

Fehlerbehebung bei Synchronisierung der Benutzer-/Gruppenidentität in Cisco Secure Access mit DIFF IDP

Inhalt

Problem

In diesem Dokument wird die Fehlerbehebung bei der Synchronisierung von Benutzer- und Gruppenidentitäten in Cisco Secure Access mit verschiedenen Identity Providern (IdPs) wie Okta, Microsoft Entra ID und IBM Cloud beschrieben.

Umwelt

- Cisco Secure Access - Integration der SCIM-Bereitstellung
- Gilt für SCIM 2.0 IdP-Connector (Okta, Azure AD)

Auflösung

Überblick

Cisco Secure Access unterstützt die direkte Bereitstellung von Benutzer- und Gruppenidentitäten von Okta und Microsoft Entra ID (ehemals Azure AD) mithilfe des SCIM 2.0-Standards. Damit entfällt die Notwendigkeit, einen standortbasierten Active Directory (AD) Connector für Identitätsquellen bereitzustellen, die nur in der Cloud verfügbar sind. Dieser Artikel fasst die Architekturannahmen, die gängigen Fehlermodi und die Anleitungen zur Fehlerbehebung zusammen, denen Außendiensttechniker und Administratoren bei der Bereitstellung oder Wartung

dieser Integration am häufigsten begegnen.

Dieses Dokument ist in vier Abschnitte gegliedert:

- Konfiguration - offizielle Installationsanweisungen
- Architekturannahmen, die, wenn sie verletzt werden, zu stillen oder schwer zu diagnostizierenden Ausfällen führen
- Anbieterspezifische Probleme (Okta und Entra-ID)
- Generische SCIM-Protokollprobleme, die unabhängig von IdP auftreten

Konfiguration

Dieser Artikel konzentriert sich auf die Fehlerbehebung, nicht auf die Ersteinrichtung. Verwenden Sie die offiziellen Cisco TechNotes in diesem Dokument für die schrittweise Konfiguration:

- Informationen zum Konfigurieren von Cisco Secure Access mit Microsoft Entra ID (Azure AD) finden Sie unter folgendem Link: Bereitstellung von Benutzern und Gruppen für den sicheren Zugriff über eine zusätzliche ID
- Informationen zur Konfiguration von Cisco Secure Access mit Okta finden Sie unter dem folgenden Link: Bereitstellung von Benutzern und Gruppen für den sicheren Zugriff über OKTA

In beiden Dokumenten wird das Generieren des SCIM-Tokens und der Bereitstellungs-URL in Secure Access, das Konfigurieren der entsprechenden Anwendung in der IdP und das Ausführen der anfänglichen Bereitstellungssynchronisierung behandelt.

Architektur-Primer

Stellen Sie vor der Fehlerbehebung sicher, dass die Bereitstellung diesen grundlegenden Annahmen entspricht. Die meisten Synchronisierungsfehler gehen auf eine dieser Annahmen zurück.

Eine Identitätsquelle nach der anderen

Die gleichzeitige Bereitstellung derselben Benutzer oder Gruppen über einen lokalen AD Connector und eine Cloud-IDp (Okta oder Entra ID) wird nicht unterstützt und führt zu einer inkonsistenten Richtliniendurchsetzung. Wenn Sie vom AD Connector zu einer Cloud-ID migrieren:

- Beenden Sie den lokalen AD Connector-Dienst.
- Vergewissern Sie sich, dass keine verbleibenden Synchronisierungsaufträge ausgeführt werden, bevor Sie die Cloud-IDp-Bereitstellung aktivieren.

Virtuelle Appliances sind die Ausnahme

Entra ID oder Okta können keine Identitätsintegration für virtuelle Appliances (VAs) bereitstellen, da der IdP keine Transparenz für private Zuordnungen von IP zu Benutzern aufweist, die von VAs benötigt werden. Für VA-Bereitstellungen ist ungeachtet der für andere Komponenten verwendeten Komponenten weiterhin der standortbasierte AD Connector erforderlich.

Zuweisen und Drücken

- Aktion: Zuweisen von Benutzern oder Gruppen zur Anwendung
 - Ihre tatsächlichen Funktionen: Gewährt den Mitgliedern dieser Gruppe sicheren Zugriff
- Aktion: Gruppe drücken (Okta)
 - Ihre tatsächlichen Funktionen: Stellt das Gruppenobjekt selbst bereit (für das Richtlinienziel). Es synchronisiert keine Benutzer.



