

Procédure de remplacement du châssis Nexus 7000

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Remplacer un commutateur Cisco Nexus 7000](#)

[Avant de commencer](#)

[Fenêtre de remplacement du châssis](#)

[Option 1. Approche progressive](#)

[Option 2. Remplacement direct](#)

[Comment s'assurer que le bit rémanent vPC est correctement défini](#)

Introduction

Ce document décrit les étapes nécessaires pour remplacer un châssis dans un environnement vPC (Virtual Port Channel). Ce scénario se produit en raison d'une défaillance matérielle ou de limitations de la prise en charge des fonctionnalités/matériels.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CLI du système d'exploitation Nexus
- Règles vPC

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

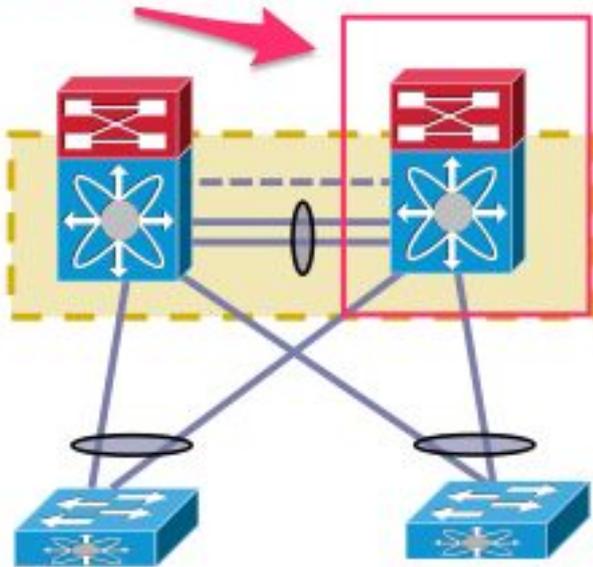
- Supervisor 1 version 5.2(3a) ou ultérieure
- Supervisor 2 version 6.x ou ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Remplacer un commutateur Cisco Nexus 7000

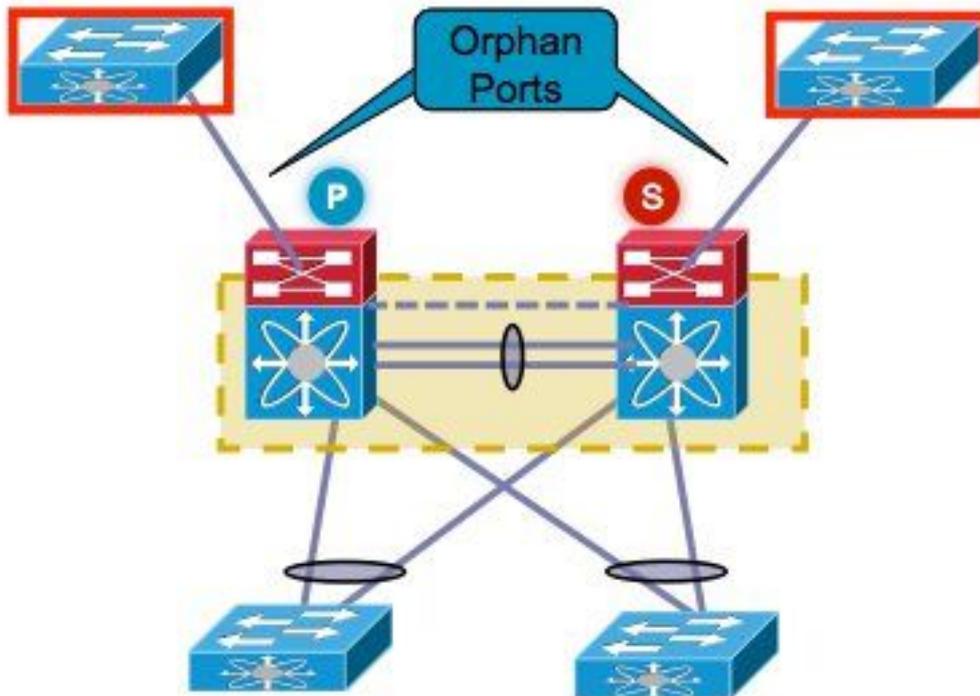
Lorsque vous remplacez un commutateur de la gamme Cisco Nexus 7000, vous devez effectuer cette procédure afin de vous assurer qu'il y a un minimum ou aucune panne. Cette image montre comment remplacer le châssis.

