Verfahren zum Austausch von Chassis des Nexus 7000

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Ersetzen Sie einen Cisco Nexus Switch der Serie 7000.](#)
[Bevor Sie beginnen](#)
[Fenster "Chassis Replacement"](#)
[Option 1: Phasenweiser Ansatz](#)
[Option 2: Direkter Austausch](#)
[So stellen Sie sicher, dass das vPC Sticky Bit korrekt eingestellt ist](#)

Einführung

In diesem Dokument werden die Schritte beschrieben, die zum Durchführen eines Chassis-Ersatzes in einer vPC-Umgebung (Virtual Port Channel) erforderlich sind. Dieses Szenario ist auf Hardwarefehler oder Einschränkungen bei Funktionen/Hardware-Support zurückzuführen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CLI des Nexus-Betriebssystems
- vPC-Regeln

Verwendete Komponenten

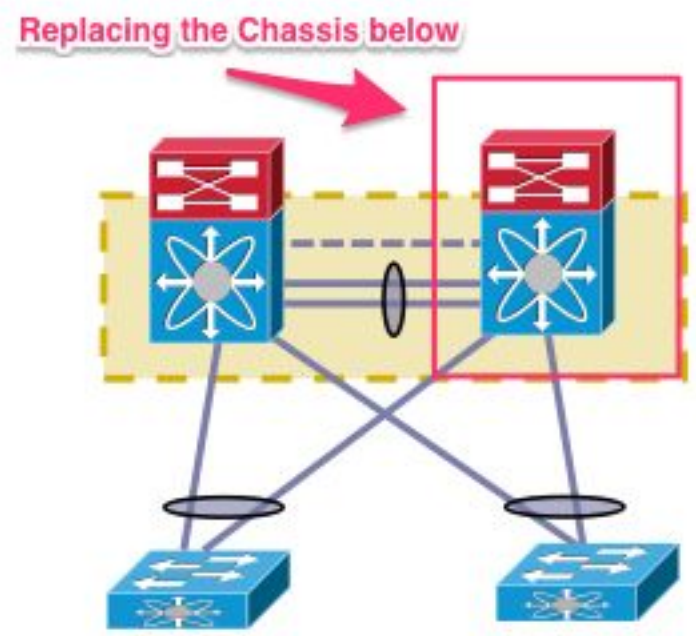
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Supervisor 1 Version 5.2(3a) oder höher
- Supervisor 2 Version 6.x oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

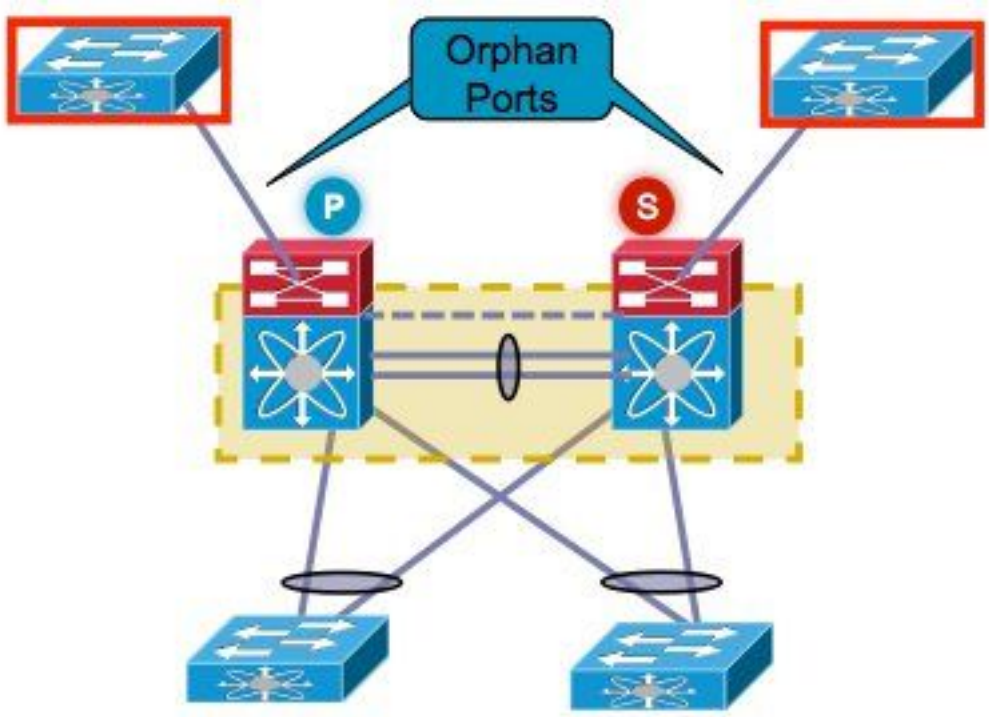
Ersetzen Sie einen Cisco Nexus Switch der Serie 7000.

