使用WMI和DCOM日志收集排除Umbrella连接器故障

目录

简介

本文档介绍如何收集和审核WMI和DCOM日志，以解决Active Directory的Umbrella连接器权限问题。

概述

Umbrella连接器服务使用Windows Management Instrumentation(WMI)和分布式组件对象模型(DCOM)连接到Active Directory。 如果此过程失败，通常是由于OpenDNS_Connector用户缺少对DCOM或WMI命名空间的正确权限。在这种情况下，此错误可能会出现在OpenDNS连接器日志中：

```
EventMonitor Attach error: [AccessDenied] Access denied
```

要解决此问题，请使用《Active Directory集成安装指南》中详述的必备条件。如果需要进一步调试，或者需要确认权限问题，请查看Windows域控制器(DC)上的相关日志。

WMI和DCOM事件日志

必须从Umbrella连接器连接的域控制器（不一定是在安装连接器的位置）收集事件日志。

DCOM日志

在查看DCOM日志之前，请在域控制器上启用其他调试：

1. 打开Windows注册表编辑器(regedit.exe)。

2. 导航至：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole
```

3. 创建一个名为ActivationFailureLoggingLevel的新DWORD并将值设置为1。
4. 创建一个名为CallFailureLoggingLevel的新DWORD并将值设置为1。
5. 通过重新启动连接器重现“Access Denied”错误。
6. 打开Windows事件查看器(eventvwr.msc)。
7. 转到Windows Logs > System。
8. 过滤源中的事**DistributedCOM**件。OpenDNS_Connector的DCOM权限问题显示为相关事件。

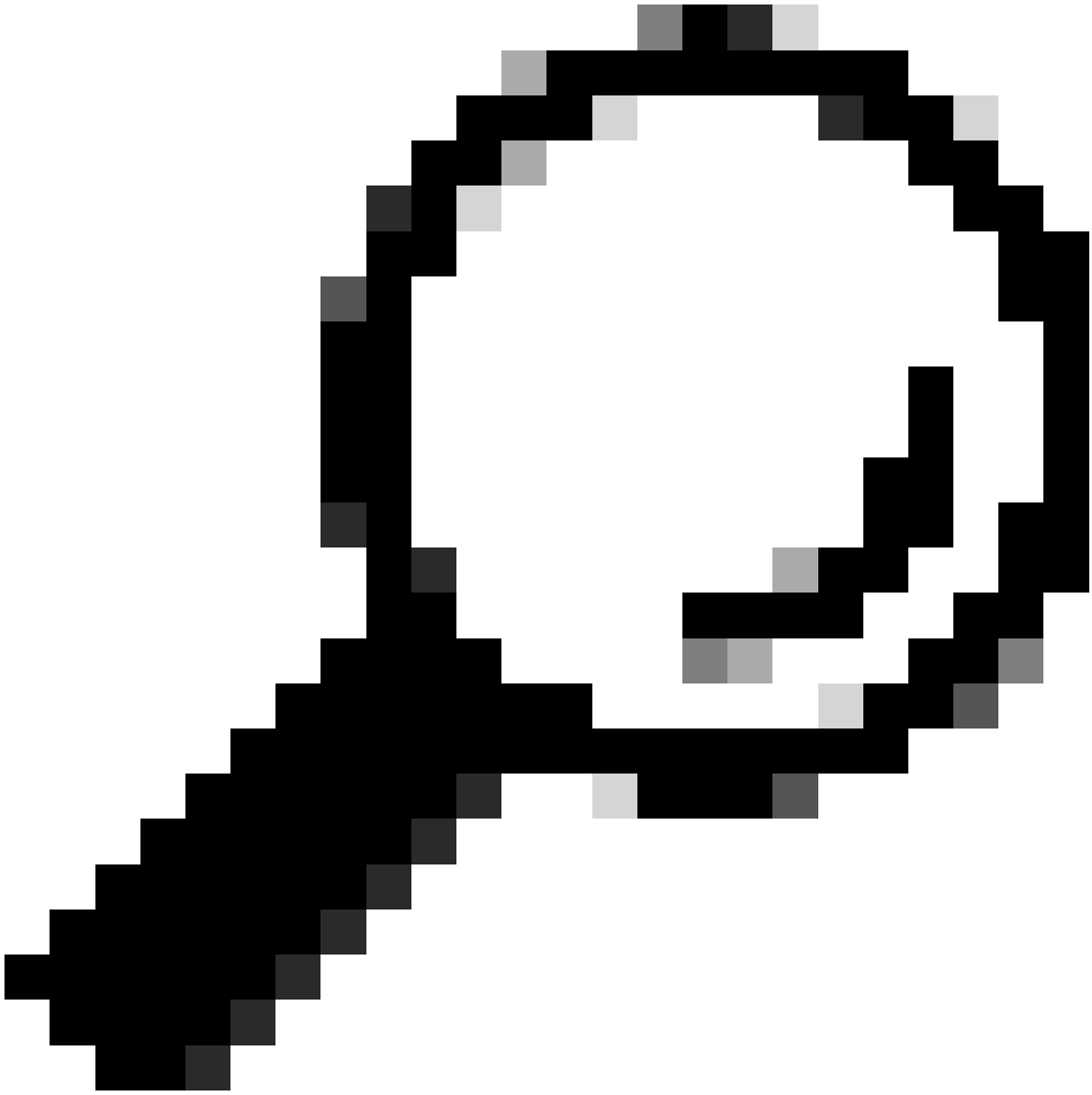
WMI日志

1. 打开Windows事件查看器(eventvwr.msc)。
2. 在“视图”菜单上，单击显示分析和调试日志。
3. 导航到应用和服务日志> Microsoft > Windows > WMI活动。
4. 提供三个日志文件：Debug、Operational和Trace。权限问题通常记录在操作日志中。
5. 在此处记录的WMIOpenDNS_Connector权限问题。

WMI跟踪日志

默认情况下未启用跟踪日志记录，但可以提供有关WMI查询的详细信息，包括成功的尝试和失败的尝试。

1. 打开Windows事件查看器(eventvwr.msc)。
2. 在“视图”菜单中，选择显示分析和调试日志。
3. 导航到应用和服务日志> Microsoft > Windows > WMI活动。
4. 右键单击Trace日志并选择Properties。
5. 选择Enable Logging，然后单击OK。一旦启用，系统将为接收的每个WMI查询记录信息事件。
6. 重新启动OpenDNS_Connector服务以生成新事件，从而确认是否正在处理查询。



提示：要结合此日志记录测试权限，请使用WBEMtest工具。

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）。