Solución de problemas de sincronización de identidad de usuario/grupo en Cisco Secure Access con diff IDP

Contenido

Problema

Este documento describe cómo resolver problemas de sincronización de identidad de usuarios y grupos en Cisco Secure Access con diferentes proveedores de identidad (IdPs) como Okta, Microsoft Entra ID e IBM Cloud.

Entorno

- Cisco Secure Access: integración de aprovisionamiento de SCIM
- Se aplica al conector IdP SCIM 2.0 (Okta, Azure AD)

Resolución

Overview

Cisco Secure Access admite el aprovisionamiento de identidades de usuarios y grupos directamente desde Okta y Microsoft Entra ID (anteriormente Azure AD) mediante el estándar SCIM 2.0, que elimina la necesidad de implementar un conector de Active Directory (AD) en las instalaciones para orígenes de identidad solo en la nube. En este artículo se consolidan las suposiciones sobre la arquitectura, los modos de fallo habituales y la guía de resolución de problemas con los que se encuentran con más frecuencia los administradores e ingenieros de

campo al implementar o mantener esta integración.

Este documento está organizado en cuatro secciones:

- Configuración: dónde dirigirse para obtener instrucciones de configuración oficiales
- Suposiciones de arquitectura que, si se infringen, provocan errores silenciosos o difíciles de diagnosticar
- Problemas específicos del proveedor (Okta frente a Entra ID)
- Problemas de protocolo SCIM genérico que se aplican independientemente del IdP

Configuración

Este artículo se centra en la resolución de problemas, no en la configuración inicial. Utilice las notas técnicas oficiales de Cisco de este documento para realizar una configuración paso a paso:

- Para configurar Cisco Secure Access con Microsoft Entra ID (Azure AD), consulte este enlace: Aprovisionamiento de usuarios y grupos para proteger el acceso mediante ID de entrada
- Para configurar Cisco Secure Access con Okta, consulte este enlace: Aprovisionamiento de usuarios y grupos para un acceso seguro mediante OKTA

Ambos documentos cubren la generación del token SCIM y la URL de aprovisionamiento en Secure Access, la configuración de la aplicación correspondiente en el IdP y la ejecución de la sincronización de aprovisionamiento inicial.

Manual de arquitectura

Antes de solucionar el problema, confirme que la implementación coincide con estas suposiciones principales. La mayoría de los errores de sincronización se remontan a una de estas suposiciones.

Un origen de identidad cada vez

No se admite el aprovisionamiento simultáneo de los mismos usuarios o grupos desde un conector AD en las instalaciones y un idP de nube (Okta o ID de Entra), lo que provoca una aplicación de políticas incoherente. Si migra desde el conector de AD a un idP de nube:

- Detenga el servicio del conector AD local.
- Confirme que no se estén ejecutando trabajos de sincronización residuales antes de activar el aprovisionamiento de IdP en la nube.

Los dispositivos virtuales son la excepción

Entra ID u Okta no pueden proporcionar integración de identidad para Virtual Appliances (VA), porque el IdP no tiene visibilidad en las asignaciones de IP a usuario privadas, que requieren los VA. Las implementaciones de VA siguen necesitando el conector AD en las instalaciones, independientemente de lo que se utilice para otros componentes.

Asignar frente a pulsar

- Acción: Asignar usuarios o grupos a la aplicación
    - Lo que realmente hace: Aprovisiona a los usuarios miembros de ese grupo a Secure Access
- Acción: Empujar un grupo (Okta)
    - Lo que realmente hace: Aprovisiona el propio objeto de grupo (para destinos de directiva). No sincroniza a ningún usuario.

Nota: No inserte un grupo que también esté asignado a la aplicación para el aprovisionamiento de usuarios. Esto puede crear un estado de grupo duplicado o conflictivo.

Límites de grupos y usuarios

No existe un límite en el número de usuarios aprovisionados desde cualquier IdP.

Los grupos están limitados. Históricamente, se trataba de 200 grupos por organización de Okta o Entra ID; algunos documentos actuales muestran un techo más alto (hasta 1.000) para Okta específicamente. Trate el número exacto como dependiente del entorno y confírmelo con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) o con la documentación actual de Cisco. Los grupos que se encuentran más allá del límite no se aprovisionan de forma silenciosa y no aparece ningún error.

