TAC를 통해 Cisco IOS®/Cisco IOS® XE Platform에서 예기치 않은 재로드 문제 해결

목차

소개

이 문서에서는 Cisco IOS®/Cisco IOS XE에서 예기치 않은 다시 로드의 원인을 파악하고 TAC 케이스에 업로드하는 데 필요한 파일에 대해 설명합니다. SDWAN 구축은 논의되지 않습니다.

사전 요구 사항

요구 사항

- 이 문서는 Cisco IOS/Cisco IOS XE 소프트웨어를 실행하는 Cisco 라우터 및 스위치에 적용됩니다.
- 이 문서에 설명된 파일을 수집하려면 장치가 가동 및 안정적이어야 합니다.
- 전송 프로토콜을 통해 파일을 추출하려면 L3 연결성을 갖춘 서버(파일 전송 애플리케이션/서비스가 설치되어 있음)가 필요합니다.
- 디바이스에 대한 SSH/텔넷을 통한 콘솔 또는 원격 연결이 필요합니다.

참고: 예기치 않은 다시 로드 이벤트의 경우, 일부 파일이 다시 로드 및 플랫폼의 특성에 따라

생성되지 않을 수 있습니다.

기술 지원 파일 표시

show tech-support 명령 출력에는 디바이스 현재 상태(메모리 및 CPU 사용률, 로그, 컨피그레이션 등)에 대한 일반 정보와 예기치 않은 다시 로드 이벤트가 발생한 시점과 관련된 생성된 파일에 대한 정보가 포함됩니다.

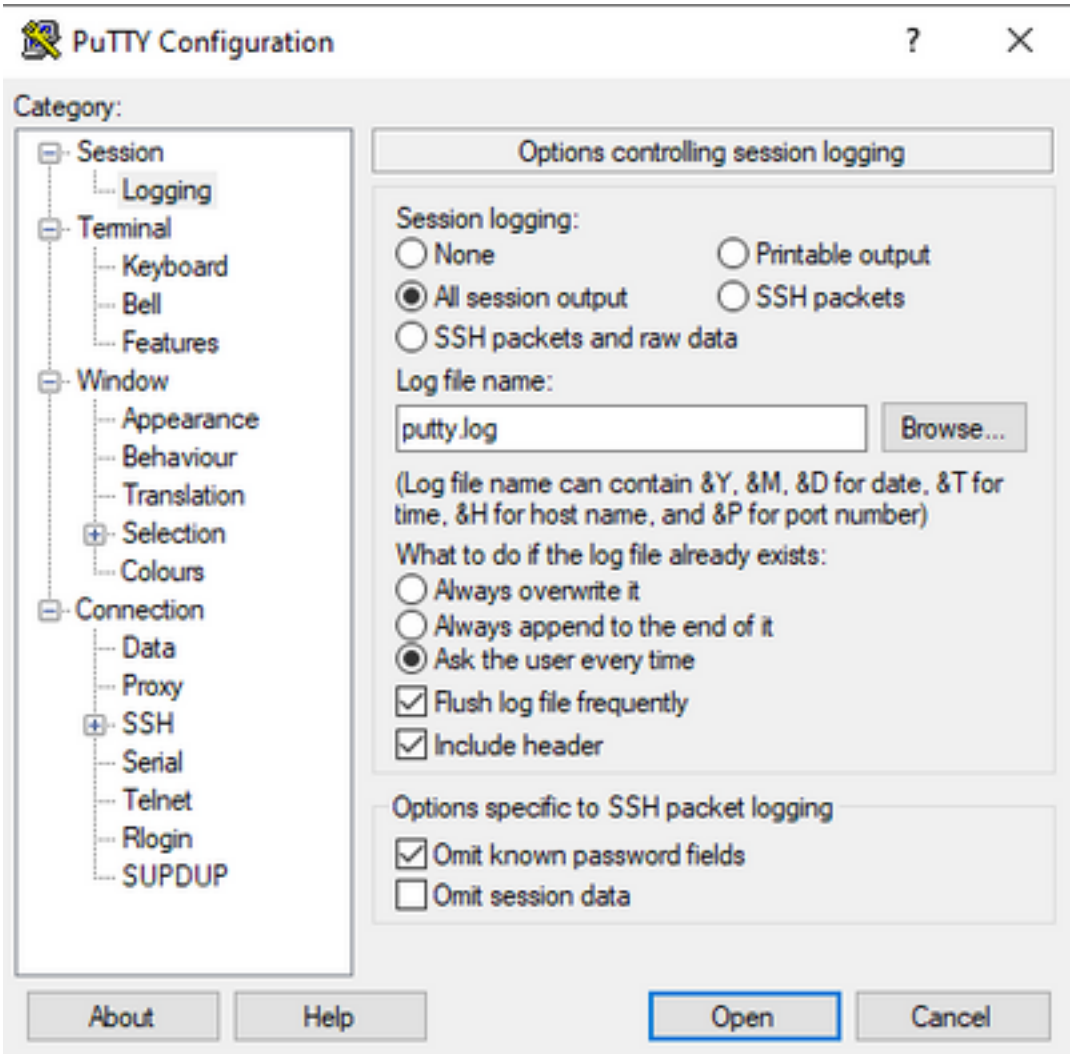
예기치 않은 재부팅 상황의 경우 검토해야 할 핵심 사항은 다음과 같습니다.

