

Nexus 9000에서 예기치 않은 재로드 또는 충돌 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[Nexus 9000 스위치의 고장 방식](#)

[다시 로드 및 충돌 문제를 해결하기 위한 중요 데이터](#)

[시스템 재설정 이유](#)

[코어 파일](#)

[온보드 로그](#)

[프로세스 로그](#)

[Logflash의 로그 파일](#)

[일반적인 재설정 이유](#)

[전원 관련 다시 로드](#)

[설명](#)

[권장:](#)

[프로세스 충돌](#)

[설명](#)

[권장:](#)

[EOBC 실패](#)

[설명](#)

[권장:](#)

[패리티 오류](#)

[설명](#)

[권장:](#)

[PCIe 오류](#)

[설명](#)

[권장:](#)

[Watchdog 시간 초과](#)

[설명](#)

[권장:](#)

[CLI 또는 업그레이드로 인해 수동으로 다시 로드](#)

[설명](#)

[권장:](#)

[Cisco 버그 ID](#)

소개

이 문서에서는 Nexus 9000 스위치에서 예기치 않은 재로드 또는 충돌 문제를 해결하는 방법

사전 요구 사항

이 문서에 대한 요구 사항이 없습니다.

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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Nexus 9000 스위치의 고장 방식

Cisco NX-OS는 네트워크, 시스템 및 프로세스 레벨에서 고가용성을 보장하도록 특별히 설계된 탄력적인 운영 체제입니다.

Nexus 9000에서 예기치 않은 다시 로드가 발생할 수 있는 3가지 이유는 다음과 같습니다.

- 사용자 공간의 프로세스에서 충돌이 발생할 수 있습니다.
- 프로세스 또는 하드웨어에서 watchdog 시간 초과 또는 하트비트 오류가 발생할 수 있습니다.
- 커널 자체가 복구할 수 없는 조건을 발견하여 충돌합니다.

다시 로드 및 충돌 문제를 해결하기 위한 중요 데이터

- 다시 로드의 정확한 날짜 및 시간입니다.
- 다시 로드하기 전에 무슨 일이 있었습니까? 구성이 변경되었습니까? 확장 변경 사항이 있습니까? 디바이스에 로그가 있습니까? 환경 변화라도 있나요? CPU/메모리 사용량이 증가했습니까?
- 스위치가 부팅되고 안정되면 출력을 수집하고 확인합니다.
- 스위치가 작동하지 않을 경우 콘솔을 통해 액세스한 다음 출력이 있는지 확인합니다. 스위치 LED도 확인합니다. LED 세부 정보는 하드웨어 설치 가이드에서 확인할 수 있습니다.

시스템 재설정 이유

```
<#root>
```

```
N9K#show system reset-reason module 1
```

```
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---  
1) At 21301 usecs after Tue Jan 17 20:29:20 2023  
Reason: Reset Requested due to Fatal Module Error  
Service: ipfib hap reset  
Version: 9.3(8)
```

코어 파일

<#root>

N9K#show cores

```
VDC Module Instance Process-name PID Date(Year-Month-Day Time)
-----
A B C D E 2024-01-04 19:17:25
copy core://<module-number>/<process-id>[/instance-num]
copy core://B/E/C ftp://<address>/<directory>
```

