

Reprise de panne de superviseur d'épine du Nexus 9500

Contenu

[Introduction](#)

[Problème](#)

[Solution](#)

[Préparez pour convertir le superviseur de rechange en mode interception commandée en vol](#)

[Procédure 1 - Conversion de NX-OS à l'interception commandée en vol](#)

[Procédure 2 - Conversion de chargeur à l'interception commandée en vol](#)

Introduction

Ce document décrit le processus pour remplacer le superviseur d'une épine, qui a en raison d'un défaut d'une erreur matérielle, en mode central de l'infrastructure d'application (interception commandée en vol).

Problème

Le superviseur actif a en raison d'un défaut d'une défaillance matérielle. Le superviseur de réserve a succédé comme active, rechargé dans un état de détection de matrice, et automatiquement joint la matrice. Un superviseur de rechange a été reçu et doit être installé et converti en mode interception commandée en vol.

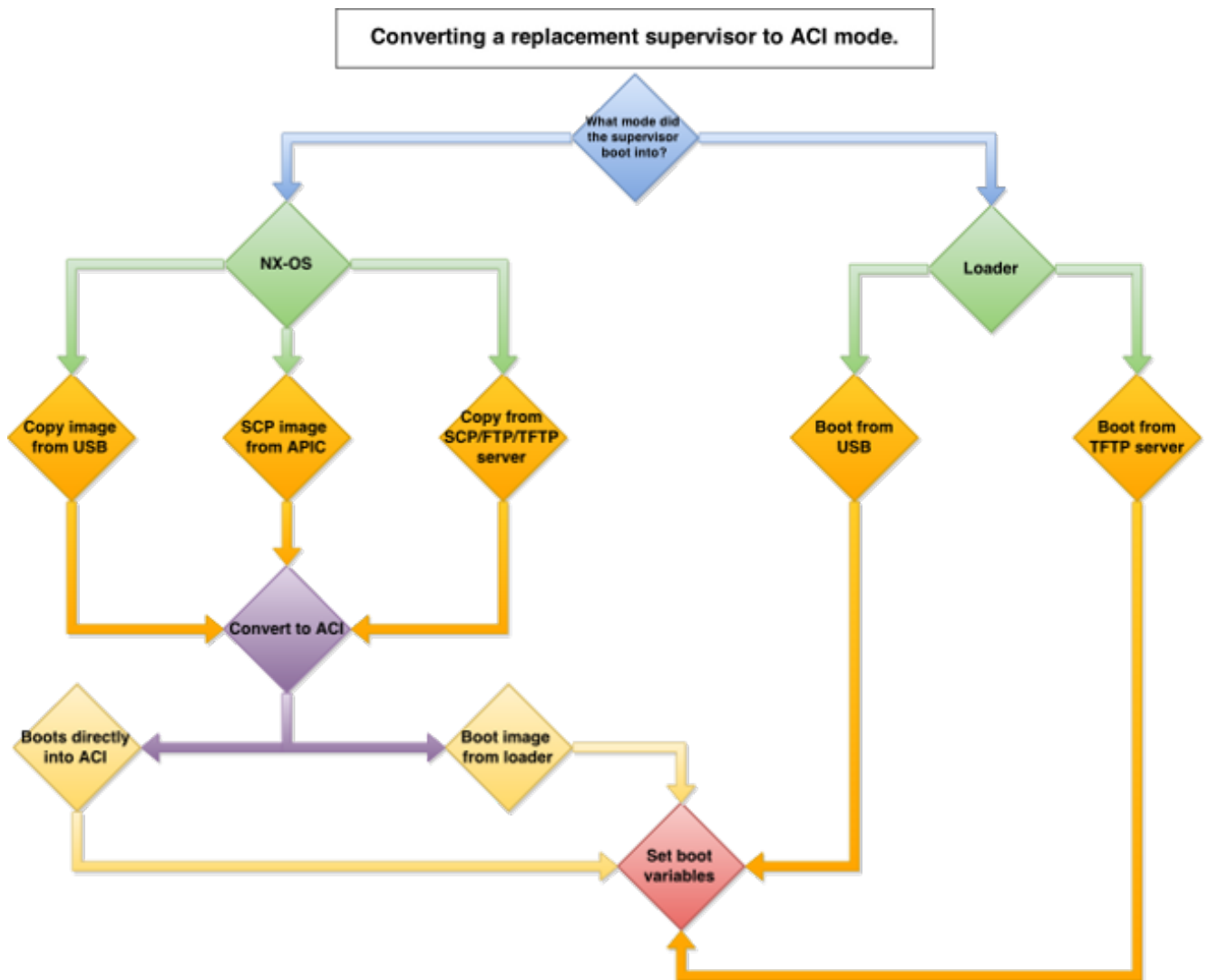
Solution

Note: La conversion du superviseur en mode interception commandée en vol a besoin de le temps d'arrêt pour l'épine pendant que quelques composants doivent être déconnectés.

