

Risoluzione dei problemi relativi alla sincronizzazione delle identità di utenti/gruppi in Cisco Secure Access con IDP diff

Sommario

Problema

In questo documento viene descritto come risolvere i problemi relativi alla sincronizzazione delle identità di utenti e gruppi in Cisco Secure Access con diversi provider di identità (IdP), ad esempio Okta, Microsoft Entra ID e IBM Cloud.

Ambiente

- Cisco Secure Access: integrazione del provisioning SCIM
- Si applica al connettore IdP di SCIM 2.0 (Okta, Azure AD)

Risoluzione

Panoramica

Cisco Secure Access supporta il provisioning delle identità di utenti e gruppi direttamente da Okta e Microsoft Entra ID (in precedenza Azure AD) utilizzando lo standard SCIM 2.0, che elimina la necessità di distribuire un connettore Active Directory (AD) locale per origini di identità solo cloud. In questo articolo vengono consolidati i presupposti dell'architettura, le modalità di errore comuni e le indicazioni per la risoluzione dei problemi che i tecnici e gli amministratori di zona incontrano più spesso quando implementano o mantengono questa integrazione.

Il documento è suddiviso in quattro sezioni:

- Configurazione: percorso per le istruzioni ufficiali di installazione
- Presupposti dell'architettura che, se violati, causano errori invisibili o difficili da diagnosticare
- Problemi specifici del provider (Okta vs Entra ID)
- Problemi generici del protocollo SCIM applicabili indipendentemente dall'IdP

Configurazione

In questo documento viene descritta la risoluzione dei problemi e non la configurazione iniziale. Per la configurazione dettagliata, consultare le note tecniche ufficiali di Cisco riportate in questo documento:

- Per configurare Cisco Secure Access con Microsoft Entra ID (Azure AD), fare riferimento a questo collegamento: [Assegnare a utenti e gruppi la protezione dell'accesso tramite Entra ID](#)
- Per configurare Cisco Secure Access con Okta, fare riferimento a questo collegamento: [Assegnazione dell'accesso sicuro a utenti e gruppi tramite OKTA](#)

Entrambi i documenti riguardano la generazione del token SCIM e l'URL di provisioning in Secure Access, la configurazione dell'applicazione corrispondente nell'IdP e l'esecuzione della sincronizzazione di provisioning iniziale.

Primer architettura

Prima di eseguire la risoluzione dei problemi, verificare che la distribuzione corrisponda a questi presupposti fondamentali. La maggior parte degli errori di sincronizzazione è riconducibile a uno di questi presupposti.

Un'origine identità alla volta

Il provisioning simultaneo degli stessi utenti o gruppi da un connettore AD locale e un ID cloud (Okta o Entra ID) non è supportato e determina un'applicazione dei criteri incoerente. Se si

esegue la migrazione da AD Connector a un IdP cloud:

- Arrestare il servizio AD Connector locale.
- Verificare che non siano in esecuzione processi di sincronizzazione residui prima di abilitare il provisioning IdP del cloud.

Le appliance virtuali rappresentano un'eccezione

Entra ID o Okta non sono in grado di fornire l'integrazione dell'identità per le appliance virtuali (VA), poiché l'IdP non ha visibilità sui mapping IP-utente privati richiesti dalle VA. Le distribuzioni VA richiedono ancora il connettore AD locale, indipendentemente da ciò che viene utilizzato per altri componenti.

Assegna e spingi

- Azione: Assegnazione di utenti o gruppi all'applicazione
 - Effetti: Assegna agli utenti membri di tale gruppo il ruolo Accesso protetto
- Azione: Spostamento di un gruppo (Okta)
 - Effetti: Esegue il provisioning dell'oggetto gruppo stesso (per la definizione della destinazione dei criteri). Non sincronizza alcun utente.



Nota: Non eseguire il push di un gruppo assegnato all'applicazione per il provisioning degli utenti. Ciò può creare uno stato di gruppo duplicato o in conflitto.

Limiti utenti e gruppi

Non esiste alcun limite rigido per il numero di utenti di cui è stato eseguito il provisioning da uno dei due IdP.

I gruppi sono limitati. Storicamente, si trattava di 200 gruppi per organizzazione, sia da Okta che da Entra ID; alcuni documenti attuali mostrano un tetto più alto (fino a 1.000) per Okta nello specifico. Tratta il numero esatto come dipendente dall'ambiente e conferma con il Cisco

Technical Assistance Center (TAC) o la documentazione Cisco corrente. Il provisioning dei gruppi oltre il limite non viene eseguito in modo invisibile all'utente e non viene rilevato alcun errore.

