Integrate Active Directory Offline After Deployment of Secure Access Virtual Appliances

Contents

Issue

After deploying two Secure Access Virtual Appliances (VAs), Active Directory (AD) integration stopped functionin

Environment

- Technology: Solution Support (SSPT - contract required)
- Subtechnology: Secure Access
- Software Version: ALL
- Secure Access (DNS-Advantage/Umbrella)
- Deployment of two Secure Access Virtual Appliances (VAs) at headquarters
- Change event: Installation of VAs immediately preceded AD connector failure
- AD Connector previously operational and now displays as offline in the Secure Access portal

Resolution

To address the issue of AD integration showing as offline in the Secure Access portal after VA deployment, perform

Capture Network Traffic During Connector Restart

Run a Wireshark capture on all interfaces of the AD connector/domain controller while restarting the connector serv

Step 1: Start Wireshark Capture on All Relevant Interfaces

Start Wireshark and begin capturing on all AD connector/domain controller interfaces.

Step 2: Restart Connector Services via Windows Services Manager

Open services.msc, locate OpenDNS Connector service, and click **Restart**.

Step 3: Save Capture File for Further Analysis

Stop the capture and export the .pcap file.

Collect Connector Logs

Gather logs from the AD connector for deeper insight into errors or authentication issues:

1. Navigate to the log directory.

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\vX.X.X
```

1. Collect relevant log files and prepare them for review. Copy all log files from the aforementioned directory t

Verify AD Connector Account Permissions

After introducing Virtual Appliances, the AD Connector account requires specific permissions to function correctly.

1. Assign **Event Log Reader** permission to the AD Connector account. Use Active Directory Users and Comput **Event Log Readers** group.
2. Confirm the account has the new permission. Check group membership for the AD Connector account to verif

Common Exception Found

During troubleshooting, this exception can be observed in logs or connector status output:

```
* Exception type: system.unauthorizedaccessexception
message: Attempted to perform an unauthorized operation.
```

This indicates the AD Connector account does not have sufficient permissions, specifically the **Event Log Reader** r

No CLI command found which shows the change from AD connector status offline to online.

Cause

The underlying cause is insufficient permissions for the AD Connector account after the deployment of Secure Acce

Related Content

- Cisco Technical Support & Downloads