Understand the Umbrella AD Integration and Virtual Appliances

Contents

Introduction

This document describes how the Umbrella Active Directory (AD) integration works when using Virtual Appliances.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

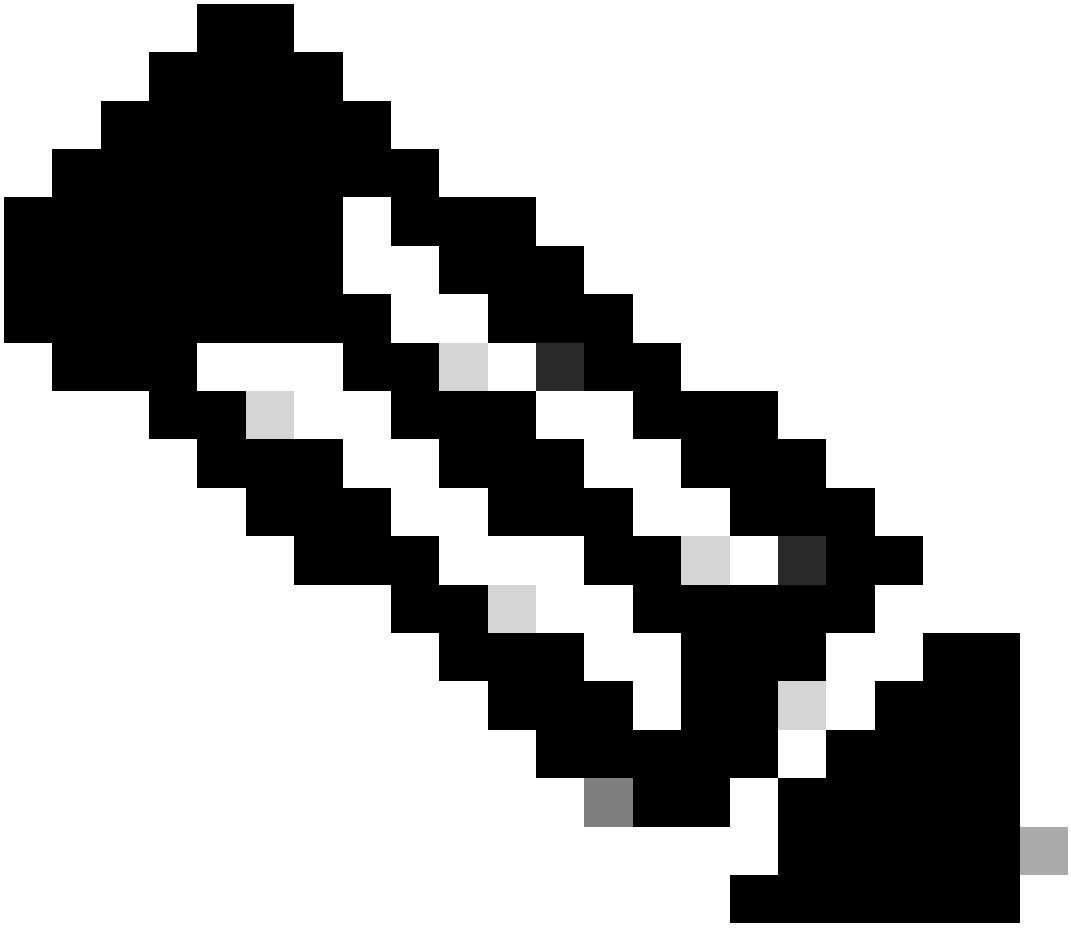
The information in this document is based on Cisco Umbrella.

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 of the Umbrella Active Directory Integration Functionality with Virtual Appliances

1. The Umbrella Connector service pulls logon events with ID 4624, 528, 540, 538, 4647, 4634, 4768, and 4769 from the Windows Event Viewer on all Domain Controllers in the same Umbrella Site as the Connector server. Those logon events include AD User/Computer name and the IP address of the workstation.

2. The Connector forwards a summary of new FOUND EVENT entries to all of the Virtual Appliances in the same Umbrella Site.



Note: The Connector caches logon event information to optimize performance, so summaries are not always sent. Also, summaries are not sent for AD Users, AD Groups, or IP addresses that have been added to the Umbrella Service Account Exceptions list.

3. Each individual VA uses the summary to create a mapping file between the IP address and the Active Directory User/Computer.

4. When a DNS request is sent to a VA from a particular IP address, the mapping file is used to find the associated AD User/Computer.

5. The User/Computer determines the policy for the request and identifies the request in reports.

Intended Functionality

1. A user logs in to the AD domain using a DC that has been registered with Umbrella.

2. An Umbrella Connector in the same Umbrella Site as that DC forwards a summary to all VAs in that same Umbrella Site.

3. DHCP or some other method ensures that the user's DNS servers are VAs in the same Umbrella Site as that DC.

4. DNS requests from the user are properly identified by Umbrella.

Scenario for Unregistered DC in Umbrella

Conversely, suppose a user logs in to the AD domain using a DC that has not been registered with Umbrella:

1. The Umbrella Connector never sees the logon event and has no AD User/Computer + IP address to forward to the VAs.

2. The VAs cannot add/edit a mapping entry.

3. DNS requests from the user cannot be associated with the user (unless there was something cached).