对Umbrella连接器阻止Active Directory服务帐户进行故障排除

目录

简介

本文档介绍如何对Active Directory服务帐户被Umbrella连接器阻止的原因进行故障排除。

概述

Umbrella连接器服务对属于同一Umbrella站点的任何已注册域控制器(DC)的事件日志进行WMI连接，以便读取登录事件信息。 然后分析这些登录事件并将其上传到位于同一Umbrella站点的所有虚拟设备(VA)。然后，VA为该用户名/源IP地址创建临时用户到IP映射。有一点值得注意：

- Umbrella Insights一次只能支持每个IP一个登录用户
- 源IP的最近处理的登录事件“wins”

由于所有登录事件都是相同的，因此连接器有一个硬编码列表，其中包含忽略其事件的常见AD服务帐户。 您可以查看连接器日志文件中提取的来自这些帐户的登录事件。例如：

已忽略列入黑名单的用户的事件：OpenDNS_Connector

这样做是为了防止服务帐户（就像标准用户在DC安全事件日志中生成登录事件一样）覆盖实际登录用户的用户到IP映射。

在大型环境中，根据服务帐户使用的进程/应用程序，它们每分钟也会生成数千个登录事件。这也是连接器的额外负载，它可能表现为用户登录和应用的正确策略之间的延迟，或随后丢失的已应用的正确策略。

阻止的帐户列表

- _vmware_user_
- 管理员
- 匿名
- 匿名登录
- ASPNET
- 本地服务

- McAfeeMVSUser
- MHConcontrol
- 网络服务
- netwrix
- OpenDNS_Connector
- peersyncsvc
- s-pcadmin
- SophosUpdateMgr
- SophosUpdMgr
- svc-altiris
- svc.iCreate

更多信息

您还可以排除连接器处理任何其他AD帐户登录事件。有关说明，请参阅本文：

https://support.umbrella.com/hc/en-us/articles/231266088

此外，可以从连接器的AD同步中排除AD组，执行AD同步是为了使用AD用户、计算机和组的列表填充仪表板策略区域。您可以在以下位置找到此项：

https://support.umbrella.com/hc/en-us/articles/115005206526

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）。