

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Fichiers journal requis](#)

[Analyse des logs pour des indices initiaux](#)

[Informations de rassemblement sur l'installation UCS](#)

[Suggestion pour surveiller proactivement le fi](#)

[Informations connexes](#)

Introduction

Le document fournit des étapes pour étudier le crash de Fabric Interconnect d'Unified Computing System (fi) ou la panne inattendue de réinitialisation.

Sur un de haut niveau, les problèmes suivants ont pu avoir comme conséquence la réinitialisation du fi

- Processus de l'espace de noyau tombé en panne (aka kernel panic)
- Le noyau a manqué de mémoire (hors de la mémoire - OOM détruisant un processus utilisateur pour reprendre la mémoire)
- Processus de l'espace d'utilisateur tombé en panne (ex. - netstack, fcoe_mgr, callhome etc.)
- Question de micrologiciel fi (scénario, exemple rares - [CSCuq46105](#)) ou panne de composant matériel (comme le disque transistorisé utilisé pour la mémoire)

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

Gestionnaire du Système d'informatique unifiée Cisco (UCS)

Interface de ligne de commande de gestionnaire du Système d'informatique unifiée Cisco (UCS) (CLI)

Fichiers journal requis

Quand le fi redémarre inopinément, collectez les logs suivants et téléchargez-les à la demande de service TAC.

- Paquet de log de techsupport UCSM
- Vérifiez si le fichier de vidage de mémoire est créé autour de la période de l'événement de réinitialisation.

Vous pouvez vérifier des fichiers de vidage de mémoires par l'intermédiaire du CLI ou du GUI

UCS-FI # surveillance de portée

UCS-FI /monitoring # sysdebug de portée

UCS-FI /monitoring/sysdebug # exposition creuse le détail

- Si le fi a été configuré pour exporter des logs au serveur de Syslog, recueillez s'il vous plaît les messages de log du serveur de Syslog pour le périphérique qui fournit 7 jours d'historique avant l'horodateur de réinitialisation.
- Suivi de pile de noyau (si la réinitialisation est due au kernel panic)

Analyse des logs pour des indices initiaux

1) Vérifiez la raison de réinitialisation et le groupe date/heure de la sortie de commande de « **show version** » du système d'exploitation de Nexus (NX-OS)

2) Vérifiez la sortie de commande de « **show logging nvram** » pour des messages de log avant le groupe date/heure de réinitialisation

3) Vérifiez les messages de log enregistrés sur le serveur de Syslog pour des indices supplémentaires

4) Si la réinitialisation était déclenchée par crash de processus de l'espace d'utilisateur, vérifiez le vidage de mémoire qui apparie le groupe date/heure de nom du processus et de réinitialisation.

6) Si c'est kernel panic, vérifiez les informations de suivi de pile de noyau dans nommé par fichier le « **sw_kernel_trace_log** »

D'UCSM 2.2.1b, ce fichier est paquet inclus de techsupport d'exposition UCSM.

Pour la version UCSM plus tôt que 2.2.1b, collectez s'il vous plaît la sortie des commandes suivantes

7) « **topout.log** » contient la sortie de la commande « supérieure » toutes les deux secondes. Avant réinitialisation, UCSM enregistre le vieil ensemble de logs pendant que le fichier de /opt/sam_logs.tgz il peut fournir des informations au sujet de mémoire, d'utilisation ou de processus.

8) Si vous notez les messages comme hors de la mémoire (OOM) ont détruit un processus et le crash de processus pourraient déclencher la réinitialisation du fi et isted comme raison de la réinitialisation. Dans de tels scénarios, il est le plus susceptible le processus est victime d'état de taille mémoire basse et ne pourrait pas être la cause derrière le crash ou la fuite de mémoire.

Informations de rassemblement sur l'installation UCS

Suivre de réponse remet en cause des aides pour comprendre mieux que l'installation et ce de système est état avant la réinitialisation.

- 1) Ce problème s'est-il produit avant ?
- 2) Y avait-il une activité spécifique d'utilisateur autour de la période de la réinitialisation ?
- 3) Des modifications récentes de logiciel/matériel/configuration apportées au fi ?
- 4) Le fi est-il surveillé par des applications externes (au-dessus de SNMP)
- 5) si oui, combien fréquemment les applications votent-elles le fi pour des données ? Quelles informations sont votées à intervalles réguliers par des ces application ? (requêtes ex SNMP)
- 6) Y a-t-il eu une tempête du trafic vers le port de gestion fi ?
- 7) Cette échelle est-elle installée ? (Nombre de châssis, de lames, d'interfaces virtuelles)

Suggestion pour surveiller proactivement le fi

- 1) Configurez UCSM pour exporter des logs au serveur de Syslog
- 2) Collectez la sortie du « show processes » des gens du pays-gestion à intervalles réguliers pour surveiller la tendance dans la CPU et mémoire

utilisation des processus. Ce tis non requis si le fi est arleady surveillé par application externe.

[Informations connexes](#)

[Guide de configuration de Cisco UCS Manager](#)