

了解终端服务、Citrix和与Active Directory的集成

目录

[简介](#)

[概述](#)

[Web策略：适用于RDS和VDI](#)

[DNS策略：RDS与AD集成](#)

[DNS策略：解决方案 — RDS与AD集成](#)

[DNS策略：使用VDI与AD集成](#)

简介

本文档介绍终端服务、Citrix和Umbrella与Active Directory的集成。

概述

适用于：Windows终端服务和远程桌面服务、Windows 10企业多会话、Citrix XenApp和XenDesktop

终端服务和Citrix服务器能够在服务器上托管多个同时发生的客户端会话。有两种不同的配置：

- 远程桌面服务(RDS)。多个用户在同一服务器上的单个虚拟机上运行一个会话。这些会话共享相同的操作系统和IP地址。这通常称为终端服务。
- 虚拟桌面基础设施(VDI)。服务器运行一个虚拟机池，每个用户使用自己的操作系统和IP地址连接到一个唯一的VM

Web策略：适用于RDS和VDI

通过PAC文件、CDFW隧道和代理链进行基于SAML cookie的身份验证的安全网络网关，支持多个用户访问单个IP地址。这意味着每个用户的Web策略实施都支持虚拟桌面(Citrix/TS)。

DNS策略：RDS与AD集成

不支持RDS/远程桌面会话主机/终端服务器进行每用户识别。这包括仅Azure Windows 10 Enterprise多会话操作系统。

这些服务器上托管的客户端会话共享一个IP地址：属于主机的。Umbrella Active Directory(AD)与虚拟设备(VA)的集成依赖于唯一的用户到IP地址映射才能正常工作。简而言之，这意味着在用户共享同一源IP地址的任何情况下，无法进行每用户识别。

当多个登录用户共享同一IP时，这会对策略应用和报告产生负面影响。所有用户都收到相同的策略，并且标识的用户可以基于上次登录的用户连续更改。

DNS策略：解决方案 — RDS与AD集成

解决此问题的最佳方法是为您的终端服务器或Citrix服务器的IP地址配置一个唯一策略。这意味着终端服务器的所有用户都将收到相同的、一致的策略。

1. 在Deployments > Internal Networks中创建内部网络。这包括终端服务器的/32 IP地址。将网络分配给适用的虚拟设备所在的Umbrella站点。
2. 导航到Policy Wizard (策略向导) 并创建新的Policy。
3. 在Select Identities部分中，选择“Sites”，然后打开相关的Umbrella站点。
4. 选择您之前创建的内部网络身份
5. 按照正常方式配置策略
6. 为终端服务器创建策略后，请务必将此策略放在策略列表的顶部，以便其优先于任何基于用户的策略。

或者，可以根据AD计算机标识为终端服务器创建策略。这种方法以相同的方式运行；服务器的所有用户都被标识为终端服务器计算机名。但是，为了保持一致运行，必须以优化主机到IP映射的方式配置VA。有关详细信息，请参阅AD主机GUID超时说明，或与Umbrella支持联系以获得帮助。

DNS策略：使用VDI与AD集成

VDI类型部署（其中为每个用户运行一个唯一的虚拟机）仍然可以接收每个用户的身份。要求如下：

- 虚拟设备 — 每个用户都必须具有对虚拟设备可见的唯一源IP。源IP在到达设备之前不能接受“源NATing”。
- 漫游客户端 — 当漫游客户端安装在每个虚拟机上时，可以在漫游客户端中进行AD集成。当每个用户具有持久性(例如，个人)虚拟机。

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）。