Examine the Umbrella Active Directory Integration Flow

Contents

Introduction

This document describes the communication flow between operational components in a Cisco Umbrella Active Directory (AD) integration.

Background Information

Understanding the Active Directory communication flow can assist in troubleshooting and ensuring a correctly configured environment before deployment.

Communication Flow with Umbrella Active Directory Implementation

When the AD Connector Script Runs on a Domain Controller (DC)

The Windows script makes a one-time connection from the Domain Controller (DC) to the cloud on port TCP/443 using HTTPS to register the DC to the dashboard. This registration allows the connector to recognize the DC. A call is made to **https://api.opendns.com** with specific parameters. Once the script successfully registers the DC, it displays on the dashboard.

Issues can sometimes relate to Root Certificate Updates on Windows. To quickly determine this, navigate to Internet Explorer and point the browser to: https://api.opendns.com/v2/OnPrem.Asset. This action prints a message like **1005 Missing API key**. If any certificate errors or warnings appear on that page, ensure that the latest Root Certificates Update from Microsoft is installed.

How the AD Connector Communicates

The AD connector communicates with the Umbrella Cloud service or a Virtual Appliance as follows:

- **Connector to Cloud**

  The connector uploads all Active Directory (AD) data every five minutes if changes occur, using an HTTPS connection on port 443 TCP. Only information on Groups, Users, and Computers is uploaded. No passwords are uploaded, and all user information is hashed locally, making the data unique.

- **Connector to Virtual Appliances**

  The connector constantly sends AD events to the virtual appliances using port 443 TCP (unencrypted). This is a one-way communication; the appliances do not communicate back to the connectors. A mandatory prerequisite is that the connector and Virtual Appliance (VA) communicate over a trusted network.

- **Connector to Domain Controllers**

  The connector communicates with all domain controllers located in the same site using ports 389 TCP and 3268 TCP/UDP for LDAP sync. The connector also communicates with the domain controllers using WMI/RPC. Port 135 TCP is the standard port for RPC and WMI. WMI also uses a randomly assigned port between 1024 TCP and 65535 TCP for Windows 2003 and older, or between 49152 TCP and 65535 TCP for Windows 2008 and above. As of version 1.1.24, the connector also communicates with the domain controller using LDAPS (LDAP over SSL) over ports 636 TCP and 3269 TCP.

If communication issues are observed, check for any Layer-7 application proxies that can be blocking or dropping data. A common case is the inspect feature on Cisco devices that act on protocols such as DNS, HTTP, or HTTPS. For more information, refer to our documentation on Applying Application Layer Protocol Inspection.

Virtual Appliances (VA) to Cloud

The virtual appliances frequently communicate on port 443 TCP to **api.opendns.com**, as well as to 53 TCP/UDP for DNS queries or probes, and 22, 25, 53, 80, 443, or 4766 TCP to establish the support tunnel. The Virtual Appliances communicate with the cloud using ports 53 UDP/TCP, 443 TCP, 123 TCP, and 80 TCP. They receive data from the connectors on port 443 TCP (not an HTTPS connection) but do not require communication back to them.