- 디바이스에 설치된 현재 Cisco IOS/Cisco IOS XE 버전.
- 포트, 카드 및 모듈 세부사항이 포함된 시스템 컨피그레이션
- 파일 시스템에서 근본 원인 분석을 제공하는 추가 파일이 있는 경우

show tech-support 출력은 두 가지 방법으로 캡처할 수 있습니다. **터미널 세션을 로깅하거나 스토리지에 파일을 만들어 디바이스에서 전송합니다**.

터미널 세션 기록

Putty에서 **Session > Logging**으로 이동하고 **Session logging** 탭 내부에서 **All session output 옵션**을 선택합니다.



파일은 기본적으로 putty.log 이름으로 Putty 폴더에 저장됩니다. 찾아보기 버튼을 사용하여 파일의

폴더와 이름을 변경할 **수** 있습니다.

컨피그레이션이 완료되면 Putty **세션**은 **콘솔**, 텔넷 또는 SSH를 통해 디바이스**에** 연결되어야 **합니다**.

디바이스 세션에서는 **터미널** 길이 **0** 명령을 **권한 모드**로 설정한 다음 show tech**-support 명령을 사용하는 것이** 좋습니다.

```
# terminal length 0
# show tech-support
```

참고: 명령을 실행하는 데 몇 초가 걸릴 수 있습니다. 실행을 중단하지 마십시오.

저장소에서 파일 만들기

show **tech-support 파일**은 디바이스에 생성되고 파일 시스템 스토리지(내부 또는 외부) 중 하나에 저장될 수 있습니다. 명령 구문은 모든 디바이스에서 동일하게 유지되지만 사용되는 파일 시스템은 변경될 수 있습니다. 외부 서버에서 직접 파일을 생성할 수도 있습니다. 이 섹션에서는 로컬 파일 시스템의 구문을 보여줍니다.

플래시 내부에 파일을 생성하려면 **show tech-support** 명령을 사용해야 합니다 **| 플래시 리디렉션:권한 모드**에서 Showtech.txt:

```
# show tech-support | redirect flash:Showtech.txt
```

텍스트 파일이 생성되는 동안 터미널을 몇 초 동안 사용할 수 없습니다. 완료되면 **show [file system]**을 사용하여 파일 생성이 올바른지 확인할 수 있습니다. 명령을 사용합니다; 파일은 일반 텍스트 파일이므로 디바이스에 **더** 많은 명령으로 콘텐츠를 표시할 수 있습니다.

```
# show flash:
# more flash:Showtech.txt
```

파일이 생성되면 선택 전송 프로토콜(FTP/TFTP/SCP)을 사용하여 외부 스토리지로 압축을 풀고 분석을 위해 공유할 수 있습니다.

Crashinfo 파일

crashinfo **파일**은 텍스트 파일이며, 충돌 원인을 식별하는 데 도움이 되는 디버그 세부 정보를 포함합니다. 컨텐츠는 플랫폼마다 다를 수 있습니다. 일반적으로, 여기에는 **암호화 모드**에서 충돌 전에 로깅 버퍼와 충돌 전에 프로세서에 의해 실행된 기능이 있습니다. Cisco IOS 플랫폼에서 이는 충돌 후 파일 시스템에서 찾을 수 있는 가장 일반적인 파일입니다. Cisco IOS XE 플랫폼에서 이 파일은 IOSd 프로세스에서만 충돌이 발생할 때 생성됩니다. 다른 프로세스가 실패하면 디바이스는 crashinfo 파일을 생성하지 않습니다.

Crashinfo 파일은 플랫폼의 플래시, 부트플래시, 하드 디스크 또는 crashinfo 스토리지에서 찾을 수 있습니다. 이중 컨트롤 플레인 플랫폼의 경우, 캐시 파일은 액티브 및/또는 스탠바이 수퍼바이저에서 찾을 수 있습니다.

