# Untersuchen des Umbrella Active Directory Integration Flow

## Inhalt



## Einleitung

In diesem Dokument wird der Kommunikationsfluss zwischen den Betriebskomponenten bei der Integration von Cisco Umbrella Active Directory (AD) beschrieben.

## Hintergrundinformationen

Ein Verständnis des Active Directory-Kommunikationsflusses kann bei der Fehlerbehebung und der Sicherstellung einer korrekt konfigurierten Umgebung vor der Bereitstellung hilfreich sein.

## Kommunikationsfluss mit Umbrella Active Directory-Implementierung

### Wenn das AD Connector-Skript auf einem Domänencontroller (DC) ausgeführt wird

Das Windows-Skript stellt eine einmalige Verbindung vom Domänencontroller (DC) zur Cloud auf Port TCP/443 her und verwendet HTTPS, um den DC beim Dashboard zu registrieren. Durch diese Registrierung kann der Stecker das Rechenzentrum erkennen. Ein Aufruf von wird mit **https://api.opendns.com** bestimmten Parametern durchgeführt. Sobald das Skript das Rechenzentrum erfolgreich registriert hat, wird es auf dem Dashboard angezeigt.

Probleme können sich manchmal auf Stammzertifikataktualisierungen unter Windows beziehen. Um dies schnell zu ermitteln, navigieren Sie zu Internet Explorer, und zeigen Sie im Browser auf: https://api.opendns.com/v2/OnPrem.Asset. Bei dieser Aktion wird die Meldung ausgegeben, dass **1005 Missing API key**. das neueste Microsoft-Stammzertifikatupdate installiert ist, wenn auf dieser Seite

Zertifikatfehler oder -warnungen angezeigt werden.

## Kommunikation des AD-Anschlusses

Der AD-Connector kommuniziert wie folgt mit dem Umbrella Cloud-Service oder einer virtuellen Appliance:

- Verbindung zur Cloud

  Der Connector lädt alle fünf Minuten alle Active Directory (AD)-Daten hoch, wenn Änderungen auftreten. Dazu wird eine HTTPS-Verbindung auf Port 443 TCP verwendet. Es werden nur Informationen zu Gruppen, Benutzern und Computern hochgeladen. Es werden keine Passwörter hochgeladen, und alle Benutzerinformationen werden lokal gehasht, wodurch die Daten eindeutig sind.

- Verbindung zu virtuellen Appliances

  Der Connector sendet kontinuierlich AD-Ereignisse über Port 443 TCP (unverschlüsselt) an die virtuellen Appliances. Dies ist eine unidirektionale Kommunikation. Die Geräte kommunizieren nicht mit den Anschlüssen. Eine zwingende Voraussetzung ist, dass der Connector und die virtuelle Appliance (VA) über ein vertrauenswürdiges Netzwerk kommunizieren.

- Verbindung zu Domänencontrollern

  Der Connector kommuniziert mit allen Domänencontrollern am gleichen Standort über die Ports 389 TCP und 3268 TCP/UDP für die LDAP-Synchronisierung. Der Connector kommuniziert auch über WMI/RPC mit den Domänencontrollern. Port 135 TCP ist der Standardport für RPC und WMI. WMI verwendet außerdem einen zufällig zugewiesenen Port zwischen 1024 TCP und 65535 TCP für Windows 2003 und ältere Versionen bzw. zwischen 49152 TCP und 65535 TCP für Windows 2008 und höher. Ab Version 1.1.24 kommuniziert der Connector auch über LDAPS (LDAP over SSL) über die Ports 636 TCP und 3269 TCP mit dem Domain Controller.

Wenn Kommunikationsprobleme auftreten, überprüfen Sie, ob Layer-7-Anwendungsproxys Daten blockieren oder verwerfen. Ein gängiger Fall ist die "inspect"-Funktion auf Cisco Geräten, die auf Protokollen wie DNS, HTTP oder HTTPS basieren. Weitere Informationen finden Sie in unserer Dokumentation zum Anwenden der Protokollüberprüfung auf Anwendungsebene.

## Virtuelle Appliances (VA) in die Cloud

Die virtuellen Appliances kommunizieren häufig über Port 443 (TCP an **api.opendns.com**) sowie über Port 53 (TCP/UDP) für DNS-Abfragen oder -Tests und über Port 22, 25, 53, 80, 443 oder 4766 (TCP), um den Support-Tunnel einzurichten. Die virtuellen Appliances kommunizieren mit der Cloud über die Ports 53, UDP/TCP, 443, 123 und 80, TCP. Sie empfangen Daten von den

Anschlüssen an Port 443 (keine HTTPS-Verbindung), benötigen jedoch keine Rückkommunikation.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.