Préparez pour convertir le superviseur de rechange en mode interception commandée en vol

Terminez-vous ces étapes afin de convertir le superviseur de rechange :

1. Retirez le superviseur défectueux du châssis d'épine.
2. Déconnectez chaque linecard interception commandée en vol et le superviseur actif fonctionnant. On ne l'exige pas pour que les linecards et le superviseur actif soit complètement retiré du châssis. Puis, insérez le superviseur de rechange. Si le superviseur de rechange démarre dans le mode autonome (NX-OS) il doit être converti en mode interception commandée en vol par la procédure 1. Autrement, s'il démarre dans une demande de loader> suivez la procédure 2.



Procédure 1 - Conversion de NX-OS à l'interception commandée en vol

1. Terminez-vous une de ces trois options afin de charger une image interception commandée en vol dans le bootflash du superviseur de rechange : Option A - Copiez l'image interception commandée en vol d'un lecteur USB dans le bootflash. Répertoriez le contenu du lecteur USB (usb1 : ou usb2 :) pour le nom d'image interception commandée en vol afin de se terminer ceci :

```
switch# dir usb1:
switch# copy usb1:aci-n9000-dk9.11.0.3f.bin bootflash:
```

Option B - Permettez aux services de Secure Copy (SCP) afin de pousser l'image interception commandée en vol d'un contrôleur d'infrastructure de stratégie d'application (APIC). Configurez l'interface de la Gestion 0 avec une adresse IP, installez une passerelle par défaut pour l'exemple virtuel de routage et d'expédition de Gestion (VRF), et activez la caractéristique de serveur SCP.

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# ip address ipv4-address{ [/length] | [subnet-mask]}
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# vrf context management
switch(config-vrf)# ip route 0.0.0.0/0 default-gw-ip
switch(config-vrf)# exit
switch(config)# feature scp-server
switch(config)# exit
```

```
switch# copy running-config startup-config
```

Note: Avant que vous poursuiviez, vérifiez l'APIC peut être cinglé du VRF de Gestion. Sélectionnez cette commande sur l'APIC :

```
admin@apic:~>
```

```
scp /firmware/fwrepos/fwrepo/<aci_image.bin> admin@<node-mgmt-ip>:<aci_image.bin>
```

Note: <aci_image.bin> est le nom du fichier de l'image de commutateur interception commandée en vol située sur l'APIC. le <node-mgmt-ip> est l'adresse IP de Gestion qui a été précédemment configurée sur le commutateur. **Conseil :** Les noms d'image de commutateur interception commandée en vol commencent toujours par 'aci-n9000.C d'option - Copiez l'image d'un serveur accessible SCP/FTP/TFTP. Configurez l'interface de la Gestion 0 avec une adresse IP, installez une passerelle par défaut pour l'exemple de VRF de Gestion, et copiez l'image dans le bootflash. Cet exemple utilise le SCP.

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# ip address ipv4-address{ [/length] | [subnet-mask] }
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# vrf context management
switch(config-vrf)# ip route 0.0.0.0/0 default-gw-ip
switch(config-vrf)# end
```

Vérifiez le serveur peut être cinglé du VRF de Gestion et puis copier l'image du serveur dans le bootflash.

```
switch#
```

```
copy scp://scpuser@10.0.0.10/path/to/aci-n9000-dk9.11.0.3f.bin bootflash: vrf management
```

Vérifiez l'image interception commandée en vol a transféré avec succès vers le commutateur autonome avec le bootflash de dir :
commande.

```
switch# dir bootflash:
6626      Nov 18 14:22:33 2014 20141118_142200_poap_6132_init.log
500237761 Nov 14 18:24:12 2014 aci-n9000-dk9.11.0.2j.1.0-2j.bin
328541633 Nov 18 14:13:02 2014 auto-s
2         Nov 18 14:15:24 2014 diag_bootup
53       Nov 18 14:15:01 2014 disk_log.txt
4096     Nov 14 19:43:26 2024 lost+found/
3093     Nov 18 14:10:01 2014 mem_log.txt.old.gz
309991424 Nov 18 14:10:52 2014 n9000-dk9.6.1.2.I2.1.bin
4096     Nov 08 14:28:49 2014 scripts/
```

2. Convertissez le superviseur en mode interception commandée en vol. Si le superviseur exécute la version 6.1(2)I3(3) ou ultérieures NX-OS, utilisez la méthode 1. Autrement, la méthode 2 de la méthode 2. d'utilisation pourrait également être utilisée comme sauvegarde si la méthode 1 échoue. [Méthode 1](#)

