Active Directory integreren met VA of CSC

Inhoud

Inleiding

In dit document worden twee methoden beschreven voor de integratie van Active Directory (AD) met Umbrella: Virtual Appliance (VA) of Cisco Secure Client (CSC).

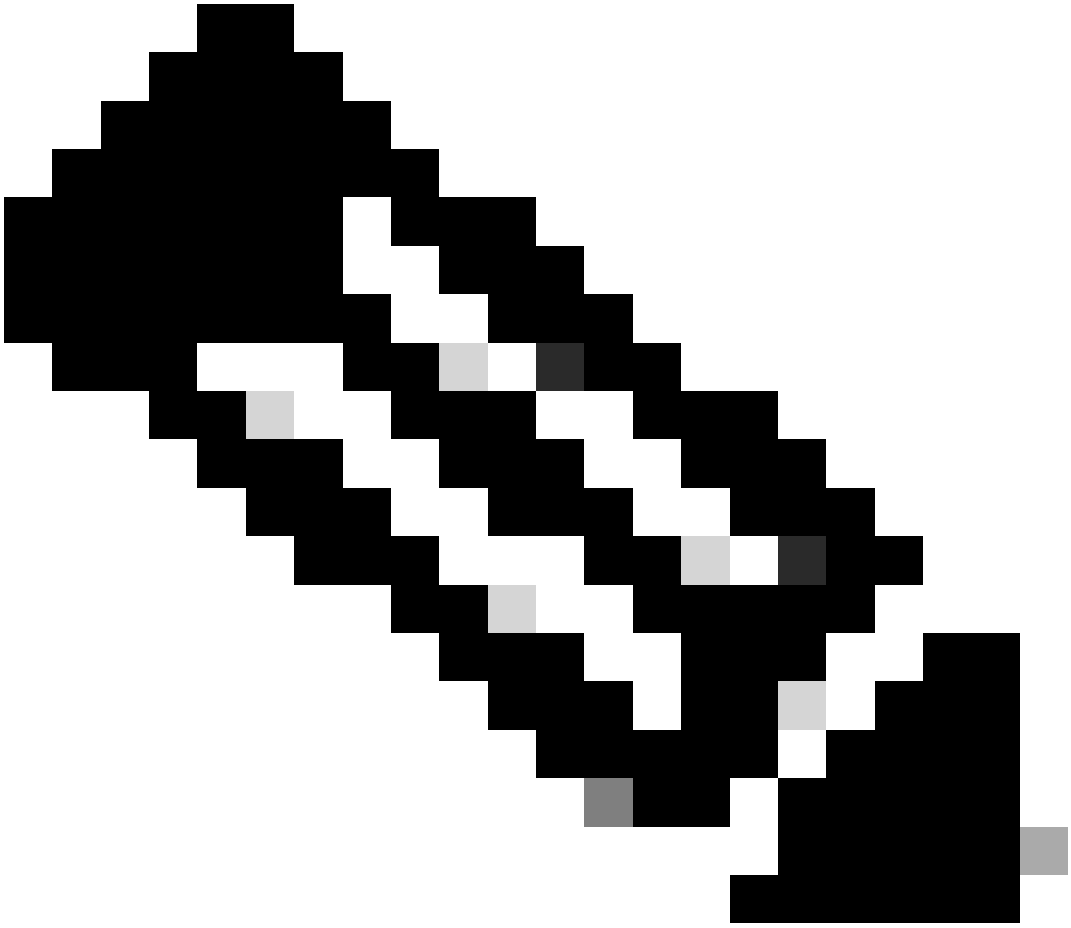
Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- AD Connector: hiermee wordt de AD-structuur van één Active Directory-domein gesynchroniseerd met het dashboard. Voor de VA-implementatie synchroniseert het ook actief de inloggebeurtenissen van de DC's op dezelfde Umbrella-site met de VA's. De AD-structuur voor de organisatie wordt gesynchroniseerd met de Umbrella Cloud door de AD Connector, waardoor deze gegevens uit de geregistreerde DC worden gehaald. Er worden boomupdates gedetecteerd en de Umbrella Cloud wordt binnen enkele uren bijgewerkt.
- Domain Controller (AD Server): DC's worden geregistreerd op het dashboard via het .wsf-script voor de registratieconfiguratie zoals gedownload van het dashboard. Hiermee worden de naam, het domein en het interne IP-adres aan het Dashboard toegevoegd om de Connector te laten weten met welke IP's moet worden gesynchroniseerd. Als u het script niet kunt uitvoeren, is handmatige registratie ook mogelijk. Neem contact op met Umbrella Support voor meer informatie en ondersteuning.
- Virtual Appliance: de paraplu op locatie DNS-forwarder. Hiermee past u een (optionele) AD-

identiteit toe op het netwerk en interne IP's op rapporten. Dit zorgt ervoor dat alle roamende clients erachter DNS-bescherming uitschakelen en de modus "Achter VA-bescherming" uitstellen.
- Cisco Secure Client: De Umbrella on premise-softwaredienst die DNS-codering en gebruikersidentificatie biedt voor Windows en macOS. Het wordt ook geleverd als een AnyConnect-module.



Opmerking: de vereisten verschillen aanzienlijk tussen de twee implementaties. Raadpleeg de specifieke implementatie voor de volledige vereisten.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Overzicht

Dit artikel verduidelijkt en verkent de twee verschillende methoden voor het integreren van Active Directory met het Umbrella Dashboard. Momenteel kunnen AD-gebruikers worden toegepast op beleid en rapportage via de virtuele apparaten van Umbrella of de Cisco Secure Client.