Wenn Sie einen Cisco Nexus-Switch der Serie 7000 ersetzen, müssen Sie dieses Verfahren durchführen, um sicherzustellen, dass nur minimale oder keine Ausfälle auftreten. Dieses Bild zeigt, wie das Chassis ersetzt wird.



Bevor Sie beginnen

1. Wenn die Retourengenehmigung (Return Material Authorization, RMA) für das Chassis für den Austausch erstellt wurde, stellen Sie sicher, dass ein Ticket beim Lizenzierungsteam geöffnet wird, um die Lizenz erneut auf dem neuen Chassis zu hosten. Das Lizenzierungsteam kann eine neue Lizenzdatei für das Ersatzchassis generieren. Durch die Generierung einer neuen Lizenzdatei wird die aktuelle Lizenz für das Chassis nicht ungültig. Bewahren Sie die E-Mail mit dem Lizenzschlüssel auf.
2. Speichern Sie die aktuelle Konfiguration aller VDCs (Virtual Device Contexts).
3. Sichern Sie die aktuelle Konfiguration für alle VDCs im Bootflash und auf einem FTP/Secure FTP (SFTP)/TFTP-Server.
4. Identifizieren Sie, dass alle Geräte über verwaiste Ports am Ziel-Nexus 7000 verbunden sind. Verbindungsverluste treten auf, wenn die Umgebung von den verwaisten Ports unterstützt wird, die keine redundante Verbindung mit dem Netzwerk haben.



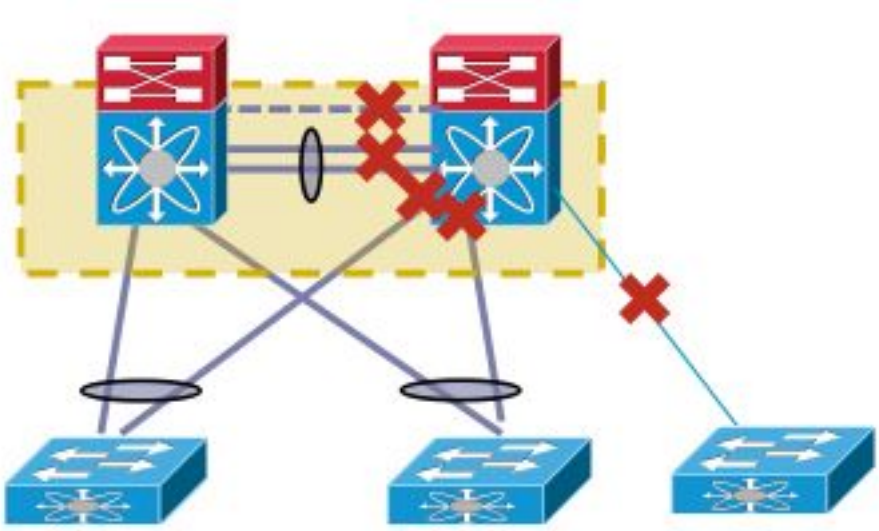
5. Planen Sie ein Failover aller aktiven Firewall-/Load Balancer-/ähnlichen Geräte, die sich derzeit auf dem Nexus 7000-Zielgerät befinden, auf den anderen Nexus 7000.
6. Ermitteln Sie die in dieser Liste angezeigte Befehlsausgabe aus beiden Nexus 7000-Geräten (mit Ausnahme der Verifizierung nach der Implementierung). Dies muss auch pro VDC durchgeführt werden. AnzeigeversionSchaumodulBestand anzeigenvPC anzeigenvPC-Rolle anzeigenPort-Channel-Zusammenfassung anzeigenAnzeigedauerVLAN-Summe anzeigenshow running-configshow ip int brief vrallint-Status anzeigenshow cdp neiHauptleitungPings an bestimmte Server, um deren Erreichbarkeit zu bestätigen, oder das entsprechende Network Management Systems (NMS)-Tool verwendenJe nach Umgebung jedes Kunden müssen die zusätzlichen Befehlsausgaben erfasst werden.

Fenster "Chassis Replacement"

Es gibt zwei Möglichkeiten, den Chassis-Austausch durchzuführen. Option 1 dokumentiert einen kontrollierteren Ansatz, der es dem Kunden ermöglicht, die Schritte in mehreren Phasen durchzuführen, aber mehr Zeit in Anspruch nimmt. Eine zweite Option ist ebenfalls verfügbar. Beide Optionen sind unabhängig von der vPC-Rolle.