Replacing the Chassis below



Avant de commencer

1. Une fois que l'autorisation de retour de matériel (RMA) du châssis de remplacement est créée, assurez-vous qu'un dossier est ouvert avec l'équipe de licences afin d'obtenir la réhébergement de la licence sur le nouveau châssis. L'équipe de gestion des licences peut générer un nouveau fichier de licence pour le châssis de remplacement. La génération d'un nouveau fichier de licence n'invalide pas la licence actuelle sur le châssis. Conservez l'e-mail avec la clé de licence.
2. Enregistrez la configuration en cours de tous les VDC (Virtual Device Contextes).
3. Sauvegardez la configuration en cours de tous les VDC sur le bootflash et sur un serveur FTP/FTP sécurisé (SFTP)/TFTP.
4. Identifiez que tous les périphériques sont connectés via des ports orphelins sur le Nexus 7000 cible. Une perte de connectivité est constatée si l'environnement est pris en charge par les ports orphelins qui ne disposent pas d'une liaison redondante vers le réseau.



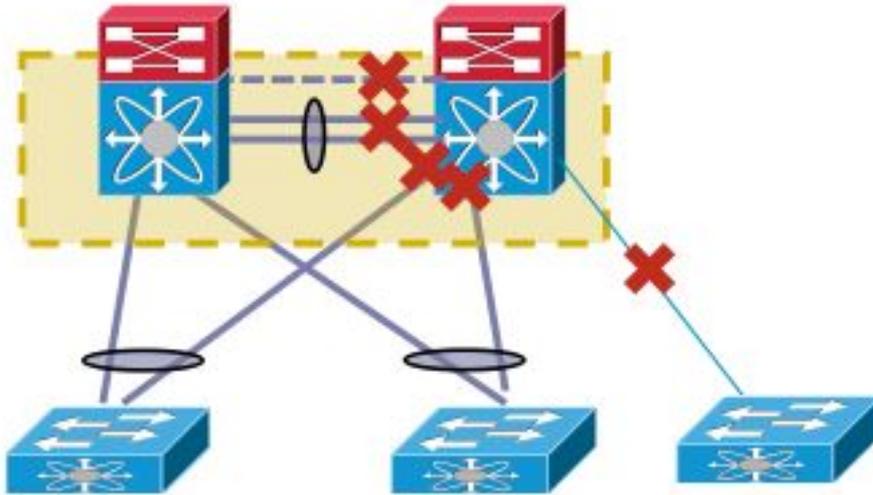
5. Prévoyez de basculer tout pare-feu/équilibreur de charge/périphérique similaire actuellement sur le Nexus 7000 cible vers l'autre Nexus 7000.
6. Collectez le résultat de la commande présentée dans cette liste à partir des deux Nexus 7000 (sauf pour la vérification post-implémentation). Cela doit également être effectué par VDC.
`show versionshow moduleshow inventaireshow vPCshow vPC roleshow port-channel summaryshow span sumshow vlan sumshow running-configshow ip int brief vrf allshow int statusshow cdp neishow trunk`
envoi de requêtes ping à des serveurs spécifiques afin de confirmer leur accessibilité ou d'utiliser l'outil NMS (Network Management Systems) appropriéconformément à l'environnement de chaque client, les sorties de commande supplémentaires doivent être capturées

Fenêtre de remplacement du châssis

Il existe deux méthodes pour remplacer le châssis. L'option 1 décrit une approche plus contrôlée qui permet au client d'effectuer les étapes par phases, mais qui prend plus de temps. Une deuxième option est également disponible. Les deux options répertoriées sont indépendantes du rôle vPC.

