排除Umbrella Insights和AD集成故障不检测用户流量

目录

简介

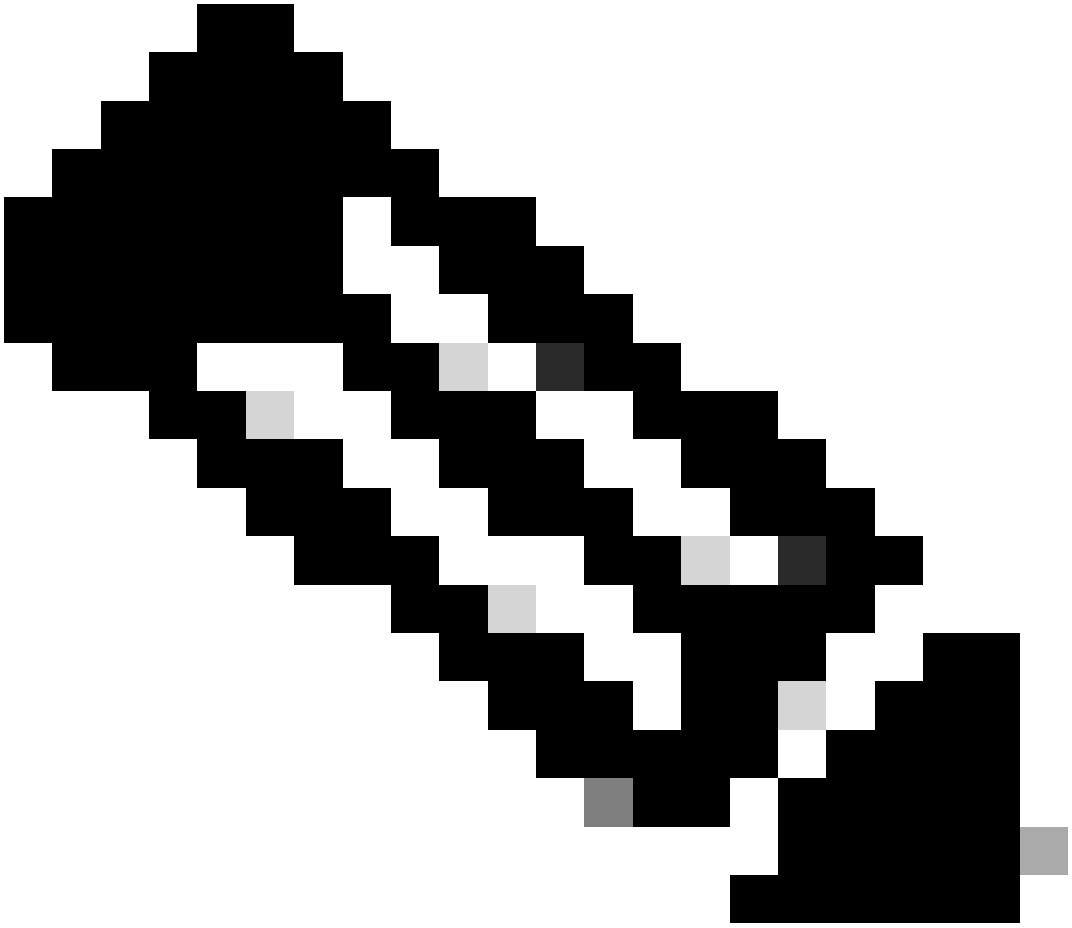
本文档介绍如何对不检测用户流量的Umbrella Insights AD集成进行故障排除。

概述

您已安装Umbrella Insights、设置连接器和虚拟设备并注册了域控制器。 所有组件都显示为绿色，并在控制面板中的`deployments-> Sites and Active Directory`下工作。但是，您已经配置了一个策略来使用AD用户或组对象，但是您仍然看不到控制面板中报告的用户活动或策略被正确应用。

您还可能注意到OpenDNSAuditClient.log文件中的此条目重复

'上次接收事件时间为1970-01-01 00:00:00'



注意：日志文件位于C:\Program Files(x86)\OpenDNS\OpenDNS Connector\<VERSION>\
VERSION =连接器服务的实际安装版本，例如v1.1.22

