Solucionar problemas de sincronización del conector de AD de Secure Access

Contenido

Problema

El conector de AD instalado en un controlador de dominio no se está sincronizando correctamente con Cisco Secure Access. El conector experimenta múltiples fallas de sincronización, entre ellas:

- Errores de sincronización Delta con errores de acceso denegado (COMException 0x80070005).
- Errores de lectura del registro de eventos del DC con "UnauthorizedAccessException: Se ha intentado realizar una operación no autorizada".
- Problemas de registro en la nube que muestran el "formato URI no válido" al descargar el manifiesto.
- HTTP 404: errores "object_not_found" para un AssetID específico durante los intentos de sincronización.

El conector parece tener conectividad con el servicio en la nube Cisco Secure Access, pero falla tanto en el lado de los permisos de Active Directory como en la configuración del registro en la nube.

Entorno

- Cisco Secure Access con conector AD
- Versión 1.15.2 del conector de AD
- Conector de AD instalado en controlador de dominio
- Cuenta de servicio personalizada (svcCiscoUmbrella) en lugar de la cuenta predeterminada Cisco_Connector
- Configuración del entorno de prueba/piloto

Resolución

La resolución implicaba abordar tanto los problemas de permisos de Active Directory como los problemas de registro en la nube a través de un proceso de reinstalación completo:

Paso 1: Verificar y limpiar las entradas existentes del conector de AD

En el panel de acceso seguro, compruebe la entrada del conector de AD para el host y quite las entradas obsoletas o duplicadas para el mismo servidor, si las hay.

Paso 2: Asegúrese de completar la desinstalación

Desinstale por completo el servicio AD Connector existente para asegurarse de que no quede ninguna configuración residual que pueda causar problemas de registro.

Paso 3: Ejecutar scripts del controlador de dominio

Antes de reinstalar el conector, ejecute las secuencias de comandos de configuración del controlador de dominio para asegurarse de que se han establecido los permisos adecuados. La secuencia de comandos debe ejecutarse en cada controlador de dominio aplicable, aunque el conector en sí puede residir fuera del controlador de dominio en otro equipo unido al dominio.

Paso 4: Configurar permisos de cuenta de servicio

Otorgue los permisos necesarios de Active Directory a la cuenta de servicio:

- Permisos de sincronización de AD (dominio/ámbito raíz, según corresponda):
    - Leer
    - Replicación de cambios de directorio

    - Replicar todos los cambios de directorio (si es necesario en el entorno)
    - Replicación de los cambios de directorio en el conjunto filtrado (si es necesario en el entorno)
- Acceso al registro de eventos en el controlador de dominio:
    - Agregue la cuenta de servicio al grupo Lectores de registro de eventos.
    - Asegúrese de contar con permisos equivalentes basados en directivas para leer el registro de seguridad.

Paso 5: Vuelva a instalar el conector AD

Reinstale el servicio del conector de AD para generar un manifiesto nuevo y un AssetID válido, garantizando un registro adecuado en la nube.

Paso 6: Reiniciar y validar

Después de la instalación y la configuración de permisos:

1. Reinicie el servicio del conector de AD.
2. Supervise los registros del conector para confirmar que se ha denegado el acceso y que se han detenido los errores no autorizados.
3. Verifique que las entradas de sincronización correctas aparezcan en los registros (por ejemplo, "ADSync LDIF RESPONSE: 200 Éxito").

Causa

Los problemas de sincronización fueron causados por dos factores principales:

1. Permisos insuficientes de Active Directory: La cuenta de servicio personalizada (svcCiscoUmbrella) carecía de los permisos de AD necesarios para la sincronización delta y el acceso al registro de eventos DC, lo que provocaba los errores "Access is denied" y

"UnauthorizedAccessException".
2. Problemas de registro en la nube: La instancia del conector estaba mal registrada o apuntaba a un AssetID no válido/antiguo, lo que causaba errores de "formato URI no válido" al descargar el manifiesto y errores de HTTP 404 "object_not_found" durante los intentos de sincronización.

Estos problemas se vieron agravados por procedimientos de instalación incompletos en los que las secuencias de comandos de configuración del controlador de dominio no se ejecutaron correctamente antes de la instalación del conector.

Contenido relacionado

- Configuración del conector de Cisco Secure Access AD
- Requisitos de permisos del conector AD
- Guía de instalación del conector AD
- Resolución de problemas del conector AD
- Configuración de cuenta de servicio de AD Connector
- Soporte técnico y descargas de Cisco

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).