온보드 로그

<#root>

show logging onboard

show logging onboard kernel-trace

show logging onboard stack-trace

```
*****
STACK TRACE GENERATED AT Sun Sep 10 19:06:39 2023 CCT
*****
```

```
<snip> >>>dumps kernel messages
<0>[10925084.972289] [1694343998] sysServices Unexpected call in interrupt context, serviceId=824
<0>[10925084.980666] [1694343998] cctrl_set_card_offline - EOBC switch reset failed
<0>[10925084.987824] [1694343998] sysServices Unexpected call in interrupt context, serviceId=824
<0>[10925084.996200] [1694343998] cctrl_set_card_offline - EPC switch reset failed
<snip>
<4>[10925085.040600] [1694343998] Dumping interrupt statistics >>>dump interrupt statict
<4>[10925085.045928] [1694343998] CPU0 CPU1
<4>[10925085.051732] [1694343998] 3: 0 0 axp_irq Armada Error Handler
<4>[10925085.059909] [1694343998] 4: 0 0 axp_irq Armada MBUS unit Error Handle
<4>[10925085.068957] [1694343998] 5: 1012335907 809985523 axp_irq axp_local_clockevent
<4>[10925085.077136] [1694343998] 8: 1260801154 0 axp_irq mv_eth
<4>[10925085.084108] [1694343998] 31: 11230 0 axp_irq mv64xxx_i2c
<4>[10925085.091508] [1694343998] 41: 7111 1 axp_irq serial
<4>[10925085.098471] [1694343998] 51: 2 0 axp_irq mv_xor.0
<4>[10925085.105602] [1694343998] 52: 2 0 axp_irq mv_xor.1
<4>[10925085.112760] [1694343998] 94: 1 0 axp_irq mv_xor.2
<4>[10925085.119890] [1694343998] 95: 1 0 axp_irq mv_xor.3
<4>[10925085.127029] [1694343998] 107: 0 0 axp_irq axp-temp
<4>[10925085.134200] [1694343998] 168: 0 0 axp_irq cctrl_mrv_nmi_irq
<4>[10925085.142134] [1694343998] 195: 29 0 axp_msi_irq cctrl_sc_msi_irq
<4>[10925085.150225] [1694343998] 196: 0 2399172865 axp_msi_irq linux-kernel-bde
<4>[10925085.158325] [1694343998] IPIO : 0 0 Timer broadcast interrupts
```

```
<4>[10925085.166130] [1694343998] IPI1 : 1711470501 3532640372 Rescheduling interrupts
<4>[10925085.173672] [1694343998] IPI2 : 0 0 Function call interrupts
<4>[10925085.181302] [1694343998] IPI3 : 44582 118572 Single function call interrupts
<4>[10925085.189541] [1694343998] IPI4 : 0 0 CPU stop interrupts
<4>[10925085.196734] [1694343998] PMU: : 0 0
<4>[10925085.202186] [1694343998] Err : 0
```

```
show logging onboard exception-log
```

```
>>>Check if any exception is raised before reload
```

프로세스 로그

```
<#root>
```

```
N9K# show processes log details
```

```
>>>detail process memory usage prior to crash
```

```
Service: ethpm
```

```
Description: Test Ethernet Port Manager
```

```
Executable: /isan/bin/ethpm
```

```
Started at Wed Jun 5 18:20:46 2023 (251615 us)
```

```
Stopped at Sat Jun 8 00:08:53 2023 (661042 us)
```

```
Uptime: 2 days 5 hours 48 minutes 7 seconds
```

```
Start type: SRV_OPTION_RESTART_STATELESS (23)
```

```
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
```

```
Last heartbeat 48.10 secs ago
```

```
System image name:
```

```
System image version: 7.0(3)I7(6)
```

```
PID: 28914
```

```
Exit code: signal 5 (core dumped)
```

```
CWD: /var/sysmgr/work
```

```
RLIMIT_AS: 1019819820
```

```
>>>limit memory usage
```

```
Virtual Memory:
```

```
CODE 1007E000 - 1068DBD4
```

```
DATA 1068E000 - 106DC3E8
```

```
BRK 1194F000 - 11CF9000
```

```
STACK FFA28650
```

```
TOTAL 576004 KB
```

```
>>>memory usage before crash
```

Logflash의 로그 파일

Nexus 9000에는 내장형 logflash가 있으므로 로그 파일은 다시 로드한 후에도 유지됩니다.

<#root>

```
N9K#dir logflash:log | grep messages
```

```
3714961 Jan 13 18:05:31 2024 messages
4194331 Jan 13 17:30:14 2021 messages.1
5497842 May 11 15:59:00 2021 messages.2
4194341 Jul 30 07:25:36 2022 messages.3
4194510 Feb 09 14:50:50 2023 messages.4
4194426 Jun 04 05:00:40 2023 messages.5
```

```
N9K#show file logflash:log/messages
N9K#show file logflash:log/messages.1
N9K#show file logflash:log/messages.2
N9K#show file logflash:log/messages.3
N9K#show file logflash:log/messages.4
N9K#show file logflash:log/messages.5
```

일반적인 재설정 이유

전원 관련 다시 로드

<#root>

```
N9K#show system reset-reason
```

```
----- reset reason for module 1 (from Supervisor in slot 1) ---
1) At 280125 usecs after Fri Aug 4 02:01:14 2023
```

```
Reason: Module PowerCycled
```

```
Service: HW check by card-client
Version:
```

설명

Nexus 9000 스위치는 N+1 전원 이중화를 지원합니다. 대부분의 전원 또는 모든 전원에서 정전이 발생하면 다시 로드가 발생합니다.

