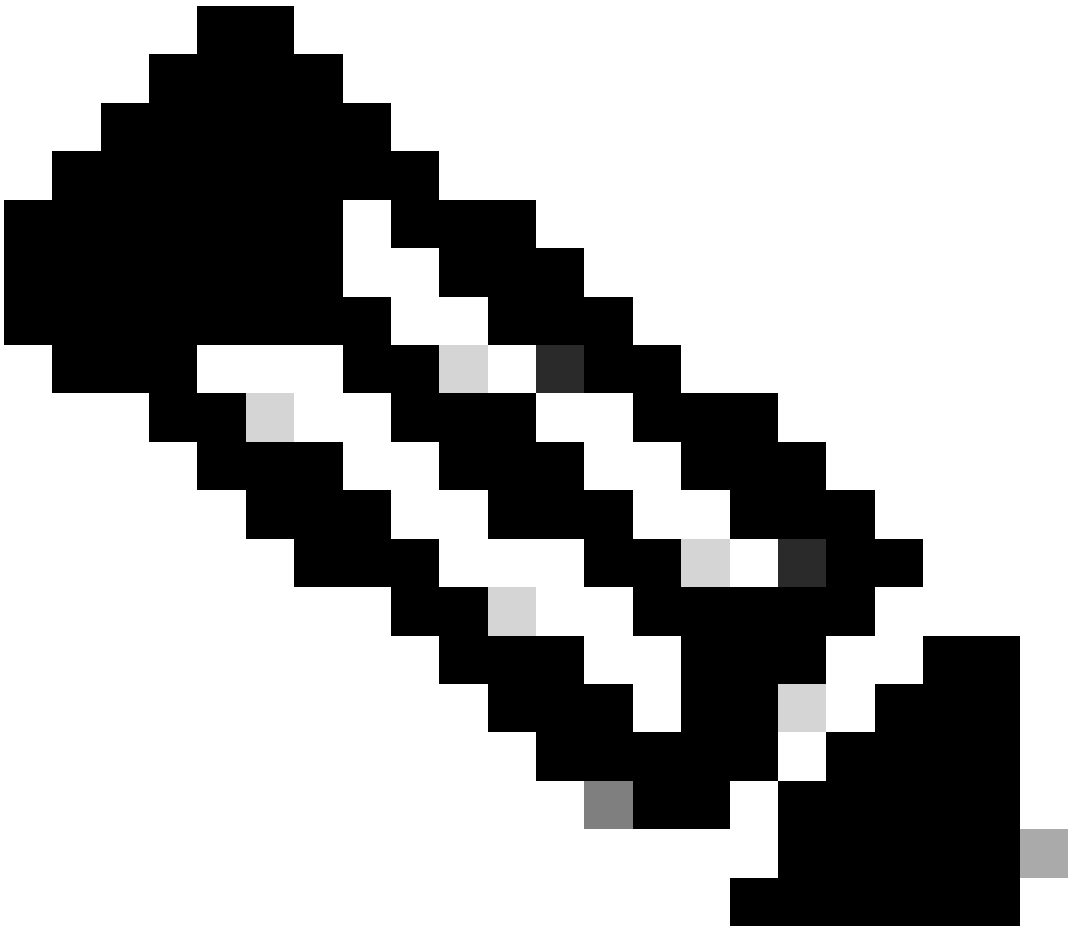
Umbrella Virtual Appliance는 Windows 도메인 컨트롤러로부터 Active Directory 로그온 정보를 수신합니다. 소스 IP 주소를 기반으로 Active Directory 사용자를 캐시하고 식별합니다.

- 도메인 컨트롤러는 로컬 사용자 로그온을 추적하지 않으므로 이러한 사용자를 가상 어플라이언스에서 직접 식별할 수 없습니다.
- Active Directory 사용자가 IP 주소에서 최근에 로그인한 경우에도 캐시의 ID를 계속 사용할 수 있습니다. Virtual Appliance는 AD 사용자가 로컬 계정으로 대체되었음을 알 수 없습니다.
- 캐시된 사용자가 없는 경우 가상 장치는 기본(비 AD) ID를 사용합니다. 트리거된 ID는 다음 중 하나일 수 있습니다.
  - Umbrella 사이트 이름(예: 기본 사이트)
  - 내부 네트워크(내부 IP 주소)
  - 네트워크(외부 IP 주소)

Umbrella Virtual Appliance 권장 사항

- 로컬 계정 및 비밀번호에 대한 액세스를 제한합니다.
- Umbrella 사이트 이름에 대한 별도의 정책을 생성합니다(예: 기본 사이트). 이 정책을 표준 Active Directory 사용자 정책보다 낮은 우선 순위를 할당합니다. 이 더 제한적인 정책은 AD 사용자가 탐지되지 않을 때 적용됩니다.
- 로컬 사용자 계정에 대해 다른 정책이 필요한 경우 Umbrella Roaming Client 구축을 고려하십시오.

Umbrella Roaming 클라이언트 및 로컬 계정 정책



참고: Active Directory와 로밍 클라이언트 통합을 사용하려면 Identities(ID) > Roaming Computers(로밍 컴퓨터)로 이동하여 Enable Active Directory user and group policy enforcement(Active Directory 사용자 및 그룹 정책 시행 활성화) 설정을 활성화합니다.

로밍 클라이언트는 Windows 레지스트리에서 로그온한 사용자를 검색하여 고유한 AD GUID를 통해 Active Directory 사용자를 식별할 수 있게 합니다.

- 로밍 클라이언트는 정책상 로컬 사용자 이름을 식별할 수 없습니다.
- AD 사용자가 탐지되면 AD 사용자 ID가 정책 시행에 적용되며, 여기에는 네트워크 외부 동안 캐시된 자격 증명으로 로그인한 AD 사용자가 포함됩니다.
- AD 사용자가 탐지되지 않은 경우(예: 로컬 사용자가 로그온된 경우) 정책 시행을 위해 로밍 컴퓨터 ID가 사용됩니다.

Umbrella Roaming Client 권장 사항

- 로컬 계정 및 비밀번호에 대한 액세스를 제한합니다.
- 표준 AD 사용자 정책보다 우선 순위가 낮은 로밍 컴퓨터에 대해 별도의 정책을 만듭니다. 이 정책은 도메인에 가입되지 않았거나 로컬 사용자가 사용하지 않는 로밍 컴퓨터에 적용됩니다.

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.