Troubleshoot Secure Access AD Connector Synchronization Issues

Contents

Issue

The AD Connector installed on a domain controller is not syncing properly with Cisco Secure Access. The connector experiences multiple synchronization failures including:

- Delta sync failures with "Access is denied" errors (COMException 0x80070005).
- DC event log read failures with "UnauthorizedAccessException: Attempted to perform an unauthorized operation".
- Cloud registration issues showing "Invalid URI format" when downloading the manifest.
- HTTP 404 "object_not_found" errors for specific AssetID during sync attempts.

The connector appears to have connectivity to Cisco Secure Access cloud service but fails on both the Active Directory permissions side and cloud registration configuration.

Environment

- Cisco Secure Access with AD Connector
- AD Connector version 1.15.2
- AD Connector installed on domain controller
- Custom service account (svcCiscoUmbrella) instead of default Cisco_Connector account
- Test/pilot environment setup

Resolution

The resolution involved addressing both Active Directory permissions issues and cloud registration problems through a complete reinstallation process:

Step 1: Verify and Clean Existing AD Connector Entries

In the Secure Access dashboard, verify the AD Connector entry for the host and remove any stale or duplicate entries for the same server if present.

Step 2: Ensure Complete Uninstallation

Completely uninstall the existing AD Connector service to ensure no residual configuration remains that could cause registration issues.

Step 3: Run Domain Controller Scripts

Before reinstalling the connector, run the proper domain controller configuration scripts to ensure appropriate permissions are set. The script needs to be run on each applicable domain controller, though the connector itself can reside outside the domain controller on another domain-joined computer.

Step 4: Configure Service Account Permissions

Grant the required Active Directory permissions to the service account:

- **AD sync permissions** (domain/root scope as appropriate):
    - Read
    - Replicating Directory Changes
    - Replicating Directory Changes All (if required in environment)
    - Replicating Directory Changes In Filtered Set (if required in environment)
- **Event log access on the Domain Controller**:
    - Add the service account to Event Log Readers group.
    - Ensure equivalent policy-based permission to read the Security log.

Step 5: Reinstall AD Connector

Reinstall the AD Connector service to generate a fresh manifest and valid AssetID, ensuring proper cloud registration.

Step 6: Restart and Validate

After installation and permission configuration:

1. Restart the AD Connector service.
2. Monitor the connector logs to confirm access denied and unauthorized errors stop.
3. Verify successful sync entries appear in logs (for example, "ADSync LDIF RESPONSE: 200 Success").

Cause

The synchronization issues were caused by two primary factors:

1. **Insufficient Active Directory Permissions:** The custom service account (svcCiscoUmbrella) lacked the required AD permissions for delta synchronization and DC event log access, resulting in "Access is denied" and "UnauthorizedAccessException" errors.
2. **Cloud Registration Problems:** The connector instance was mis-registered or pointing to an invalid/old AssetID, causing "Invalid URI format" errors when downloading the manifest and HTTP 404 "object_not_found" errors during sync attempts.

These issues were compounded by incomplete installation procedures where the domain controller configuration scripts were not properly executed before connector installation.

Related Content

- Cisco Secure Access AD Connector Configuration
- AD Connector Permissions Requirements
- AD Connector Installation Guide
- AD Connector Troubleshooting
- AD Connector Service Account Configuration

- Cisco Technical Support & Downloads