Anmerkung: Pushen Sie keine Gruppe, die auch der Anwendung zur Benutzerbereitstellung zugewiesen ist. Dies kann zu doppeltem oder in Konflikt stehendem Gruppenstatus führen.

Gruppen- und Benutzerbeschränkungen

Es gibt keine feste Grenze für die Anzahl von Benutzern, die von beiden IdP bereitgestellt werden.

Gruppen sind begrenzt. Früher waren es 200 Gruppen pro Organisation von entweder Okta oder

Entra ID; einige aktuelle Dokumentationen zeigen eine höhere Obergrenze (bis zu 1.000) für Okta speziell. Die genaue Anzahl ist abhängig von der Umgebung. Nähere Informationen erhalten Sie vom Cisco Technical Assistance Center (TAC) oder in der aktuellen Cisco Dokumentation. Gruppen jenseits der Obergrenze werden ohne weitere Änderungen bereitgestellt, und es wird kein Fehler angezeigt.

Wenn Sie eine breitere Abdeckung benötigen, verwenden Sie eine dynamische Gruppe "Alle Benutzer" (Entra ID) oder "Alle" (Okta), anstatt zu versuchen, jede Gruppe einzeln zu verschieben.

SCIM-Token-Lebenszyklus

In Cisco Secure Access werden Token generiert, wenn Sie Verbinden > Benutzer, Gruppen und Endgeräte > Konfigurationsverwaltung > Verzeichnis integrieren auswählen. Das Token wird nur einmal bei der Erstellung angezeigt.

Wenn Sie das Token neu generieren, wird die Bereitstellung auf der IdP-Seite sofort unterbrochen, bis das neue Token in die Bereitstellungskonfiguration von Microsoft Entra ID oder Okta eingegeben wird. Es gibt keine Kulanzfrist, und der IdP-seitige Fehler ist häufig nicht ein abgelaufenes Token, sondern ein generischer Fehler (Authentifizierungsfehler).

Aktualisieren Sie den Token regelmäßig auf Sicherheitshygiene und testen Sie die Verbindung auf der IdP-Seite unmittelbar nach der Rotation.

Okta-spezifische Probleme

- Symptom: Gruppen werden in sicherem Zugriff nicht angezeigt.
 - Ursache: Das Pushen einer Gruppe stellt nur das Gruppenobjekt bereit. Member werden nicht synchronisiert.
 - Auflösung: Stellen Sie sicher, dass die relevanten Gruppenmitglieder der Anwendung unter "Zuweisungen" separat zugewiesen sind.
- Symptom: Benutzer bereitgestellt, aber Attribute fehlen oder sind falsch
 - Ursache: Secure Access zeigt nur Anzeigenamen und Benutzernamen an; Angegebene Namen und Familiennamen werden nicht aufgelistet.
 - Auflösung: Bestätigen, dass erforderliche Attribute explizit für die Synchronisierung

ausgewählt wurden; nicht davon ausgehen, dass sich alle Okta-Profilfelder ausbreiten.

- Symptom: Die Bereitstellung führt ohne Probleme zu Problemen.
 - Ursache: Benutzer erstellen, Benutzerattribute aktualisieren oder Benutzer deaktivieren sind nicht aktiviert.
 - Auflösung: Überprüfen Sie, ob alle drei Optionen unter Provisioning > To App (Bereitstellung > Auf App) in der Administratorkonsole von Okta aktiviert sind.
- Symptom: objectGUID oder benutzerdefiniertes Attribut wird nicht synchronisiert
 - Ursache: Das Attribut wird nicht über die Benutzerprofilzuordnung hinzugefügt und zugeordnet.
 - Auflösung: Fügen Sie das objectGUID-Attribut hinzu, und erstellen Sie die entsprechende Profilzuordnung, wenn dieser Bezeichner erforderlich ist.
- Symptom: Synchronisierung nach Tokenrotation beendet
 - Ursache: SCIM oder API-Token in Secure Access neu generiert, jedoch nicht in Okta aktualisiert.
 - Auflösung: Geben Sie das neue Token unter Provisioning > Configure API Integration ein, und führen Sie Test API Credentials erneut aus.
- Symptom: Warum ein bestimmter Benutzer oder eine bestimmte Gruppe fehlschlug, kann nicht ermittelt werden
 - Ursache: Die Protokolle wurden nicht zuerst überprüft.
 - Auflösung: Überprüfen Sie Reports > System Log in Okta, gefiltert nach Cisco User Management Connector, bevor Sie eskalieren.
- Symptom: Die Gruppengröße überschreitet die Obergrenze, einige fehlen ohne Fehler.
 - Ursache: Die Organisation hat mehr Gruppen, als Secure Access unterstützt.
 - Auflösung: Reduzieren Sie den Geltungsbereich auf die richtlinienrelevanten Gruppen, oder wenden Sie sich an das Cisco TAC für Support auf höherer Ebene.