권장:

1. 전원 공급 장치의 전원 코드를 확인합니다.
2. 동일한 입력 회로를 공유하는 다른 장치에도 장애가 발생했는지 확인합니다.
3. Nexus 9000 또는 PDU에 전원 관련 알람이 있는지 확인합니다.

프로세스 충돌

<#root>

N9K#show system reset-reason module 1

----- reset reason for Supervisor-module 1 (from Supervisor in slot 1)
1) At 21301 usecs after Tue Jan 17 20:29:20 2023
Reason: Reset Requested due to Fatal Module Error

Service: ipfib hap reset

>>>ipfib process reset

Version: 9.3(8)

설명

각 서비스에는 하트비트 타이머, 재시작 방법 및 상태 저장 재시작 최대 재시도를 비롯한 자체 HA(고가용성) 정책이 있습니다. Cisco NX-OS Software는 대부분의 프로세스 및 서비스의 상태 저장 재시작을 허용합니다. 다시 로드하는 프로세스 ha 정책이 재설정된 경우(프로세스 재시작 중에 NX-OS가 작동하지 않음) 또는 프로세스 재시작 시간이 최대 재시도에 도달하는 경우 발생합니다.

권장

<#root>

`show cores`

VDC	Module	Instance	Process-name	PID	Date(Year-Month-Day Time)
1	1	1	ipfib	27446	2023-01-17 20:30:30

copy core://1/27446/1 ftp://<address>/<directory>

대부분의 프로세스 충돌이 소프트웨어 결함이며 코어 파일이 저장됩니다. 서비스 요청 사례를 열어 확인하십시오.

- 코어 파일은 TAC 엔지니어가 디코딩할 수 있습니다.
- 서비스 요청을 열려면 Product(제품) > Unexpected Reboot(예기치 않은 재부팅) > Software Failure(소프트웨어 실패)를 선택하여 적절한 팀과 함께 케이스를 여십시오.

EOBC 실패

2018 Jan 21 01:56:42.789 N9K#%KERN-0-SYSTEM_MSG: [4590707.849157] [1516460202] EMON: module 2 is not re
2018 Jan 21 01:56:43.071 N9K#%MODULE-2-MOD_DIAG_FAIL: Module 2 (Serial number: xxxxxxxxxx) reported fai

설명

EOBC는 Ethernet Out of Band Channel의 약어입니다. 일반 keepalive가 수퍼바이저와 라인 카드 사이를 오가고 있습니다. 수신한 오류 메시지는 SUP와 라인 카드 사이에 하트비트가 누락되었음을 나타냅니다. 단일 하트비트가 누락되면 자동으로 무시될 수 있습니다. 그러나 여러 하트비트가 동시에 손실되면 라인 카드가 재설정됩니다.

EOBC 실패에는 일반적으로 3가지 이유가 있습니다.

1. EOBC 혼잡 EOBC가 1개 이상 손실된 라인 카드 경험을 볼 수 있습니다.
2. 특정 모듈의 CPU 과다 사용 라인 카드/수퍼바이저 CPU가 사용 중이어서 EOBC 메시지를 처리할 수 없습니다. Nexus 9000부터 7.0(3)I7(3)까지 소프트웨어 개선 사항이 있습니다.
3. 하드웨어 장애

권장

1. 다시 로드 시 영향을 받는 라인 카드의 CPUhog이 있는지 확인합니다.
2. 다른 라인 카드가 EOBC 손실을 다시 로드하는지 확인합니다.
3. 배포된 BFD 또는 Netflow CPU가 최근에 서비스를 사용하고 있는지 확인합니다.
4. 정보 없이 여러 번 발생하는 경우 하드웨어를 교체합니다.

