对Umbrella Active Directory中的本地帐户应用策略

目录

简介

本文档介绍将Umbrella内部产品与Active Directory和本地用户帐户同步时的预期策略行为。

Umbrella虚拟设备和本地帐户标识

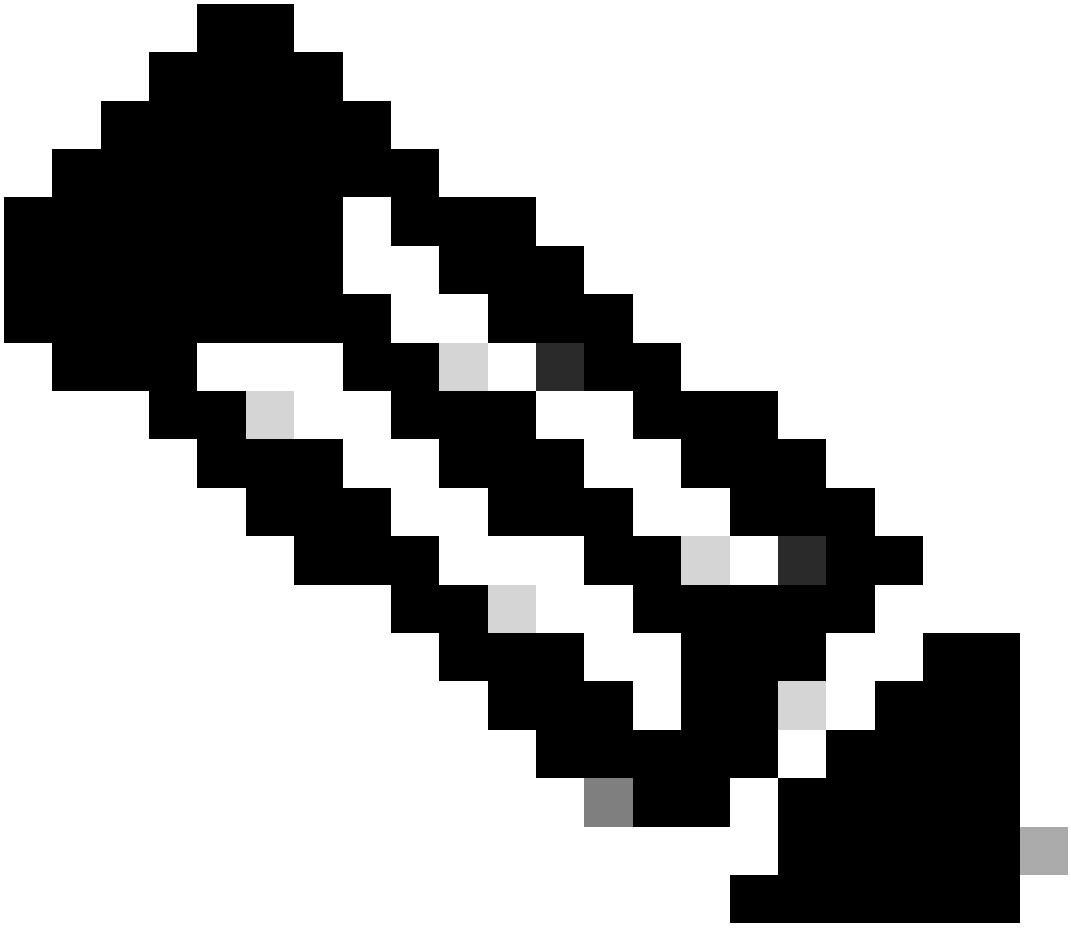
Umbrella虚拟设备从Windows域控制器接收Active Directory登录信息。它根据源IP地址缓存和标识Active Directory用户。

- 域控制器不会跟踪本地用户登录，因此虚拟设备无法直接识别这些用户。
- 如果Active Directory用户最近从IP地址登录，仍可以根据缓存使用缓存的标识。虚拟设备无法知道AD用户已替换为本地帐户。
- 如果不存在缓存的用户，虚拟设备将使用默认（非AD）身份。触发的身份可以是：
  - Umbrella站点名称（例如，默认站点）
  - 内部网络（内部IP地址）
  - 网络（外部IP地址）

Umbrella虚拟设备建议

- 限制对本地帐户和密码的访问。
- 为Umbrella站点名称创建单独的策略（例如，默认站点）。 为此策略分配比标准Active Directory用户策略更低的优先级。如果未检测到AD用户，则应用此限制更严格的策略。
- 如果本地用户帐户需要不同的策略，请考虑部署Umbrella漫游客户端。

Umbrella漫游客户端和本地帐户策略



注意：要将Active Directory与漫游客户端集成，请导航到身份>漫游计算机，并启用设置启用Active Directory用户和组策略实施。

漫游客户端从Windows注册表中检测登录用户，启用通过其唯一AD GUID标识Active Directory用户。

- 漫游客户端无法识别本地用户名以用于策略目的。
- 当检测到AD用户时，AD用户身份适用于策略实施，包括离线时使用缓存凭证登录的AD用户。
- 如果未检测到任何AD用户（例如，本地用户登录时），则使用漫游计算机身份执行策略。

Umbrella漫游客户端建议

- 限制对本地帐户和密码的访问。
- 使用低于标准AD用户策略的优先级为漫游计算机创建单独的策略。此策略适用于未加入域或由本地用户使用的漫游计算机。

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）。