Integrate Active Directory Using VA or CSC

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Overview

Secure Client Implementation

- Requirements
- How it Works
- Where It Works
- Limitations

Virtual Appliance Implementation

- Requirements
- Where It Works
- Limitations

Introduction

This document describes two methods of integrating Active Directory (AD) with Umbrella: Virtual Appliance (VA) or Cisco Secure Client (CSC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- AD Connector: Syncs the AD tree of a single Active Directory domain to the dashboard. For the VA implementation, it also actively syncs the login events from the DCs on the same Umbrella site to the VAs. The AD tree for the organization is synced to the Umbrella cloud by the AD Connector, pulling this data from the registered DC. Tree updates are detected and the Umbrella cloud is updated within several hours.
- Domain Controller (AD Server): DCs are registered to the dashboard via the registration configuration .wsf script as downloaded from the dashboard. This adds its name, domain, and internal IP to the Dashboard to inform the Connector which IPs to attempt to sync with. If you cannot run the script, manual registration is also possible. Contact Umbrella Support for more information and support.
- Virtual Appliance: The Umbrella on premise DNS forwarder. Applies (optional) AD identity on network as well as internal IPs on reports. This triggers all roaming clients behind it to disable DNS protection and defer to "Behind VA protection" mode.
- Cisco Secure Client: The Umbrella on premise software service which provides DNS encryption as well as user identification to Windows and macOS. Also comes as an AnyConnect module.

Note: Prerequisites differ between the two implementations significantly. Please refer to the specific implementation for full prerequisites.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

This article clarifies and explores the two different methods of integrating Active Directory with the Umbrella Dashboard. Currently, AD users can be applied to policy and reporting via the Umbrella virtual appliances or the Cisco Secure Client.

Secure Client Implementation

Requirements

- One AD Connector
- One DC on the Dashboard
- OpenDNS_Connector user must have Read Only Domain Controller permission.
- Secure Client minimum versions for the standalone client (AnyConnect Module):
    - Windows: 2.1.0 (4.5.01044)
    - OSX: 2.0.39 (4.5.02033).

How it Works

- The currently logged-in AD user is determined directly at the local computer by the roaming client reading the local registry.
- Supports a maximum of one concurrently logged in user on the workstation.
- Two concurrent users can result in no AD user applying.
- The AD user GUID and internal IP are attached via EDNS0 within the roaming client's DNS proxy to the DNS query sent to the Umbrella resolvers, uniquely identifying the AD user.
- All policies are applied on the resolver side.
- No active connector is required. However, AD user and group policy application can reflect the most recent successful AD tree sync.

Where It Works

- Any network globally.
- Does not work behind an Umbrella virtual appliance as the DNS layer is disabled to defer to the local VAs.

Limitations

- Requires endpoint agent active and enabled on the workstation.
- Does not support server OSes.
- Cannot apply policy based on internal network IP.
- Cannot apply policy or reporting for AD Computer (use roaming hostname instead).

Connector can still attempt to pull AD login events from the one DC registered. This can result in a Dashboard error which is not relevant to roaming client-based AD integration. To remove errors with permissions related to pulling login events without actually pulling any events, disable login event auditing (if not otherwise used) via the reverse of the auditing instructions from here.

Virtual Appliance Implementation

Requirements

- Two VAs per Umbrella site
- One AD Connector (redundant second one optional) per Umbrella site
- Every DC (which is not a Read Only DC) must be registered to the Dashboard.
- OpenDNS_Connector user must have the full set of prerequisite permissions.
- Login events must be enabled to log 4624 security event logs on all DCs. See full troubleshooting tips.

How It Works

- The VAs receive AD user mappings based on the Windows DCs' security login event logs.

- Each workstation login is logged to the login server DC's security event log as a unique login event, with the AD username or AD computer name and the internal IP of the workstation.
- The connector parses these events in real time via a WMI subscription and syncs these events to **each** VA on the Umbrella site via TCP 443.
- The VA builds a live user mapping between the internal IP of an AD user/computer and the username of the AD user/computer.
- The VA only has visibility in to the internal source IP of a DNS query and utilizes the previously-mentioned mapping file created by the connector-synced events. **The VA has no direct visibility into who is currently logged into a machine.** This attaches the AD user GUID and internal IP via EDNS0 to the DNS query sent to the Umbrella resolvers by the VA, uniquely identifying the AD user.
- The AD computer hash is applied in the same way.
- All policies are applied on the resolver side.
- A connector must be functional and active on the organization to receive an AD user, and login events must be current.
- The user must be the last AD user to authenticate to this machine as seen in the event logs.

Where It Works

On the local corporate network where all DNS is pointed at an Umbrella virtual appliance belonging to the same Umbrella site as the DC the user has authenticated to.

Limitations

- The computer cannot point to a VA belonging to a different AD domain or Umbrella site (large deployments on multiple domains cannot see AD application off their base network).
- Large deployments can require subdivision into Umbrella sites with separate VAs.
- AD User exceptions can be needed for service AD users.
- There exists a maximum login events per second throughput for the previously-mentioned connector which can delay user application. This is a factor of network latency and number of VAs.