使用Umbrella Active Directory连接器进行身份验证

目录

简介

本文档介绍如何使用Umbrella Active Directory连接器通过802.1x、Radius或ISE进行身份验证。

概述

Cisco Umbrella Active Directory(AD)连接器通过将AD用户/计算机映射到内部IP地址来工作。为了使映射正确，AD用户必须根据已配置为与Cisco Umbrella AD连接器通信的域控制器进行身份验证。

如果您的AD用户通过其他方式进行身份验证，则可能根本没有在域控制器上生成登录事件，或者可能存在导致应用错误策略的意外映射。

通过802.1x、RADIUS或ISE进行身份验证

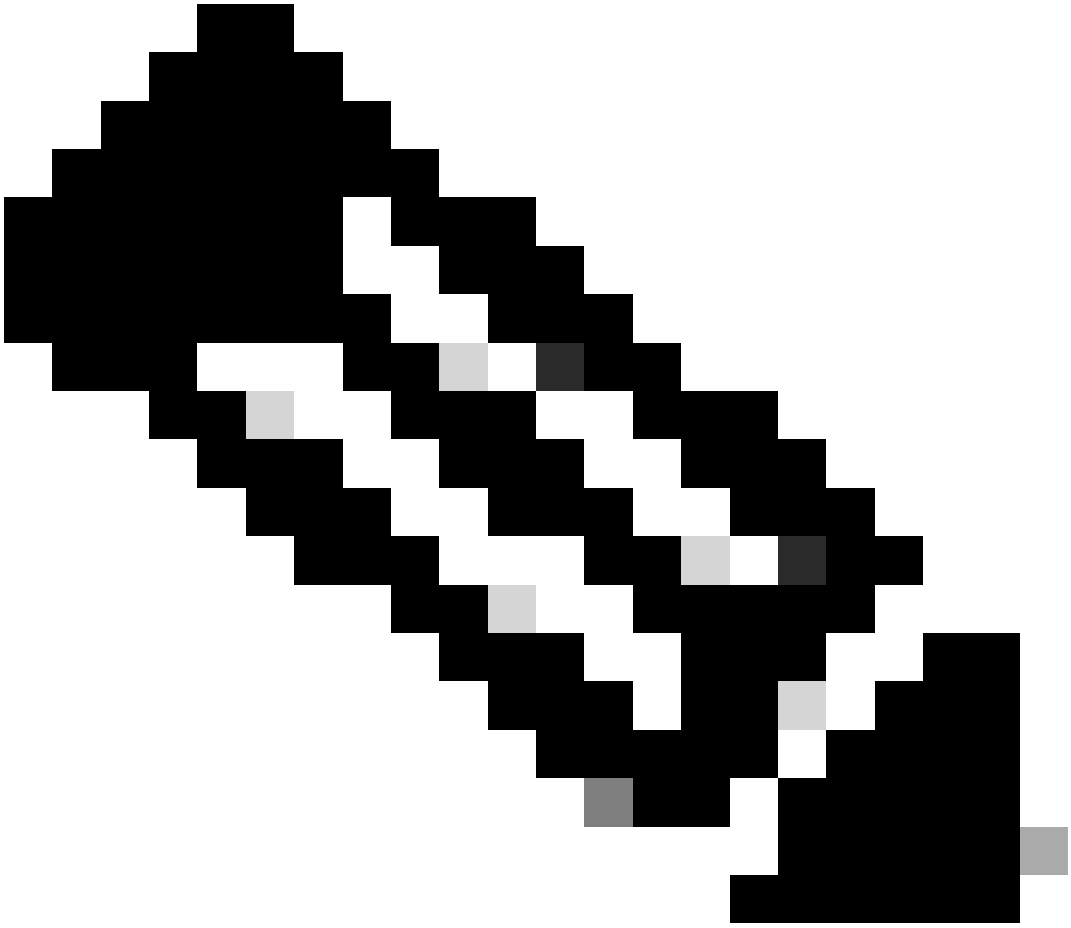
由于Active Directory登录使用这些解决方案的方式存在限制，因此不支持通过802.1x、RADIUS或ISE进行身份验证。AD连接器查找的登录事件通常不会生成。

阅读有关AD连接器查找的事件ID的详细信息，请访问：连接器服务正在查找哪些Window Events/EventID?

最常见的是，身份验证服务的IP地址映射到AD用户，而不是用户计算机的IP地址。

替代解决方案

通过使用启用了身份支持功能的漫游客户端，也可以实现AD集成。有关此功能的详细信息，请参阅我们的部署文档。



注意：此解决方案要求网络中不存在虚拟设备，因为这会导致漫游客户端进入禁用的“VA后”状态。

如果在网络中使用虚拟设备，则可以使用内部IP地址进行标识。例如，可以为无线网络的地址范围创建“内部网络”标识，然后对此标识应用策略。此方法的唯一缺点是，此地址范围内的所有设备都接收相同的策略。

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）。