Troubleshoot "Access Denied" Alert in Umbrella AD Connector

Contents

Introduction

This document describes troubleshooting "Access Denied" when the Cisco Umbrella Active Directory (AD) Connector is in Alert or Error states.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

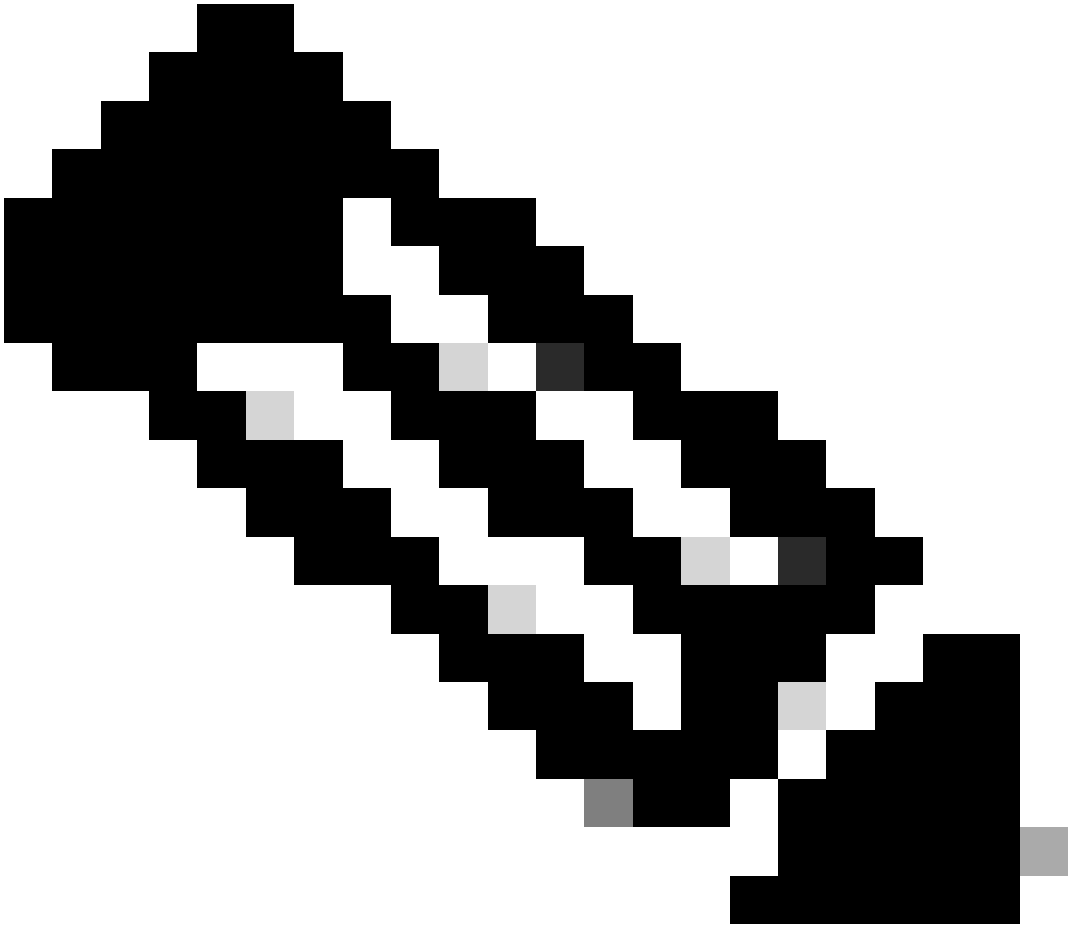
You notice that an AD Connector is showing alert or error state, and the message listed when you hover over the alert include "Access Denied" to one of the registered AD servers.

Solution

Please ensure that the OpenDNS_Connector user is a member of these AD Groups:

- Event Log Readers
- Distributed COM users
- Enterprise Read-only Domain Controllers

The solution is to make sure **DCOM**, **WMI** and **Manage Audit and Security Log** are setup correctly on the AD server in question.



> **Note**: Multiple domains or multiple forests are not supported by default. Please refer to the Multi-AD Domain Support in Umbrella announcement. You can also contact Umbrella Support about your configuration to get assistance if you run into these issues.

