Fehlerbehebung: UCS Fabric Interconnect-Absturz oder unerwarteter Neustart

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Erforderliche Protokolldateien](#)
[Analysieren von Protokollen für erste Hinweise](#)
[Sammeln von Informationen zur UCS-Einrichtung](#)
[Vorschlag für eine proaktive Überwachung des FI](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden Schritte zur Untersuchung eines Absturzes des Unified Computing System Fabric Interconnect (FI) oder eines unerwarteten Neustart-Fehlers beschrieben.

Auf allgemeiner Ebene können die folgenden Probleme zu einem Neustart der FI führen

- Kernel Space-Prozess ist abgestürzt (auch Kernel Panic genannt)
- Dem Kernel ist der Arbeitsspeicher ausgegangen (Out of Memory - OOM zum Töten eines Benutzerprozesses, um Arbeitsspeicher zurückzugewinnen)
- Der Platz-Prozess ist abgestürzt (z. B. - netstack, fcoe_mgr, callhome usw.)
- FI-Firmware-Problem (seltenes Szenario , Beispiel - CSCuq46105) oder Hardware-Komponentenfehler (wie SSD zum Speichern verwendet)

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

Cisco Unified Computing System (UCS) Manager

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

Erforderliche Protokolldateien

Wenn FI unerwartet neu startet, sammeln Sie die folgenden Protokolle und laden Sie sie auf TAC

Service Request hoch.

- UCSM-Technologie-Support-Protokollpaket
- Überprüfen Sie, ob die Core-Dump-Datei zum Zeitpunkt des Neustarts erstellt wird. Sie können über CLI oder GUI nach Dump-Dateien für Kerne suchen.

    UCS-FI # Überwachung des Umfangs

    UCS-FI/Monitoring # Scope Sysdebug

    UCS-FI/monitoring/sysdebug # Angabe der Kerne

- Wenn die FI so konfiguriert wurde, dass Protokolle auf den Syslog-Server exportiert werden, sammeln Sie Protokollmeldungen vom Syslog-Server für das Gerät, das 7 Tage im Verlauf vor dem Neustart-Timestamp bereitstellt.
- Kernel-Stack-Trace (Wenn der Neustart auf die Kernel-Panik zurückzuführen ist)

Analysieren von Protokollen für erste Hinweise

1) Überprüfen Sie den Grund- und Zeitstempel des Neustarts vom Nexus-Betriebssystem (NX-OS) **Ausgabe** des Befehls **show version** ".

2) Aktivieren Sie die Befehlsausgabe **show logging nvram** für Protokollmeldungen vor dem Neustart des Zeitstempels.

3) Überprüfen Sie die Protokollmeldungen, die auf dem Syslog-Server gespeichert sind, um weitere Hinweise zu erhalten.

4) Wenn der Neustart durch einen Absturz des Benutzerplatzprozesses ausgelöst wurde, überprüfen Sie das Core Dump, das dem Prozessnamen und dem Neustart-Zeitstempel entspricht.

6) Wenn es sich um eine Kernel-Panic handelt, suchen Sie in der Datei " **sw_kernel_trace_log** " nach der Kernelstack-Ablaufverfolgungsausgabe.

Ab UCSM 2.2.1b ist diese Datei im UCSM-Supportpaket enthalten.

Für UCSM-Version vor 2.2.1b erfassen Sie die Ausgabe der folgenden Befehle.

```
connect nxos
show logging onboard  kernel-trace | no-more
show logging onboard  obfl-history | no-more
show logging onboard  stack-trace | no-more
show logging onboard internal kernel | no-more
```

```
show logging onboard internal kernel-big | no-more
show logging onboard internal platform | no-more
show logging onboard internal reset-reason | no-more
```

7) " **topout.log** " enthält alle zwei Sekunden die Ausgabe des Befehls " top ". Vor dem Neustart speichert UCSM alte Protokollsätze als /opt/sam_logs.tgz. Es kann Informationen über Arbeitsspeicher, Nutzung oder Prozesse bereitstellen.

8) Wenn Sie feststellen, dass Meldungen wie Out of Memory (OOM) einen Prozess beendet haben und der Prozess abstürzen könnte einen Neustart des FI auslösen und als Grund für das Zurücksetzen angegeben werden.In solchen Szenarien ist der Prozess höchstwahrscheinlich das Opfer eines niedrigen Speicherzustands und möglicherweise nicht die Ursache für einen Absturz oder Speicherlecks.

Sammeln von Informationen zur UCS-Einrichtung

Die Beantwortung der folgenden Fragen hilft, die Systemeinrichtung und ihren Zustand vor dem Neustart besser zu verstehen.

1) Ist dieses Problem schon einmal aufgetreten?

2) Gab es zum Zeitpunkt des Neustarts irgendwelche Benutzeraktivitäten?

3) Jegliche kürzlich vorgenommenen Software-/Hardware-/Konfigurationsänderungen am FI?

4) Wird Wi-Fi von externen Anwendungen überwacht (über SNMP , XML API)?

5) Falls ja, wie häufig fragen die Anwendungen das FI nach Daten ab? Welche Informationen werden von dieser Anwendung in regelmäßigen Abständen abgefragt? (ohne SNMP-Abfragen)

6) Wurde Datenverkehr zum FI-Management-Port gestürmt?

7) Ist diese Skalierung konfiguriert? (Anzahl Chassis, Blades, virtuelle Schnittstellen)

Vorschlag für eine proaktive Überwachung des FI

1) Konfigurieren Sie UCSM für den Export von Protokollen auf den Syslog-Server

2) Ermitteln Sie in regelmäßigen Abständen die Ausgabe von " show process " von local-mgmt, um den Trend in CPU und Arbeitsspeicher zu überwachen.

Nutzung von Prozessen. Dies ist nicht erforderlich, wenn die FI bereits von einer externen Anwendung überwacht wird.

Zugehörige Informationen

Konfigurationsleitfaden für Cisco UCS Manager