예기치 않은 재부팅 전에 DRAM 메모리의 스냅만 가져오고 프로세스의 메모리 영역만 가져오므로 이 파일의 내용은 제한됩니다. 경우에 따라 재부팅의 근본 원인을 파악하기 위해 추가 파일/출력이 필요할 수 있습니다.

코어 파일

Cisco IOS XE 플랫폼에서는 런타임 오류로 인해 프로세스 또는 서비스가 실행을 종료하고 예기치 않은 재부팅이 발생하면 코어 파일이 생성됩니다. 이 파일에는 다시 로드 이벤트에 대한 컨텍스트 정보가 포함되어 있습니다.

Cisco IOS XE 플랫폼에서는 예기치 않은 재부팅이 소프트웨어 기반일 때 기본적으로 생성됩니다. 코어 파일은 모든 Linux 프로세스(IOSd 프로세스 포함)에서 생성할 수 있습니다.

코어 파일은 충돌을 트리거한 특정 프로세스에서 사용하는 실행 중인 모든 메모리의 정보를 포함하는 압축 파일입니다. 이 파일을 디코딩하려면 특별한 툴이 필요하므로 일관성을 유지하기 위해 변경 없이 파일을 추출해야 합니다. 파일의 압축을 풀거나 정보를 텍스트로 추출합니다(예: **추가** 명령 사용). 지원 팀이 콘텐츠를 디코딩하는 기능은 허용되지 않습니다.

일반적으로 코어 파일은 bootflash 또는 **하드** 디스크 내부의 **core** 폴더에 **저장됩니다**.

다음은 bootflash 파일 시스템의 코어 폴더 내에 코어 파일이 나타나는 방법을 보여 주는 예입니다.

```
------------------ show bootflash: all ------------------

 9   10628763 Jul 14 2021 09:58:49 +00:00
/bootflash/core/Router_216_Router_RP_0_ucode_pkt_PPE0_3129_1626256707.core.gz
10   10626597 Jul 23 2021 13:35:26 +00:00
/bootflash/core/Router_216_Router_RP_0_ucode_pkt_PPE0_2671_1627047304.core.gz
```

> **참고:** TAC에서 코어 파일을 성공적으로 분석하려면 수정 또는 변경 없이 파일을 추출해야 합니다.

디바이스에서 이 파일을 추출하는 방법을 확인하려면 Extract Files(파일 추출) 섹션으로 이동합니다.

트레이스로그

tracelog는 Cisco IOS XE 내의 각 프로세스에 대한 내부 로그입니다. tracelogs 디렉토리는 기본적으로 생성되며 해당 내용은 주기적으로 덮어씁니다. 이 폴더는 bootflash 또는 **하드 디스크**에서 찾을 **수 있습니다**.

이 폴더는 예기치 않은 다시 로드 이벤트의 경우 추가 정보를 제공할 수 있으므로 권장되지 않지만 안전하게 제거할 수 있습니다.

폴더의 내용을 추출하기 위해 가장 쉬운 방법은 모든 tracelogs 파일을 포함하는 압축 파일을 생성하는 것입니다. 플랫폼을 기반으로 다음 명령을 사용할 수 있습니다.

Cisco IOS XE 라우터의 경우:

```
# request platform software trace slot rp active archive target bootflash:TAC_tracelogs
```

Cisco IOS XE 스위치 및 무선 컨트롤러의 경우:

```
# request platform software trace archive target bootflash:TAC_tracelogs
```

Tracelogs는 디코딩하기 위한 추가 도구가 필요한 인코딩된 파일이므로 압축 파일이 생성될 때 압축을 풀어야 합니다.

디바이스에서 이 파일을 추출하는 방법을 확인하려면 Extract Files(파일 추출) 섹션으로 이동합니다.

시스템 보고서

시스템 보고서는 예기치 않은 다시 로드가 발생할 때 소프트웨어 실행에서 사용 가능한 대부분의 정보를 수집하는 압축된 파일입니다. 시스템 보고서에는 tracelogs, crashinfo 및 core 파일이 포함됩니다. 이 파일은 Cisco IOS XE 스위치 및 무선 컨트롤러에서 예기치 않은 다시 로드가 발생할 경우 생성됩니다.

파일은 부트플래시 또는 하드 디스크의 주 디렉토리에서 찾을 수 있습니다.

항상 리부팅 직전에 생성된 tracelogs를 포함합니다. 예기치 않은 다시 로드의 경우 이벤트의 캐시 파일과 코어 파일이 있습니다.

