Troubleshoot Unexpected Reloads on Catalyst 9000 Switches

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Common Reload Reasons

Collect Relevant Data

- Last Reload Reason
- Tech-Support Command

Commands to Collect for TAC

- Tracelogs
- System Reports

Troubleshoot

- PowerOn
  - Explanation
  - Remediation
- Stack Merge due to Incompatibility
  - Explanation
  - Remediation
- Reload Command
  - Explanation
  - Remediation
- LocalSoft or CPU Catastrophic Err
  - Explanation
  - Remediation
- Power failure or Unknown
  - Explanation
  - Remediation
- Redundancy Force-Switchover
  - Explanation
  - Remediation
- Image Install
  - Explanation
  - Remediation
- Core File Present or Crash
  - Explanation
  - Remediation

Cisco Bug IDs

Related Information

Introduction

This document describes how to troubleshoot unexpected reloads and what specific information to collect post-event on the Catalyst 9000 switches.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

There can be a variety of reasons an unexpected reload or silent reload event can occur. To troubleshoot and find the root cause, it is imperative to know the date/time of the event and collect all the information possible from the device right away. This guarantees that all the log collection is accurate and complete (not overwritten by the device as time goes on).

Common Reload Reasons

ReloadReason	**Explanation**	**Recommendation**
PowerOn	The power supply or the inlet circuit was manually shut off and on.	If power event was unexpected, confirm health of physical power, battery backups, UPS, and so on.
Stack Merge due to Incompatibility	The Standby switch of the stack lost communication with the Active and triggered a merge to re-elect a new Active switch.	Check the stacking data cables, make sure they are properly seated. Replace the stacking cables.
Reload Command	The command reload was executed on the CLI of the switch to instruct a manual software reload.	The reload command was issued (If this was not expected you can confirm when this action was performed via iosrp parser traces)
LocalSoft or CPU Catastrophic Err	An error condition encountered in the software or CPU and the device was	Collect data and open a TAC case.

	forced to be reset.	
Power failure or Unknown	The power supply of the device or inlet circuit must have suddenly failed, momentarily stopping the supply of power to the switch.	Check if the power supplies are healthy, color of the LEDs and verify the inlet input circuit.
Redundancy force-switchover	The command redundancy force-switchover was executed, causing the Standby to take the Active role and previous Active to go for a software reset.	None.
Image Install	The device was reloaded as a result of a new Cisco IOS® XE image installation.	None.

Collect Relevant Data

- Exact date/time of the occurrence.
- What was happening prior to the unexpected reload event? Perhaps a configuration change, log in to the device, or the device was untouched.
- Are there any Syslog messages of errors reported prior to the event? If there are any external Syslog servers, check if there are error logs related.
- Collect the show tech-support command from the device.
- Any other insight or observations that can help understand what preceded the event (power failures, and so on)

⚠ **Caution**: It is really important to collect the information right after the event occurred. There are no guarantees of providing a proper root cause if log collection happens days or weeks after the reload event took place.

Once the device is up and stable, collect this additional information to help determine the cause of the reload event.

Last Reload Reason

Check what was the last Reload Reason recorded by the system.

<#root>

Switch#

show version | include uptime|returned|reload|Version

```
Cisco IOS XE Software, Version 16.12.08
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.12.8, RELEASE SOF
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
GPL code under the terms of GPL Version 2.0. For more details, see the
BOOTLDR: System Bootstrap, Version 17.10.1r, RELEASE SOFTWARE (P)
Switch uptime is 3 hours, 14 minutes
```

```
System returned to ROM by Reload Command

Last reload reason: Reload Command

Next reload AIR license Level: AIR DNA Advantage
Switch Ports Model SW Version SW Image Mode
Configuration register is 0x102 (will be 0x2102 at next reload)
```

The device stores historical data on the latest reload events experienced. This information is important to check if the reloads have been recurrent and what was the reason recorded by the switch. The command used to see this data is show logging onboard switch <id> uptime detail.