Microsoft Entra ID-spezifische Probleme

- Symptom: Die dynamische Gruppenmitgliedschaft spiegelt sich nicht in Secure Access wider.
 - Ursache: Die Regel für dynamische Gruppen ist falsch konfiguriert, oder die Gruppe

befindet sich nicht im bereitgestellten Bereich.

- Auflösung: Validieren Sie die dynamische Mitgliedschaftsregel direkt in Entra ID, bevor Sie einen Fehler bei der Synchronisierung von Secure Access annehmen.
- Symptom: SAML SSO soll SWG-Identität fördern
 - Ursache: AnyConnect Secure Web Gateway (SWG) unterstützt keine SAML-Authentifizierung gegen Entra ID. Er verwendet den gleichen passiven Authentifizierungsmechanismus wie AD am Standort.
 - Auflösung: Keine SAML-gesteuerte SWG-Identität für die Entra-ID; verwenden Sie die dokumentierte passive Authentifizierung.
- Symptom: Der Benutzer zeigt fälschlicherweise deaktiviert an.
 - Ursache: Entra-ID wurde aktiv gesendet: false, weil der Benutzer aus einem zugewiesenen Gruppenbereich gefallen ist, oder weil eine aktive Attributzuordnung falsch konfiguriert ist.
 - Auflösung: Überprüfen, ob der Benutzer aus einer Gruppe mit Gültigkeitsbereich entfernt wurde; Überprüfen der aktiven Zuordnung (muss i. d. R. als `Not([isSoftDeleted])` ausgewertet werden).
- Symptom: Anwendung unter Quarantäne, Bereitstellung gestoppt
 - Ursache: Die Zielanwendung hat wiederholt nicht SCIM-konforme Antworten zurückgegeben.
 - Auflösung: Überprüfen Sie den Bereitstellungsstatus der Enterprise-Anwendung auf eine Quarantäne-Markierung, bevor Sie einzelne Benutzerfehler annehmen.
- Symptom: Erster Bereitstellungszyklus schlägt fehl
 - Ursache: Vorübergehender Synchronisierungsfehler beim ersten Durchlauf.
 - Auflösung: Klicken Sie auf der Seite "Overview" auf Restart Provisioning, um zu erzwingen, dass die Entra-ID erneut die erste Synchronisierung durchführt.
- Symptom: Unerwartetes Zusammenführen doppelter Benutzer
 - Ursache: Zwei Quellidentitäten verwenden dieselbe E-Mail oder denselben Benutzernamen (User Principal Name, UPN).
 - Auflösung: Eindeutigkeit von E-Mail und UPN im Quellverzeichnis sicherstellen; Überprüfen Sie, ob das E-Mail-Attribut von einer verifizierten Domäne stammt.
- Symptom: Attribut wird nach einer Schemaänderung nicht mehr aktualisiert
 - Ursache: Der Attributtyp wurde auf der Zielseite geändert (z. B. Zeichenfolge in Boolesch), aber die Entra-ID-Zuordnung wurde nicht aktualisiert.

- Auflösung: Korrigieren Sie den Typ unter Erweiterte Einstellungen unter Attributzuordnungen manuell.
- Symptom: Manager-Referenz wird nie aufgefüllt
 - Ursache: Ein Benutzer hatte bereits vor seinem Vorgesetzten einen Gültigkeitsbereich; wird bei der Bereitstellung nicht automatisch ein Backfill erstellt.
 - Auflösung: Starten Sie die Bereitstellung neu, um eine vollständige Neubewertung aller betroffenen Benutzer zu erzwingen.