이 파일은 압축 파일이며 폴더의 압축을 풀 수 있지만 정보를 디코딩하기 위한 추가 도구가 필요합니다.

디바이스에서 이 파일을 추출하는 방법을 확인하려면 Extract Files(파일 추출) 섹션으로 이동합니다.

커널 코어

커널 코어는 Cisco IOS XE 프로세스가 아니라 Linux 커널에 의해 생성됩니다. 커널 오류로 인해 디바이스가 다시 로드되면 일반적으로 완전한 커널 코어(압축 파일) 및 커널 코어(일반 텍스트) 파일의 요약이 생성됩니다.

예기치 않은 재부팅을 발생시킨 프로세스를 검토할 수 있지만, 다시 로드 이유를 완벽하게 분석하기 위해서는 Cisco TAC에 파일을 제공하는 것이 좋습니다.

커널 코어 파일은 bootflash 또는 하드 디스크의 주 디렉토리에서 **찾**을 수 있습니다.

파일 추출 방법

이 섹션에서는 Cisco IOS/Cisco IOS XE 플랫폼에서 외부 스토리지 클라이언트로 필수 파일을 전송하는 데 필요한 기본 컨피그레이션에 대해 설명합니다.

디바이스에서 서버로의 연결이 가능할 것으로 예상됩니다. 필요한 경우 디바이스에서 서버로의 트래픽을 차단하는 방화벽 또는 컨피그레이션이 없는지 확인합니다.

이 섹션에서는 특정 서버 애플리케이션을 권장하지 않습니다.

TFTP

TFTP를 통해 파일을 전송하려면 **TFTP** 서버 애플리케이션에 대한 연결성을 **설정해야** 합니다. 추가 컨피그레이션은 필요하지 않습니다.

기본적으로 일부 디바이스는 관리 인터페이스를 통해 **ip tftp 소스** 인터페이스 컨피그레이션이 활성화되어 있습니다. 관리 인터페이스를 통해 서버에 연결할 수 없는 경우 다음 명령을 실행하여 이 컨피그레이션을 제거합니다.

```
(config)# no ip tftp source interface
```

서버에 연결하기 위한 컨피그레이션이 완료되면 파일을 전송하기 위해 다음 명령을 실행할 수 있습니다.

```
#copy :<file> tftp:
Address or name of remote host []? X.X.X.X
Destination filename [<file>]?
```

FTP

FTP를 통해 파일을 전송하려면 **FTP** 서버 애플리케이션에 대한 연결성을 설정해야 합니다. 디바이스 및 **FTP** 서버 애플리케이션에서 **FTP** 사용자 이름 및 비밀번호를 구성해야 합니다. 디바이스에서 자격 증명을 설정하려면 다음 명령을 실행합니다.

```
(config)#ip ftp username username
(config)#ip ftp password password
```

선택적으로, 다음 명령을 사용하여 디바이스에서 FTP 소스 인터페이스를 구성할 수 있습니다.

```
(config)# ip ftp source interface interface
```

서버에 연결하기 위한 컨피그레이션이 완료되면 파일을 전송하기 위해 다음 명령을 실행할 수 있습니다.

```
#copy :<file> ftp:
Address or name of remote host []? X.X.X.X
Destination filename [<file>]?
```

SCP

SCP를 통해 파일을 전송하려면 **SCP** 서버 애플리케이션에 대한 연결 가능성**을 설정해야** 합니다. 디바이스(전송을 시작하려면 자격 증명이 필요함) 및 **SCP** 서버 애플리케이션에서 로컬 사용자 이름과 비밀번호를 구성해야 합니다. 또한 디바이스에 SSH**가** 구성되어 있어야 합니다. SSH 서비스가 **구성되었는지** 확인하려면 다음 명령을 실행합니다.

```
#show running-config | section ssh
ip ssh version 2
ip ssh server algorithm encryption 3des-cbc aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption 3des-cbc aes128-ctr aes192-ctr aes256-ctr
transport input ssh
transport input ssh
```

디바이스에서 자격 증명을 설정하려면 다음 명령을 실행합니다.

```
(config)#username USER password PASSWORD
```

> **참고:** SSH 사용자 **인증**에 TACACS 또는 다른 서비스가 사용되는 경우, SCP 서버에 사용자 정보가 있으면 이러한 자격 증명을 사용할 수 있습니다.

컨피그레이션이 완료되면 파일을 전송하기 위해 다음 명령을 실행할 수 있습니다.

```
#copy :<file> scp:
Address or name of remote host []? X.X.X.X
Destination filename [<file>]?
```

USB

USB 플래시를 통한 파일 전송에는 네트워크의 외부 서버에 연결할 필요는 없지만 디바이스에 대한 물리적 액세스가 필요합니다.