Se è necessaria una copertura più ampia, utilizzare un gruppo dinamico "Tutti gli utenti" (Entra ID) o "Tutti" (Okta) anziché tentare di eseguire il push di ogni gruppo singolarmente.

Ciclo di vita dei token SCIM

In Cisco Secure Access, i token vengono generati quando si sceglie Connetti > Utenti, gruppi e dispositivi endpoint > Gestione configurazione > Directory integrata. Il token viene visualizzato una sola volta al momento della creazione.

Quando si rigenera il token, il provisioning sul lato IdP viene interrotto immediatamente finché il nuovo token non viene immesso nella configurazione di provisioning di Microsoft Entra ID o Okta. Non è previsto alcun periodo di prova e l'errore sul lato IdP è spesso generico (errore di autenticazione) anziché un messaggio di token scaduto.

Aggiornare periodicamente il token per motivi di sicurezza e verificare la connessione sul lato IdP subito dopo la rotazione.

Problemi Specifici Di Okta

- Sintomo: I gruppi non vengono visualizzati in Accesso protetto
 - Causa principale: Se si spinge un gruppo, viene attivato solo l'oggetto gruppo; i membri non vengono sincronizzati.
 - Risoluzione: Assicurarsi che i membri del gruppo pertinenti siano assegnati separatamente all'applicazione in Assegnazioni.
- Sintomo: Provisioning degli utenti eseguito, ma attributi mancanti o errati
 - Causa principale: Il nome visualizzato e il nome utente delle superfici di Secure Access sono; I nomi indicati e i cognomi non sono elencati.
 - Risoluzione: Confermare che gli attributi obbligatori siano selezionati in modo esplicito per la sincronizzazione. non presumere che tutti i campi del profilo di Okta si propaghino.

- Sintomo: Il provisioning in modo invisibile all'utente non esegue alcuna operazione
 - Causa principale: Gli interruttori Crea utenti, Aggiorna attributi utente o Disattiva utenti non sono abilitati.
 - Risoluzione: Verificare che tutte e tre siano selezionate in Provisioning > To App nella console di amministrazione di Okta.
- Sintomo: objectGUID o attributo personalizzato non in sincronizzazione
 - Causa principale: L'attributo non viene aggiunto e mappato tramite Mapping profili utente.
 - Risoluzione: Aggiungere l'attributo objectGUID e creare il mapping del profilo corrispondente se questo identificatore è obbligatorio.
- Sintomo: Sincronizzazione interrotta dopo la rotazione del token
 - Causa principale: Token SCIM o API rigenerato in Secure Access ma non aggiornato in Okta.
 - Risoluzione: Immettere il nuovo token in Provisioning > Configura integrazione API ed eseguire nuovamente Test API Credentials.
- Sintomo: Impossibile determinare il motivo per cui un utente o un gruppo specifico non è riuscito
 - Causa principale: I registri non sono stati controllati per primi.
 - Risoluzione: Selezionare Report > Log di sistema in Okta, filtrato per l'applicazione Cisco User Management Connector, prima di procedere con l'escalation.
- Sintomo: Il conteggio dei gruppi supera il limite massimo, alcuni risultano mancanti senza errori
 - Causa principale: L'organizzazione ha più gruppi con ambito di quelli supportati da Accesso sicuro.
 - Risoluzione: Ridurre l'ambito di applicazione ai soli gruppi rilevanti per le politiche aziendali o richiedere a Cisco TAC il supporto di gruppi di livello superiore.

Problemi specifici di Microsoft Entra ID

- Sintomo: L'appartenenza dinamica ai gruppi non si riflette nell'accesso protetto
 - Causa principale: La regola di gruppo dinamico non è configurata correttamente oppure il gruppo non è incluso nell'ambito del provisioning.

