Troubleshoot Secure Shell Connections to Azure Cloud Servers on Catalyst Switches

Contents

Introduction

This document describes how to identify and resolve issues when Cisco switches are unable to connect to Microsoft Blob storage using Secure Shell.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Understanding of Secure File Transfer Protocol (SFTP) operations and configuration on Cisco switches
- Familiarity with Secure Shell (SSH) protocol and its negotiation phases
- Knowledge of Microsoft Blob storage service configuration for SFTP access
- Experience with reading and interpreting switch syslog/debug messages
- Basic troubleshooting for network connectivity and protocol compatibility between Cisco switches and external SFTP services

Components Used

The information in this document is based on these software and hardware versions:

- Product Family: Catalyst 9300 Series Switches
- Software Version: Cisco IOS® XE 17.9.5
- Technology: LAN Switching
- SSH connections to Azure Cloud platform

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Microsoft Blob Storage now offers SFTP access, enabling file transfers from network devices such as Cisco switches. Backing up device configurations to off site cloud storage, like Microsoft Blob, is a common practice for disaster recovery and operational continuity. SFTP leverages the SSH protocol for secure file transfer. It requires successful SSH negotiation, key exchange, and the ability to open a secure data channel. While local SFTP servers can have standard or well-supported protocol implementations, cloud-based services such as Microsoft Blob SFTP can introduce compatibility or protocol negotiation differences that can affect successful file transfer. Troubleshooting such interoperability issues requires careful analysis of syslog/debug outputs and a methodical approach to isolate protocol, configuration, or environmental causes.

Problem

When attempting to back up configurations from Cisco switches to a Microsoft Blob storage SFTP endpoint, the backup fails after the SSH negotiation completes. Backups to local SFTP servers succeed without issue, indicating that the switch SFTP client is functional in other scenarios.

Symptoms:

- Switches successfully complete SSH key exchange and authentication with Microsoft Blob SFTP.
- Backup fails at the channel opening phase, preventing file transfer.
- Syslog/debug messages indicate failure during SFTP write operation.

Relevant debug/syslog output recorded during the failure:

<#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
```

Key observations from the logs:

- SSH key exchange and signature verification are successful.
- The failure occurs at the SSH channel open stage: Channel open failed, reason = 1.
- SFTP write process fails (err 1545) and the session disconnects immediately after.

Solution

The issue is resolved by increasing the SSH window size configuration on the Catalyst 9300 switch to accommodate Azure Cloud server requirements. Azure Cloud servers require a larger SSH window size than the default value configured on Cisco switches before 17.10.1 Cisco IOS XE version.

Step 1. Configure SSH Window Size

Configure the SSH window size to a value of at least 16384. The recommended maximum value is 65536 to avoid excessive CPU impact on low-end devices:

```
<#root>

device(config)#

ip ssh window-size 65536
```

After executing this command, you receive this warning message:

```
%% 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
```

Step 2. Configure TCP Window Size

Configure the TCP window size to match the SSH window size value:

<#root>

```
device(config)#
```

ip tcp window-size 65536

Configuration Verification

After implementing both configuration changes, the SSH connection between the switch and the Azure Cloud server function properly, allowing successful SFTP backup operations.

Note: Beginning from Cisco IOS XE Dublin 17.10.1, SSH bulk data transfer mode is enabled by default with a default window size of 128 KB. Although the maximum supported SSH window size value is 131072, it is recommended to use a maximum value of 65536 to minimize CPU impact on lower-end devices.

Caution: The minimum required window size for Azure Cloud servers is 16384. Both SSH and TCP window sizes must be configured with matching values for the solution to work effectively.

Cause

The root cause of this issue is a mismatch between the default SSH window size configured on Cisco Catalyst 9300 switches and the minimum SSH window size requirements of Microsoft Azure Cloud servers. By default, Cisco switches use an SSH window size value of 8912, which is insufficient for Azure Cloud servers that require a minimum window size of at least 16384. This incompatibility prevents the establishment of the SSH channel required for SFTP file transfers, even though the initial SSH authentication and key exchange processes complete successfully.

Related Information

- Cisco Support Assistant
- Cisco Worldwide Contact
- Cisco Technical Support & Downloads