Option 1: Phasenweiser Ansatz

1. Fahren Sie alle vPC-Verbindungen im Chassis herunter, die ersetzt werden sollen. Dies gilt für den VDC, in dem der vPC konfiguriert ist.
2. Fahren Sie alle physischen Layer-3-Verbindungen herunter.
3. Fahren Sie alle verwaisten Ports herunter.
4. Fahren Sie den Link Peer Keep Alive (PKA) herunter.
5. Fahren Sie den Peer-Link herunter. Unabhängig von der vPC-Rolle hält die andere Seite die vPC-Verbindung aufrecht, da diese Schritte zu einem Dual-Active-Szenario führen.
6. Bestätigen Sie, dass keine Verbindungsprobleme auftreten.



Gehen Sie wie folgt vor, um den Switch zu ersetzen:

1. Schalten Sie das Ziel-Nexus 7000 aus.
2. Ziehen Sie die Kabel von den Modulen ab.
3. Installieren Sie den neuen Switch.
4. Installieren Sie die Supervisoren und Module.
5. Schalten Sie den Switch ein.
6. Stellen Sie sicher, dass der Supervisor über die richtige NX-OS-Version verfügt.

Gehen Sie wie folgt vor, um die Lizenz zu installieren:

1. Installieren Sie die Lizenz für das Chassis, die Sie in Schritt 1 im Abschnitt "Bevor Sie beginnen" erhalten haben.
2. Kopieren Sie die Konfiguration aus dem Bootflash in die aktuelle Konfiguration.
3. Überprüfen Sie, ob die Konfiguration mit der Sicherung übereinstimmt.

Stellt den Switch wieder in die Produktion ein. Es ist wichtig, die LACP-Rolle zu überprüfen und das Bit anzuheften, bevor Sie die Schnittstellen aufrufen. Im nächsten Abschnitt werden die Schritte erläutert.

LACP-Rollenprüfung

Wenn die Peer-Verbindung zwischen zwei vPC-Peers auftaucht, werden neben den vPC-Rollen auch die permanenten LACP-Rollen festgelegt (ein Peer wird zum Master, der andere zum Slave).

Eine LACP-Rollenwahl wird durchgeführt, wenn beide Peers dieselbe Rolle spielen (Master oder Slave). Das System mit der niedrigeren MAC-Adresse erhält den Master, und diese Auswahl wird nicht durch die vPC-Rollenprioritätskonfiguration bestimmt.

Eine erneute Auswahl veranlasst die erneute Initialisierung von vPC-LACP-Port-Channels, was zu einem möglichen Datenverkehrsausfall führt.

Geben Sie die folgenden Befehle ein, um die LACP-Rolle zu überprüfen:

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

Empfehlung

Bevor Sie ein bereits isoliertes vPC-Gerät wieder in die Produktion einführen, überprüfen Sie die LACP-Rollen auf beiden Feldern. Wenn dieselbe Rolle verwendet wird, deaktivieren Sie die automatische Wiederherstellung ohne **automatische Wiederherstellung** unter der vPC-Domäne auf beiden Peers, und laden Sie das isolierte Gerät neu. Nach dem Neuladen wird dem isolierten Gerät die LACP-Rolle "none created" (Keine vorhanden) angezeigt und kann ohne erneute Auswahl der LACP-Rolle in den vPC eingefügt werden.

Sticky-Bit-Prüfung

Stellen Sie sicher, dass das klebrige Bit auf false festgelegt ist.

1. Geben Sie die **show sys internal vpcm info all ein. | i stick**-Befehl, um zu überprüfen, ob das klebrige Bit auf false festgelegt ist.
2. Wenn das klebende Bit auf false festgelegt ist, fahren Sie mit Schritt 5 fort. Wenn das klebende Bit auf true festgelegt ist, müssen Sie die vPC-Rollenpriorität neu konfigurieren. Dies bedeutet, dass die ursprüngliche Konfiguration für die Rollenpriorität erneut angewendet wird. Wenn die Rollenpriorität die Standardeinstellung ist, wenden Sie sie erneut an. In diesem Beispiel ist die Rollenpriorität 2000, und der gleiche Wert wird erneut angewendet.
   ```
   vpc domain 30
   role priority 2000
   ```
   Hinweis: Dieser Schritt setzt das klebrige Bit von true auf false zurück.
3. Geben Sie die **show sys internal vpcm info all ein. | i i stick** Befehl, um zu bestimmen, ob das klebrige Bit auf false festgelegt ist.
4. Wenn das Haftbit immer noch stimmt, laden Sie den VDC oder das Gehäuse neu.
5. Wenn das klebrige Bit false ist, rufen Sie die PKA- und Peer-Link-Datei (PL) auf.