- Risoluzione: Convalidare la regola di appartenenza dinamica direttamente in Entra ID prima di assumere un bug di sincronizzazione di Secure Access.
- Sintomo: Previsto SSO SAML per guidare l'identità SWG
 - Causa principale: AnyConnect Secure Web Gateway (SWG) non supporta l'autenticazione SAML (Security Assertion Markup Language) con Entra ID; utilizza lo stesso meccanismo di autenticazione passiva di AD locale.
 - Risoluzione: non progettare intorno all'identità SWG basata su SAML per Entra ID; utilizzare l'autenticazione passiva come documentato.
- Sintomo: L'utente non visualizza correttamente la disattivazione
 - Causa principale: Entra ID inviato attivo: false perché l'utente è stato escluso da un ambito di gruppo assegnato o un mapping di attributi attivo non è configurato correttamente.
 - Risoluzione: Verificare se l'utente è stato rimosso da un gruppo con ambito; verificare il mapping attivo (in genere deve essere valutato come Not([isSoftDeleted])).
- Sintomo: Applicazione in quarantena, provisioning interrotto
 - Causa principale: L'applicazione di destinazione ha restituito risposte ripetute non conformi a SCIM.
 - Risoluzione: Verificare lo stato di provisioning dell'applicazione enterprise per un flag di quarantena prima di assumere errori di singoli utenti.
- Sintomo: Il ciclo di provisioning iniziale non riesce in modo definitivo
 - Causa principale: Errore di sincronizzazione temporaneo alla prima esecuzione.
 - Risoluzione: Fare clic su Riavvia provisioning dalla pagina Panoramica per forzare Entra ID a tentare di nuovo la sincronizzazione iniziale.
- Sintomo: Unione imprevista di utenti duplicati
 - Causa principale: Due identità di origine condividono lo stesso indirizzo di posta elettronica o lo stesso nome dell'entità utente (UPN).
 - Risoluzione: Garantire l'univocità di posta elettronica e UPN nella directory di origine; verificare che l'attributo mail provenga da un dominio verificato.
- Sintomo: L'aggiornamento dell'attributo viene interrotto dopo una modifica dello schema
 - Causa principale: Il tipo di attributo è stato modificato sul lato di destinazione (ad esempio, da stringa a booleano) ma il mapping di ID Entra non è stato aggiornato.
 - Risoluzione: Correggere manualmente il tipo in Impostazioni avanzate in Mapping attributi.

- Sintomo: Il riferimento al manager non viene mai popolato
 - Causa principale: Un utente rientrava nel campo di applicazione prima che il suo responsabile lo fosse; il provisioning non esegue automaticamente il backfill.
 - Risoluzione: Riavviare il provisioning per forzare una rivalutazione completa di tutti gli utenti nell'ambito.

Problemi specifici della verifica della sicurezza IBM

- Sintomo: Gli utenti eseguono il provisioning ma i gruppi non vengono mai visualizzati in Accesso sicuro
 - Causa principale: Verificare che il connettore SCIM personalizzato esegua solo operazioni utente. non viene mai inviata alcuna chiamata POST /Groups (gap della funzionalità di provisioning dell'account, non errore di mapping).
 - Risoluzione: Acquisire una traccia del connettore e confermare se si verificano chiamate /Groups; se nessuno, effettuare il provisioning dei gruppi tramite Cisco AD Connector, l'importazione CSV o uno script pianificato sull'endpoint Secure Access SCIM.
- Sintomo: L'aggiornamento dell'appartenenza al gruppo non riesce con 400 o 404
 - Causa principale: members[].value fa riferimento a Verify internal user IDs (Verifica ID utente interni) anziché a SCIM ID Secure Access (Accesso protetto ID SCSi) restituito durante la creazione dell'utente.
 - Risoluzione: Correggere il mapping dei membri per utilizzare l'ID SCIM Secure Access ed eseguire di nuovo una sincronizzazione completa.
- Sintomo: I gruppi sono vuoti
 - Causa principale: Gruppo sottoposto a push prima che i relativi utenti membri esistessero in Secure Access; la PATCH di appartenenza fa riferimento a utenti sconosciuti.
 - Risoluzione: Eseguire di nuovo una sincronizzazione completa ora che gli utenti esistono; assicurarsi che l'ordinamento della sincronizzazione crei gli utenti prima dei gruppi.
- Sintomo: Loop di accesso SAML o reindirizzamenti ripetuti
 - Causa principale: Verificare che l'endpoint IdP sia stato inserito nel proxy o decrittografato dal file SWG, interrompendo così il flusso di autenticazione.