패리티 오류

<#root>

N9K#show logging onboard stack-trace

```
*****
      STACK TRACE GENERATED AT Tue Sep 21 02:27:58 2021 UTC
*****
<0>[88302546.800770] [1632158876] ERROR: MACHINE: Uncorrectable
<0>[88302546.809202] [1632158876] L2CACHE ERROR: Cause 0x88
<0>[88302546.814368] [1632158876] TAG Parity Error
                >>>>Parity error
<0>[88302546.818750] [1632158876] Kernel panic - not syncing: L2CACHE ERROR
<4>[88302546.825212] [1632158876] Cpu: 0 Pid: 0, comm: swapper/0
```

설명

패리티 에러는 정보의 비트가 1에서 0으로 또는 0에서 1로 플립될 때 발생한다.

패리티 에러들의 대부분은 정전기 또는 자기 관련 환경 조건들에 의해 야기된다. 이러한 이벤트는 무작위로 발생하며 방지할 수 없습니다.

시스템은 이 오류가 발생했음을 감지하고 잘못된 데이터가 처리되지 않도록 시스템을 강제로 충돌시킵니다. 발생 한 번은 하드웨어 또는 소프트웨어 문제를 나타내는 것이 아닙니다.

권장

패리티 오류는 일시적인 SEU(Single-Event Upset)이거나 하드웨어 결함으로 인해 발생할 수 있습니다. 이를 확인하려면 48시간 동안 디바이스를 모니터링하여 재발이 있는지 확인해야 합니다.

48시간 내에 두 번째 문제가 발생하지 않으면 일시적인 문제로 간주되므로 별도의 조치가 필요하지 않습니다.

빈번하거나 반복 가능한(하드) 패리티 오류는 메모리 또는 읽기 및 쓰기에 사용되는 회로의 물리적 오작동으로 인해 발생합니다. 이 경우 하드웨어를 교체합니다.

PCIE 오류

<#root>

```
N9K#show logging onboard stack-trace
```

```
<6>[ 105.196227]      CTRL PANIC DUMP
<6>[ 105.196229] =====
<6>[ 105.196231] WDT last punched at 105192052644
<6>[ 105.196234] REG(0x60) = 3c
<6>[ 105.196238] REG(0x64) = 0
<6>[ 105.196241] REG(0x300) = baadbeef
<6>[ 105.196245] REG(0x304) = baadbeef
<6>[ 105.196246] =====
<0>[ 105.197303] nxos_panic: Kernel panic - not syncing: PCIE Uncorrectable error
    >>>>>PCIE Uncorrectable error
```

설명

PCIE 오류는 수정 가능한 오류와 수정 불가능한 오류의 두 가지 유형으로 분류됩니다. 이러한 분류는 이러한 오류의 영향을 기반으로 하며, 이로 인해 성능 저하 또는 기능 장애가 발생합니다.

수정 가능한 오류는 인터페이스의 기능에 영향을 주지 않습니다. PCIE 프로토콜은 소프트웨어 개입 또는 데이터 손실 없이 복구할 수 있습니다. 이러한 오류는 하드웨어에 의해 탐지되고 수정됩니다.

수정 불가능한 오류는 인터페이스의 기능에 영향을 미칩니다. 수정 불가능한 오류는 특정 트랜잭션 또는 특정 PCIE 링크를 신뢰할 수 없게 만들 수 있습니다. 이러한 오류 조건에 따라 수정 불가능한 오류는 치명적이지 않은 오류와 치명적 오류로 더 분류됩니다. 치명적이지 않은 오류는 특정 거래를 신뢰할 수 없게 만들지만 PCIE 링크 자체는 완전히 작동합니다. 반면 치명적인 오류는 링크를 신뢰할 수 없게 만듭니다.

Nexus 9000은 치명적인 PCIE 오류를 감지하고 잘못된 데이터가 처리되지 않도록 시스템을 강제로 다시 로드합니다.

권장

패리티 오류와 동일합니다.

48시간 내에 두 번째 문제가 발생하지 않으면 일시적인 문제로 간주되므로 별도의 조치가 필요하지 않습니다.

자주 또는 반복 가능한 오류는 물리적 오작동으로 인해 발생합니다. 이 경우 하드웨어를 교체합니다.

