

# Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Required Log files](#)

[Analyzing logs for initial clues](#)

[Gather information about UCS setup](#)

[Suggestion for proactively monitoring FI](#)

[Related Information](#)

## Introduction

The document provides steps to investigate Unified Computing System Fabric Interconnect ( FI ) crash or unexpected reboot failure.

**On a high-level, the following problems could result in reboot of FI**

- Kernel space process crashed ( aka Kernel panic )
- Kernel ran out of memory ( Out of Memory - OOM killing a user process to reclaim memory )
- User space process crashed ( ex. - netstack, fcoe\_mgr , callhome etc )
- FI firmware issue ( rare scenario , example - [CSCuq46105](#) ) or hardware component failure ( like SSD used for storage )

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

Cisco Unified Computing System (UCS) Manager

Cisco Unified Computing System (UCS) Manager Command Line Interface (CLI)

## Required Log files

When FI reboots unexpectedly, collect following logs and upload it to TAC Service Request.

- UCSM techsupport log bundle
- Check if core dump file is created around the time of reboot event.

You can check for cores dump files via CLI or GUI

UCS-FI /monitoring/sysdebug # show cores detail

- If the FI has been configured to export logs to syslog server, please gather log messages from syslog server for the device that provides 7 days of history prior to reboot timestamp.
- Kernel stack trace ( If reboot is due to kernel panic )

## Analyzing logs for initial clues

- 1) Check for reboot reason and time stamp from Nexus Operating System (NX-OS) " **show version** " command output
- 2) Check " **show logging nvram** " command output for log messages prior to reboot time stamp
- 3) Check log messages stored on syslog server for additional clues
- 4) If reboot was triggered by user space process crash, check core dump that matches process name and reboot time stamp.
- 6) If it is kernel panic, check for kernel stack trace output in file named " **sw\_kernel\_trace\_log** "

From UCSM 2.2.1b, this file is included UCSM show techsupport bundle.

For UCSM version earlier than 2.2.1b, please collect output of following commands

- 7) " **topout.log** " contains output of " top " command every two seconds. Before reboot, UCSM saves old set of logs as /opt/sam\_logs.tgz file It can provide information about memory, utilization or processes.
- 8) If you notice messages like Out of Memory ( OOM ) killed a process and the process crash could trigger reboot of FI and would be listed as reset reason. In such scenarios, it is most likely the process is victim of low memory condition and might not be the cause behind crash or memory leak.

## Gather information about UCS setup

Answering following questions helps to better understand the system setup and it's state prior to reboot.

- 1) Has this problem happened before ?

- 2) Was there any specific user activity around the time of reboot ?
- 3) Any recent software / hardware / configuration changes made to the FI ?
- 4) Is Fi being monitored by any external applications ( over S
- 5) If yes, how frequently the applications poll the FI for data ? What information is polled at regular intervals by these application ? ( ex SNMP queries )
- 6) Has there been any traffic storm towards FI management port ?
- 7) Is this scale setup ? ( Number of chassis, blades , virtual interfaces )

## **Suggestion for proactively monitoring FI**

- 1) Configure UCSM to export logs to syslog server
- 2) Collect output of " show processes " from local-mgmt at regular intervals to monitor the trend in CPU and memory

usage of processes. This tis not required if the FI is arleady being monitored by external application.

## **Related Information**

[Cisco UCS Manager Configuration Guide](#)