使用VA或CSC集成Active Directory

目录

简介

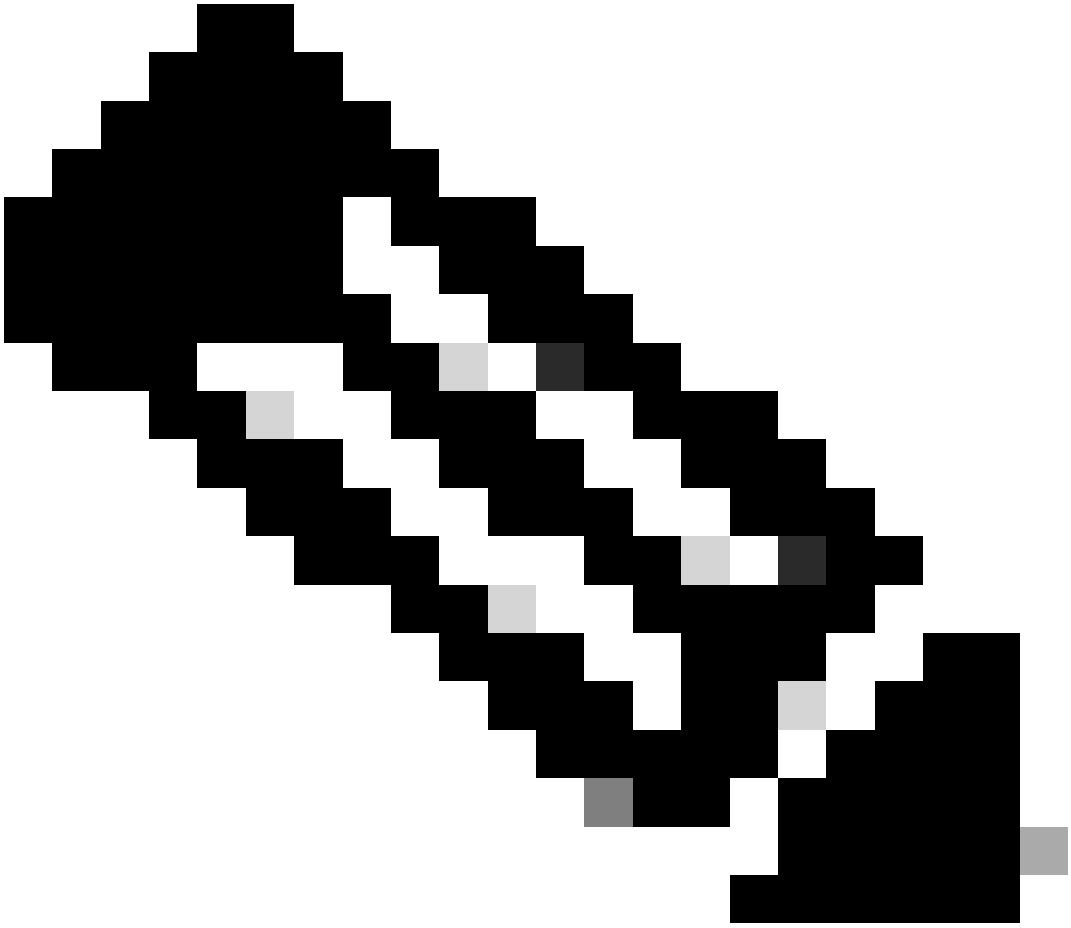
本文档介绍将Active Directory(AD)与Umbrella集成的两种方法：虚拟设备(VA)或思科安全客户端(CSC)。

先决条件

要求

Cisco 建议您了解以下主题：

- AD连接器:将单个Active Directory域的AD树同步到仪表板。对于VA实施，它还主动将登录事件从同一Umbrella站点上的DC同步到VA。组织的AD树通过AD连接器同步到Umbrella云，从注册的DC提取此数据。检测到树更新，并在数小时内更新Umbrella云。
- 域控制器（AD服务器）:DC通过从控制面板下载的注册配置.wsf脚本注册到控制面板。这会将其名称、域和内部IP添加到仪表板，以通知连接器尝试与哪些IP同步。如果无法运行脚本，也可以手动注册。请与Umbrella支持联系以获取更多信息和支持。
- 虚拟设备:Umbrella内部部署DNS转发器。在网络中应用（可选）AD身份，并在报告中应用内部IP。这会触发其后面的所有漫游客户端禁用DNS保护并转到“VA保护后面”模式。
- 思科安全客户端：Umbrella内部软件服务，为Windows和macOS提供DNS加密以及用户识别。也作为AnyConnect模块提供。



