

De integratiestroom van de overkoepelende Active Directory onderzoeken

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Communicatiestroom met overkoepelende Active Directory-implementatie](#)

[Wanneer het AD Connector Script wordt uitgevoerd op een Domain Controller \(DC\)](#)

[Hoe de AD-connector communiceert](#)

[Connector naar de cloud](#)

[Connector voor virtuele apparaten](#)

[Connector naar domeincontrollers](#)

[Virtuele apparaten \(VA\) naar cloud](#)

Inleiding

Dit document beschrijft de communicatiestroom tussen operationele componenten in een Cisco Umbrella Active Directory (AD)-integratie.

Achtergrondinformatie

Inzicht in de Active Directory-communicatiestroom kan helpen bij het oplossen van problemen en het garanderen van een correct geconfigureerde omgeving voordat deze wordt geïmplementeerd.

Communicatiestroom met overkoepelende Active Directory-implementatie

Wanneer het AD Connector Script wordt uitgevoerd op een Domain Controller (DC)

Het Windows-script maakt een eenmalige verbinding van de Domain Controller (DC) naar de cloud op poort TCP/443 met behulp van HTTPS om de DC te registreren op het dashboard. Met deze registratie kan de connector de gelijkstroom herkennen. Er wordt een oproep gedaan om met <https://api.opendns.com> specifieke parameters te communiceren. Zodra het script met succes de DC registreert, wordt het weergegeven op het dashboard.

Problemen kunnen soms betrekking hebben op Root Certificate Updates op Windows. Om dit snel te bepalen, navigeert u naar Internet Explorer en wijst u de browser aan

op: <https://api.opendns.com/v2/OnPrem.Asset>. Met deze actie wordt een bericht afgedrukt, zoals **1005 Missing API key**. Als er fouten of waarschuwingen in het certificaat op die pagina worden weergegeven, moet u

controleren of de meest recente update voor basiscertificaten van Microsoft is geïnstalleerd.

Hoe de AD-connector communiceert

De AD-connector communiceert als volgt met de Umbrella Cloud-service of een virtueel apparaat:

- Connector naar de cloud

De connector uploadt alle Active Directory (AD)-gegevens elke vijf minuten als er wijzigingen optreden, met behulp van een HTTPS-verbinding op poort 443 TCP. Alleen informatie over groepen, gebruikers en computers wordt geüpload. Er worden geen wachtwoorden geüpload en alle gebruikersinformatie wordt lokaal gehasht, waardoor de gegevens uniek zijn.

- Connector voor virtuele apparaten

De connector verzendt voortdurend AD-gebeurtenissen naar de virtuele apparaten met behulp van poort 443 TCP (niet-gecodeerd). Dit is een eenrichtingscommunicatie; de apparaten communiceren niet terug naar de aansluitingen. Een verplichte voorwaarde is dat de connector en Virtual Appliance (VA) communiceren via een vertrouwd netwerk.

- Connector naar domeincontrollers

De connector communiceert met alle domeincontrollers op dezelfde locatie met behulp van poorten 389 TCP en 3268 TCP/UDP voor LDAP-synchronisatie. De connector communiceert ook met de domeincontrollers via WMI/RPC. Port 135 TCP is de standaardpoort voor RPC en WMI. WMI gebruikt ook een willekeurig toegewezen poort tussen 1024 TCP en 65535 TCP voor Windows 2003 en ouder, of tussen 49152 TCP en 65535 TCP voor Windows 2008 en hoger. Vanaf versie 1.1.24 communiceert de connector ook met de domeincontroller via LDAPS (LDAP over SSL) via poorten 636 TCP en 3269 TCP.

Als communicatieproblemen worden waargenomen, controleert u of er Layer-7-toepassingsproxy's zijn die gegevens kunnen blokkeren of laten vallen. Een veel voorkomend geval is de inspectiefunctie op Cisco-apparaten die werken op protocollen zoals DNS, HTTP of HTTPS. Raadpleeg voor meer informatie onze documentatie over het [toepassen van Application Layer Protocol Inspection](#).

Virtuele apparaten (VA) naar cloud

De virtuele apparaten communiceren vaak op poort 443 naar TCP, [api.opendns.com](#) evenals op 53 TCP / UDP voor DNS-query's of sondes, en 22, 25, 53, 80, 443 of 4766 TCP om de ondersteuningstunnel tot stand te brengen. De virtuele apparaten communiceren met de cloud met behulp van poorten 53 UDP / TCP, 443 TCP, 123 TCP en 80 TCP. Ze ontvangen gegevens van de connectoren op poort 443 TCP (geen HTTPS-verbinding), maar hebben geen communicatie terug naar hen nodig.

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.