Option 1. Approche progressive

1. Arrêtez toutes les liaisons vPC du châssis qui sont remplacées. Cela s'applique au VDC dans lequel le vPC est configuré.
2. Arrêtez toutes les liaisons physiques de couche 3.
3. Arrêtez tous les ports orphelins.
4. Arrêtez la liaison PKA (Peer Keep Alive).
5. Arrêtez la liaison homologue. Quel que soit le rôle vPC, l'autre côté maintient la liaison vPC active car ces étapes mènent à un scénario actif double.
6. Vérifiez qu'il n'y a aucun problème de connectivité.



Complétez ces étapes afin de remplacer le commutateur :

1. Mettez le Nexus 7000 cible hors tension.
2. Débranchez les câbles des modules.
3. Installez le nouveau commutateur.
4. Installez les superviseurs et les modules.
5. Mettez le commutateur sous tension.
6. Vérifiez que le superviseur dispose de la version correcte de NX-OS.

Complétez ces étapes afin d'installer la licence :

1. Installez la licence du châssis, obtenue à l'étape 1 de la section « Avant de commencer ».
2. Copiez la configuration du bootflash dans la configuration en cours.
3. Vérifiez que la configuration est cohérente avec la sauvegarde.

Redémarrez le commutateur en production. Il est important de vérifier le rôle LACP et le bit collant avant d'activer les interfaces. La section suivante passe en revue les étapes.

Vérification du rôle LACP

Lorsque la liaison homologue apparaît entre deux homologues vPC, en dehors des rôles vPC, les rôles permanents LACP sont également décidés (un homologue devient le maître, tandis que l'autre devient l'esclave).

Une sélection de rôle LACP se produit si les deux homologues ont le même rôle (maître ou esclave). Le système dont l'adresse MAC est inférieure gagne en tant que maître et cette sélection n'est pas régie par la configuration de priorité de rôle vPC.

Une réélection entraîne la réinitialisation des canaux de port LACP vPC, ce qui peut entraîner une panne de trafic.

Entrez ces commandes afin de vérifier le rôle LACP :

```
show system internal vpcm info all | i "LACP Role"
show system internal vpcm info all | i "LACP Per"
```

Recommandation

Avant de réintroduire un périphérique vPC déjà isolé dans la production, cochez les rôles LACP dans les deux cases. Si le même rôle est défini, désactivez la récupération automatique **sans**

récupération automatique sous le domaine vPC sur les deux homologues et rechargez le périphérique isolé. Après le rechargement, le périphérique isolé apparaît avec le rôle LACP 'aucun établi' et peut être introduit dans le vPC sans réélection de rôle LACP.

Contrôle des bits rémanents

Vérifiez que le bit rémanent est défini sur false.

1. Entrez la commande **show sys internal vpcm info all | i stick** commande afin de vérifier si le bit sticky est défini sur false.
2. Si le bit rémanent est défini sur false, passez à l'étape 5. Si le bit rémanent est défini sur true, reconfigurez la priorité du rôle vPC. Cela signifie que vous devez réappliquer la configuration d'origine pour la priorité de rôle. Si la priorité de rôle est par défaut, réappliquez la valeur par défaut. Dans cet exemple, la priorité de rôle est 2000 et la même valeur est réappliquée.

```
vpc domain 30
role priority 2000
```

Note: Cette étape réinitialise le bit collant de true à false.

3. Entrez la commande **show sys internal vpcm info all | i stick** commande afin de déterminer si le bit sticky est défini sur false.
4. Si le bit adhésif est toujours vrai, rechargez le VDC ou le châssis.
5. Si le bit collant est faux, activez PKA et Peer Link (PL).