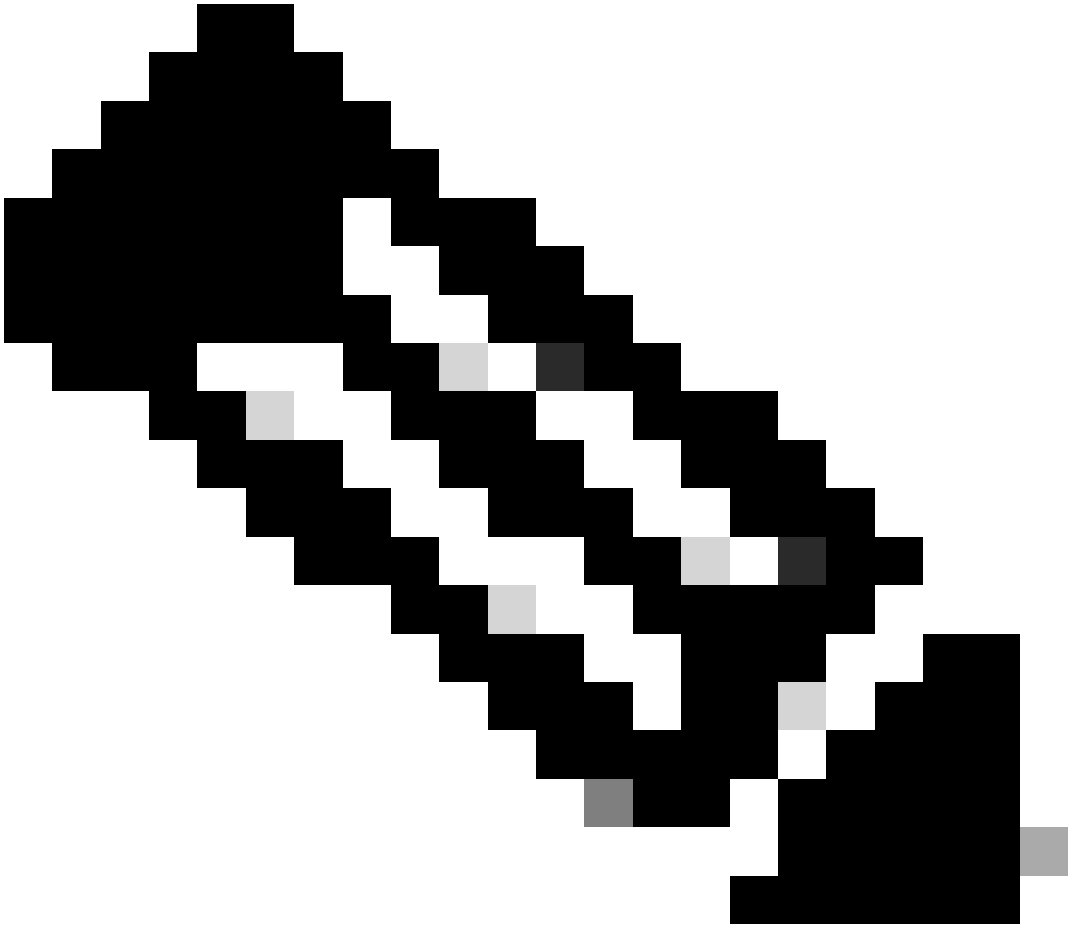
To verify WMI Permissions:

1. Select **Start > Run > wmimgmt.msc** to access the Windows Management Infrastructure Control console.
2. Right-click **WMI Control > Properties > Security tab**.
3. Select **Root > CIMV2 namespace** and select the **Security** button.
4. Add the **OpenDNS_Connector** user and **Allow** these permissions:

- Enable Account
- Remote Enable
- Read Security

To verify DCOM Permissions:

1. From a command line, run **dcomcnfg**.
2. Navigate to **Console Root > Component Services > Computers**.
3. Right-click on **My Computer** and select **Properties**.
4. From **My Computer Properties**, select the **COM Security** tab.
5. In the **Launch and Activation Permissions** section, select **Edit Limits**.
6. Add the OpenDNS_Connector user and allow **Remote Launch** and **Remote Activation** permissions.
7. Select **OK** to confirm and close My Computer Properties.



> **Note**: In most cases, if DCOM changes are made, a reboot of that DC is required for the changes to take effect.

To verify "Manage Audit and Security Logs" on Windows 2003 servers:

1. On a Domain Controller, open a command prompt and type this command (if you are running Windows 2003, replace /r with /v):

```
gpresult /scope computer /r
```

2. Look for the **Applied Group Policy Objects** line. Under it is a list of policies applied to that Domain Controller. Make note of one that can be applied to all Domain Controllers.
(like "Default Domain Controllers Policy"). If none exist, you need to create one and apply it.

To edit the proper policy:

3. Open the **Group Policy Management** panel (via Start/Administrative Tools). Select the desired policy. Something in the "Domain Controllers" folder is a likely candidate.

4. Right-click that policy and select **Edit** to bring up the **Group Policy Management Editor.**

5. Browse to the **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment** folder and select **Manage audit and security log** to view its properties.

6. Select **Define these policy settings >Add user or group**. Browse and select the OpenDNS_Connector user.

7. Run the "gpupdate /force" command on the Domain Controller to make sure the policy is applied.

Cause

This error usually indicates the OpenDNS_Connector user has insufficient permissions to operate.

The Windows Connector script normally sets the required permissions for the OpenDNS_Connector user. However, in strict AD environments, some administrators are not permitted to run VB scripts on their Domain Controllers, and thus needs to manually replicate the actions of the Windows Configuration script.

Additional Information

For the more information about resolving this issue please visit Complete Topics for Access Denied Resolution.

If after confirming/changing the aforementioned settings, you are still seeing "Access Denied" messages in the Dashboard, please send Support the Connector logs as outlined in this article: Provide Support with AD Connector Logs.