<#root>

Switch#

show logging onboard switch active uptime detail

```
--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 04/28/2022 01:24:40
Total uptime : 0 years 41 weeks 2 days 9 hours 55 minutes
Total downtime : 0 years 22 weeks 4 days 7 hours 3 minutes
Number of resets : 326
Number of slot changes : 2
Current reset reason : Reload Command
Current reset timestamp : 07/19/2023 15:23:33
Current slot : 1
Chassis type : 215
Current uptime : 0 years 0 weeks 0 days 3 hours 0 minutes
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp | Reset | Uptime
MM/DD/YYYY HH:MM:SS | Reason | years weeks days hours minutes
--------------------------------------------------------------------------------
07/13/2023 17:57:49 Image Install 0 0 0 0 0
07/13/2023 18:48:58 Reload Command 0 0 0 0 40
07/14/2023 00:55:30 Reload Command 0 0 0 6 0
07/14/2023 11:15:44 Reload Command 0 0 0 10 0
07/14/2023 20:02:26 Reload Command 0 0 0 8 0
07/17/2023 11:32:29 Reload Command 0 0 2 15 0
07/17/2023 21:00:59 Reload Command 0 0 0 9 0
07/18/2023 08:36:20 Reload Command 0 0 0 11 0
07/18/2023 11:00:28 Reload Command 0 0 0 2 0
07/19/2023 07:02:14 Reload Command 0 0 0 19 0

07/19/2023 15:23:33 Reload Command 0 0 0 8 0

--------------------------------------------------------------------------------
```

Tech-Support Command

This command gathers general information of the system and its current status. The commands described

previously are included in this support package. This output file is requested by TAC when opening a case.

There are different ways to collect it:

- **Logged Terminal Session:** Use a terminal program and record the session to a text file. Then, from CLI, run the command **show tech-support** and wait for the collection to finish. Provide the text file to the TAC case.
- **Redirected to a File:** From the CLI, run the command **show tech-support | redirect flash:** *ShowTech.txt*. This creates a text file on the flash of the device with the results of the tech-support command. Afterwards, need to extract the file from the device using any transfer protocol available in your network. (TFTP, FTP, SCP, and so on).

```
<#root>

Switch#

show tech-support | redirect flash:ShowTech.txt


Switch#

dir flash: | include .txt

499721 -rw- 16090 Jul 19 2023 15:24:02 +00:00 rdope_out.txt
499728 -rw- 1328023 Jul 19 2023 19:12:57 +00:00 ShowTech.txt

Switch#

copy flash:ShowTech.txt tftp:

Address or name of remote host []? 192.168.1.1
Destination filename [ShowTech.txt]?
!!!
```

Commands to Collect for TAC

The switch stores system logging information that can be used to analyze in depth what was happening prior and after the unexpected reload event occurred. If there was a crash, the switch also stores the crash data into a encrypted file that can be analyzed by TAC experts.

Tracelogs

The tracelogs are internal logs of each process within Cisco IOS® XE. The tracelogs directory is created by default and its content is overwritten periodically. This folder can be found in the bootflash or flash of the Catalyst device.

Generate the Tracelogs

```
<#root>

Switch#

request platform software trace archive

Creating archive file [flash:Switch_1_RP_0_trace_archive-20230719-192115.tar.gz]
Done with creation of the archive file: [flash:Switch_1_RP_0_trace_archive-20230719-192115.tar.gz]
```

```
Switch#
dir flash: | include .gz
499729 -rw- 29573907 Jul 19 2023 19:21:22 +00:00
Switch_1_RP_0_trace_archive-20230719-192115.tar.gz
```

System Reports

A system report is a compressed file that collects most of the information available in the software execution when an unexpected reload occurs. The system report contains tracelogs, crashinfo, and core files. This file is automatically created in the case of an unexpected reload on Cisco IOS® XE switches that was caused by a crash or software error. The file can be found in the crashinfo directory. This file is encrypted and requires TAC support for decoding and analysis.

```
<#root>
Switch#
dir crashinfo: | include .gz

Directory of crashinfo:/
19 -rwx 655080 Aug 7 2013 16:31:31 +00:00
system-report_1_20130807-163050-UTC.gz
```

Note: These files ending in .gz extension need to be extracted out of the device using any transfer protocol available in your network. (TFTP, FTP, SCP, and so on).

Troubleshoot

PowerOn

Explanation

The power supply was manually shut off and on. This can also be related to a long interruption of power. In this scenario, no crash or core files are generated.

Remediation

1. Check if the power supplies were manually switched off. If they were not, continue with the verifications.

2. Verify power cords of the power supplies, they must not be loose or easily disconnected.

3. Check if other devices sharing the same inlet circuit also had an outage or not. If only the switch had the outage, continue with the verifications.