Cisco IOS/Cisco IOS XE를 사용하는 모든 물리적 디바이스에는 외부 스토리지로 사용할 수 있는 USB 포트가 있습니다.

USB 플래시 드라이브가 인식되는지 확인하려면 show file systems **명령을** 실행합니다.

```
#show file systems
File Systems:

Size(b) Free(b) Type Flags Prefixes - - opaque rw system: - - opaque rw tmpsys: * 11575476224
10111098880 disk rw bootflash: flash: 2006351872 1896345600 disk ro webui: - - opaque rw null: -
- opaque ro tar: - - network rw tftp: 33554432 33527716 nvram rw nvram: - - opaque wo syslog: -
- network rw rcp: - - network rw pram: - - network rw http: - - network rw ftp: - - network rw
scp: - - network rw sftp - - network rw https: - - network ro cns: 2006351872 1896345600 disk rw
usbflash0:
```

> **참고:** Cisco IOS/Cisco IOS XE 디바이스는 공식 Cisco USB 플래시 드라이브를 지원합니다. 서드파티 USB 플래시의 경우 지원이 제한됩니다.

적절한 슬롯(usbflash0 또는 usbflash1)의 디바이스에서 USB 플래시를 인식하고 사용 가능한 공간이 충분하면 다음 명령을 사용하여 파일을 전송합니다.

```
#copy :<file> usbflashX:
Destination filename [<file>]?
```

문제 해결

이 섹션에서는 Cisco IOS 또는 Cisco IOS XE 디바이스에서 외부 방식으로 파일을 전송하는 동안 발견하고 사용할 수 있는 몇 가지 일반적인 오류와 해결 방법에 대해 설명합니다.

열린 포트 확인

서버에 대한 연결 가능성이 확인되었을 때 디바이스에 연결 거부 오류가 표시되는 경우 디바이스측 포트가 사용 가능한지(트래픽을 차단하는 ACL 항목 없음), 서버측 포트도 사용 가능한지(마지막 부분에서 필요한 포트를 포함하는 telnet 명령을 사용할 수 있음)를 확인하는 것이 유용합니다.

사용된 프로토콜에 따라 다음 명령을 실행합니다.

TFTP

```
#telnet X.X.X.X 69
```

FTP
```
#telnet X.X.X.X 21
```

SCP
```
#telnet X.X.X.X 22
```

참고: 이전 포트는 각 프로토콜의 기본 포트이며 이러한 포트는 변경될 수 있습니다.

명령이 성공적인 오픈 포트를 제공하지 않으면 트래픽을 삭제할 수 있는 잘못된 컨피그레이션(서버 측 또는 경로의 방화벽)을 확인하는 것이 좋습니다.

USB 형식

대부분의 Cisco IOS 및 Cisco IOS XE 디바이스에서는 서드파티 USB를 인식할 수 없습니다.

4GB보다 큰 USB는 Cisco IOS 라우터 및 스위치에서 인식할 수 없습니다. 크기가 4GB보다 큰 USB는 Cisco IOS XE 플랫폼에서 인식할 수 있습니다.

서드파티 USB의 경우 FAT32 또는 FAT16 포멧으로 테스트가 가능하다. 호환되는 USB 메모리 드라이브에 대해서도 다른 형식을 인식할 수 없습니다.

전송 중단

홉이 많은 서버에 대해 파일 전송이 중단되고 전송을 다시 시작해야 할 수 있습니다.

이 시나리오에서는 vty 라인에서 이 컨피그레이션을 사용하는 것이 유용할 수 있습니다.

```
(config)#line vty 0 4
(config-line)#exec-timeout 0 0
```
이전 컨피그레이션에서는 제어 패킷이 경로에서 삭제되거나 패킷이 승인되는 데 시간이 너무 오래 걸리는 경우에도 전송 세션이 삭제되지 않도록 합니다.

전송이 완료되면 vty 행에서 이 컨피그레이션을 제거하는 것이 좋습니다.

파일 서버를 디바이스에 최대한 가깝게 배치하는 것이 좋습니다.

중간 TFTP 서버입니다.

Cisco 디바이스는 로컬 파일 서버로 직접 수행할 수 없는 전송을 위한 임시 TFTP 서버로 사용할 수 있습니다.

추출이 필요한 파일이 있는 디바이스에서 다음 명령을 실행할 수 있습니다.

```
(config)#tftp-server :<file>
```
클라이언트로 구성된 디바이스에서 TFTP 섹션에 나타나는 명령을 실행할 수 있습니다.

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.