对Catalyst交换机上与Azure云服务器的安全外壳连接进行故障排除

目录

简介

本文档介绍当思科交换机无法使用Secure Shell连接到Microsoft Blob存储时，如何识别和解决问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解思科交换机上的安全文件传输协议(SFTP)操作和配置
- 熟悉Secure Shell(SSH)协议及其协商阶段
- 了解SFTP访问的Microsoft Blob存储服务配置
- 阅读和解释交换机系统日志/调试消息的经验
- Cisco交换机和外部SFTP服务之间的网络连接和协议兼容性的基本故障排除

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 产品系列：Catalyst 9300 系列交换机
- 软件版本:思科IOS® XE 17.9.5
- 技术：LAN 交换
- 到Azure Cloud平台的SSH连接

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Microsoft Blob存储现在提供SFTP访问，支持从网络设备（如思科交换机）传输文件。将设备配置备份到非现场云存储（如Microsoft Blob）是灾难恢复和操作连续性的常见做法。SFTP利用SSH协议进行安全文件传输。它需要成功的SSH协商、密钥交换和打开安全数据通道的能力。本地SFTP服务器可以采用标准或受良好支持的协议实施，而基于云的服务（如Microsoft Blob SFTP）可能会引入可能影响成功文件传输的兼容性或协议协商差异。排除此类互操作性问题需要仔细分析syslog/debug输出，并使用系统方法隔离协议、配置或环境原因。

问题

当尝试将配置从思科交换机备份到Microsoft Blob存储SFTP终端时，备份在SSH协商完成之后失败。备份到本地SFTP服务器不会出现问题，表明交换机SFTP客户端在其他情况下可以正常工作。

症状：

- 交换机使用Microsoft Blob SFTP成功完成SSH密钥交换和身份验证。
- 备份在通道打开阶段失败，导致文件传输无法进行。
- Syslog/debug消息指示SFTP写入操作期间失败。

在故障期间记录的相关调试/系统日志输出：

<#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
```

日志中的主要观察结果：

- SSH密钥交换和签名验证成功。
- 故障发生在SSH通道打开阶段：通道打开失败，原因= 1。
- SFTP写入过程失败（错误1545），会话随后立即断开。

解决方案

通过增加Catalyst 9300交换机上的SSH窗口大小配置以满足Azure云服务器要求来解决此问题。Azure云服务器需要的SSH窗口大小大于在17.10.1 Cisco IOS XE版本之前的思科交换机上配置的默认值。

步骤1.配置SSH窗口大小

将SSH窗口大小配置为至少为16384的值。建议的最大值为65536，以避免对低端设备产生过多的CPU影响：

```
<#root>

device(config)#

ip ssh window-size 65536
```

执行此命令后，您将收到以下警告消息：

```
%% 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
```

步骤2.配置TCP窗口大小

配置TCP窗口大小以匹配SSH窗口大小值：

```
<#root>

device(config)#

ip tcp window-size 65536
```

配置验证

实施两次配置更改后，交换机和Azure云服务器之间的SSH连接可正常工作，从而允许SFTP备份操作成功。

注意：从Cisco IOS XE Dublin 17.10.1开始，默认启用SSH批量数据传输模式，默认窗口大小为128 KB。虽然支持的最大SSH窗口大小值为131072，但建议使用最大值65536以最大程度降低对低端设备的CPU影响。

警告：Azure云服务器所需的最小窗口大小为16384。SSH和TCP窗口大小都必须配置有匹配的值，解决方案才能有效运行。

原因

此问题的根本原因是在Cisco Catalyst 9300交换机上配置的默认SSH窗口大小与Microsoft Azure云服务器的最低SSH窗口大小要求不匹配。默认情况下，思科交换机使用SSH窗口大小值8912，该值对于要求最小窗口大小至少为16384的Azure云服务器来说不足。这种不兼容将阻止建立SFTP文件传输所需的SSH通道，即使初始SSH身份验证和密钥交换过程成功完成。

相关信息

- Cisco Support Assistant
- 思科全球联系人
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。