Beveiligde clientimplementatie

Vereisten

- Eén AD-connector
- Een DC op het dashboard
- OpenDNS_Connector-gebruiker moet toestemming hebben voor alleen-lezen domeincontroller.
- Minimumversies van Secure Client voor de zelfstandige client (AnyConnect-module):
  - Windows: 2.1.0 (4.5.01044)
  - OSX: 2.0.39 (4.5.02033).

Hoe het werkt

- De momenteel ingelogde AD-gebruiker wordt rechtstreeks op de lokale computer bepaald door de roamende client die het lokale register leest.
- Ondersteunt maximaal één gelijktijdig ingelogde gebruiker op het werkstation.
- Twee gelijktijdige gebruikers kunnen ertoe leiden dat er geen AD-gebruiker wordt toegepast.
- De AD-gebruikershandleiding en interne IP worden via EDNS0 in de DNS-proxy van de roamende client gekoppeld aan de DNS-query die naar de overkoepelende resolvers wordt verzonden, waardoor de AD-gebruiker uniek wordt geïdentificeerd.
- Alle beleidsregels worden toegepast aan de kant van de oplosser.
- Er is geen actieve connector vereist. De toepassing voor het AD-gebruikers- en groepsbeleid kan echter de meest recente succesvolle AD-boomsynchronisatie weergeven.

Waar het werkt

- Elk netwerk wereldwijd.
- Werkt niet achter een Umbrella virtual appliance omdat de DNS-laag is uitgeschakeld om uit te stellen naar de lokale VA's.

Beperkingen

- Endpoint Agent actief en ingeschakeld op het werkstation.
- Ondersteunt geen server-besturingssystemen.
- Beleid op basis van interne IP-netwerkgegevens kan niet worden toegepast.
- Kan geen beleid of rapportage toepassen voor AD Computer (gebruik in plaats daarvan een

roaming-hostnaam).

Connector kan nog steeds proberen AD-aanmeldingsgebeurtenissen uit de ene DC-geregistreerde te trekken. Dit kan leiden tot een Dashboardfout die niet relevant is voor de integratie van roaming-clientgebaseerde AD. Om fouten met machtigingen met betrekking tot het trekken van aanmeldingsgebeurtenissen te verwijderen zonder daadwerkelijk gebeurtenissen te trekken, schakelt u de controle van aanmeldingsgebeurtenissen uit (indien niet anderszins gebruikt) via de achterkant van de auditinstructies van hier.

Implementatie van virtuele apparaten

Vereisten

- Twee VA's per overkoepelende locatie
- Eén AD-connector (redundante tweede, één optioneel) per overkoepelende site
- Elke DC (die geen alleen-lezen DC is) moet worden geregistreerd op het Dashboard.
- OpenDNS_Connector-gebruiker moet de volledige set van vereiste machtigingen hebben.
- Aanmeldingsgebeurtenissen moeten zijn ingeschakeld om 4624-beveiligingseventlogboeken op alle DC's te registreren. Bekijk de volledige tips voor probleemoplossing.

Hoe het werkt

- De VA's ontvangen AD-gebruikerstoewijzingen op basis van de logboeken voor beveiligingsaanmeldingen van Windows DC's.
- Elke aanmelding bij een werkstation wordt geregistreerd in het beveiligingseventlogboek van de aanmeldingsserver van de DC als een unieke aanmeldingsgebeurtenis, met de AD-gebruikersnaam of AD-computernaam en het interne IP-adres van het werkstation.
- De connector parseert deze gebeurtenissen in realtime via een WMI-abonnement en synchroniseert deze gebeurtenissen met elke VA op de Umbrella-site via TCP 443.
- De VA bouwt een live gebruikerstoewijzing op tussen het interne IP van een AD-gebruiker/computer en de gebruikersnaam van de AD-gebruiker/computer.
- De VA heeft alleen inzicht in de interne bron-IP van een DNS-query en maakt gebruik van het eerder genoemde toewijzingsbestand dat is gemaakt door de connector-gesynchroniseerde gebeurtenissen. De VA heeft geen direct zicht op wie er momenteel is ingelogd op een machine. Hiermee worden de AD-gebruikershandleiding en interne IP via EDNS0 gekoppeld aan de DNS-query die door de VA naar de overkoepelende oplossers is verzonden en die de AD-gebruiker uniek identificeert.
- De AD computer hash wordt op dezelfde manier toegepast.
- Alle beleidsregels worden toegepast aan de kant van de oplosser.
- Een connector moet functioneel en actief zijn in de organisatie om een AD-gebruiker te ontvangen en aanmeldingsgebeurtenissen moeten actueel zijn.
- De gebruiker moet de laatste AD-gebruiker zijn die zich op dit systeem heeft geverifieerd, zoals te zien is in de gebeurtenislogboeken.

Waar het werkt

Op het lokale bedrijfsnetwerk waar alle DNS is gericht op een virtuele Umbrella-apparaat dat tot dezelfde Umbrella-site behoort als de DC waaraan de gebruiker zich heeft geauthenticeerd.

Beperkingen

- De computer kan geen VA aanwijzen die tot een ander AD-domein of een andere overkoepelende site behoort (grote implementaties op meerdere domeinen kunnen geen AD-toepassing van hun basisnetwerk zien).
- Voor grote implementaties kan onderverdeling in overkoepelende locaties met afzonderlijke VA's nodig zijn.
- Uitzonderingen voor AD-gebruikers kunnen nodig zijn voor AD-gebruikers.
- Er is een maximum aantal aanmeldingsgebeurtenissen per seconde doorvoer voor de eerder genoemde connector, waardoor de toepassing van de gebruiker kan worden vertraagd. Dit is een factor van netwerklatentie en aantal VA's.

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.