소프트웨어 강제 충돌 이해

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[가능한 원인](#)
[문제 해결](#)
[구성 절차](#)
[TFTP 서버 호스트 구성 절차](#)
[TAC 서비스 요청을 열 경우 수집할 정보](#)
[관련 정보](#)

소개

이 문서에서는 소프트웨어 강제 충돌의 가장 빈번한 원인을 설명하고 트러블슈팅을 위해 수집해야 하는 정보를 설명합니다.소프트웨어 장애 발생 시 TAC 서비스 요청을 열 경우, 수집해야 할 정보가 문제 해결에 필수적입니다.

사전 요구 사항

요구 사항

이 문서의 독자는 다음 주제에 대해 알고 있어야 합니다.

- 라우터 충돌 문제를 해결하는 방법.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

소프트웨어 강제 충돌은 라우터가 심각한 복구 불가능한 오류를 감지하고 손상된 데이터를 전송하지 않도록 자체적으로 다시 로드될 때 발생합니다.소프트웨어 장애의 대부분은 Cisco IOS® 소프트웨어 버그로 인해 발생하지만 일부 플랫폼(예: 기존 Cisco 4000)은 하드웨어 문제를 소프트웨어 장애 상태로 보고할 수 있습니다.

라우터의 전원을 껐다가 다시 로드하지 않았거나 수동으로 다시 로드한 경우 **show version** 명령의 출력에서 다음을 표시합니다.

```
Router uptime is 2 days, 21 hours, 30 minutes
System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt
System image file is "flash:c2500-is-l.112-15a.bin", booted via flash
```

Cisco 디바이스에서 **show version** 명령의 출력이 있는 경우 Cisco CLI Analyzer(등록된 고객만)를 사용하여 잠재적인 문제 및 수정 사항을 표시할 수 있습니다.

가능한 원인

이 표에서는 소프트웨어 강제 충돌의 가능한 이유에 대해 설명합니다.

이유	설명

워치독 시간 초과	프로세서는 타이머를 사용하여 무한 루프를 방지하며 라우터가 응답을 중지합니다.정상 작동 CPU는 해당 타이머를 일정한 간격으로 재설정합니다.이렇게 하지 않으면 시스템이 다시 로드 니다.소프트웨어 강제 충돌로 보고된 워치독 시간 초과는 소프트웨어 관련 사항입니다.다른 유 의 워치독 시간 초과에 대한 자세한 내용은 워치독 시간 초과 문제 해결을 참조하십시오.시스템 다시 로드되기 전에 루프에 고정되었습니다.따라서 스택 추적은 반드시 관련이 있는 것은 아닙 다.콘솔 로그의 다음 행에서 이 유형의 소프트웨어 강제 충돌을 인식할 수 있습니다.
	`%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec`
	`and`
	`*** System received a Software forced crash ***`
	`signal = 0x17, code = 0x24, context= 0x60ceca60`

메모리 부족	라우터의 메모리가 너무 부족하면 결국 다시 로드되어 소프트웨어 강제 크래시로 보고할 수 있 니다.이 경우 메모리 할당 실패 오류 메시지가 콘솔 로그에 나타납니다.
	`%SYS-2-MALLOCFAIL: Memory allocation of 734 bytes failed from 0x6015EC84,`
	`pool Processor, alignment 0`

손상된 소프트웨어 이미지	부팅 시 라우터는 Cisco IOS 소프트웨어 이미지가 손상되었음을 감지하고 메시지 반환하고 시 로드하려고 시도합니다.이 경우, 이벤트가 소프트웨어 강제 충돌로 보고됩니다.
	`Error : compressed image checksum is incorrect 0x54B2C70A`
	`Expected a checksum of 0x04B2C70A`
	`*** System received a Software forced crash ***`
	`signal= 0x17, code= 0x5, context= 0x0`
	`PC = 0x800080d4, Cause = 0x20, Status Reg = 0x3041f003`
	이는 라우터로 전송하는 동안 실제로 손상된 Cisco IOS 소프트웨어 이미지 때문일 수 있습니다 경우 새 이미지를 라우터에 로드하여 문제를 해결할 수 있습니다.[플랫폼에 대한 ROMMON 복 방법은 Cisco 7200, 7300, 7400, 7500, RSP7000, Catalyst 5500 RSM, uBR7100, uBR72000, ROM 복구 절차를 참조하십시오. 10000 및 12000 Series 라우터입니다.] 메모리 하드웨어 오류 는 소프트웨어 버그로 인해 발생할 수도 있습니다.

