Dépannage d'un verrouillage CFS sur les commutateurs Nexus 5000

Contenu

Introduction

Ce document décrit comment dépanner un verrou Cisco Fabric Services (CFS) sur un commutateur de la gamme Nexus 5000.

Informations générales

CFS fournit une infrastructure commune pour la synchronisation automatique de configuration dans le fabric. Il fournit la fonction de transport ainsi qu'un ensemble riche de services communs aux applications. CFS peut détecter des commutateurs compatibles CFS dans le fabric ainsi que leurs capacités d'application. Certaines des applications pouvant être synchronisées à l'aide de CFS sur un commutateur Nexus 5000 incluent :

- arp
- rappel
- device-alias
- dhcp_snoop
- dpvm
- eth_port_sec
- fc-port-security
- fcdomain
- fctimer
- fscm
- fwm
- icmpv6
- igmp
- mcectest
- msp
- ntp
- rscn

- session-mgr
- stp
- syslogan
- taper
- vem_mgr
- vim
- vms
- vpc

Lorsque vous configurez une application qui utilise l'infrastructure CFS, cette fonctionnalité démarre une session CFS et verrouille le fabric. Lorsqu'un fabric est verrouillé, le logiciel Nexus n'autorise aucune modification de configuration à partir d'un commutateur, autre que le commutateur qui maintient le verrouillage. Le logiciel Nexus émet également un message d'erreur indiquant « Échec de l'opération. Le fabric est déjà verrouillé. »

Si vous démarrez une session CFS qui nécessite un verrouillage de fabric mais que vous oubliez de mettre fin à la session, un administrateur peut effacer la session. Si vous verrouillez un fabric à tout moment, votre nom d'utilisateur est mémorisé lors des redémarrages et des commutateurs. Si un autre utilisateur (sur la même machine) tente d'effectuer des tâches de configuration, les tentatives de cet utilisateur sont rejetées et un message d'erreur « session actuellement détenue par un autre utilisateur » s'affiche.

Problème

Un utilisateur ne peut pas effectuer de modification de configuration pour l'application correspondante, pour laquelle un verrou CFS est bloqué ou ne peut pas effectuer une mise à niveau logicielle en service (ISSU) si le CFS est verrouillé pour le gestionnaire de session.

Cette liste affiche quelques messages d'erreur courants causés par un verrou CFS :

- Échec de l'opération. Le fabric est déjà verrouillé
- Session actuellement détenue par un autre utilisateur
- Le service « cfs » a renvoyé une erreur : Échec de l'opération. Le fabric est déjà verrouillé (0x40B30029)

Solution

Vous pouvez utiliser deux méthodes pour effacer un verrou CFS :

- Entrez la commande **clear <application> session**.
- Identifiez l'ID SAP de l'application et déverrouillez le fabric de l'application à l'aide de la commande masquée **cfs internal unlock <sap-id>**. Sap-ID est l'ID numérique attribué de manière unique à chaque processus.

Cette procédure inclut les deux méthodes :

1. Valider si CFS est verrouillé et identifier l'application concernée.Cet exemple de sortie montre que CFS est actuellement verrouillé pour Virtual Port Channel (VPC) :
   ```
   cisco-N5k# show cfs lock
   ```

```
Application: vpc
Scope : Physical-eth
--------------------------------------------------------------
Switch WWN  IP Address  User Name  User Type
--------------------------------------------------------------
20:00:00:2a:6a:6d:03:c0 0.0.0.0  CLI/SNMP v3

Total number of entries = 1


Cisco-N5k# show cfs lock name vpc

Scope : Physical-eth
--------------------------------------------------------------
Switch WWN  IP Address  User Name  User Type
--------------------------------------------------------------
20:00:00:2a:6a:6d:03:c0 0.0.0.0  CLI/SNMP v3

Total number of entries = 1

cisco-N5k#

cisco-N5k# show system internal csm info trace
Thu Feb 19 13:20:40.856718 csm_get_locked_ssn_ctxt[515]: Lock not yet taken.
Thu Feb 19 11:21:11.106929 Unlocking DB, Lock Owner Details:Client:2 ID:-1
Thu Feb 19 11:21:11.104247 DB Lock Successful by Client:2 ID:-1
Mon Feb 16 20:45:16.320494 csm_get_locked_ssn_ctxt[515]: Lock not yet taken.
Mon Feb 16 20:45:14.223875 csm_get_locked_ssn_ctxt[515]: Lock not yet taken.
Mon Feb 16 20:44:59.40095 csm_get_locked_ssn_ctxt[515]: Lock not yet taken.
```

