Solucionar Problemas de Conexões Shell Seguras para Servidores de Nuvem do Azure em Switches Catalyst

Contents

Introdução

Este documento descreve como identificar e resolver problemas quando os switches da Cisco não conseguem se conectar ao armazenamento do Microsoft Blob usando o Secure Shell.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão das operações e da configuração do protocolo SFTP em switches Cisco
- Familiaridade com o protocolo Secure Shell (SSH) e suas fases de negociação
- Conhecimento da configuração do serviço de armazenamento Microsoft Blob para acesso SFTP
- Experiência com leitura e interpretação de mensagens de syslog/debug do switch
- Solução básica de problemas para conectividade de rede e compatibilidade de protocolo

entre switches Cisco e serviços SFTP externos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Linha de produtos: Catalyst 9300 Series Switches
- Versão de software: Cisco IOS® XE 17.9.5
- Tecnologia: LAN Switching
- Conexões SSH para a plataforma de Nuvem do Azure

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Microsoft Blob Storage agora oferece acesso SFTP, permitindo transferências de arquivos de dispositivos de rede, como switches da Cisco. Fazer backup das configurações do dispositivo para armazenamento em nuvem fora do local, como o Microsoft Blob, é uma prática comum para recuperação de desastres e continuidade operacional. O SFTP aproveita o protocolo SSH para transferência segura de arquivos. Requer negociação SSH bem-sucedida, troca de chaves e a capacidade de abrir um canal de dados seguro. Embora os servidores SFTP locais possam ter implementações de protocolo padrão ou bem suportadas, serviços baseados em nuvem, como o Microsoft Blob SFTP, podem introduzir diferenças de compatibilidade ou negociação de protocolo que podem afetar a transferência de arquivos bem-sucedida. A identificação e solução de problemas de interoperabilidade exige uma análise cuidadosa das saídas de syslog/debug e uma abordagem metódica para isolar o protocolo, a configuração ou as causas ambientais.

Problema

Ao tentar fazer backup das configurações dos switches Cisco para um endpoint SFTP de armazenamento Microsoft Blob, o backup falha após a conclusão da negociação SSH. Os backups em servidores SFTP locais foram bem-sucedidos sem problemas, indicando que o cliente SFTP do switch está funcionando em outros cenários.

Sintomas:

- Os switches concluíram com êxito a troca de chave SSH e a autenticação com o Microsoft Blob SFTP.
- O backup falha na fase de abertura do canal, impedindo a transferência de arquivos.
- As mensagens de syslog/debug indicam falha durante a operação de gravação SFTP.

Saída relevante de debug/syslog registrada durante a falha:

<#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
```

Principais observações dos registros:

- A troca de chave SSH e a verificação de assinatura foram bem-sucedidas.
- A falha ocorre no estágio aberto do canal SSH: Falha na abertura do canal, motivo = 1.
- O processo de gravação do SFTP falha (erro 1545) e a sessão é desconectada imediatamente depois.

Solução

O problema é resolvido aumentando a configuração do tamanho da janela SSH no switch Catalyst 9300 para acomodar os requisitos do servidor de Nuvem do Azure. Os servidores de Nuvem do Azure exigem um tamanho de janela de SSH maior do que o valor padrão configurado nos switches Cisco antes da versão 17.10.1 do Cisco IOS XE.

Etapa 1. Configurar o tamanho da janela do SSH

Configure o tamanho da janela do SSH para um valor de pelo menos 16384. O valor máximo recomendado é 65536 para evitar o impacto excessivo da CPU em dispositivos low-end:

```
<#root>

device(config)#

ip ssh window-size 65536
```

Após executar esse comando, você receberá esta mensagem de aviso:

```
%% 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
```

Etapa 2. Configurar o Tamanho da Janela TCP

Configure o tamanho da janela TCP para corresponder ao valor do tamanho da janela SSH:

```
<#root>

device(config)#

ip tcp window-size 65536
```

Verificação de configuração

Depois de implementar as duas alterações de configuração, a conexão SSH entre o switch e o servidor de Nuvem do Azure funciona corretamente, permitindo operações de backup de SFTP bem-sucedidas.

Note: A partir do Cisco IOS XE Dublin 17.10.1, o modo de transferência de dados em massa SSH é ativado por padrão com um tamanho de janela padrão de 128 KB. Embora o valor de tamanho máximo de janela SSH suportado seja 131072, é recomendável usar um valor máximo de 65536 para minimizar o impacto da CPU em dispositivos de extremidade inferior.

⚠ Caution: O tamanho de janela mínimo necessário para os servidores de Nuvem do Azure é 16384. Os tamanhos de janela SSH e TCP devem ser configurados com valores correspondentes para que a solução funcione efetivamente.

Causa

A causa raiz desse problema é uma incompatibilidade entre o tamanho de janela SSH padrão configurado nos switches Cisco Catalyst 9300 e os requisitos mínimos de tamanho de janela SSH dos servidores de Nuvem do Microsoft Azure. Por padrão, os switches Cisco usam um valor de tamanho de janela SSH de 8912, que é insuficiente para servidores de Nuvem do Azure que exigem um tamanho de janela mínimo de pelo menos 16384. Essa incompatibilidade impede o estabelecimento do canal SSH necessário para transferências de arquivos SFTP, mesmo que os processos iniciais de autenticação SSH e troca de chave sejam concluídos com êxito.

Informações Relacionadas

- Cisco Support Assistant
- Contato mundial da Cisco
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.