기타 결함	충돌을 일으키는 오류는 종종 프로세서 하드웨어에서 감지되며 ROM 모니터에서 특수 오류 처 코드를 자동으로 호출합니다.ROM 모니터는 오류를 식별하고, 메시지를 인쇄하고, 오류에 대한 보를 저장하고, 시스템을 다시 시작합니다.이러한 문제가 발생하지 않는 충돌이 있습니다 (Watchdog 시간 제한 참조). 소프트웨어가 문제를 탐지하고 crashdump 함수를 호출하는 충돌 발생합니다.이것은 진정한 "소프트웨어 강제" 충돌입니다.Power PC 플랫폼에서는 crashdump 수가 호출될 때 "software-forced crash"가 인쇄된 재시작 사유가 아닙니다. 최소한 최근까지도 입니다.이러한 플랫폼(Cisco IOS Software Release 12.2(12.7) 이전)에서 이러한 예외를 "SIGTRAP" 예외라고 합니다.다른 모든 방법으로 SIGTRAP과 SFC는 동일합니다.

문제 해결

소프트웨어 강제 충돌은 일반적으로 Cisco IOS 소프트웨어 버그로 인해 발생합니다.로그에 메모리 할당 실패 오류 메시지가 있는 경우 메모리 문제 해결을 참조하십시오.

메모리 할당 실패 오류 메시지가 표시되지 않고 소프트웨어 강제 충돌 후 라우터를 수동으로 다시 로드하거나 전원을 껐을 경우, 사용할 수 있는 가장 좋은 툴은 Cisco CLI Analyzer(등록된 고객만 해당)가 알려진 일치하는 버그 ID를 검색하는 것입니다.이 툴은 이전 Stack Decoder 툴의 기능을 통합합니다.

예:

1. 라우터에서 **show stack**의 출력을 수집합니다.
2. Cisco CLI Analyzer(등록된 고객만 해당) 툴로 이동합니다.
3. 풀다운 메뉴에서 show stack을 선택합니다.
4. 수집한 출력에 붙여 넣습니다.
5. 제출을 **클릭합니다**.**show stack** 명령의 디코딩된 출력이 알려진 소프트웨어 버그와 일치하면 소프트웨어 강제 충돌을 일으킬 가능성이 가장 높은 소프트웨어 버그의 버그 ID를 받게 됩니다.
6. 버그 ID 하이퍼링크를 클릭하면 정확한 버그 ID 일치를 확인할 수 있는 Cisco Bug Toolkit(등록된 고객만 해당)에서 추가 버그 세부사항을 볼 수 있습니다.

오류와 일치하는 버그 ID를 식별한 경우 "fixed in" 필드를 참조하여 버그에 대한 수정 사항이 포함된 첫 번째 Cisco IOS 소프트웨어 버전을 확인합니다.

버그 ID 또는 문제에 대한 수정 사항이 포함된 Cisco IOS 소프트웨어 버전에 대해 잘 모르는 경우 Cisco IOS 소프트웨어를 릴리스 교육에서 최신 버전으로 업그레이드하십시오.이는 최신 버전에 많은 수의 버그에 대한 수정 사항이 포함되어 있기 때문에 도움이 됩니다.이 방법으로 문제를 해결할 수 없더라도, 최신 버전의 소프트웨어를 사용할 경우 버그 보고 및 해결 프로세스가 더 간단하고 빠르게 수행됩니다.

Cisco CLI Analyzer를 사용한 후 해결되지 않은 버그를 의심하거나 긍정적으로 식별한 경우 TAC 서비스 요청을 열어 버그를 해결하는 데 도움이 되는 추가 정보를 제공하고 버그가 궁극적으로 해결될 때 더 빨리 알림을 받는 것이 좋습니다.

구성 절차

문제가 새 소프트웨어 버그로 식별되면 Cisco TAC 엔지니어가 *코어 덤프*를 수집하도록 라우터를 구성하도록 요청할 수 있습니다.소프트웨어 버그를 수정하기 위해 수행할 수 있는 작업을 식별하기 위해 코어 덤프가 필요한 경우가 있습니다.

코어 덤프에서 더 유용한 정보를 수집하려면 숨겨진 **debug sanity** 명령을 사용하는 것이 좋습니다.이렇게 하면 시스템에서 사용되는 모든 버퍼가 할당될 때와 해제될 때 온전하게 점검됩니다.**debug sanity** 명령은 특별 권한 EXEC 모드(활성화 모드)에서 실행해야 하며 일부 CPU는 포함되지만 라우터의 기능에는 크게 영향을 주지 않습니다.온전성 검사를 비활성화하려면 undebug **sanity** privileged EXEC 명령을 사용합니다.

