Beleid toepassen voor lokale accounts in Umbrella Active Directory

Inhoud

Inleiding

In dit document wordt het verwachte beleidsgedrag beschreven bij het synchroniseren van lokale producten van Umbrella met Active Directory en lokale gebruikersaccounts.

Umbrella Virtual Appliance en lokale accountidentificatie

De Umbrella Virtual Appliance ontvangt aanmeldingsgegevens voor Active Directory van Windows Domain Controllers. Het cachet en identificeert Active Directory-gebruikers op basis van hun IP-adres van de bron.

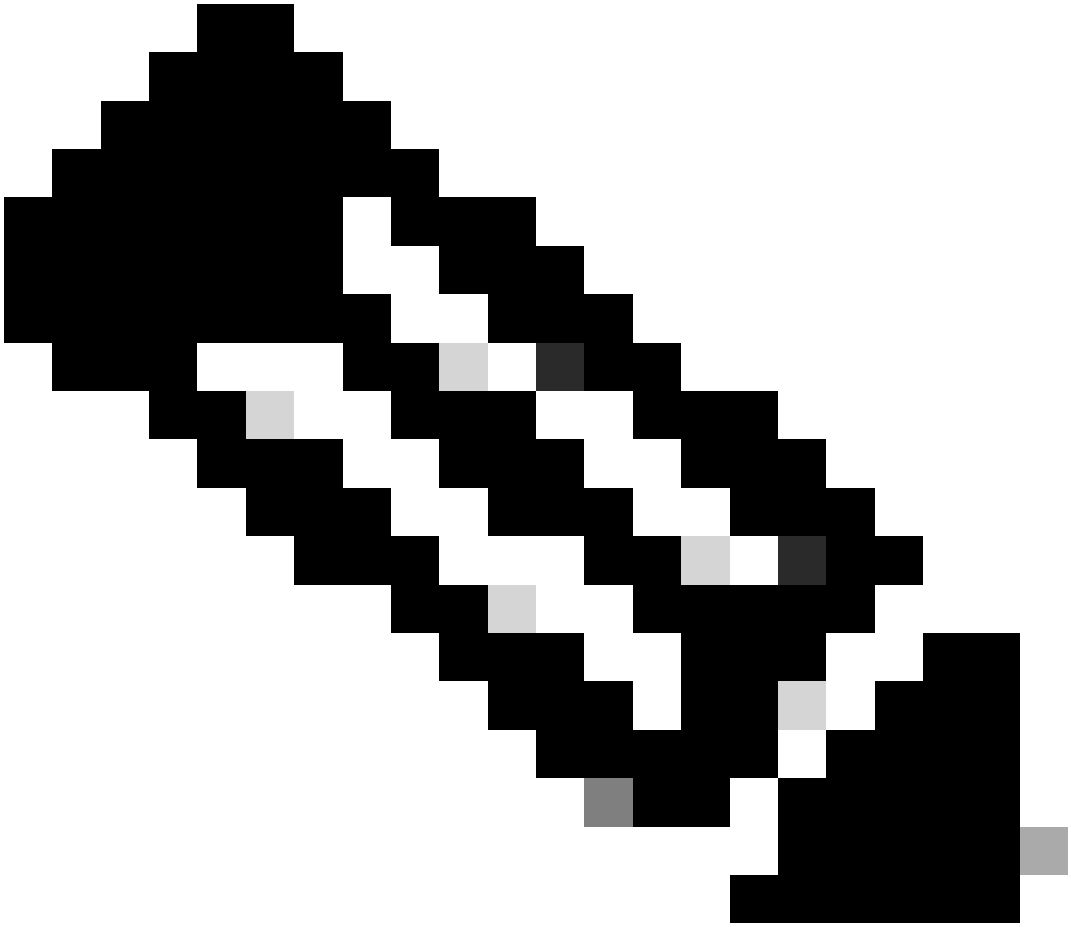
- De domeincontroller houdt de lokale gebruikersaanmeldingen niet bij, zodat deze gebruikers niet rechtstreeks door het virtuele apparaat kunnen worden geïdentificeerd.
- Als een Active Directory-gebruiker zich onlangs heeft aangemeld vanaf een IP-adres, kan de identiteit in de cache nog steeds worden gebruikt op basis van onze cache. Het virtuele apparaat kan niet weten of de AD-gebruiker is vervangen door een lokaal account.
- Als er geen gebruiker in de cache aanwezig is, gebruikt het virtuele toestel een standaard (niet-AD)-identiteit. De getriggerde identiteit kan zijn:
  - Naam van overkoepelende site (bijvoorbeeld Standaardsite)
  - Intern netwerk (intern IP-adres)
  - Netwerk (extern IP-adres)

Aanbevelingen voor Umbrella Virtual Appliance

- Toegang tot lokale accounts en wachtwoorden beperken.
- Maak een apart beleid voor de naam van de overkoepelende site (bijvoorbeeld Standaardsite). Wijs dit beleid een lagere prioriteit toe dan uw standaard Active Directory-gebruikersbeleid. Dit restrictievere beleid is van toepassing wanneer er geen AD-gebruiker wordt gedetecteerd.
- Als u andere beleidsregels voor lokale gebruikersaccounts nodig hebt, kunt u overwegen de

Umbrella Roaming Client te implementeren.

Overkoepelende klant- en lokaal accountbeleid



Opmerking: Als u Active Directory-integratie met de zwervende client wilt gebruiken, gaat u naar Identiteiten > Zwervende computers en schakelt u de instelling Active Directory-gebruiker en groepsbeleidshandhaving inschakelen in.

De zwervende client detecteert ingelogde gebruikers uit het Windows-register, zodat gebruikers van Active Directory kunnen worden geïdentificeerd aan de hand van hun unieke AD GUID.

- De roamende klant kan geen lokale gebruikersnamen identificeren voor beleidsdoeleinden.
- Wanneer een AD-gebruiker wordt gedetecteerd, is de AD-gebruikersidentiteit van toepassing op de handhaving van het beleid, inclusief AD-gebruikers die zijn aangemeld met referenties in de cache terwijl ze buiten het netwerk zijn.

- Als er geen AD-gebruiker wordt gedetecteerd (bijvoorbeeld wanneer een lokale gebruiker is aangemeld), wordt de identiteit van de Zwervende computer gebruikt voor beleidshandhaving.

Aanbevelingen voor Umbrella Roaming Client

- Toegang tot lokale accounts en wachtwoorden beperken.
- Maak een apart beleid voor zwervende computers met een lagere prioriteit dan uw standaard AD-gebruikersbeleid. Dit beleid is van toepassing op roamingcomputers die niet zijn aangesloten op het domein of die worden gebruikt door lokale gebruikers.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.