Catalyst 스위치에서 Azure 클라우드 서버에 대한 보안 셸 연결 문제 해결

목차

소개

이 문서에서는 Cisco 스위치가 Secure Shell을 사용하여 Microsoft Blob 저장소에 연결할 수 없는 경우 문제를 식별하고 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 스위치의 SFTP(Secure File Transfer Protocol) 작업 및 컨피그레이션 이해
- SSH(Secure Shell) 프로토콜 및 협상 단계 숙지
- SFTP 액세스를 위한 Microsoft Blob 저장소 서비스 구성에 대한 지식
- 스위치 syslog/디버그 메시지 읽기 및 해석 경험
- Cisco 스위치와 외부 SFTP 서비스 간의 네트워크 연결 및 프로토콜 호환성에 대한 기본 문제 해결

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 제품군: Catalyst 9300 시리즈 스위치
- 소프트웨어 버전: Cisco IOS® XE 17.9.5
- 기술: LAN 스위칭
- Azure 클라우드 플랫폼에 대한 SSH 연결

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Microsoft Blob Storage는 이제 SFTP 액세스를 제공하여 Cisco 스위치와 같은 네트워크 장치에서 파일을 전송할 수 있도록 합니다. Microsoft Blob과 같이 장치 구성을 오프 사이트 클라우드 스토리지에 백업하는 것은 재해 복구 및 운영 연속성을 위한 일반적인 방법입니다. SFTP는 안전한 파일 전송을 위해 SSH 프로토콜을 활용합니다. 성공적인 SSH 협상, 키 교환, 보안 데이터 채널 열기 기능이 필요합니다. 로컬 SFTP 서버는 표준 또는 잘 지원되는 프로토콜 구현을 가질 수 있지만, Microsoft Blob SFTP와 같은 클라우드 기반 서비스는 성공적인 파일 전송에 영향을 미칠 수 있는 호환성 또는 프로토콜 협상 차이를 도입할 수 있습니다. 이러한 상호 운용성 문제를 해결하려면 syslog/디버그 출력을 신중하게 분석하고 프로토콜, 컨피그레이션 또는 환경 원인을 격리하는 체계적인 접근 방식이 필요합니다.

문제

Cisco 스위치에서 Microsoft Blob 스토리지 SFTP 엔드포인트로 컨피그레이션을 백업하려고 하면 SSH 협상이 완료된 후 백업이 실패합니다. 로컬 SFTP 서버에 대한 백업은 문제 없이 성공하며, 이는 스위치 SFTP 클라이언트가 다른 시나리오에서 작동하고 있음을 나타냅니다.

증상:

- 스위치에서 Microsoft Blob SFTP와의 SSH 키 교환 및 인증을 성공적으로 완료합니다.
- 채널 열기 단계에서 백업이 실패하여 파일 전송이 차단됩니다.
- Syslog/디버그 메시지는 SFTP 쓰기 작업 중 실패를 나타냅니다.

실패 중에 기록된 관련 디버그/syslog 출력:

<#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
```

로그의 주요 관찰 내용:

- SSH 키 교환 및 서명 확인에 성공했습니다.
- SSH 채널 열기 스테이지에서 오류가 발생합니다. 채널 열기가 실패했습니다. 이유 = 1.
- SFTP 쓰기 프로세스가 실패하고(오류 1545) 즉시 세션 연결이 끊깁니다.

솔루션

Azure 클라우드 서버 요구 사항을 수용하기 위해 Catalyst 9300 스위치의 SSH 창 크기 구성을 늘려 문제를 해결합니다. Azure 클라우드 서버에서는 17.10.1 Cisco IOS XE 버전 이전에 Cisco 스위치에 구성된 기본값보다 큰 SSH 창 크기가 필요합니다.

1단계. SSH 창 크기 구성

SSH 창 크기를 16384 이상의 값으로 구성합니다. 권장되는 최대값은 로우엔드 디바이스에 과도한 CPU가 영향을 미치지 않도록 65536.

<#root>

```
device(config)#

ip ssh window-size 65536
```

이 명령을 실행하면 다음과 같은 경고 메시지가 표시됩니다.

```
%% 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
```

2단계. TCP 창 크기 구성

SSH 창 크기 값과 일치하도록 TCP 창 크기를 구성합니다.

<#root>

```
device(config)#

ip tcp window-size 65536
```

컨피그레이션 확인

두 가지 컨피그레이션 변경을 구현하면 스위치와 Azure 클라우드 서버 간의 SSH 연결이 제대로 작동하여 성공적인 SFTP 백업 작업을 수행할 수 있습니다.

참고: Cisco IOS XE Dublin 17.10.1부터 SSH 대량 데이터 전송 모드는 기본 창 크기 128KB로 기본적으로 활성화됩니다. 지원되는 최대 SSH 창 크기 값은 131072이지만, 하위 엔드 디바이스에 미치는 CPU 영향을 최소화하기 위해 최대 65536 값을 사용하는 것이 좋습니다.

주의: Azure 클라우드 서버에 필요한 최소 창 크기가 16384. 솔루션이 효과적으로 작동하려면 SSH 및 TCP 창 크기를 모두 일치하는 값으로 구성해야 합니다.

원인

이 문제의 근본 원인은 Cisco Catalyst 9300 스위치에 구성된 기본 SSH 창 크기와 Microsoft Azure 클라우드 서버의 최소 SSH 창 크기 요구 사항이 일치하지 않기 때문입니다. 기본적으로 Cisco 스위치는 SSH 창 크기 값 8912를 사용하는데, 이 값은 최소 16384개 이상의 창 크기가 필요한 Azure 클

라우드 서버에는 충분하지 않습니다. 이러한 비호환성으로 인해 초기 SSH 인증 및 키 교환 프로세스가 성공적으로 완료되더라도 SFTP 파일 전송에 필요한 SSH 채널을 설정할 수 없습니다.

관련 정보

- Cisco Support Assistant
- Cisco Worldwide 연락처
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.