Risoluzione dei problemi relativi alle connessioni Secure Shell ai server cloud di Azure sugli switch Catalyst

Sommario

Introduzione

In questo documento viene descritto come identificare e risolvere i problemi quando gli switch Cisco non sono in grado di connettersi all'archiviazione BLOB di Microsoft utilizzando Secure Shell.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Informazioni sulle operazioni e la configurazione del protocollo SFTP (Secure File Transfer Protocol) sugli switch Cisco
- Familiarità con il protocollo SSH (Secure Shell) e le relative fasi di negoziazione
- Conoscenza della configurazione del servizio di archiviazione BLOB Microsoft per l'accesso SFTP

- Lettura e interpretazione dei messaggi syslog/debug dello switch
- Risoluzione dei problemi di base per la connettività di rete e la compatibilità del protocollo tra switch Cisco e servizi SFTP esterni

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Famiglia di prodotti: Switch Catalyst serie 9300
- Versione del software: Cisco IOS® XE 17.9.5
- Tecnologia: Switching per LAN
- Connessioni SSH alla piattaforma cloud Azure

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Microsoft Blob Storage offre ora l'accesso SFTP, consentendo il trasferimento di file da dispositivi di rete come gli switch Cisco. Il backup delle configurazioni dei dispositivi su sistemi di storage cloud esterni, come Microsoft Blob, è una pratica comune per il ripristino di emergenza e la continuità operativa. SFTP sfrutta il protocollo SSH per il trasferimento sicuro dei file. Richiede la riuscita della negoziazione SSH, lo scambio di chiavi e la capacità di aprire un canale dati sicuro. Mentre i server SFTP locali possono avere implementazioni di protocollo standard o ben supportate, i servizi basati su cloud come Microsoft Blob SFTP possono introdurre differenze di compatibilità o negoziazione del protocollo che possono influire sul corretto trasferimento dei file. La risoluzione di questi problemi di interoperabilità richiede un'attenta analisi degli output di syslog/debug e un approccio metodico per isolare le cause ambientali, di configurazione o del protocollo.

Problema

Quando si cerca di eseguire il backup delle configurazioni da switch Cisco a un endpoint SFTP di archiviazione BLOB Microsoft, il backup non riesce dopo il completamento della negoziazione SSH. I backup sui server SFTP locali vengono eseguiti senza problemi, a indicare che il client

SFTP dello switch funziona anche in altri scenari.

Sintomi:

- Gli switch hanno completato correttamente lo scambio di chiavi SSH e l'autenticazione con Microsoft Blob SFTP.
- Il backup non riesce nella fase di apertura del canale, impedendo il trasferimento dei file.
- I messaggi syslog/debug indicano un errore durante l'operazione di scrittura SFTP.

Output di debug/syslog pertinente registrato durante l'errore:

<#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
```

Principali osservazioni tratte dai registri:

- Lo scambio di chiavi SSH e la verifica della firma sono stati completati.
- Il guasto si verifica nella fase di apertura del canale SSH: Apertura del canale non riuscita, motivo = 1.
- Il processo di scrittura SFTP non riesce (err 1545) e la sessione si disconnette immediatamente dopo.

Soluzione

Il problema viene risolto aumentando la configurazione delle dimensioni della finestra SSH sullo switch Catalyst 9300 per soddisfare i requisiti del server cloud di Azure. I server cloud di Azure richiedono dimensioni della finestra SSH più grandi del valore predefinito configurato sugli switch

Cisco prima della versione 17.10.1 di Cisco IOS XE.

Passaggio 1. Configurazione delle dimensioni della finestra SSH

Configurare le dimensioni della finestra SSH su un valore almeno di 16384. Il valore massimo consigliato è 65536 per evitare un impatto eccessivo sulla CPU dei dispositivi di fascia bassa:

<#root>

```
device(config)#

ip ssh window-size 65536
```

Dopo aver eseguito questo comando, viene visualizzato questo messaggio di avviso:

```
%% 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
```

Passaggio 2. Configurare le dimensioni della finestra TCP

Configurare le dimensioni della finestra TCP in modo che corrispondano al valore delle dimensioni della finestra SSH:

<#root>

```
device(config)#

ip tcp window-size 65536
```

Verifica della configurazione

Dopo aver implementato entrambe le modifiche alla configurazione, la connessione SSH tra lo switch e il server cloud di Azure funziona correttamente, consentendo operazioni di backup SFTP riuscite.

Nota: A partire da Cisco IOS XE Dublin 17.10.1, la modalità di trasferimento dei dati in blocco SSH è abilitata per impostazione predefinita con una dimensione della finestra predefinita di 128 KB. Anche se il valore massimo supportato per le dimensioni della finestra SSH è 131072, si consiglia di usare un valore massimo di 65536 per ridurre al minimo l'impatto della CPU sui dispositivi di fascia bassa.

⚠ Attenzione: Le dimensioni minime richieste per le finestre dei server cloud di Azure sono 16384. Per un funzionamento efficace della soluzione, è necessario configurare le dimensioni delle finestre SSH e TCP con valori corrispondenti.

Causa

La causa principale di questo problema è una mancata corrispondenza tra le dimensioni predefinite della finestra SSH configurate sugli switch Cisco Catalyst 9300 e i requisiti minimi delle dimensioni della finestra SSH per i server cloud Microsoft Azure. Per impostazione predefinita, gli switch Cisco usano un valore di dimensioni della finestra SSH pari a 8912, un valore insufficiente per i server cloud di Azure che richiedono dimensioni minime della finestra pari ad almeno 16384. Questa incompatibilità impedisce la creazione del canale SSH necessario per i trasferimenti di file SFTP, anche se i processi iniziali di autenticazione SSH e scambio di chiavi sono stati completati correttamente.

Informazioni correlate

- Cisco Support Assistant
- Contatti Cisco internazionali
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).