Vous pouvez également entrer la commande **show cfs application** afin de voir les applications qui utilisent actuellement CFS :

```
cisco-N5k# show cfs application

-----------------------------------------------
Application  Enabled  Scope
-----------------------------------------------
arp  Yes  Physical-eth
fwm  Yes  Physical-eth
ntp  No  Physical-fc-ip
stp  Yes  Physical-eth
vpc  Yes  Physical-eth
fscm  Yes  Physical-fc
igmp  Yes  Physical-eth
role  No  Physical-fc-ip
rscn  No  Logical
icmpv6  Yes  Physical-eth
radius  No  Physical-fc-ip
fctimer  No  Physical-fc
syslogd  No  Physical-fc-ip
fcdomain  No  Logical
session-mgr  Yes  Physical-ip
device-alias  Yes  Physical-fc

Total number of entries = 16
```

2. Effacez le verrou CFS. Choisissez l'une des deux méthodes fournies dans cette étape :**Méthode 1 :** Entrez la commande **clear <application> session** afin d'effacer le verrou.Un verrou CFS pour l'application NTP est effacé dans cet exemple :

```
cisco-N5k#clear ntp session
```

Note: Cette commande ne s'applique pas à toutes les applications. Par exemple, les

applications qui tombent sous le champ d'application « Physical-eth », telles que ARP (Address Resolution Protocol), FWM (Forwarding Manager), STP (Spanning Tree Protocol), VPC, IGMP (Internet Group Management Protocol) et ICMP6 (Internet Control Message Protocol). Vous devez utiliser la commande masquée dans la méthode 2 afin de déverrouiller la session.**Méthode 2 :** Identifiez l'application sap-id et déverrouillez le fabric à l'aide de la commande masquée **cfs internal unlock <sap-id>**.

```
cisco-N5k# show system internal sysmgr service all

Name  UUID  PID  SAP  state  Start count  Tag  Plugin ID
--------------- ------- ---- ----- -----  ----------  ----- ---------
aaa  0x000000B5 3221 111  s0009  1  N/A  0
cert_enroll  0x0000012B 3220 169  s0009  1  N/A  0
Flexlink  0x00000434 [NA] [NA] s0075  None  N/A  0
psshelper_gsvc 0x0000021A 3159 398  s0009  1  N/A  0
radius  0x000000B7 3380 113  s0009  1  N/A  0
securityd  0x0000002A 3219 55  s0009  1  N/A  0
tacacs  0x000000B6 [NA] [NA] s0075  None  N/A  0
eigrp  0x41000130 [NA] [NA] s0075  None  N/A  0
isis_fabricpath0x41000243 3876 436  s0009  1  N/A  0
vpc  0x00000251 3900 450  s0009  1  N/A  0 < <
vsan  0x00000029 3817 15  s0009  1  N/A  2
vshd  0x00000028 3149 37  s0009  1  N/A  0
vtp  0x00000281 3902 478  s0009  1  N/A  0
```

Identifiez l'ID sap à partir du résultat et déverrouillez le fabric comme le montre cet exemple :

```
cisco-N5k# cfs internal unlock 450
Application Unlocked
cisco-N5k#
```

Note: La commande **cfs internal unlock** est une commande cachée Nexus OS utilisée pour déverrouiller le CFS et peut être exécutée en production en toute sécurité.

3. Émettez ces commandes **show** afin de valider la solution :

```
cisco-N5k# show cfs lock name vpc
cisco-N5k#

cisco-N5k# show cfs internal session-history name vpc
------------------------------------------------------------
Time Stamp  Source WWN  Event
User Name  Session ID
------------------------------------------------------------
 Tue May 26 23:35:51 2015 20:00:00:05:73:d0:c0:00 LOCK_OBTAINED
admin 147513262
Tue May 26 23:53:52 2015 20:00:00:05:73:d0:c0:00 LOCK_CLEAR
admin 147513262
------------------------------------------------------------
```

Problèmes identifiés

Voici quelques-uns des défauts logiciels connus liés au CFS :

- ID de bogue Cisco CSCtj40756 - Échec ISSU -« cfs » a renvoyé l'erreur :Le fabric est déjà verrouillé (0x40B30029)
- ID de bogue Cisco CSCue03528 - Base de données de session / Synchronisation de configuration / CFS verrouillée d'un côté sans validation