注意：两种实施之间的先决条件差异很大。有关完整的必备条件，请参阅特定实施。

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。

概述

本文阐明并探讨了将Active Directory与Umbrella Dashboard集成的两种不同方法。目前，AD用户可通过Umbrella虚拟设备或Cisco安全客户端应用于策略和报告。

安全客户端实施

要求

- 一个AD连接器
- 控制面板上有一个DC
- OpenDNS_Connector用户必须拥有只读域控制器权限。
- 独立客户端（AnyConnect模块）的安全客户端最低版本：
  - Windows 窗口版本:2.1.0(4.5.01044)
  - OSX:2.0.39(4.5.02033)。

工作原理

- 当前登录的AD用户由读取本地注册表的漫游客户端在本地计算机上直接确定。
- 支持工作站上最多有一个并发登录用户。
- 两个并发用户可能导致没有AD用户应用。
- AD用户GUID和内部IP通过漫游客户端的DNS代理中的EDNS0附加到发送到Umbrella解析器的DNS查询，以唯一标识AD用户。
- 所有策略都应用于解析器端。
- 不需要活动连接器。但是，AD用户和组策略应用可以反映最近成功的AD树同步。

工作场所

- 任何全球网络。
- 不在Umbrella虚拟设备后工作，因为DNS层已禁用以服从本地VA。

限制

- 需要在工作站上激活并启用终端代理。
- 不支持服务器OS。
- 无法根据内部网络IP应用策略。
- 无法为AD计算机应用策略或报告（请改用漫游主机名）。

连接器仍然可以从一个注册的DC拉取AD登录事件。这会导致与基于漫游客户端的AD集成不相关的控制面板错误。要删除权限相关的错误，而不实际拉取任何事件，请通过此处审核说明的反面禁用登录事件审核（如果未使用）。

虚拟设备实施

要求

- 每个Umbrella站点两个VA
- 每个Umbrella站点一个AD连接器（冗余第二个可选）
- 每个DC（不是只读DC）都必须注册到仪表板。
- OpenDNS_Connector用户必须拥有完整的必备权限。
- 必须启用登录事件才能记录所有DC上的4624安全事件日志。查看完整的故障排除提示。

工作原理

- VA根据Windows DC的安全登录事件日志接收AD用户映射。
- 每个工作站登录都会以唯一登录事件的形式记录到登录服务器DC的安全事件日志中，并带有AD用户名或AD计算机名称以及工作站的内部IP。
- 连接器通过WMI订阅实时解析这些事件，并通过TCP 443将这些事件同步到Umbrella站点上的每个VA。
- VA在AD用户/计算机的内部IP和AD用户/计算机的用户名之间建立实时用户映射。
- VA仅能查看DNS查询的内部源IP，并使用由连接器同步事件创建的上述映射文件。VA无法直接查看当前登录到计算机的用户。这会通过EDNS0将AD用户GUID和内部IP附加到VA发送到Umbrella解析器的DNS查询，以唯一标识AD用户。
- AD计算机散列以相同方式应用。
- 所有策略都应用于解析器端。
- 连接器必须正常工作且组织上处于活动状态才能接收AD用户，并且登录事件必须是当前事件。
- 用户必须是最后一个AD用户才能向此计算机进行身份验证，如事件日志中所见。

工作场所

在本地企业网络中，所有DNS都指向与用户身份验证的DC属于同一Umbrella站点的Umbrella虚拟设备。

限制

- 计算机无法指向属于其他AD域或Umbrella站点的VA（多个域上的大型部署无法从其基本网络中看到AD应用）。
- 大型部署可能需要使用单独的VA细分Umbrella站点。
- 服务AD用户可能需要AD用户例外。
- 上述连接器存在每秒最大登录事件吞吐量，可以延迟用户应用。这是网络延迟和VA数量的一个因素。

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）。