Risoluzione dei problemi di sincronizzazione di Secure Access AD Connector

Sommario

Problema

Il connettore AD installato in un controller di dominio non è sincronizzato correttamente con Cisco Secure Access. Il connettore presenta più errori di sincronizzazione, tra cui:

- Errori di sincronizzazione delta con errori di accesso negato (COMException 0x80070005).
- Errori di lettura nel registro eventi del controller di dominio con "UnauthorizedAccessException: Tentativo di eseguire un'operazione non autorizzata".
- Problemi di registrazione del cloud che indicano "Formato URI non valido" durante il download del manifesto.
- HTTP 404 - "object_not_found" errori per AssetID specifico durante i tentativi di sincronizzazione.

Il connettore risulta connesso al servizio cloud Cisco Secure Access ma ha esito negativo sia sul lato delle autorizzazioni di Active Directory che sulla configurazione della registrazione del cloud.

Ambiente

- Cisco Secure Access con AD Connector
- AD Connector versione 1.15.2
- Connettore AD installato nel controller di dominio
- Account del servizio personalizzato (svcCiscoUmbrella) anziché account Cisco_Connector predefinito
- Impostazione ambiente di prova/pilota

Risoluzione

La risoluzione prevedeva la risoluzione dei problemi relativi alle autorizzazioni di Active Directory e dei problemi di registrazione del cloud mediante un processo di reinstallazione completo:

Passaggio 1: Verifica e pulitura delle voci esistenti del connettore AD

Nel dashboard Accesso sicuro verificare la voce Connettore AD per l'host e rimuovere eventuali voci non aggiornate o duplicate per lo stesso server, se presenti.

Passaggio 2: Assicurare la completa disinstallazione

Disinstallare completamente il servizio AD Connector esistente per garantire che non rimanga alcuna configurazione residua che potrebbe causare problemi di registrazione.

Passaggio 3: Esegui script controller di dominio

Prima di reinstallare il connettore, eseguire gli script di configurazione del controller di dominio appropriati per assicurarsi che siano impostate le autorizzazioni appropriate. Lo script deve essere eseguito in ogni controller di dominio applicabile, anche se il connettore stesso può risiedere all'esterno del controller di dominio in un altro computer aggiunto al dominio.

Passaggio 4: Configura autorizzazioni account del servizio

Concedere le autorizzazioni di Active Directory necessarie all'account del servizio:

- Autorizzazioni di sincronizzazione AD (dominio/ambito radice appropriato):
    - Lettura
    - Replica delle modifiche alla directory

    - Replica di tutte le modifiche alla directory (se richiesto nell'ambiente)
    - Replica delle modifiche delle directory nel set filtrato (se richiesto nell'ambiente)
- Accesso al registro eventi nel controller di dominio:
    - Aggiungere l'account del servizio al gruppo Lettori registro eventi.
    - Assicurarsi di disporre di autorizzazioni equivalenti basate su criteri per la lettura del registro protezione.

Passaggio 5: Reinstalla AD Connector

Reinstallare il servizio AD Connector per generare un nuovo manifesto e un AssetID valido, garantendo la corretta registrazione del cloud.

Passaggio 6: Riavvia e convalida

Dopo l'installazione e la configurazione delle autorizzazioni:

1. Riavviare il servizio AD Connector.
2. Monitorare i registri dei connettori per confermare l'accesso negato e l'interruzione degli errori non autorizzati.
3. Verificare che le voci di sincronizzazione completate vengano visualizzate nei log (ad esempio, "ADSync LDIF RESPONSE: 200 Success").

Causa

I problemi di sincronizzazione sono stati causati da due fattori principali:

1. Autorizzazioni di Active Directory insufficienti: L'account del servizio personalizzato (svcCiscoUmbrella) non disponeva delle autorizzazioni AD necessarie per la sincronizzazione delta e l'accesso al registro eventi del controller di dominio, con conseguenti errori di tipo "Accesso negato" e "EccezioneAccessoNonAutorizzato".

2. Problemi di registrazione cloud: L'istanza del connettore non è stata registrata correttamente o fa riferimento a un AssetID non valido/precedente, causando errori di "Formato URI non valido" durante il download del manifesto e errori HTTP 404 "object_not_found" durante i tentativi di sincronizzazione.

A questi problemi si sono aggiunte procedure di installazione incomplete in cui gli script di configurazione del controller di dominio non sono stati eseguiti correttamente prima dell'installazione del connettore.

Contenuto correlato

- Configurazione di Cisco Secure Access AD Connector
- Requisiti di autorizzazione per il connettore AD
- Guida all'installazione di AD Connector
- Risoluzione dei problemi del connettore AD
- Configurazione account del servizio AD Connector
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).