

Error de conexión VPN de Cisco Secure Client con errores de autenticación SAML y diccionario Bencode

Contenido

Problema

Las conexiones VPN que utilizan Cisco Secure Client no se pueden establecer cuando se utiliza la autenticación SAML con Google IdP. Aunque la autenticación SAML es exitosa en el lado del IdP, el cliente falla durante el procesamiento posterior a la autenticación y pasa a un estado desconectado, lo que impide que se cree el túnel VPN.

Entorno

- Cisco Secure Client versión 5.1.13.177
- Autenticación SAML configurada con Google IdP
- Acceso seguro: acceso remoto seguro con cliente (VPN, estado, recurso privado)
- Los registros de autenticación de Google IdP muestran una autenticación SAML satisfactoria

Resolución

El problema se resolvió reinstalando Cisco Secure Client. Se documentó el siguiente enfoque de solución de problemas:

Pasos de diagnóstico iniciales

Paso 1: Recopilar registros DART del terminal afectado:

<https://www.cisco.com/c/en/us/support/docs/security/secure-client/221919-collect-dart-bundle-for-secure-client.html>

Extraiga Dart Bundle > Cisco Secure client > Anyconnect VPN > Logs > Under VPN Folder > AnyConnectVPN.txt: muestre los siguientes errores al leer la configuración interna, con los siguientes errores que aparecen de forma continua:

- Error de internalización del diccionario Bencode
- No se pudo crear el diccionario Bencode
- PHONEHOMEVPN_ERROR_UNEXPECTED
- GLOBAL_ERROR_UNEXPECTED

Paso 2: Verificar el estado de autenticación SAML en el lado IdP

Confirme que los registros de Google IdP muestren una autenticación SAML exitosa para aislar el problema al procesamiento posterior a la autenticación del lado del cliente.

Implementación de resolución

Paso 1: Reinstalar Cisco Secure Client

Desinstale la instalación existente de Cisco Secure Client y realice una reinstalación limpia del software cliente.

Paso 2: Verificar restauración de conectividad VPN

Después de la reinstalación, pruebe la conexión VPN con autenticación SAML para confirmar que la conexión se establece correctamente y que el túnel se ha creado correctamente.

La reinstalación de Cisco Secure Client restauró la funcionalidad de VPN, permitiendo una autenticación SAML exitosa y el establecimiento de túneles.

Causa

La causa raíz parece estar relacionada con datos de configuración interna dañados en la instalación de Cisco Secure Client, lo que afecta específicamente a la capacidad del componente CPhoneHomeVpn/PhoneHomeAgent para procesar los datos del diccionario Bencode durante el procesamiento posterior a la autenticación. Los errores repetidos "Bencode dictionary internalize failed" y "Failed to create Bencode dictionary" indican que el cliente no pudo analizar o procesar correctamente los datos de configuración interna requeridos para establecer el túnel VPN después de una autenticación SAML exitosa.

El problema se resolvió mediante la reinstalación del cliente, lo que sugiere que el problema estaba relacionado con datos dañados del lado del cliente en lugar de con problemas de configuración del lado del servidor o de integración de IdP.

Contenido relacionado

- [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).