了解Umbrella AD集成和虚拟设备

目录

简介

本文档介绍在使用虚拟设备时Umbrella Active Directory(AD)集成的工作原理。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

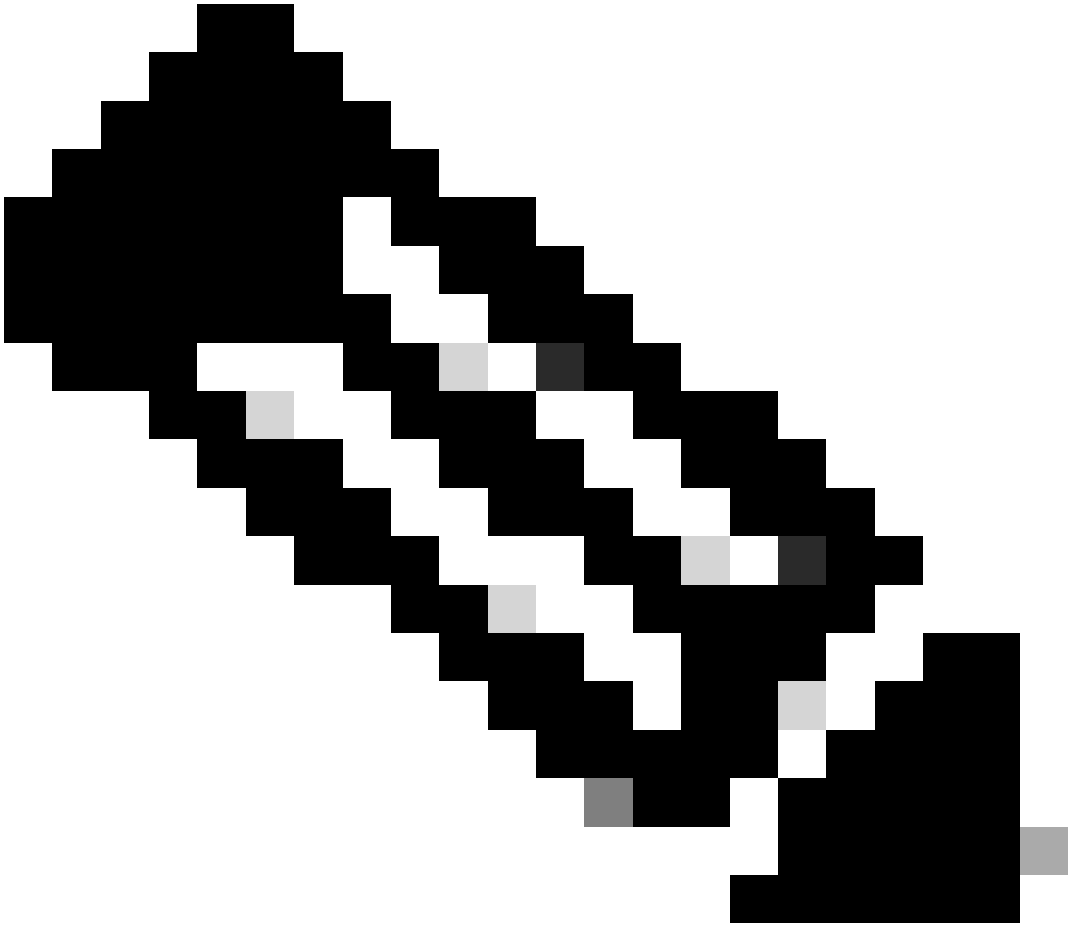
本文档中的信息基于Cisco Umbrella。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

Umbrella Active Directory与虚拟设备的集成功能概述

1. Umbrella连接器服务从与连接器服务器位于同一Umbrella站点的所有域控制器上的Windows事件查看器中提取ID为4624、528、540、538、4647、4634、4768和4769的登录事件。这些登录事件包括AD用户/计算机名和工作站的IP地址。

2.连接器将新的FOUND EVENT条目的摘要转发到同一Umbrella站点中的所有虚拟设备。



注意：连接器会缓存登录事件信息以优化性能，因此并不总是发送摘要。此外，不会发送已添加到Umbrella服务帐户例外列表的AD用户、AD组或IP地址的摘要。

3.每个VA都使用摘要在IP地址和Active Directory用户/计算机之间创建一个映射文件。

4.从特定IP地址向VA发送DNS请求时，映射文件用于查找关联的AD用户/计算机。

5.用户/计算机确定请求的策略并在报告中标识请求。

预期功能

1.用户使用已向Umbrella注册的DC登录到AD域。

2.与数据中心位于同一Umbrella站点的Umbrella连接器将摘要转发到同一Umbrella站点内的所有VA。

3. DHCP或其他方法可确保用户的DNS服务器与该DC位于同一Umbrella站点中的VA。

4.用户的DNS请求由Umbrella正确识别。

Umbrella中未注册的数据中心的场景

反之，假设用户使用未向Umbrella注册的DC登录到AD域：

1. Umbrella连接器从未看到登录事件，并且没有要转发到VA的AD用户/计算机+ IP地址。

2.VA无法添加/编辑映射条目。

3.来自用户的DNS请求不能与用户关联（除非缓存了某些内容）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。