Dépannage des connexions Secure Shell aux serveurs cloud Azure sur les commutateurs Catalyst

Table des matières

Introduction

Ce document décrit comment identifier et résoudre les problèmes lorsque les commutateurs Cisco ne parviennent pas à se connecter au stockage Blob Microsoft à l'aide de Secure Shell.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension des opérations et de la configuration du protocole SFTP (Secure File Transfer Protocol) sur les commutateurs Cisco
- Connaissance du protocole Secure Shell (SSH) et de ses phases de négociation
- Connaissance de la configuration du service de stockage Blob Microsoft pour l'accès SFTP
- Expérience de la lecture et de l'interprétation des messages syslog/debug du commutateur
- Dépannage de base de la connectivité réseau et de la compatibilité des protocoles entre les

commutateurs Cisco et les services SFTP externes

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gamme de produits : Commutateurs Catalyst 9300
- Version du logiciel: Cisco IOS® XE 17.9.5
- Technologie : Commutation LAN
- Connexions SSH à la plateforme cloud Azure

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Microsoft Blob Storage offre désormais un accès SFTP, permettant les transferts de fichiers à partir de périphériques réseau tels que les commutateurs Cisco. La sauvegarde des configurations des périphériques sur un stockage cloud hors site, comme Microsoft Blob, est une pratique courante pour la reprise après sinistre et la continuité opérationnelle. Le protocole SFTP utilise le protocole SSH pour sécuriser le transfert de fichiers. Elle nécessite une négociation SSH réussie, un échange de clés et la possibilité d'ouvrir un canal de données sécurisé. Alors que les serveurs SFTP locaux peuvent avoir des implémentations de protocole standard ou bien prises en charge, les services cloud tels que Microsoft Blob SFTP peuvent introduire des différences de compatibilité ou de négociation de protocole qui peuvent affecter le transfert de fichiers. Le dépannage de tels problèmes d'interopérabilité nécessite une analyse minutieuse des sorties syslog/debug et une approche méthodique pour isoler le protocole, la configuration ou les causes environnementales.

Problème

Lorsque vous tentez de sauvegarder des configurations à partir de commutateurs Cisco sur un point d'extrémité SFTP de stockage Blob Microsoft, la sauvegarde échoue une fois la négociation SSH terminée. Les sauvegardes vers les serveurs SFTP locaux réussissent sans problème, ce qui indique que le client SFTP du commutateur fonctionne dans d'autres scénarios.

Symptômes :

- Les commutateurs ont réussi l'échange de clés SSH et l'authentification avec Microsoft Blob SFTP.
- La sauvegarde échoue à la phase d'ouverture du canal, empêchant le transfert de fichiers.
- Les messages Syslog/debug indiquent un échec pendant l'opération d'écriture SFTP.

Sortie de débogage/syslog pertinente enregistrée pendant la panne :

<#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
```

Principales observations tirées des journaux :

- L'échange de clés SSH et la vérification de signature ont réussi.
- La défaillance se produit au stade d’ouverture du canal SSH : Échec de l'ouverture du canal, raison = 1.
- Le processus d'écriture SFTP échoue (err 1545) et la session se déconnecte immédiatement après.

Solution

Le problème est résolu en augmentant la configuration de la taille de fenêtre SSH sur le commutateur Catalyst 9300 pour répondre aux exigences du serveur cloud Azure. Les serveurs cloud Azure nécessitent une taille de fenêtre SSH supérieure à la valeur par défaut configurée sur les commutateurs Cisco antérieurs à la version 17.10.1 de Cisco IOS XE.

Étape 1 : configuration de la taille de fenêtre SSH

Configurez la taille de la fenêtre SSH sur une valeur d'au moins 16384. La valeur maximale recommandée est 65536 pour éviter un impact excessif du processeur sur les périphériques bas de gamme :

```
<#root>

device(config)#

ip ssh window-size 65536
```

Après avoir exécuté cette commande, vous recevez le message d'avertissement suivant :

```
%% 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
```

Étape 2 : configuration de la taille de fenêtre TCP

Configurez la taille de fenêtre TCP pour qu'elle corresponde à la valeur de taille de fenêtre SSH :

```
<#root>

device(config)#

ip tcp window-size 65536
```

Vérification de la configuration

Après avoir implémenté les deux modifications de configuration, la connexion SSH entre le commutateur et le serveur cloud Azure fonctionne correctement, ce qui permet des opérations de sauvegarde SFTP réussies.

Remarque : À partir de Cisco IOS XE Dublin 17.10.1, le mode de transfert de données en masse SSH est activé par défaut avec une taille de fenêtre par défaut de 128 Ko. Bien

---

que la valeur maximale de taille de fenêtre SSH prise en charge soit 131072, il est recommandé d'utiliser une valeur maximale de 65536 pour minimiser l'impact du processeur sur les périphériques bas de gamme.

⚠ Mise en garde : La taille de fenêtre minimale requise pour les serveurs cloud Azure est 16384. Les tailles de fenêtre SSH et TCP doivent être configurées avec des valeurs correspondantes pour que la solution fonctionne efficacement.

Motif

La cause principale de ce problème est une non-correspondance entre la taille de fenêtre SSH par défaut configurée sur les commutateurs Cisco Catalyst 9300 et la taille de fenêtre SSH minimale requise par les serveurs cloud Microsoft Azure. Par défaut, les commutateurs Cisco utilisent une valeur de taille de fenêtre SSH de 8912, ce qui est insuffisant pour les serveurs cloud Azure qui nécessitent une taille de fenêtre minimale d'au moins 16384. Cette incompatibilité empêche l'établissement du canal SSH requis pour les transferts de fichiers SFTP, même si les processus initiaux d'authentification SSH et d'échange de clés se terminent correctement.

Informations connexes

- Assistant de soutien Cisco
- Contact mondial Cisco
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.