Si necesita una cobertura más amplia, utilice un grupo dinámico "Todos los usuarios" (ID de entrada) o "Todos" (Okta) en lugar de intentar presionar cada grupo individualmente.

Ciclo de vida del token SCIM

En Cisco Secure Access, los tokens se generan cuando elige Connect > Users, Groups and Endpoint Devices > Configuration Management > Integrate Directory. El token se muestra solo una vez en la creación.

Cuando se regenera el token, se interrumpe inmediatamente el aprovisionamiento en el lado IdP hasta que se introduce el nuevo token en la configuración de aprovisionamiento de Microsoft Entra ID u Okta. No hay período de gracia, y el error del lado IdP es a menudo genérico (falla de autenticación) en lugar de un mensaje de token caducado.

Actualice el token periódicamente para la higiene de la seguridad y pruebe la conexión en el lado del IdP inmediatamente después de la rotación.

Problemas Específicos De Okta

- Síntoma: Los grupos no aparecen en Secure Access
    - Causa raíz: Al enviar un grupo sólo se aprovisiona el objeto de grupo; no sincroniza los miembros.
    - Resolución: Asegúrese de que los miembros pertinentes del grupo se asignen por separado a la solicitud en Asignaciones.
- Síntoma: Usuarios aprovisionados pero atributos faltantes o incorrectos
    - Causa raíz: Secure Access sólo superficies Mostrar nombre y nombre de usuario; Los nombres dados y los nombres de familia no aparecen en la lista.

    - Resolución: Confirmar que los atributos requeridos se seleccionan explícitamente para la sincronización; no asuma que todos los campos de perfil Okta se propagan.
- Síntoma: El aprovisionamiento silencioso no hace nada
    - Causa raíz: Las opciones Crear usuarios, Actualizar atributos de usuario o Desactivar usuarios no están habilitadas.
    - Resolución: Verifique que los tres estén marcados en Provisioning > To App en la consola del administrador de Okta.
- Síntoma: objectGUID o atributo personalizado sin sincronizar
    - Causa raíz: El atributo no se agrega ni se asigna mediante Asignación de perfiles de usuario.
    - Resolución: Agregue el atributo objectGUID y cree la asignación de perfil correspondiente si se requiere este identificador.
- Síntoma: La sincronización se detuvo después de la rotación de token
    - Causa raíz: Token SCIM o API regenerado en Secure Access pero no actualizado en Okta.
    - Resolución: Ingrese el nuevo token en Provisioning > Configure API Integration y ejecute Test API Credentials nuevamente.
- Síntoma: No se puede determinar por qué falló un usuario o grupo específico
    - Causa raíz: Los registros no se comprobaron primero.
    - Resolución: Verifique Reports > System Log en Okta, filtrado a la aplicación Cisco User Management Connector, antes de escalar.
- Síntoma: El recuento de grupos supera el límite máximo; faltan algunos sin errores
    - Causa raíz: La organización tiene más grupos de ámbito que los admitidos por Secure Access.
    - Resolución: Reduzca el alcance solo a grupos relevantes para las políticas o recurra al TAC de Cisco para obtener asistencia de grupo de nivel superior.

Problemas específicos de Microsoft Intra ID

- Síntoma: La pertenencia a grupos dinámicos no se refleja en Secure Access
    - Causa raíz: La regla de grupo dinámico está mal configurada o el grupo no está en el

ámbito aprovisionado.

    - Resolución: Valide la regla de pertenencia dinámica directamente en el ID de entrada antes de asumir un error de sincronización de Secure Access.

- Síntoma: SSO de SAML espera impulsar la identidad SWG

    - Causa raíz: AnyConnect Secure Web Gateway (SWG) no admite la autenticación del lenguaje de marcado de aserción de seguridad (SAML) frente a la ID de Entra; utiliza el mismo mecanismo de autenticación pasiva que AD en las instalaciones.

    - Resolución: No diseñe en torno a la identidad SWG impulsada por SAML para Entra ID; utilice la autenticación pasiva como se documenta.

- Síntoma: El usuario muestra incorrectamente desactivado

    - Causa raíz: ID de entrada enviada activa: false porque el usuario no pudo entrar en un ámbito de grupo asignado o porque una asignación de atributo activa está mal configurada.

    - Resolución: Compruebe si el usuario se quitó de un grupo de ámbito; compruebe la asignación activa (normalmente debe evaluarse como Not([isSoftDeleted])).