Watchdog 시간 초과

<#root>

```
N9K#show system reset-reason
```

```
----- reset reason for module 1 (from Supervisor in slot 1) ---
```

```
1) At 88659 usecs after Mon Sep 24 18:33:04 2023
```

```
Reason: Watchdog Timeout
```

```
Service:
```

```
Version: 7.0(3)I7(9)
```

설명

Watchdog 타이머는 내장형 시스템 및 기타 컴퓨터 제어 장비에서 일반적으로 발견되며, 이 경우 사람이 장비에 쉽게 액세스할 수 없거나 장애에 적시에 대처할 수 없습니다.

Nexus 9000은 FPGA를 통해 워치독 타이머 기능을 구축합니다. 이렇게 하면 Nexus 9000에서 소프트웨어 중단을 감지하고 스위치를 신속하게 재부팅할 수 있습니다.

권장

1. 알려진 소프트웨어 버그가 현재 버전에 영향을 미치는지 확인합니다.
2. 문제가 다시 발생하면 커널 추적 및 추가 로깅 데이터를 수집합니다.
3. 서비스 요청 케이스를 엽니다.

CLI 또는 업그레이드로 인해 수동으로 다시 로드

<#root>

```
N9K# show system reset-reason
```

```
----- reset reason for module 1 (from Supervisor in slot 1) ---
```

```
1) At 343832 usecs after Sat
```

```
Jan 13 17:58:53 2024
```

Reason: Reset Requested by CLI command reload

Service:

Version: 10.2(5)

>

4) At 282886 usecs after Fri

Jan 12 07:42:33 2024

Reason: Reset due to upgrade

Service:

Version: 10.3(4a)

>>>>version prior to upgrading

설명

Nexus 9000 Series 스위치는 기본적으로 소프트웨어 업그레이드 중단을 지원하고 다운그레이드를 지원합니다. 업그레이드 과정에서 Nexus 9000이 다시 로드됩니다.

권장

필요한 동작입니다. 자세한 CLI 세션 세부 정보는 어카운팅 로그를 확인하십시오.

CLI 다시 로드 예:

```
Sat Jan 13 17:58:40 2024:type=update:id=console0:user=admin:cmd=reload (REDIRECT)
```

```
Sat Jan 13 17:58:47 2024:type=update:id=console0:user=admin:cmd=Rebooting the switch
```

업그레이드 다시 로드 예:

```
Fri Jan 12 07:35:52 2024:type=update:id=console0:user=admin:cmd=install all nxos bootflash:/nxos64-cs.1
```

Cisco 버그 ID

일부 결함으로 인해 Nexus 9000 스위치가 예기치 않게 다시 로드될 수 있습니다. 알려진 소프트웨어 버그가 발생했는지 확인하려면 TAC 케이스를 여십시오.

Cisco 버그 ID	버그 제목	버전 수정
-------------	-------	-------

Cisco 버그 ID CSCwd53591	코어/추적 없이 watchdog 시간 초과로 인한 다시 로드	9.3(13)
Cisco 버그 ID CSCvz65993	tahoe0이 다운되어 대역 내 연결 장애가 발생했습니다.	9.3(9)
Cisco 버그 ID CSCvs00400	링크 플랩 후 Watchdog 시간 초과로 인해 커널 패닉 및 다시 로드	9.3(3) 및 7.0(3)I7(8)
Cisco 버그 ID CSCvr57551	커널 패닉 상태에서 Cisco Nexus 9000이 다시 로드됨 - 커널 페이징 요청을 처리할 수 없음	7.0(3)I7(8) 및 9.3(4)
Cisco 버그 ID CSCvo86286	Nexus 9500 1세대 라인 카드가 장착된 7.0(3)I7(x)에서 커널 패닉 발생	7.0(3)I7(7)
Cisco 버그 ID CSCvx38752	메모리 누수로 인해 Nexus 9k에서 "ipfib"를 다시 로드합니다.	7.0(3)I7(9) 및 9.3(2)
Cisco 버그 ID CSCvh13039	CPU가 시간 타이머를 서비스하고 있을 때 EOBC 하트비트로 인해 LC/FM이 다시 로드됩니다.	7.0(3)I4(8) 및 7.0(3)I7(3)

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.