IBM Security - Überprüfung bestimmter Probleme

- Symptom: Bereitstellung durch Benutzer, Gruppen werden jedoch nie in Secure Access angezeigt
 - Ursache: Überprüft, ob der benutzerdefinierte SCIM-Connector nur Benutzervorgänge ausgibt. POST/Gruppen-Anrufe werden nie gesendet (Lücke bei der Kontobereitstellungsfunktion, kein Zuordnungsfehler).
 - Auflösung: Erfassung einer Connector-Ablaufverfolgung und Überprüfung, ob irgendwelche /Gruppen-Anrufe auftreten; Falls nicht, stellen Sie Gruppen über den Cisco AD Connector, den CSV-Import oder ein geplantes Skript für den Secure Access SCIM-Endpunkt bereit.
- Symptom: Aktualisierung der Gruppenmitgliedschaft schlägt mit 400 oder 404 fehl
 - Ursache: members[].value referenziert Überprüfen Sie die internen Benutzer-IDs anstelle der SCIM-ID Sicherer Zugriff, die bei der Benutzererstellung zurückgegeben wurde.
 - Auflösung: Korrigieren Sie die Memberzuordnung, um die Secure Access SCIM-ID zu verwenden, und führen Sie eine vollständige Synchronisierung erneut aus.
- Symptom: Gruppen werden angezeigt, sind aber leer.
 - Ursache: Gruppe verschoben, bevor ihre Mitglieder Benutzer in Secure Access existierten; Mitgliedschaft PATCH verweist auf unbekannte Benutzer.
 - Auflösung: Führen Sie erneut eine vollständige Synchronisierung durch, sobald Benutzer vorhanden sind. sicherstellen, dass die Synchronisierungsreihenfolge Benutzer vor Gruppen erstellt.
- Symptom: SAML-Anmeldeschleifen oder wiederholte Weiterleitungen
 - Ursache: Überprüfen Sie, ob der IdP-Endpunkt von der SWG weitergeleitet oder

entschlüsselt wird, wodurch der Authentifizierungs-Workflow unterbrochen wird.

- Auflösung: Umgehen der Verify-IdP-URL von SAML oder der Entschlüsselung (Liste externer Domänen oder selektive Entschlüsselung).
- Symptom: Benutzer authentifiziert sich über SAML, aber keine benutzerbasierten Richtlinienübereinstimmungen
 - Ursache: SAML-NameID stimmt nicht mit dem bereitgestellten BenutzerauthName überein.
 - Auflösung: Richten Sie das Format NameID > in der Anwendung "Verify SAML" an der authName-Attributzuordnung aus (i. d. R. E-Mail oder UPN). erneut testen.
- Symptom: Bereitstellung funktioniert nach Wochen oder Monaten der Stabilität nicht mehr
 - Ursache: Das SCIM-Token wurde in Secure Access gedreht oder ist abgelaufen, wurde jedoch im Verify-Connector nicht aktualisiert.
 - Auflösung: Aktualisieren Sie das Token in Secure Access, und aktualisieren Sie es in der benutzerdefinierten Anwendung Verify. Kalender des Aktualisierungsrhythmus.
- Symptom: Bei erneuter Synchronisierung erstellte doppelte Benutzer
 - Ursache: externalId wird einem wandelbaren oder nicht eindeutigen Attribut zugeordnet (z. B. Anzeigename, wandelbare E-Mail).
 - Auflösung: Ordnen Sie externalId einem unveränderlichen Bezeichner zu (Überprüfung der Benutzer-ID oder objectGUID). Duplikate bereinigen und erneut synchronisieren.
- Symptom: Deaktiviert Überprüfung, ob Benutzer im sicheren Zugriff aktiv bleiben
 - Ursache: Aussetzaktion, die nicht active:false zugeordnet ist, oder Deaktivierungsvorgang, der im Connector deaktiviert ist.
 - Auflösung: Aktivieren Sie den Deaktivierungsvorgang, und ordnen Sie Suspend dem Befehl active:false zu. mit einem Testbenutzer überprüfen.
- Symptom: Attributänderungen in "Überprüfen" werden nicht weitergegeben
 - Ursache: Benutzer oder Attribut außerhalb des Bereitstellungsrichtlinienbereichs oder Aktualisierungsvorgang deaktiviert
 - Auflösung: Überprüfung der Bereitstellungsrichtlinie für Anwendungen oder der Berechtigungen Updates aktivieren; eine manuelle Synchronisierung auslösen.
- Symptom: Secure Access lehnt Anforderungen mit Schema- oder 501-ähnlichen Fehlern ab.
 - Ursache: Nicht-SCIM-konforme Nutzlast (fehlendes Schemaarray, falsches URN, nicht unterstützter Betrieb).