说明

发生这种情况的主要原因是可能未在您的Active Directory域中配置审核登录事件。日志消息表明连接器自安装后未看到一个单一用户事件。 目前，这不会在控制面板中生成错误。

分辨率

要检查的主要内容是检查AD组策略以查找正确的审核策略配置：

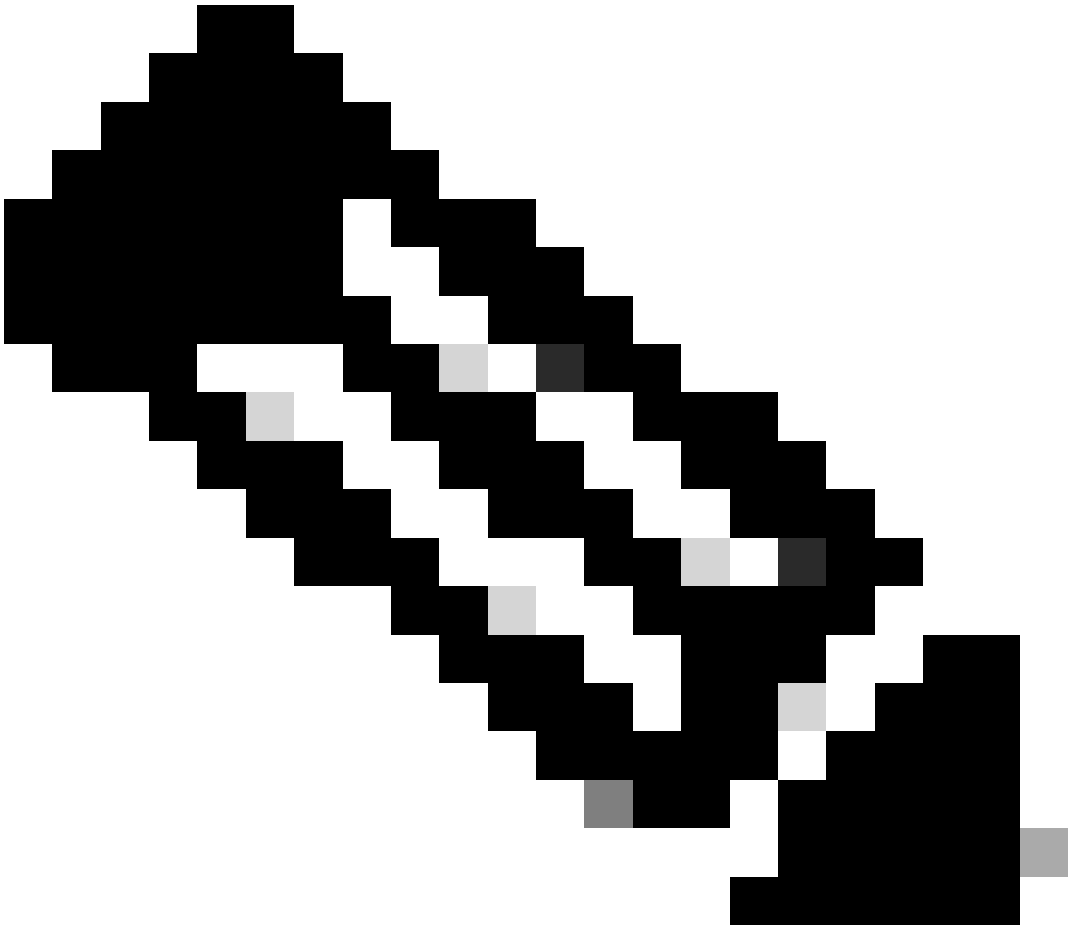
1. 在域控制器上，打开位于管理工具内的组策略管理面板，并选择适用于域控制器的策略（默认域控制器策略可能是候选策略）。

2. 右击该策略，然后选择Edit以启动组策略管理编辑器。

3. 浏览到“Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy”文件夹，然后选择Audit logon events以查看其属性。

4. 此策略必须用于审核Success尝试。

5. 运行gpupdate命令以应用策略。



注意：在某些情况下，“Default Domain Controllers and the Default Domain Policy”可能需要配置该设置。

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）。