Beispielausgabe:

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

Aufrufen der physischen Schnittstellen

1. Öffnen Sie den PKA-Link.
2. Aufrufen der vPC-PL
3. Überprüfen Sie, ob die vPC-Rolle korrekt eingerichtet wurde.
4. Aufrufen der vPC-Verbindungen einzeln, indem die Schnittstelle nicht deaktiviert wird.
5. Aufrufen der verwaisten Ports
6. Aufrufen der physischen Layer-3-Schnittstellen

Überprüfen Sie nach Abschluss der Schritte, ob keine Verbindungsprobleme vorliegen.

Erstellen Sie einen Snapshot der zuvor erfassten Ausgaben, und vergleichen Sie diese zur Validierung.

- Anzeigeversion
- Schaumodul
- Bestand anzeigen
- vPC anzeigen
- vPC-Rolle anzeigen
- Port-Channel-Zusammenfassung anzeigen
- Anzeigedauer

- VLAN-Summe anzeigen
- show running-config
- show ip int brief vrall
- int-Status anzeigen
- show cdp nei
- Hauptleitung
- Pings an bestimmte Server senden, um deren Erreichbarkeit zu bestätigen oder das entsprechende NMS-Tool zu verwenden
- Je nach Umgebung jedes Kunden müssen die zusätzlichen Befehlsausgaben erfasst werden.

Option 2: Direkter Austausch

Der Unterschied zwischen dem direkten Austausch und dem phasenweisen Ansatz besteht darin, dass die einzelnen Links nicht beim direkten Austausch abgeschaltet werden.

1. Schalten Sie das Ziel-Nexus 7000 aus.
2. Ziehen Sie die Kabel von den Modulen ab.
3. Installieren Sie den neuen Switch.
4. Installieren Sie die Supervisoren und Module.
5. Schalten Sie den Switch ein.
6. Stellen Sie sicher, dass der Supervisor über die richtige NX-OS-Version verfügt.

Gehen Sie wie folgt vor, um die Lizenz zu installieren:

1. Installieren Sie die Lizenz für das Chassis. Dies wurde in Schritt 1 im Abschnitt "Bevor Sie beginnen" ermittelt.
2. Kopieren Sie die Konfiguration aus dem Bootflash in die aktuelle Konfiguration.
3. Überprüfen Sie, ob die Konfiguration mit der Sicherung übereinstimmt.

Gehen Sie wie folgt vor, um den Switch wieder in die Produktionsumgebung zu bringen:

1. Schalten Sie den Nexus 7000 erneut aus. Schließen Sie alle Links wieder an den Nexus 7000 an.
2. Schalten Sie das System wieder ein. Der vPC wird wieder aktiviert, nachdem der ursprüngliche Status hergestellt wurde.
3. Erstellen Sie einen Snapshot der Befehle, um sie nach dem Austausch zu vergleichen.

Dies ähnelt einem Neustart des Nexus 7000, bei dem eine nahtlose Wiederherstellung des Nexus 7000 erwartet wird.

Die beiden vorgeschlagenen Ansätze haben ihre Vor- und Nachteile. Option 1 bietet mehr Kontrolle auf Kosten eines längeren Änderungsfensters. Es gibt keine Empfehlung, welcher Ansatz der beste ist, da er vom Netzwerktyp und vom Typ der gehosteten Anwendung abhängt.

So stellen Sie sicher, dass das vPC Sticky Bit korrekt eingestellt ist

In diesem Abschnitt wird erläutert, wie sichergestellt wird, dass das vPC-Haftbit korrekt eingestellt ist, um einen möglichen Ausfall zu vermeiden, wenn ein isolierter Switch in die vPC-Falte integriert wird.

Gehen Sie wie folgt vor, bevor Sie die PKA und PL aufrufen:

1. Geben Sie die **show sys internal vpcm info all ein. | i i stick** Befehl, um zu überprüfen, ob das klebrige Bit auf false festgelegt ist.
2. Wenn das klebrige Bit auf false festgelegt ist, fahren Sie mit Schritt 5 fort. Wenn das klebende Bit auf true festgelegt ist, müssen Sie die vPC-Rollenpriorität neu konfigurieren. Dies bedeutet, dass die ursprüngliche Konfiguration für die Rollenpriorität erneut angewendet wird. Wenn die Rollenpriorität die Standardeinstellung ist, wenden Sie sie erneut an. In diesem Beispiel ist die Rollenpriorität 2000, und der gleiche Wert wird erneut angewendet.
   ```
   vpc domain 30
   role priority 2000
   ```
   Hinweis: Dieser Schritt setzt das klebrige Bit von true auf false zurück.
3. Geben Sie die **show sys internal vpcm info all ein. | i i stick** Befehl, um zu bestimmen, ob das klebrige Bit auf false festgelegt ist.
4. Wenn das Haftbit immer noch stimmt, laden Sie den VDC oder das Gehäuse neu.
5. Wenn das klebrige Bit falsch ist, rufen Sie PKA und PL auf.