기본 메모리가 16MB 이하인 라우터의 경우 TFTP(Trivial File Transfer Protocol)를 사용하여 코어 덤프를 수집할 수 있습니다.라우터에 기본 메모리가 16MB를 초과하는 경우 FTP(File Transfer Protocol)를 사용하는 것이 좋습니다.이 섹션의 컨피그레이션 절차를 사용합니다.또는 코어 덤프 생성을 참조하십시오.

라우터를 구성하려면 다음 단계를 완료합니다.

1. configure **terminal** 명령으로 라우터를 구성합니다.
2. 유형 **예외 덤프 n.n.n.n**, 여기서 n.n.n.n은 원격 TFTP(Trivial File Transfer Protocol) 서버 호스트의 IP 주소입니다.
3. 컨피그레이션 모드를 종료합니다.

TFTP 서버 호스트 구성 절차

TFTP 서버 호스트를 구성하려면 다음 단계를 완료합니다.

1. 선택한 편집기의 도움을 받아 원격 호스트의 /tftpboot 디렉토리 아래에 파일을 생성합니다.파일 이름은 Cisco 라우터 호스트 이름 코어입니다.
2. UNIX 시스템에서는 "hostname-core" 파일의 사용 권한 모드를 전역적으로 호환(666)하도록 변경합니다. 해당 파일에서 copy running-**config tftp** 명령을 통해 TFTP 설정을 확인할 수 있습니다.
3. /tftpboot 아래에 16MB 이상의 사용 가능한 디스크 공간이 있는지 확인합니다.시스템이 충돌하면 **예외 덤프** 명령은 위 파일에 출력을 생성합니다.라우터에 16MB가 넘는 기본 메모리가 있는 경우 FTP(File Transfer Protocol) 또는 RCP(Remote Copy Protocol)를 사용하여 코어 덤프를 가져옵니다.라우터에서 다음을 구성합니다.

   ```
   exception protocol ftp
   exception dump n.n.n.n
   ip ftp username ip ftp password ip ftp source-interface exception core-file
   ```

   코어 덤프를 수집했으면 ftp://ftp-sj.cisco.com/incoming에 업로드합니다(UNIX에서 **pftp-sj.cisco.com을** 입력한 다음 **cd incoming**). 케이스 소유자에게 알리고 파일 이름을 포함합니다.

TAC 서비스 요청을 열 경우 수집할 정보

위의 트러블슈팅 단계를 거친 후에도 지원이 필요한 경우 Cisco TAC에서 서비스 요청을 생성하려면 다음를 포함해야 합니다.

- **show technical-support** output - show **technical-support** 명령의 출력에서는 라우터의 현재 상태에 대한 보와 충돌 전에 라우터가 저장한 주요 정보를 제공합니다.
- 콘솔 로그 - syslog 서버에 저장되는 콘솔 로그는 충돌 전에 라우터에서 발생하는 이벤트에 대한 중요한 보를 제공할 수 있습니다.이러한 단서들은 여러분이 수집할 수 있는 가장 중요한 정보입니다.
- crashinfo 파일(있는 경우) - crashinfo 기능을 지원하는 Cisco IOS 소프트웨어 릴리스를 사용하여 성공로 문제를 해결할 것을 권장합니다.이를 위해 버전은 네트워크의 다른 요구 사항을 충족해야 합니다 .Crashinfo File(Crashinfo 파일)에서 정보 검색을 참조하거나 Software Advisor(등록된 고객만 해당) 툴 용하여 crashinfo 기능을 지원하는 Cisco IOS 소프트웨어 버전을 찾습니다.또한 이전 버전의 Cisco IOS 프트웨어가 있는 경우 이 기능을 지원하는 최신 IOS 소프트웨어 릴리스에 이미 버그가 수정될 수 있습

서비스 요청에 정보를 첨부하려면 TAC 서비스 요청 툴(등록된 고객만 해당)을 통해 업로드합니다. TAC Se Request Tool에 액세스할 수 없는 경우 이메일 첨부 파일의 정보를 attach@cisco.com으로 보낼 수 있습니 이스 번호는 메시지의 제목 줄에 있습니다.

주의: 위 정보를 수집하기 전에 라우터를 수동으로 다시 로드하거나 전원을 껐다가 다시 켜지 마십시오. 가 경우 문제의 근본 원인을 파악하는 데 필요한 중요한 정보가 손실될 수 있습니다.

관련 정보

- 라우터 충돌 트러블슈팅
- Crashinfo 파일에서 정보 검색
- 코어 덤프 생성
- 메모리 문제 해결
- Technical Support - Cisco Systems