- Risoluzione: Ignorare l'URL Verify IdP da SAML o decrittografia (elenco di domini esterni o decrittografia selettiva).
- Sintomo: L'utente esegue l'autenticazione tramite SAML ma non corrisponde ai criteri basati sull'utente
 - Causa principale: SAML NameID non corrisponde all'authName dell'utente di cui è stato eseguito il provisioning.
 - Risoluzione: Allineare il formato NameID > nell'applicazione Verify SAML con il mapping di attributi authName (in genere email o UPN). prova di nuovo.
- Sintomo: Il provisioning smette di funzionare dopo settimane o mesi di stabilità
 - Causa principale: Il token SCIM è stato ruotato o è scaduto in Secure Access ma non è stato aggiornato nel connettore Verify.
 - Risoluzione: Aggiornare il token in Secure Access e aggiornarlo nell'applicazione personalizzata Verify; calendario la frequenza di aggiornamento.
- Sintomo: Utenti duplicati creati alla risincronizzazione
 - Causa principale: externalId mappato a un attributo modificabile o non univoco (ad esempio, nome visualizzato, indirizzo di posta elettronica modificabile).
 - Risoluzione: Eseguire il mapping di externalId a un identificatore non modificabile (verificare l'ID utente o objectGUID); eliminare i duplicati e ripetere la sincronizzazione.
- Sintomo: Disattivato Verificare che gli utenti rimangano attivi in Accesso sicuro
 - Causa principale: Azione di sospensione non mappata su active:false o operazione di disattivazione disabilitata nel connettore.
 - Risoluzione: Abilitare l'operazione di disattivazione e mappare la sospensione su active:false; verificare con un utente di test.
- Sintomo: Le modifiche degli attributi in Verifica non vengono propagate
 - Causa principale: Utente o attributo fuori dall'ambito dei criteri di provisioning o operazione di aggiornamento disabilitata.
 - Risoluzione: Rivedere la politica o i diritti di provisioning delle applicazioni; abilitare gli aggiornamenti; attiva una sincronizzazione manuale.
- Sintomo: Accesso sicuro rifiuta le richieste con errori di schema o di tipo 501
 - Causa principale: Payload non conforme a SCIM (array di schemi mancante, URN errato, operazione non supportata).
 - Risoluzione: riprodursi con la prova di curl di base; correggere il payload o la mappatura; passare a IBM se il connettore emette una richiesta non valida.

- Sintomo: Identità SWG mancante per gli utenti in roaming nonostante il funzionamento di SAML
- Causa principale: Previsto SAML per l'identità dell'unità per una modalità di distribuzione che utilizza un'identità passiva o basata su agente.
- Risoluzione: confermare il metodo di acquisizione dell'identità per ogni modalità di distribuzione in base alla documentazione di Secure Access; non progettare SAML come unica origine di identità.

Problemi SCIM generici

Questi non sono specifici di Cisco ma vengono visualizzati in modo coerente nelle distribuzioni Secure Access perché il trasporto sottostante è lo standard SCIM 2.0:

- Gli stati di quarantena nascondono i singoli errori: Se la sincronizzazione sembra essere stata interrotta completamente, anziché non avere esito negativo per singolo utente, verificare lo stato di quarantena o sospensione a livello di applicazione prima di esaminare i singoli problemi relativi agli attributi.
- 409 Conflitto sulla disattivazione: Modello comune in cui l'IdP tenta di disattivare un utente e la destinazione genera un conflitto. Si tratta in genere di un problema di mapping degli attributi o di ambito di gruppo attivo, non di un vero errore di sistema.
- I campi vuoti o cancellati non vengono sempre propagati: Alcune implementazioni di server SCIM mantengono l'ultimo valore non nullo; quando si cancella un campo nell'IdP, può essere necessario inserire prima un valore segnaposto.
- Le modifiche all'URL o alla configurazione invalidano automaticamente l'autenticazione: Qualsiasi modifica all'URL dell'endpoint SCIM in genere richiede l'immissione successiva del token di connessione. Gli errori vengono rilevati come URL non valido anche quando il problema reale è un token non aggiornato.
- Nessun webhook o flusso di eventi nativo: Per l'automazione che prevede notifiche push in tempo reale su modifiche di utenti o criteri, è invece necessario eseguire il polling dell'API di reporting o l'integrazione tramite Cisco XDR. Secure Access non genera webhook di provisioning in uscita.

Passare a Cisco TAC con i log di provisioning dal lato IdP se i passaggi precedenti non risolvono il problema. I log di provisioning back-end sul lato Secure Access in genere richiedono l'accesso TAC per il pull.

Causa

L'integrazione del provisioning SCIM non è riuscita a eseguire il push di uno o più record a causa di un token di connessione scaduto, una mancata corrispondenza del mapping degli attributi, un gruppo di destinazione mancante o un ambito di provisioning insufficiente.

Contenuto correlato

- Cisco: [Assegnare a utenti e gruppi la protezione dell'accesso tramite Entra ID](#)
- Cisco: [Assegnazione dell'accesso sicuro a utenti e gruppi tramite OKTA](#)
- Informazioni su Microsoft: Problemi noti relativi alla conformità del protocollo SCIM 2.0 - Microsoft Entra ID
- Informazioni su Microsoft: Risoluzione dei problemi relativi agli errori dell'API SCIM Entra ID Microsoft
- Configurare SAML SSO nel provider di identità: <https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider>
- Provisioning per applicazioni personalizzate (SCIM): <https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications>
- Panoramica su provisioning e governance (connettore SCIM generico): <https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance>
- Bridge di provisioning locale (origini AD/LDAP): <https://docs.verify.ibm.com/verify/docs/on-premises-provisioning>

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).