Fehlerbehebung bei Secure Shell-Verbindungen zu Azure Cloud-Servern auf Catalyst-Switches

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

Problem

Lösung

- Schritt 1: Konfigurieren der SSH-Fenstergröße
- Schritt 2: Konfigurieren der TCP-Fenstergröße
- Konfigurationsverifizierung
- Ursache

Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Probleme erkannt und behoben werden, wenn Cisco Switches keine Verbindung mit Microsoft Blob Storage über Secure Shell herstellen können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnis der SFTP-Vorgänge (Secure File Transfer Protocol) und der Konfiguration auf Cisco Switches
- Vertrautheit mit dem Secure Shell (SSH)-Protokoll und dessen Verhandlungsphasen
- Kenntnis der Konfiguration des Microsoft Blob-Speicherdiensts für den SFTP-Zugriff
- Erfahrung mit dem Lesen und Interpretieren von Switch-Syslog-/Debug-Meldungen
- Grundlegende Fehlerbehebung für Netzwerkverbindungen und Protokollkompatibilität zwischen Cisco Switches und externen SFTP-Services

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Produktfamilie: Catalyst Switches der Serie 9300
- Software-Version: Cisco IOS® XE 17.9.5
- Technologie: LAN-Switching
- SSH-Verbindungen zur Azure Cloud-Plattform

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Microsoft Blob Storage bietet jetzt SFTP-Zugriff und ermöglicht so Dateiübertragungen von Netzwerkgeräten wie Cisco Switches. Die Sicherung von Gerätekonfigurationen auf externen Cloud-Speichern wie Microsoft Blob ist eine gängige Praxis für die Notfallwiederherstellung und Betriebskontinuität. SFTP nutzt das SSH-Protokoll für die sichere Dateiübertragung. Dazu sind eine erfolgreiche SSH-Aushandlung, ein Schlüsselaustausch und die Möglichkeit zum Öffnen eines sicheren Datenkanals erforderlich. Während lokale SFTP-Server über standardmäßige oder gut unterstützte Protokollimplementierungen verfügen, können Cloud-basierte Services wie Microsoft Blob SFTP Kompatibilitäts- oder Protokollaushandlungsunterschiede hervorrufen, die sich auf eine erfolgreiche Dateiübertragung auswirken können. Die Behebung solcher Interoperabilitätsprobleme erfordert eine sorgfältige Analyse der Syslog-/Debug-Ausgaben und einen methodischen Ansatz zur Isolierung von Protokoll-, Konfigurations- oder Umgebungsursachen.

Problem

Beim Versuch, Konfigurationen von Cisco Switches auf einem Microsoft Blob-Speicher-SFTP-Endpunkt zu sichern, schlägt die Sicherung nach Abschluss der SSH-Aushandlung fehl. Sicherungen auf lokalen SFTP-Servern sind ohne Probleme erfolgreich, was darauf hinweist, dass der Switch-SFTP-Client in anderen Szenarien funktioniert.

Symptome:

- Switches schließen den Austausch und die Authentifizierung von SSH-Schlüsseln mit Microsoft Blob SFTP erfolgreich ab.
- Das Backup schlägt in der Phase der Kanaleröffnung fehl und verhindert die Dateiübertragung.
- Syslog-/Debug-Meldungen weisen auf einen Fehler beim SFTP-Schreibvorgang hin.

Relevante Debug-/Syslog-Ausgabe während des Fehlers aufgezeichnet:

<#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
```

Wichtigste Beobachtungen aus den Protokollen:

- Der Austausch von SSH-Schlüsseln und die Überprüfung der Signatur sind erfolgreich.
- Der Fehler tritt in der offenen Phase des SSH-Kanals auf: Kanalöffnung fehlgeschlagen, Grund = 1.
- Der SFTP-Schreibvorgang schlägt fehl (Fehler 1545), und die Sitzung wird sofort danach getrennt.

Lösung

Das Problem wird durch eine Vergrößerung der SSH-Fenstergröße auf dem Catalyst 9300-Switch behoben, um die Azure Cloud-Serveranforderungen zu erfüllen. Azure Cloud-Server benötigen eine größere SSH-Fenstergröße als der auf Cisco Switches konfigurierte Standardwert vor der 17.10.1 Cisco IOS XE-Version.

Schritt 1: Konfigurieren der SSH-Fenstergröße

Konfigurieren Sie die Größe des SSH-Fensters auf einen Wert von mindestens 16384. Der empfohlene Höchstwert ist 65536, um übermäßige CPU-Auswirkungen auf Low-End-Geräte zu vermeiden:

<#root>

```
device(config)#

ip ssh window-size 65536
```

Nach der Ausführung dieses Befehls wird folgende Warnmeldung angezeigt:

```
%% 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
```

Schritt 2: Konfigurieren der TCP-Fenstergröße

Konfigurieren Sie die TCP-Fenstergröße so, dass sie mit der Größe des SSH-Fensters übereinstimmt:

<#root>

```
device(config)#

ip tcp window-size 65536
```

Konfigurationsverifizierung

Nach der Implementierung beider Konfigurationsänderungen funktioniert die SSH-Verbindung zwischen dem Switch und dem Azure Cloud-Server ordnungsgemäß, sodass erfolgreiche SFTP-Sicherungsvorgänge möglich sind.

Anmerkung: Ab Cisco IOS XE Dublin 17.10.1 ist der SSH-Bulk-Data-Transfer-Modus mit einer Standardfenstergröße von 128 KB standardmäßig aktiviert. Obwohl die maximal unterstützte SSH-Fenstergröße 131072 beträgt, wird empfohlen, einen Maximalwert von 65536 zu verwenden, um die CPU-Auswirkungen auf Geräten der unteren

---

Leistungsklasse zu minimieren.

Vorsicht: Die erforderliche Mindestfenstergröße für Azure Cloud-Server beträgt 16384. Sowohl SSH- als auch TCP-Fenstergrößen müssen mit übereinstimmenden Werten konfiguriert werden, damit die Lösung effektiv funktioniert.

Ursache

Die Ursache dieses Problems liegt in einer Diskrepanz zwischen der auf Cisco Catalyst 9300-Switches konfigurierten SSH-Standardfenstergröße und den Mindestanforderungen an die SSH-Fenstergröße von Microsoft Azure Cloud-Servern. Standardmäßig verwenden Cisco Switches einen SSH-Fenstergrößenwert von 8912, was für Azure Cloud-Server, die eine Mindestfenstergröße von mindestens 16384 benötigen, nicht ausreicht. Diese Inkompatibilität verhindert die Einrichtung des für SFTP-Dateiübertragungen erforderlichen SSH-Kanals, obwohl die anfänglichen SSH-Authentifizierungs- und Schlüsselaustauschprozesse erfolgreich abgeschlossen wurden.

Zugehörige Informationen

- Cisco Support Assistant
- Weltweiter Kontakt zu Cisco
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.