Troubleshoot Umbrella Connector with WMI and DCOM Log Collection

Contents

Introduction

This document describes how to collect and review WMI and DCOM logs to troubleshoot Umbrella Connector permission issues with Active Directory.

Overview

The Umbrella Connector service connects to Active Directory using Windows Management Instrumentation (WMI) and Distributed Component Object Model (DCOM). If this process fails, it is typically due to the OpenDNS_Connector user lacking correct permissions for DCOM or the WMI namespace. In such cases, this error can appear in the OpenDNS Connector logs:

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

To resolve this issue, utilize the prerequisites detailed in the Active Directory Integration Setup Guide. If further debugging is required, or if confirmation of a permissions issue is needed, review the relevant logs on the Windows Domain Controller (DC).

WMI and DCOM Event Logs

Event logs must be collected from the domain controller to which the Umbrella Connector is connecting (not necessarily where the Connector is installed).

DCOM Logs

Before viewing DCOM logs, enable additional debugging on the domain controller:

1. Open the Windows Registry Editor (regedit.exe).
2. Navigate to:

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

3. Create a new DWORD named ActivationFailureLoggingLeveland set the value to 1.
4. Create a new DWORD named CallFailureLoggingLevel and set the value to 1.
5. Reproduce the **'Access Denied'** error by restarting the Connector.
6. Open Windows Event Viewer (eventvwr.msc)**.**
7. Go to **Windows Logs > System**.
8. Filter for events with the source DistributedCOM. A DCOM permissions issue for **OpenDNS_Connector** appears as a relevant event.

WMI Logs

1. Open Windows Event Viewer (eventvwr.msc).
2. On the View menu, click **Show Analytic and Debug Logs**.
3. Navigate to **Applications and Service Logs > Microsoft > Windows > WMI Activity.**
4. Three log files are available: **Debug**, **Operational**, and **Trace**. Permissions issues are typically logged in the Operational log.
5. A WMI permissions issue for OpenDNS_Connector is recorded here.

WMI Trace Logs

Trace logging is not enabled by default but can provide detailed information about WMI queries, including both successful and failed attempts.

1. Open Windows Event Viewer (eventvwr.msc).
2. On the View menu, select **Show Analytic and Debug Logs**.
3. Navigate to **Applications and Service Logs > Microsoft > Windows > WMI Activity**.
4. Right-click the **Trace** log and select **Properties**.
5. Select **Enable Logging** and click **OK**. Once enabled, informational events is logged for each WMI query received.
6. Restart the OpenDNS_Connectorservice to generate new events, which confirms if the queries are being processed.
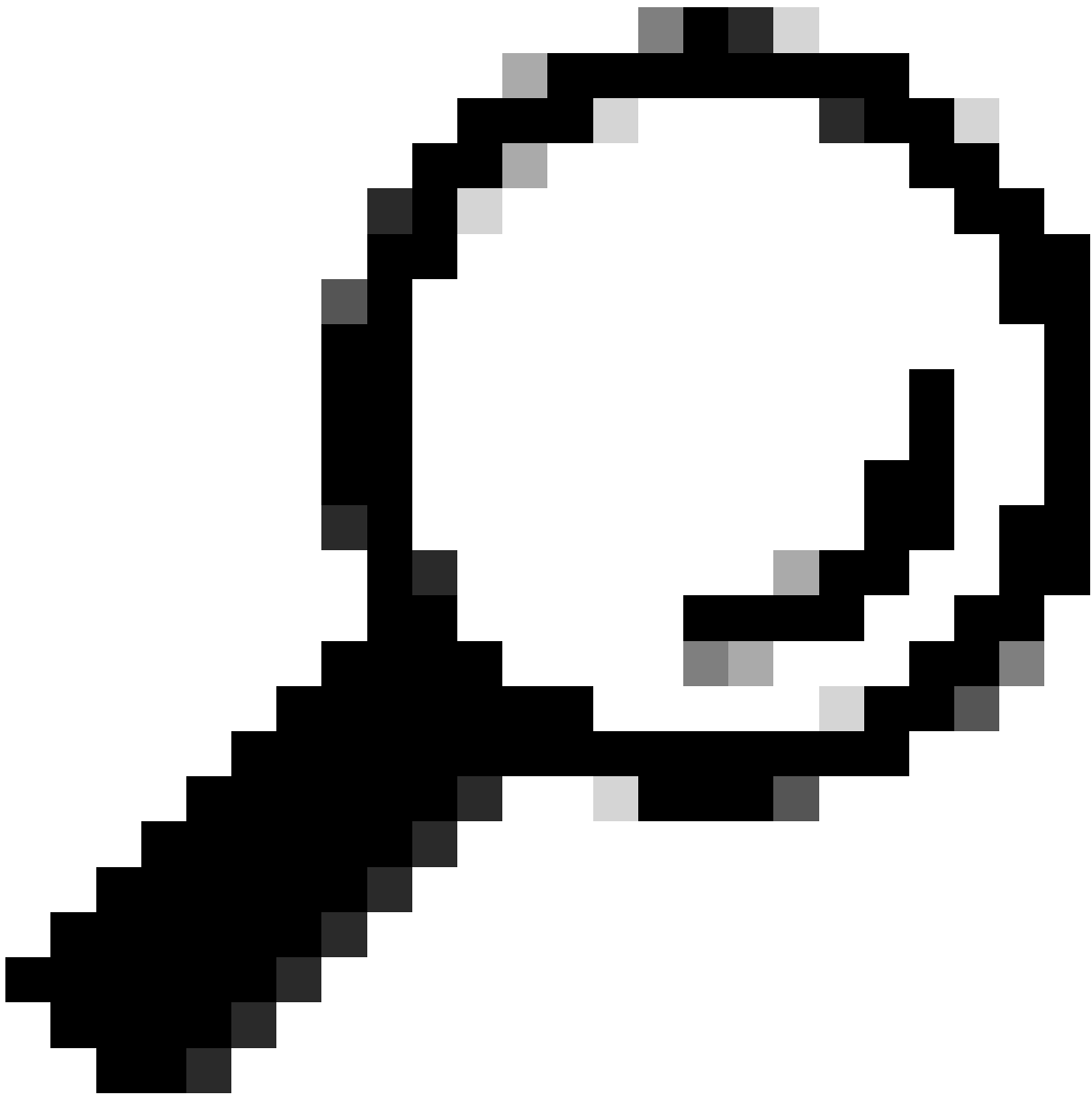
Tip: To test permissions in conjunction with this logging, use the WBEMtest tool.