了解连接器读取的窗口事件/事件ID

目录

简介

本文档介绍连接器默认读取哪些窗口事件/事件ID。

概述

Umbrella虚拟设备(VA)在技术上仅能看到接收DNS查询的源IP地址。为了让用户与DNS请求相关联，VA与连接器配合工作，导致发生用户到IP的映射。

连接器从域控制器上的安全事件日志中读取具有特定事件ID的事件。然后分析这些事件，并将用户名和源IP地址发送到VA，VA随后在该源IP和用户之间创建映射。

如果域控制器未审核这些事件，将无法正确执行VA映射过程。本文准确概述了连接器默认监视的事件ID类型。

事件ID	描述
4624	事件4624记录了每次成功登录本地计算机的尝试，无论登录类型、用户位置或帐户类型如何。
528	只要帐户登录到本地计算机，就会记录事件528，网络登录事件除外。无论用于登录的帐户是本地SAM帐户还是域帐户，都会记录事件528。
540	当网络中其他位置的用户连接到此计算机上的服务器服务提供的资源（如共享文件夹）时，会记录事件540。
4768	此事件仅在域控制器上记录，并且同时记录此事件的成功和失败实例。
4769	Windows将此事件ID用于成功和失败的服务票证请求。

如果连接器无法直接从域控制器的安全事件日志读取事件，您可以向Umbrella提交支持票证，要求将此更改为WMI订阅。对于WMI订阅，连接器将订阅上面列出的所有事件。此外，连接器还会使用以下提及的EventID预订注销事件。请注意，默认情况下，连接器不会从安全事件日志中读取这些注

销事件。

事件ID	描述
538	每当用户注销时，无论是网络连接、交互式登录还是其他登录类型，都会记录事件538(有关登录类型的图表，请参阅事件528)。
4647	此事件表示登录会话结束，并可使用登录ID关联回登录事件4624。
4634	此事件也表示登录会话的结束，并可使用登录ID关联回登录事件4624。

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）。