- Auflösung: Reproduktion mit dem Curl-Test zu Studienbeginn; die Nutzlast oder die Zuordnung korrigieren; zu IBM eskalieren, wenn der Connector die falsch geformte Anforderung aussendet.
- Symptom: SWG-Identität fehlt für Roaming-Benutzer trotz SAML-Bearbeitung
- Ursache: SAML soll die Identität für einen Bereitstellungsmodus steuern, der eine passive oder agentenbasierte Identität verwendet.
- Auflösung: die Identitätsfeststellungsmethode für jeden Bereitstellungsmodus anhand der Secure Access-Dokumentation bestätigen; entwerfen SAML nicht als alleinige Identitätsquelle.

Generische SCIM-Probleme

Diese sind nicht Cisco-spezifisch, treten jedoch bei Secure Access-Bereitstellungen konsistent auf, da der zugrunde liegende Transport der Standard-SCIM 2.0 ist:

- Einzelne Fehler werden durch Quarantänestatus maskiert: Wenn die Synchronisierung anscheinend nicht pro Benutzer fehlgeschlagen ist, sondern vollständig beendet wurde, überprüfen Sie den Quarantäne- oder Suspendierungsstatus auf Anwendungsebene, bevor Sie einzelne Attributprobleme untersuchen.
- 409 Konflikt bei Deaktivierung: Ein gängiges Muster, bei dem die IdP versucht, einen Benutzer zu deaktivieren, und das Ziel einen Konflikt auslöst. In der Regel handelt es sich dabei um ein aktives Problem mit der Attributzuordnung oder dem Gruppenbereich, nicht um einen echten Systemfehler.
- Leere oder gelöschte Felder werden nicht immer übertragen: Einige SCIM-Serverimplementierungen behalten den letzten Nicht-Null-Wert bei. Wenn Sie ein Feld in der IdP löschen, müssen Sie möglicherweise zuerst einen Platzhalterwert übertragen.
- URL- oder Konfigurationsänderungen machen die Authentifizierung automatisch ungültig: Jede Änderung an der SCIM-Endpunkt-URL erfordert in der Regel, dass Sie das Trägertoken erneut angeben. Fehler treten als ungültige URL auf, auch wenn das eigentliche Problem ein veraltetes Token ist.
- Kein nativer Webhook oder Event-Stream: Automatisierung, die Push-Benachrichtigungen in Echtzeit bei Benutzer- oder Richtlinienänderungen erwartet, muss die Reporting-API abfragen oder stattdessen über Cisco XDR integrieren. Secure Access gibt keine Webhooks für die ausgehende Bereitstellung aus.

Eskalieren Sie an das Cisco TAC mit Bereitstellungsprotokollen von der IdP-Seite, wenn das

Problem durch die vorherigen Schritte nicht behoben wird. Für Backend-Bereitstellungsprotokolle auf der Seite für sicheren Zugriff ist in der Regel ein TAC-Zugriff erforderlich.

Ursache

Bei der SCIM-Bereitstellungsintegration konnte aufgrund eines abgelaufenen Trägertokens, einer nicht übereinstimmenden Attributzuordnung, einer fehlenden Zielgruppe oder eines unzureichenden Bereitstellungsbereichs mindestens ein Datensatz nicht weitergeleitet werden.

Verwandte Inhalte

- Cisco: [Bereitstellung von Benutzern und Gruppen für den sicheren Zugriff über eine zusätzliche ID](#)
- Cisco: [Bereitstellung von Benutzern und Gruppen für den sicheren Zugriff über OKTA](#)
- Microsoft - Informationen: Bekannte Probleme mit der Einhaltung des SCIM 2.0-Protokolls - Microsoft Entra ID
- Microsoft - Informationen: Fehlerbehebung bei Fehlern der Microsoft Entra ID SCIM API
- Konfigurieren Sie SAML-SSO im Identitätsanbieter: <https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider>
- Bereitstellung benutzerdefinierter Anwendungen (SCIM): <https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications>
- Überblick über Bereitstellung und Governance (allgemeiner SCIM Connector): <https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance>
- Standortbasierte Provisioning Bridge (AD/LDAP-Quellen): <https://docs.verify.ibm.com/verify/docs/on-premises-provisioning>

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.