Secure Cisco Umbrella for Virtual Appliance and AD Connector Deployments

Contents

Introduction

This document describes best practices and recommendations around the Cisco Umbrella Virtual Appliance (VA) and Active Directory (AD) Connector deployments to mitigate the risk of any internal attacks that rise from using these components.

The VA runs a hardened version of Ubuntu Linux 20.04. Customers are provided with restricted access for configuration and troubleshooting purposes only. No additional software or scripts can be deployed on the VA by customers.

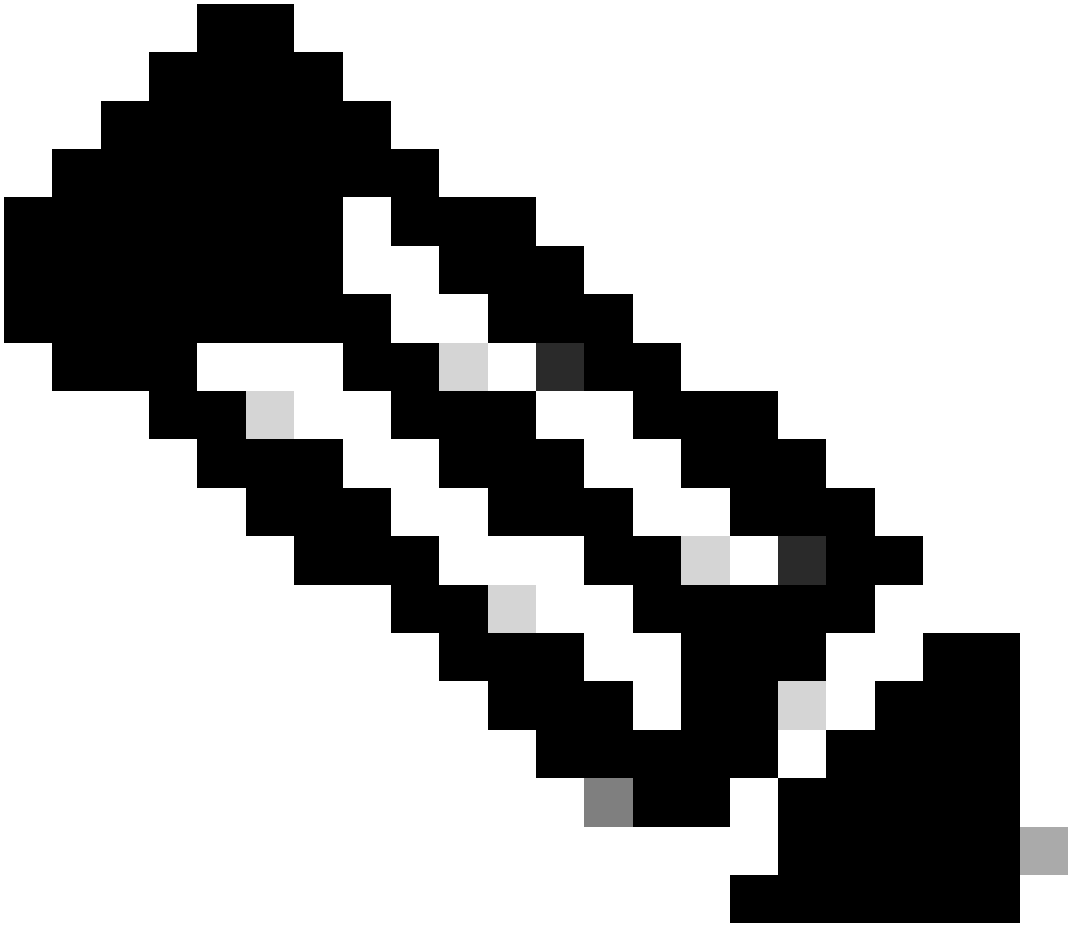
Cisco Umbrella Virtual Appliance

Managing the .tar file:

- The Cisco Umbrella Virtual Appliance (VA) software downloads from the Umbrella Dashboard as a **.tar** file that contains the actual VA image and a signature for that image.
- Cisco recommends validating the signature to verify the integrity of the VA image.