4. Check if the inlet circuit from which the switch is drawing power had any long outage which severed the

power from the switch.

5. If all of the previous conditions have been verified and no issues found with power on site, open a TAC case.

Stack Merge due to Incompatibility

Explanation

The Standby switch of the stack lost communication with the Active switch and triggered a merge between all the switches in the stack to re-elect a new Active switch. Keepalive messages are continuously been sent and received over the stack data cables, when these messages are not sent/received on time, the switches declare the loss of communication and a stack merge occurs.

Remediation

1. Check that the stacking data cables are healthy and not loosely inserted in the stack data slots.

2. Verify stack data cables are properly seated and that the screws are not too tight.

3. If the switch has stacking modules, check that the screws are not too tight and that they are not loosely inserted in the stack bays.

4. If reloads due to stack merge continues, proceed to replace the stacking data cables and stacking data modules (if the switch has stacking modules).

5. If after replacement of the data cables, the stack merge continues, open a TAC case.

Reload Command

Explanation

The command reload was executed on the CLI of the switch to instruct a manual software reload.

Remediation

No remediation actions available as the reload is expected due to the use of the specified command.

LocalSoft or CPU Catastrophic Err

Explanation

An error condition encountered in the software or CPU and the device was forced to be reset. This is a software generated reload and can be related to Cisco bug ID CSCvr77861. No core files or crash generated due to this error condition.

Remediation

1. Verify bug details and upgrade the switch to latest fixed version.

2. If issue re-occurs, collect tracelogs and any additional logging data prior and after the issue.

3. Open a TAC case.

Power failure or Unknown

Explanation

The power supply of the device or inlet circuit must have suddenly failed, momentarily stopping the supply of power to the switch. This can also be related to a very short interruption of power of the UPS (if any) connected to the switch. In this scenario, no crash or core files are generated.

Remediation

1. Verify the power supplies LEDs, they must be green. If no LEDs are on or they are displaying a red color, replace the power supply with a good working one.

2. Verify power cords of the power supplies, they must not be loose or easily disconnected.

3. If switch is connected to an UPS, verify that there was no outage with it which could have severed the power to the switch.

4. Check if other devices sharing the same inlet circuit also had an outage or not. If only the switch had the outage, continue with the verifications.

5. Check if the inlet circuit from which the switch is drawing power had any small flap or variation in the voltage/current levels.

6. If all of the previous conditions have been verified and no issues found with variations of power on site, open a TAC case.

Redundancy Force-Switchover

Explanation

The command `redundancy force-switchover` was executed, causing the Standby to take the Active role and previous Active to go for a software reset.

Remediation

No remediation actions available as the reload of the Active switch due to the specified command is expected.

Image Install

Explanation

The device was reloaded as a result of a new Cisco IOS® XE image installation.

Remediation

No remediation actions available as the reload of the stack was due to installation process and it is expected.

Core File Present or Crash

Explanation

The switch has crashed and generated a crash or core file. Check for one of these files in flash: or crashinfo: directories

This command can be run on the switch to search all directories for core files, system reports, and low memory threshold files:

- If no files are seen in the outputs and only directories are seen, then no crash has occurred due to these reasons.
- If files are seen, but they do not match the **Date** and **Time** to the event in interest or concern

<#root>

cats-c9300#

dir /recur all-filesystems | inc Directory of|crashinfo_|core.gz|fullcore|system-report|kernel.rp|thresh

Directory of system:/*
Directory of system:/
Directory of system:/memory/
Directory of system:/
Directory of tmpsys:/*
Directory of crashinfo:/*
Directory of crashinfo:/tracelogs/
Directory of crashinfo:/
Directory of crashinfo:/license_evlog/

Directory of crashinfo:/

<-Inside crashinfo:/ directory

12 -rw- 483563 Jun 27 2023 17:15:52 +00:00 cats-c9300_crashinfo_1_RP_00_00_20230627-171547-U
13 -rw- 139205443

Jun 27 2023

17:16:49 +00:00

cats-c9300_1_RP_0-system-report_1_20230627-171626-UTC.tar.gz

<-System Report (May also contain a core.gz file)

16 -rw- 223501 Jul 30 2023 13:49:41 +00:00 cats-c9300_crashinfo_1_RP_00_00_20230730-134940-U
28 -rw- 420518 Aug 29 2023 15:56:18 +00:00 cats-c9300_crashinfo_1_RP_00_00_20230829-155613-U
21 -rw- 53900932

