Solución de problemas de conexiones de Secure Shell a servidores en la nube de Azure en switches Catalyst

Contenido

Introducción

Este documento describe cómo identificar y resolver problemas cuando los switches Cisco no pueden conectarse al almacenamiento de Microsoft Blob mediante Secure Shell.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Información sobre las operaciones y la configuración del protocolo de transferencia de archivos segura (SFTP) en los switches de Cisco
- Familiaridad con el protocolo Secure Shell (SSH) y sus fases de negociación
- Conocimiento de la configuración del servicio de almacenamiento Microsoft Blob para acceso SFTP
- Experiencia con la lectura e interpretación de mensajes de registro del sistema/depuración

del switch
- Resolución de problemas básica para la conectividad de red y compatibilidad de protocolos entre los switches de Cisco y los servicios SFTP externos

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Familia de productos: Catalyst 9300 Series Switches
- Versión del software: Cisco IOS® XE 17.9.5
- Tecnología: LAN Switching
- Conexiones SSH a la plataforma Azure Cloud

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Microsoft Blob Storage ofrece ahora acceso a SFTP, lo que permite la transferencia de archivos desde dispositivos de red como switches de Cisco. Realizar copias de seguridad de las configuraciones de los dispositivos en el almacenamiento en la nube fuera de las instalaciones, como Microsoft Blob, es una práctica habitual para la recuperación ante desastres y la continuidad operativa. SFTP aprovecha el protocolo SSH para la transferencia segura de archivos. Requiere una negociación SSH exitosa, intercambio de claves y la capacidad de abrir un canal de datos seguro. Mientras que los servidores SFTP locales pueden tener implementaciones de protocolo estándar o bien admitidas, los servicios basados en la nube como Microsoft Blob SFTP pueden introducir diferencias de compatibilidad o de negociación de protocolo que pueden afectar a la transferencia de archivos correcta. La resolución de problemas de interoperabilidad requiere un análisis cuidadoso de los resultados de syslog/debug y un enfoque metódico para aislar el protocolo, la configuración o las causas ambientales.

Problema

Cuando se intenta realizar una copia de seguridad de las configuraciones de los switches de Cisco en un punto final SFTP de almacenamiento Microsoft Blob, la copia de seguridad falla

después de que se completa la negociación SSH. Las copias de seguridad en los servidores SFTP locales se realizan correctamente sin problemas, lo que indica que el cliente SFTP del switch funciona en otros escenarios.

Síntomas:

- Los switches completan con éxito el intercambio de claves SSH y la autenticación con Microsoft Blob SFTP.
- La copia de seguridad falla en la fase de apertura del canal, lo que impide la transferencia de archivos.
- Los mensajes de registro del sistema/depuración indican una falla durante la operación de escritura SFTP.

Resultado de debug/syslog relevante registrado durante la falla:

<#root>

```
Feb 12 14:05:03.272: ssh2_calculate_modulus_length: modulus len 32
Feb 12 14:05:03.280:  SSH: Signature verification successful
Feb 12 14:05:03.280: SSH2: kex_derive_keys complete
Feb 12 14:05:03.281: SSH2 CLIENT 0: SSH2_MSG_NEWKEYS sent
Feb 12 14:05:03.281: SSH2 CLIENT 0: waiting for SSH2_MSG_NEWKEYS
Feb 12 14:05:03.288: SSH2 CLIENT 0: SSH2_MSG_NEWKEYS received
Feb 12 14:05:03.330: SSH2 CLIENT 0:

Channel open failed, reason = 1

Feb 12 14:05:03.331: SSH CLIENT0: Session disconnected - error 0x00
Feb 12 14:05:03.332:

SFTP write_process: sftp_write failed err 1545

Feb 12 14:05:03.332: SFTP ifs_write: ndent stat (2) 3
```

Observaciones clave de los registros:

- El intercambio de claves SSH y la verificación de firmas son exitosos.
- La falla ocurre en la etapa de apertura del canal SSH: Error al abrir el canal, motivo = 1.
- El proceso de escritura SFTP falla (err 1545) y la sesión se desconecta inmediatamente después.

Solución

El problema se resuelve al aumentar la configuración del tamaño de la ventana SSH en el switch Catalyst 9300 para dar cabida a los requisitos del servidor en la nube de Azure. Los servidores en la nube de Azure requieren un tamaño de ventana SSH mayor que el valor predeterminado configurado en los switches Cisco antes de la versión 17.10.1 de Cisco IOS XE.

Paso 1. Configuración del Tamaño de la Ventana SSH

Configure el tamaño de la ventana SSH a un valor de al menos 16384. El valor máximo recomendado es 65536 para evitar un impacto excesivo en la CPU en los dispositivos de menor capacidad:

```
<#root>

device(config)#

ip ssh window-size 65536
```

Después de ejecutar este comando, recibirá este mensaje de advertencia:

```
%% Warning: This cli may have impact on CPU. So, use only for SCP
Please configure ip tcp window-size<> with same value, for this CLI to work
```

Paso 2. Configuración del tamaño de la ventana TCP

Configure el tamaño de la ventana TCP para que coincida con el valor de tamaño de la ventana SSH:

```
<#root>

device(config)#

ip tcp window-size 65536
```

Verificación de configuración

Después de implementar ambos cambios de configuración, la conexión SSH entre el switch y el servidor de nube de Azure funciona correctamente, lo que permite operaciones de copia de

seguridad de SFTP exitosas.

Nota: A partir de Cisco IOS XE Dublin 17.10.1, el modo de transferencia masiva de datos SSH se habilita de forma predeterminada con un tamaño de ventana predeterminado de 128 KB. Aunque el valor máximo admitido por el tamaño de la ventana SSH es 131072, se recomienda utilizar un valor máximo de 65536 para minimizar el impacto de la CPU en los dispositivos de menor capacidad.

Precaución: El tamaño mínimo de ventana requerido para los servidores en la nube de Azure es 16384. Los tamaños de ventana SSH y TCP deben configurarse con valores coincidentes para que la solución funcione eficazmente.

Causa

La causa raíz de este problema es una discordancia entre el tamaño predeterminado de la ventana SSH configurado en los switches Cisco Catalyst 9300 y los requisitos de tamaño mínimo de la ventana SSH de los servidores en la nube de Microsoft Azure. De forma predeterminada, los switches de Cisco utilizan un valor de tamaño de ventana SSH de 8912, que es insuficiente para los servidores en la nube de Azure que requieren un tamaño mínimo de ventana de al menos 16384. Esta incompatibilidad impide el establecimiento del canal SSH necesario para las transferencias de archivos SFTP, aunque los procesos iniciales de autenticación SSH e intercambio de claves se completen correctamente.

Información Relacionada

- Asistente de soporte de Cisco
- Contacto mundial de Cisco
- 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).