Exemple de rapport :

```
N7K# show system internal vpcm info all | i i sticky
      Sticky Master: FALSE
```

Activation des interfaces physiques

1. Activez la liaison PKA.
2. Activez la liste de contrôle d'accès vPC.
3. Vérifiez que le rôle vPC est correctement établi.
4. Activez les liaisons vPC une par une en n'arrêtant pas l'interface.
5. Activez les ports orphelins.
6. Activez les interfaces physiques de couche 3.

Une fois les étapes terminées, vérifiez qu'il n'y a aucun problème de connectivité.

Prenez un instantané des mêmes sorties collectées précédemment et comparez-les pour validation.

- show version
- show module
- show inventaire
- show vPC
- show vPC role
- show port-channel summary
- show span sum
- show vlan sum
- show running-config
- show ip int brief vrf all

- show int status
- show cdp nei
- show trunk
- envoi de requêtes ping à des serveurs spécifiques afin de confirmer leur accessibilité ou utiliser l'outil NMS approprié
- conformément à l'environnement de chaque client, les sorties de commande supplémentaires doivent être capturées

Option 2. Remplacement direct

La différence entre le remplacement direct et l'approche progressive est que l'approche consistant à arrêter les liaisons individuelles n'est pas utilisée dans le remplacement direct.

1. Mettez le Nexus 7000 cible hors tension.
2. Débranchez les câbles des modules.
3. Installez le nouveau commutateur.
4. Installez les superviseurs et les modules.
5. Mettez le commutateur sous tension.
6. Vérifiez que le superviseur dispose de la version correcte de NX-OS.

Complétez ces étapes afin d'installer la licence :

1. Installez la licence du châssis. Ceci a été obtenu à l'étape 1 de la section « Avant de commencer ».
2. Copiez la configuration du bootflash dans la configuration en cours.
3. Vérifiez que la configuration est cohérente avec la sauvegarde.

Complétez ces étapes afin de remettre le commutateur en production :

1. Mettez à nouveau le Nexus 7000 hors tension. Connectez à nouveau toutes les liaisons du Nexus 7000.
2. Mettez-le sous tension. Le vPC redémarre après l'état initial.
3. Prenez un instantané des commandes afin de les comparer après leur remplacement.

C'est similaire à un redémarrage du Nexus 7000, dans lequel le Nexus 7000 devrait se rétablir de manière transparente.

Les deux approches présentées présentent leurs avantages et leurs inconvénients. L'option 1 donne plus de contrôle au détriment d'une fenêtre de modification plus longue. Il n'y a aucune recommandation quant à l'approche la mieux adaptée, car elle dépend du type de réseau et du type d'application hébergée.

Comment s'assurer que le bit rémanent vPC est correctement défini

Cette section explique comment s'assurer que le bit rémanent vPC est correctement défini afin d'éviter une panne éventuelle lorsqu'un commutateur isolé est intégré au pli vPC.

Effectuez les étapes suivantes avant de passer à l'étape PKA et PL :

1. Entrez la commande **show sys internal vpcm info all | i stick** commande afin de vérifier si le bit sticky est défini sur false.
2. Si le bit rémanent est défini sur false, passez à l'étape 5. Si le bit rémanent est défini sur

true, reconfigurez la priorité du rôle vPC. Cela signifie que vous devez réappliquer la configuration d'origine pour la priorité de rôle. Si la priorité de rôle est par défaut, réappliquez la valeur par défaut. Dans cet exemple, la priorité de rôle est 2000 et la même valeur est réappliquée.

```
vpc domain 30  
role priority 2000
```

Note: Cette étape réinitialise le bit collant de true à false.

3. Entrez la commande **show sys internal vpcm info all | i stick** commande afin de déterminer si le bit sticky est défini sur false.
4. Si le bit adhésif est toujours vrai, rechargez le VDC ou le châssis.
5. Si le bit collant est faux, affichez le PKA et le PL.