Configuring ports:

- By default, upon deployment, only **ports 53 and 443** are open for inbound traffic.
- If you are running the VA on Azure, KVM, Nutanix, AWS, or GCP, then **port 22** is also enabled by default to allow SSH connections for configuring the VA.
- For VAs running on VMware and Hyper-V, **port 22** is opened only if the command to enable SSH is run on the VA.
- The VA makes outbound queries over specific ports/protocols to the destinations mentioned in the Umbrella documentation.
- Cisco Umbrella recommends setting up rules on your firewall to block any traffic from your VAs to all other destinations.



Note: All HTTPS communication to/from the VA happens over TLS 1.2 only. Older protocols are not used.

Managing passwords:

- The initial login on the VA requires a password change.
- Cisco recommends periodically rotating the password on the VA after this initial password change.

Mitigating DNS attacks:

- To mitigate the risk of an internal Denial of Service attack on the DNS service running on the VA, you can configure per-IP rate limits for the DNS on the VA.
- This is not enabled by default and must be explicitly configured using the instructions documented in the Umbrella documentation.

Monitoring VAs over SNMP:

- If you are monitoring your VAs over SNMP, Cisco Umbrella recommends using SNMPv3 with authentication and encryption.
- Instructions for the same are in the Umbrella documentation.

- Once you enable the SNMP monitoring, port 161 on the VA is opened for inbound traffic.
- You can monitor various attributes like the CPU, load, and memory on the VA over SNMP.

Using the Cisco AD integration with VAs:

- If you are using the VAs with the Cisco Umbrella Active Directory integration, it is best practice to tune (or adjust) the user cache duration on the VA to match your DHCP lease time.
- Refer to instructions in the Virtual Appliance: Tuning User Cashe Settings documentation. This minimizes the risk of incorrect user attributions.

Configuring audit logging:

- The VA maintains an audit log of all configuration changes executed on the VA.
- You can configure remote logging of this audit log to a syslog server per the instructions in the Umbrella documentation.

Configuring VAs:

- At least two VAs must be configured per Umbrella site, and the IP address of these two VAs can be distributed as the DNS servers to endpoints.
- For additional redundancy, you can configure Anycast addressing on the VA. This allows multiple VAs to share a single Anycast address.
- So effectively, you can deploy multiple VAs while still distributing just two DNS server IPs to each endpoint. If any VA fails, Anycast ensures that the DNS queries are routed to the other VA that shares the same Anycast IP.
- Read more about the steps to configure Anycast on the VA.

Configuring the Cisco Umbrella Active Directory Connector

Creating a custom account name:

- One of the best practices for the Cisco Umbrella AD Connector is to use a custom account name instead of the default OpenDNS_Connector.
- This account can be created prior to connector deployment and granted the required permissions.
- The account name needs to be specified as part of the connector installation.

Configuring LDAPS with the AD Connector:

- The Umbrella AD Connector attempts to retrieve user-group information over LDAPS (data transmitted over a secure channel), failing which it switches to LDAP over Kerberos (packet level encryption) or LDAP over NTLM (only authentication, no encryption) in that order.
- Cisco Umbrella recommends setting up LDAPS on your domain controllers so that the connector can retrieve this information over an encrypted channel.

Managing the .ldif file:

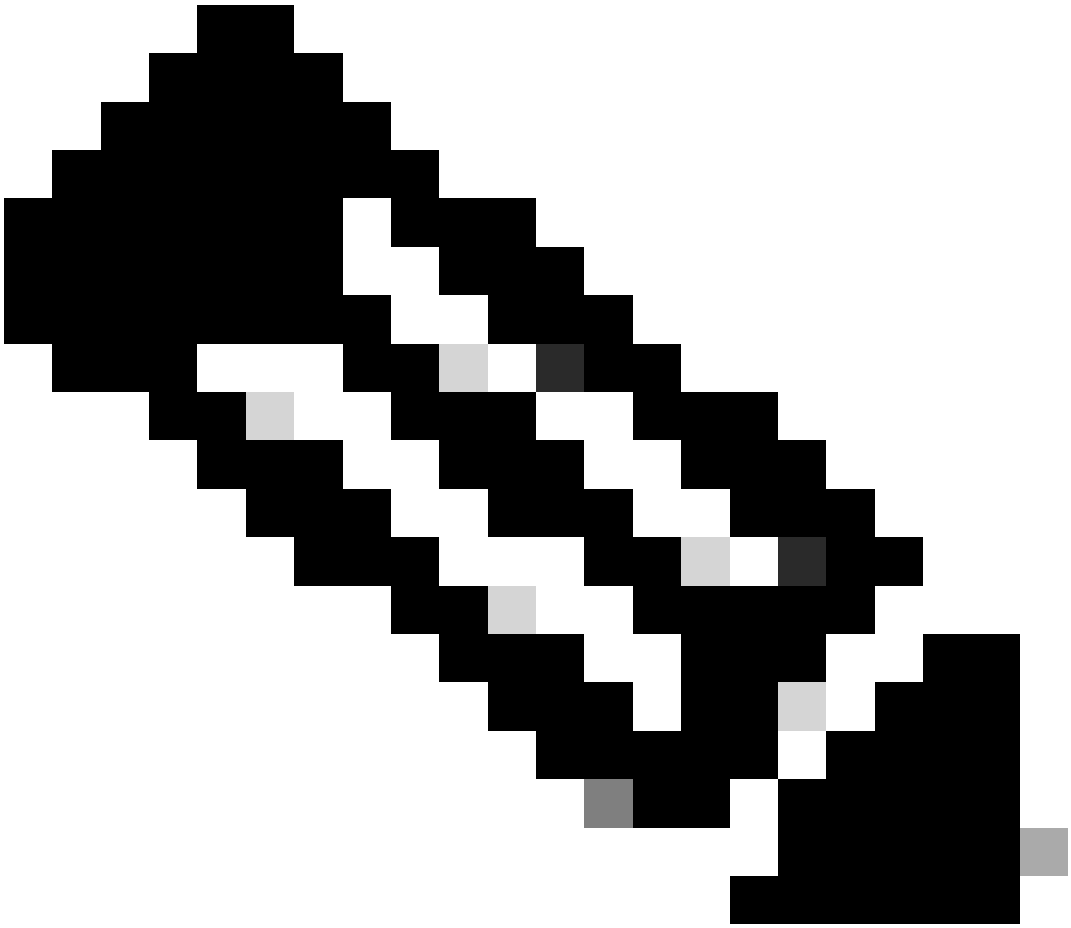
- The connector, by default, stores the details of the users and groups retrieved from the domain controllers in a **.ldif** file locally.
- Since this can be sensitive information that is stored in plain text, you can restrict access to the server that runs the connector.
- Alternatively, at install time, you can choose not to store the **.ldif** files locally.

Configuring ports:

- Because the connector is a Windows service, it does not enable/disable any ports on the host machine.

Cisco Umbrella recommends running the Cisco Umbrella AD Connector service on a dedicated Windows server.

- Similar to the VA, the connector makes outbound queries over specific ports/protocols to the destinations mentioned in the Umbrella documentation. Cisco Umbrella recommends setting up rules on your firewall to block any traffic from your connectors to all other destinations.



Note: All HTTPS communication to/from the connector happens over TLS 1.2 only. Older protocols are not used.

Managing the connector password:

- Cisco recommends rotating the connector password periodically.
- This can be done by changing the connector account password in Active Directory and then updating the password using the "PasswordManager" tool in the connector folder.

Receiving user-IP mappings:

- By default, the connector communicates private IP.
- AD sends user mappings to the VA over plaintext.
- You can choose to configure the VA and connector to communicate over an encrypted channel as per

the instructions documented in this Knowledge Base article.

Certificate management:

- Certificate management and revocation are out of scope for the VA, and you are responsible for ensuring that the latest certificate/certificate chain is present on the VA and the connector as relevant.
- Setting up an encrypted channel for this communication impacts performance for the VA and the connector.