# Fehlerbehebung bei Problemen mit der AD-Connector-Synchronisierung für sicheren Zugriff

## Inhalt

## Problem

Der auf einem Domänencontroller installierte AD Connector wird nicht ordnungsgemäß mit Cisco Secure Access synchronisiert. Der Connector hat mehrere Synchronisierungsfehler, darunter:

- Fehler bei Deltasynchronisierung mit "Zugriff verweigert" (COMException 0x80070005).
- Fehler beim Lesen des DC-Ereignisprotokolls mit "UnauthorizedAccessException: Versucht, einen nicht autorisierten Vorgang auszuführen."
- Bei der Cloud-Registrierung treten beim Herunterladen des Manifests Probleme mit einem ungültigen URI-Format auf.
- HTTP 404 "object_not_found"-Fehler für bestimmte AssetID bei Synchronisierungsversuchen.

Der Connector scheint mit dem Cisco Secure Access Cloud-Service verbunden zu sein, schlägt jedoch sowohl bei den Active Directory-Berechtigungen als auch bei der Konfiguration der Cloud-Registrierung fehl.

## Umwelt

- Cisco Secure Access mit AD Connector
- AD Connector Version 1.15.2
- AD-Anschluss auf Domänencontroller installiert
- Benutzerdefiniertes Dienstkonto (svcCiscoUmbrella) anstelle des Cisco_Connector-Standardkontos
- Einrichtung der Test-/Pilotumgebung

# Auflösung

Die Lösung umfasste die Behebung von Problemen mit Active Directory-Berechtigungen und Problemen mit der Cloud-Registrierung durch einen vollständigen Neuinstallationsprozess:

## Schritt 1: Bestehende AD-Steckereinträge überprüfen und bereinigen

Überprüfen Sie im Dashboard für sicheren Zugriff den AD Connector-Eintrag für den Host, und entfernen Sie alle veralteten oder doppelten Einträge für den gleichen Server, sofern vorhanden.

## Phase 2: Vollständige Deinstallation

Deinstallieren Sie den vorhandenen AD Connector-Dienst vollständig, um sicherzustellen, dass keine Restkonfiguration erhalten bleibt, die Registrierungsprobleme verursachen könnte.

## Schritt 3: Domänencontrollerskripts ausführen

Führen Sie vor der Neuinstallation des Connectors die richtigen Domänen-Controller-Konfigurationsskripte aus, um sicherzustellen, dass die entsprechenden Berechtigungen festgelegt wurden. Das Skript muss auf jedem anwendbaren Domänencontroller ausgeführt werden, obwohl sich der Connector selbst außerhalb des Domänencontrollers auf einem anderen Computer befinden kann, der einer Domäne angehört.

## Schritt 4: Konfigurieren von Dienstkontenberechtigungen

Gewähren Sie dem Dienstkonto die erforderlichen Active Directory-Berechtigungen:

- AD-Synchronisierungsberechtigungen (Domäne/Root-Bereich, falls zutreffend):
    - Lesen

    - Verzeichnisänderungen replizieren
    - Alle Verzeichnisänderungen replizieren (falls in der Umgebung erforderlich)
    - Replikation von Verzeichnisänderungen in gefiltertem Set (falls in der Umgebung erforderlich)
- Ereignisprotokollzugriff auf dem Domänencontroller:
    - Fügen Sie das Dienstkonto der Gruppe Ereignisprotokollleser hinzu.
    - Stellen Sie eine entsprechende richtlinienbasierte Berechtigung zum Lesen des Sicherheitsprotokolls sicher.

### Schritt 5: Neuinstallation des AD-Anschlusses

Installieren Sie den AD Connector-Dienst neu, um ein neues Manifest und eine gültige AssetID zu generieren, und stellen Sie die ordnungsgemäße Cloud-Registrierung sicher.

### Schritt 6: Neustart und Validierung

Nach der Installation und der Berechtigungskonfiguration:

1. Starten Sie den AD Connector-Dienst neu.
2. Überwachen Sie die Connector-Protokolle, um zu bestätigen, dass der Zugriff verweigert wurde und nicht autorisierte Fehler beendet wurden.
3. Überprüfen Sie, ob erfolgreiche Synchronisierungseinträge in Protokollen angezeigt werden (z. B. "ADSync LDIF RESPONSE: 200 Success").

## Ursache

Die Synchronisierungsprobleme wurden hauptsächlich durch zwei Faktoren verursacht:

1. Unzureichende Active Directory-Berechtigungen: Dem benutzerdefinierten Dienstkonto (svcCiscoUmbrella) fehlten die erforderlichen AD-Berechtigungen für die Delta-

Synchronisierung und den Zugriff auf das Ereignisprotokoll des Domänencontrollers, was zu Fehlern wie "Zugriff verweigert" und "UnauthorizedAccessException" führte.
2. Probleme bei der Cloud-Registrierung: Die Connectorinstanz war falsch registriert oder verwies auf eine ungültige/alte AssetID, was beim Herunterladen des Manifests zu Fehlern im "Ungültiges URI-Format" und bei Synchronisierungsversuchen zu HTTP 404-"object_not_found"-Fehlern führte.

Diese Probleme wurden durch unvollständige Installationsverfahren noch verschlimmert, bei denen die Konfigurationsskripte des Domänencontrollers vor der Connector-Installation nicht ordnungsgemäß ausgeführt wurden.

## Verwandte Inhalte

- Konfiguration des Cisco Secure Access AD Connectors
- AD Connector-Berechtigungsanforderungen
- AD Connector - Installationsanleitung
- Fehlerbehebung für AD Connector
- AD Connector-Dienstkontenkonfiguration
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.