Problemen oplossen met beveiligde Shell-verbindingen met Azure Cloud Servers op Catalyst-Switches

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen kunt identificeren en oplossen wanneer Cisco-switches geen verbinding kunnen maken met Microsoft Blob-opslagsystemen met Secure Shell.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Inzicht in de werking en configuratie van het Secure File Transfer Protocol (SFTP) op Cisco-switches
- Bekendheid met het Secure Shell (SSH) protocol en de onderhandelingsfasen
- Kennis van Microsoft Blob Storage Service Configuration voor SFTP-toegang
- Ervaring met het lezen en interpreteren van switch syslog/debug berichten
- Basisprobleemoplossing voor netwerkconnectiviteit en protocolcompatibiliteit tussen Cisco-

switches en externe SFTP-services

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Productfamilie: Catalyst 9300 serie Switches
- Softwareversie: Cisco IOS® XE 17.9.5
- Technologie: LAN-switching
- SSH-verbindingen met Azure Cloud-platform

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Microsoft Blob Storage biedt nu SFTP-toegang, waardoor bestandsoverdrachten van netwerkapparaten zoals Cisco-switches mogelijk zijn. Het maken van back-ups van apparaatconfiguraties naar externe cloudopslag, zoals Microsoft Blob, is een gangbare praktijk voor noodherstel en operationele continuïteit. SFTP maakt gebruik van het SSH-protocol voor veilige bestandsoverdracht. Het vereist succesvolle SSH-onderhandelingen, sleuteluitwisseling en de mogelijkheid om een veilig gegevenskanaal te openen. Hoewel lokale SFTP-servers standaard of goed ondersteunde protocolimplementaties kunnen hebben, kunnen cloudgebaseerde services zoals Microsoft Blob SFTP compatibiliteits- of protocolonderhandelingsverschillen introduceren die van invloed kunnen zijn op een succesvolle bestandsoverdracht. Het oplossen van dergelijke interoperabiliteitsproblemen vereist een zorgvuldige analyse van syslog/debug-uitgangen en een methodische aanpak om protocol-, configuratie- of omgevingsoorzaken te isoleren.

Probleem

Wanneer u probeert een back-up te maken van configuraties van Cisco-switches naar een Microsoft Blob Storage SFTP-eindpunt, mislukt de back-up nadat de SSH-onderhandeling is voltooid. Back-ups naar lokale SFTP-servers worden probleemloos uitgevoerd, wat aangeeft dat de switch SFTP-client in andere scenario's werkt.

Symptomen:

- Switches voltooien met succes de uitwisseling en verificatie van SSH-sleutels met Microsoft Blob SFTP.
- Back-up mislukt tijdens de openingsfase van het kanaal, waardoor bestandsoverdracht wordt voorkomen.
- Syslog/debug-berichten duiden op een fout tijdens de schrijfbewerking van SFTP.

Relevante debug/syslog-uitvoer geregistreerd tijdens de storing:

<#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
```

Belangrijkste opmerkingen uit de logs:

- De uitwisseling van SSH-sleutels en de verificatie van handtekeningen zijn succesvol.
- De fout treedt op in het open stadium van het SSH-kanaal: het openen van het kanaal is mislukt, reden = 1.
- SFTP-schrijfproces mislukt (fout 1545) en de sessie wordt onmiddellijk daarna verbroken.

Oplossing

Het probleem wordt opgelost door de grootte van het SSH-venster op de Catalyst 9300-switch te verhogen om tegemoet te komen aan de Azure Cloud-serververeisten. Azure Cloud-servers hebben een grotere SSH-venstergrootte nodig dan de standaardwaarde die is geconfigureerd op Cisco-switches vóór 17.10.1 Cisco IOS XE-versie.

Stap 1. De grootte van het SSH-venster configureren

Configureer de grootte van het SSH-venster tot een waarde van ten minste 16384. De aanbevolen maximale waarde is 65536 om overmatige CPU-impact op low-end apparaten te voorkomen:

```
<#root>

device(config)#

ip ssh window-size 65536
```

Nadat u deze opdracht hebt uitgevoerd, ontvangt u dit waarschuwingsbericht:

```
%% 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
```

Stap 2. TCP-venstergrootte configureren

Configureer de grootte van het TCP-venster zodat deze overeenkomt met de waarde voor de grootte van het SSH-venster:

```
<#root>

device(config)#

ip tcp window-size 65536
```

Configuratieverificatie

Nadat beide configuratiewijzigingen zijn geïmplementeerd, functioneert de SSH-verbinding tussen de switch en de Azure Cloud-server naar behoren, waardoor SFTP-back-upbewerkingen met succes kunnen worden uitgevoerd.

Opmerking: vanaf Cisco IOS XE Dublin 17.10.1 is de modus voor bulkgegevensoverdracht SSH standaard ingeschakeld met een standaardvenstergrootte

---

van 128 KB. Hoewel de maximale ondersteunde SSH-venstergrootte 131072 is, wordt aanbevolen om een maximale waarde van 65536 te gebruiken om de CPU-impact op apparaten van lagere kwaliteit te minimaliseren.

⚠ Let op: De minimaal vereiste venstergrootte voor Azure Cloud-servers is 16384. De venstergrootten van zowel SSH als TCP moeten worden geconfigureerd met overeenkomende waarden om ervoor te zorgen dat de oplossing effectief werkt.

Oorzaak

De hoofdoorzaak van dit probleem is een mismatch tussen de standaard SSH-venstergrootte die is geconfigureerd op Cisco Catalyst 9300-switches en de minimale SSH-venstergroottevereisten van Microsoft Azure Cloud-servers. Cisco-switches gebruiken standaard een SSH-venstergrootte van 8912, wat niet voldoende is voor Azure Cloud-servers die een minimale venstergrootte van ten minste 16384 vereisen. Deze incompatibiliteit verhindert de oprichting van het SSH-kanaal dat vereist is voor SFTP-bestandsoverdracht, hoewel de eerste SSH-verificatie en sleuteluitwisselingsprocessen met succes zijn voltooid.

Gerelateerde informatie

- Cisco Support Assistant
- Cisco Worldwide Contact
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.