- Síntoma: Aplicación en cuarentena, todo el aprovisionamiento detenido

    - Causa raíz: La aplicación de destino devolvió respuestas no compatibles con SCIM repetidas.

    - Resolución: Verifique el estado de aprovisionamiento de la aplicación empresarial para un indicador de cuarentena antes de asumir fallas de usuarios individuales.

- Síntoma: El ciclo de aprovisionamiento inicial falla completamente

    - Causa raíz: Error transitorio de sincronización en la primera ejecución.

    - Resolución: Haga clic en Reiniciar Provisionamiento en la página Visión General para forzar a Intra ID a intentar la sincronización inicial de nuevo.

- Síntoma: Los usuarios duplicados se fusionan inesperadamente

    - Causa raíz: Dos identidades de origen comparten el mismo correo electrónico o nombre principal de usuario (UPN).

    - Resolución: Garantizar la exclusividad del correo electrónico y UPN en el directorio de origen; verifique que el atributo de correo proviene de un dominio verificado.

- Síntoma: El atributo deja de actualizarse después de un cambio de esquema

    - Causa raíz: El tipo de atributo cambió en el lado de destino (por ejemplo, cadena a booleano), pero la asignación de ID de entrada no se actualizó.

    - Resolución: Corrija manualmente el tipo en Configuración avanzada en Asignaciones de atributos.

- Síntoma: La referencia del jefe nunca se rellena
    - Causa raíz: Un usuario estaba en el ámbito antes de que lo estuviera su administrador; el aprovisionamiento no se rellena automáticamente.
    - Resolución: Reinicie el aprovisionamiento para forzar la reevaluación completa de todos los usuarios del ámbito.

Problemas específicos de IBM Security Verify

- Síntoma: Los usuarios se aprovisionan, pero los grupos nunca aparecen en Secure Access
    - Causa raíz: Compruebe que el conector SCIM personalizado sólo está ejecutando operaciones de usuario; nunca se envían llamadas POST/Groups (brecha en la capacidad de aprovisionamiento de cuentas, no un error de asignación).
    - Resolución: Capture un seguimiento del conector y confirme si se producen llamadas /Groups; si no hay ninguno, aprovisione grupos mediante Cisco AD Connector, importación de CSV o un script programado en el extremo de Secure Access SCIM.
- Síntoma: La actualización de pertenencia a grupos falla con 400 o 404
    - Causa raíz: members[].value hace referencia a Verificar los ID de usuario internos en lugar del ID de SCIM Secure Access devuelto en la creación del usuario.
    - Resolución: Corrija la asignación de miembros para utilizar el ID de Secure Access SCIM y ejecute una sincronización completa de nuevo.
- Síntoma: Los grupos aparecen pero están vacíos
    - Causa raíz: El grupo se envió antes de que sus usuarios miembros existieran en Secure Access; membership PATCH hacía referencia a usuarios desconocidos.
    - Resolución: Vuelva a ejecutar una sincronización completa ahora que los usuarios existen; asegúrese de que el orden de sincronización crea usuarios antes que grupos.
- Síntoma: Bucles de inicio de sesión SAML o redirecciones repetidas
    - Causa raíz: Verifique que el extremo IdP sea proxy o descifrado por el SWG, lo que interrumpe el flujo de autenticación.
    - Resolución: Omitir la URL Verify IdP desde SAML o el descifrado (lista de dominios externos o descifrado selectivo).