Logiciel NXOS testé : n9000-dk9.6.1.2.I3.3a.bin

Logiciel interception commandée en vol testé : aci-n9000-dk9.11.0.3f.bin Sur le noeud autonome sélectionnez ces commandes :

```
switch# configure terminal
switch(config)# boot aci bootflash:<aci_image.bin>
switch(config)# reload
```

[Méthode 2](#)

Logiciel NXOS testé : n9000-dk9.6.1.2.i2.1.bin

Logiciel interception commandée en vol testé : aci-n9000-dk9.11.0.2j.1.0-2j.bin Sur le noeud autonome sélectionnez ces commandes :

```
switch# configure terminal
switch(config)# no boot nxos
switch(config)# end
switch# copy running-config startup-config
switch# reload
```

Ceci fait démarrer le commutateur dans la demande de « loader> ». Sélectionnez la commande de dir afin de répertorier le contenu du bootflash pour le nom d'image interception commandée en vol.

```
Loader Version 8.06

loader > dir

bootflash::

  auto-s
  mem_log.txt
  disk_log.txt
  mem_log.txt.old.gz
  lost+found
  .patch
  aci-n9000-dk9.11.0.2j.bin
  .patch-issu
  scripts
  20141121_003542_poap_6330_init.log
  n9000-dk9.6.1.2.i2.2b.bin
  20141121_005455_poap_5924_init.log
```

Démarrez l'image interception commandée en vol avec la commande **boot<aci_image_name.bin>**. Le superviseur démarre dans le mode interception commandée en vol dans un état de détection de matrice. Procédure de connexion avec l'admin de nom d'utilisateur sans le mot de passe.

```
User Access Verification
(none) login: Certificate verification passed

User Access Verification
(none) login: admin
*****
Fabric discovery in progress, show commands are not fully functional
Logout and Login after discovery to continue to use show commands.
*****
(none)# █
```

3. Placez les variables de démarrage avec le nom d'image de la commande de dir.

```
(none)# dir bootflash
(none)# setup-bootvars.sh <aci_image.bin>
```

4. Sélectionnez ces commandes afin de vérifier les variables de démarrage ont été placés correctement :

```
leaf# cat /mnt/cfg/0/boot/grub/menu.lst.local
boot aci-n9000-dk9.11.0.2j.bin
leaf# cat /mnt/cfg/1/boot/grub/menu.lst.local
```

```
boot aci-n9000-dk9.11.0.2j.bin
```

5. Rebranchez tous les linecards précédemment déconnectés aussi bien que l'autre superviseur. L'épine rejoint la matrice dans quelques minutes et l'APIC abaisse toutes les stratégies appropriées au nouveau superviseur.

Procédure 2 - Conversion de chargeur à l'interception commandée en vol

1. Démarrez une image interception commandée en vol avec une de ces deux options. Option A - Démarrage d'un lecteur USB. Répertoriez le contenu du lecteur USB (usb1 : ou usb2 :) pour le nom d'image interception commandée en vol, démarrez- alors le de l'USB.

```
loader> dir usb1:  
loader> boot usb1:aci-n9000-dk9.11.0.3f.bin
```

Option B - Démarrage d'un serveur accessible TFTP. Configurez une adresse IP et une passerelle par défaut et puis démarrez du serveur.

```
loader> set ip <ip_addr> <mask>  
loader> set gw <ip_addr>  
loader> boot tftp://<tftp_path>
```

Un exemple est montré ici :

```
loader> set ip 192.0.2.10 255.255.255.0  
loader> set gw 192.0.2.1  
loader> boot tftp://192.0.2.50/aci-n9000-dk9.11.0.3f.bin
```

Le superviseur démarre dans le mode interception commandée en vol dans un état de détection de matrice. Procédure de connexion avec l'**admin de** nom d'utilisateur sans le mot de passe.

2. Placez les variables de démarrage sur le superviseur avec le nom d'image de la commande de dir.

```
(none)# dir bootflash  
(none)# setup-bootvars.sh <aci_image_name.bin>
```

3. Rebranchez tous les linecards précédemment déconnectés aussi bien que l'autre superviseur. L'épine rejoint la matrice dans quelques minutes et l'APIC abaisse toutes les stratégies appropriées au nouveau superviseur. Vous serez incité à ouvrir une session avec les qualifications de matrice.

*Note : La non-concordance de version des défauts F1582 « FPGA détectée » peut être signalée lors de suivre la procédure. Ces défauts seront résolus la première fois que vous exécutez la mise à jour utilisant la stratégie de micrologiciel/maintenance d'APIC.