Aug 29 2023

15:56:53 +00:00

cats-c9300_1_RP_0-system-report_1_20230829-155647-UTC.tar.gz

<-System Report (May also contain a core.gz file

)
Directory of flash:/*
Directory of flash:/

Directory of flash:/pcap/
Directory of flash:/
Directory of flash:/.images/
Directory of flash:/.images/17.09.02.0.3040.1667428055/
Directory of flash:/
Directory of flash:/cflow/
Directory of flash:/cflow/ctc_pids/
Directory of flash:/.product_analytics/
Directory of flash:/.product_analytics/
Directory of flash:/.product_analytics/policies/
Directory of flash:/.product_analytics/
Directory of flash:/.product_analytics/databases/
Directory of flash:/
Directory of flash:/.installer/
Directory of flash:/.installer/issu_crash/
Directory of flash:/.installer/
Directory of flash:/
Directory of flash:/core/
Directory of flash:/core/modules/

Directory of flash:/core/

<-Inside flash:/core/

262146 -rw-   41575076

Jul 30 2023

 13:50:06 +00:00

cats-c9300_1_RP_0_x86_64_crb_linux_iosd_ngwc-universalk9-ms_27272_20230730-134942-UTC.core.gz

<-Core File

262147 -rw-   44973003

Aug 28 2023

 12:49:07 +00:00

cats-c9300_1_RP_0_x86_64_crb_linux_iosd_ngwc-universalk9-ms_18507_20230828-124841-UTC.core.gz

<-Core File

262148 -rw-   44997000

Aug 29 2023

 11:22:30 +00:00

cats-c9300_1_RP_0_x86_64_crb_linux_iosd_ngwc-universalk9-ms_1466_20230829-112204-UTC.core.g

z

 <-Core File

376833 -rw-   13189075

Sep 7 2023

 18:42:13 +00:00

cats-c9300_1_RP_0_fed_2564_20230907-184202-UTC.core.gz **<-Core**

```
Directory of flash:/.prst_sync/
Directory of flash:/.rollback_timer/
Directory of flash:/
Directory of flash:/dc_profile_dir/
Directory of flash:/
Directory of flash:/pnp-info/
Directory of flash:/
Directory of flash:/ss_disc/
Directory of flash:/tech_support/
Directory of flash:/sys_report/
Directory of flash:/
Directory of flash:/Tbot/
Directory of flash:/.dbpersist/
Directory of flash:/.dbpersist/history/
Directory of flash:/.dbpersist/
Directory of flash:/.dbpersist/DMI_STATE_DB/
Directory of flash:/.dbpersist/
Directory of flash:/onep/
Directory of flash:/onep/apps-cli/
Directory of flash:/
Directory of flash:/guest-share/
Directory of flash:/
Directory of flash:/fp_cc_crash/
Directory of flash:/.rommon_sync/
Directory of flash:/
Directory of flash:/EDScisco/
Directory of flash:/
Directory of flash:/SHARED-IOX/
Directory of flash:/
Directory of flash:/confd_debugged_dumps/
Directory of flash:/
Directory of flash:/.PATCH-backup/

Directory of flash:/

114756  -rw-      474448

Mar 30 2023

 19:50:53 +00:00

threshold_lowmem_info_20230330-195051-UTC



<-May indicate memory leak

Directory of webui:/*
Directory of webui:/
Directory of nvram:/*
Directory of nvram:/
```

Remediation

A TAC case is required to determine RCA:

- This file needs to be analyzed by the Architecture team.
- When openening the service request please choose Product > Unexpected Reboot > Software Failure in order to get the case opened with the right team

Cisco Bug IDs

There are some of the defects that can cause an unexpected reload on Catalyst 9000 Series switches.

Note: Only registered Cisco users can access internal bug information.

Cisco bug ID CSCvp56289	9300 switch silent reload with platinum power supply (PWR-C1-350WAC-P)
Cisco bug ID CSCvv27849	Cat 9K & 3K: Unexpected reload caused by the FED process.
Cisco bug ID CSCvr77861	Cat9300/C9500/C9500H switches may reload with last reload reason as LocalSoft or CpuCatastrophicErr
Cisco bug ID CSCvu97189	Show platform forward (SPF) causes device freeze or reload
Cisco bug ID CSCwe11818	C9300L stack merge happen after switchover

Related Information

- Cisco Technical Support & Downloads