- Síntoma: El usuario autentica mediante SAML pero no coincide con ninguna política basada en el usuario
    - Causa raíz: SAML NameID no coincide con el usuario aprovisionado authName .
    - Resolución: Alinee el NameID > formato en la aplicación Verify SAML con la asignación de atributo authName (normalmente correo electrónico o UPN); prueba de nuevo.
- Síntoma: El aprovisionamiento deja de funcionar después de semanas o meses de estabilidad
    - Causa raíz: El token SCIM se giró o expiró en Secure Access pero no se actualizó en el conector Verify.
    - Resolución: Actualice el token en Secure Access y actualícelo en la aplicación personalizada Verify; calendario la cadencia de actualización.
- Síntoma: Usuarios duplicados creados al volver a sincronizar
    - Causa raíz: externalId asignado a un atributo modificable o no único (por ejemplo, nombre para mostrar, correo electrónico modificable).
    - Resolución: Asigne externalId a un identificador inmutable (Verifique el ID de usuario o objectGUID); limpie los duplicados y vuelva a sincronizar.
- Síntoma: Desactivado Verifique que los usuarios permanezcan activos en Secure Access
    - Causa raíz: La acción de suspensión no asignada a active:false, o la operación de desactivación deshabilitada en el conector.
    - Resolución: Habilite la operación de desactivación y asigne la suspensión a active:false; verifíquelo con un usuario de prueba.
- Síntoma: Los cambios de atributos en Verificar no se propagan
    - Causa raíz: Usuario o atributo fuera del ámbito de la política de aprovisionamiento o operación de actualización deshabilitada.
    - Resolución: Revisar la política o los derechos de aprovisionamiento de aplicaciones; habilitar actualizaciones; desencadenar una sincronización manual.
- Síntoma: Secure Access rechaza solicitudes con errores de esquema o de estilo 501
    - Causa raíz: Carga no compatible con SCIM (falta una matriz de esquemas, URN incorrecto, operación no admitida).
    - Resolución: Reproducirse con el ensayo de rizado basal; corregir la carga útil o la asignación; escalar a IBM si el conector emite la solicitud incorrecta.
- Síntoma: Falta la identidad SWG para los usuarios de roaming a pesar de que SAML

funciona

- Causa raíz: Se espera que SAML impulse la identidad para un modo de despliegue que utilice una identidad pasiva o basada en agentes.
- Resolución: Confirme el método de adquisición de identidad para cada modo de implementación con la documentación de Secure Access; no diseñe SAML como el único origen de identidad.

Problemas genéricos de SCIM

Estos no son específicos de Cisco, pero aparecen de manera uniforme en las implementaciones de Secure Access porque el transporte subyacente es el estándar SCIM 2.0:

- Los estados de cuarentena enmascaran errores individuales: Si la sincronización parece haberse detenido por completo en lugar de fallar por usuario, compruebe si hay una cuarentena o estado de suspensión en el nivel de aplicación antes de investigar problemas de atributos individuales.
- 409 Conflicto en la desactivación: Un patrón común donde el IdP intenta desactivar un usuario y el objetivo arroja un conflicto. Normalmente, se trata de un problema de asignación de atributos o de ámbito de grupo activo, no de un verdadero error del sistema.
- Los campos vacíos o borrados no siempre se propagan: Algunas implementaciones del servidor SCIM conservan el último valor no nulo; cuando borra un campo en el IdP, puede requerir que primero se inserte un valor de marcador de posición.
- Los cambios de configuración o URL invalidan la autenticación de forma silenciosa: Cualquier cambio en la URL del punto final SCIM requiere normalmente que se proporcione nuevamente el token portador. Los errores aparecen como URL no válida incluso cuando el problema real es un token obsoleto.
- Sin webhook nativo ni secuencia de eventos: La automatización que espera recibir notificaciones automáticas en tiempo real sobre los cambios de usuarios o políticas debe sondear la API de informes o integrarse a través de Cisco XDR. Secure Access no emite webhooks de aprovisionamiento salientes.

Derive al TAC de Cisco con los registros de aprovisionamiento del lado del IdP si los pasos anteriores no resuelven el problema. Por lo general, los registros de aprovisionamiento de back-end en el lado de Secure Access requieren acceso a TAC para la extracción.

Causa

La integración de aprovisionamiento de SCIM no pudo enviar uno o más registros debido a un token portador caducado, una discordancia de asignación de atributos, un grupo de destino ausente o un ámbito de aprovisionamiento insuficiente.

Contenido relacionado

- Cisco: Aprovisionamiento de usuarios y grupos para proteger el acceso mediante ID de entrada
- Cisco: Aprovisionamiento de usuarios y grupos para un acceso seguro mediante OKTA
- Microsoft Learn: Problemas conocidos con el cumplimiento del protocolo SCIM 2.0: Microsoft Entra ID
- Microsoft Learn: Solucionar errores de API SCIM de Microsoft Entra ID
- Configuración de SSO SAML en el proveedor de identidad: https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider
- Aprovisionamiento para aplicaciones personalizadas (SCIM): https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications
- Introducción al aprovisionamiento y la administración (conector SCIM genérico): https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance
- Puente de aprovisionamiento en las instalaciones (orígenes AD/LDAP): https://docs.verify.ibm.com/verify/docs/on-premises-provisioning

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).