Konfigurationsbeispiel einer Nexus 7000-vPC-Auto-Recovery-Funktion

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Funktion zur automatischen Wiederherstellung des virtuellen PortChannel (vPC) auf dem Nexus 7000 konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

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.

Hintergrundinformationen

Warum benötigen wir vPC-Auto-Recovery?

Für diese vPC-Erweiterung gibt es zwei Hauptgründe:

- Bei einem Ausfall des Rechenzentrums oder Stromausfall sind beide vPC-Peers, die aus Nexus 7000-Switches bestehen, ausgeschaltet. Gelegentlich kann nur einer der Peers wiederhergestellt werden. Da der andere Nexus 7000 noch ausgeschaltet ist, sind auch die vPC Peer-Verbindung und die vPC Peer-Keepalive-Verbindung deaktiviert. In diesem Szenario ist vPC selbst beim Nexus 7000, der bereits eingeschaltet ist, nicht aktiviert. Alle vPC-Konfigurationen müssen aus dem Port-Channel auf diesem Nexus 7000 entfernt werden, damit der Port-Channel funktioniert. Wenn der andere Nexus 7000 eingeschaltet wird, müssen Sie erneut Konfigurationsänderungen vornehmen, um die vPC-Konfiguration für alle vPCs einzuschließen. In Version 5.0(2) und höher können Sie unter der vPC-Domänenkonfiguration den Befehl **Reload restore** konfigurieren, um dieses Problem zu beheben.
- Aus irgendeinem Grund wird die vPC-Peer-Verbindung deaktiviert. Da der vPC-Peer-Keepalive noch eingeschaltet ist, deaktiviert das sekundäre vPC-Peer-Gerät aufgrund der Dual-Active-Erkennung alle vPC-Member-Ports. Daher durchläuft der gesamte Datenverkehr den primären vPC-Switch. Aus irgendeinem Grund erlischt auch der primäre vPC-Switch. Dieser Switch löst Datenverkehrslöcher aus, da die vPCs auf dem sekundären Peer-Gerät immer noch ausgeschaltet sind, da er eine Dual-Active-Erkennung erkannte, bevor der primäre vPC-Switch ausgeschaltet wurde.

In Version 5.2(1) und höher führt die Funktion zur automatischen vPC-Wiederherstellung diese beiden Erweiterungen zusammen.

Konfiguration

Die Konfiguration der automatischen vPC-Wiederherstellung ist einfach. Sie müssen die automatische Wiederherstellung unter der vPC-Domäne auf beiden vPC-Peers konfigurieren.

Dies ist eine Beispielkonfiguration:

Ein Switch S1

```
S1 (config)# vpc domain
S1(config-vpc-domain)# auto-recovery
S1# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 5
Peer Gateway                      : Enabled
Peer gateway excluded VLANs       : -
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
```

```
Auto-recovery status             : Enabled (timeout = 240 seconds)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-112,114-120,800,810

vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
10   Po40   up     success     success                    1-112,114-1
                                                         20,800,810
```

Ein Switch S2

```
S2 (config)# vpc domain 1
S2(config-vpc-domain)# auto-recovery
S2# show vpc
Legend:
              (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : secondary
Number of vPCs configured         : 5
Peer Gateway                      : Enabled
Peer gateway excluded VLANs       : -
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-112,114-120,800,810

vPC status ----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
40   Po40   up     success     success                    1-112,114-1
                                                         20,800,810
```

Wie funktioniert die automatische Wiederherstellung wirklich?

In diesem Abschnitt wird jedes Verhalten, das im Abschnitt "Hintergrundinformationen" erwähnt wird, separat behandelt. Es wird davon ausgegangen, dass die automatische vPC-Wiederherstellung auf beiden Switches S1 und S2 konfiguriert und in der Startkonfiguration gespeichert wird.

1. Bei einem Stromausfall werden beide Nexus 7000-vPC-Peers gleichzeitig abgeschaltet, und es kann nur ein Switch eingeschaltet werden.
   - S1 und S2 sind beide aktiviert. vPC ist korrekt gebildet, wenn Peer-Link und Peer-Keepalive aktiviert sind.
   - S1 und S2 werden gleichzeitig ausgeschaltet.

- Jetzt kann nur noch ein Switch eingeschaltet werden. Beispielsweise ist S2 der einzige Switch, der eingeschaltet wird.
- S2 wartet auf das Timeout für die automatische vPC-Wiederherstellung (der Standardwert ist 240 Sekunden, das mit dem Befehl **auto-restore reload-delay x**, wobei **x** 240-3600 Sekunden beträgt) konfiguriert werden kann, um zu überprüfen, ob entweder der vPC Peer-Link oder der Peer-Keepalive-Status eingeschaltet werden. Wenn einer dieser Links eingeschaltet ist (Peer-Link- oder Peer-Keepalive-Status), wird die automatische Wiederherstellung nicht ausgelöst.
- Wenn nach dem Timeout beide Verbindungen immer noch ausgeschaltet sind (Peer-Link und Peer-Keepalive-Status), aktiviert und initiiert die automatische vPC-Wiederherstellung, um den lokalen vPC einzuschalten. Da es keine Peers gibt, wird die Konsistenzprüfung umgangen.
- Jetzt ist S1 aktiviert. Zu diesem Zeitpunkt behält S2 seine primäre Rolle bei, und S1 übernimmt eine sekundäre Rolle, eine Konsistenzprüfung wird durchgeführt, und es werden geeignete Maßnahmen ergriffen.

2. Die vPC-Peer-Verbindung wird zuerst ausgeschaltet, und dann wird der primäre vPC-Peer ausgeschaltet.
   - S1 und S2 sind beide aktiviert, und vPC ist korrekt gebildet, wobei Peer-Link und Peer-Keepalive aktiviert sind.
   - Aus irgendeinem Grund wird zuerst die vPC-Peer-Verbindung deaktiviert.
   - Da vPC-Peer-Keepalive noch eingeschaltet ist, wird eine Dual-Active-Erkennung erkannt. Der sekundäre vPC S2 deaktiviert alle lokalen vPCs.
   - Nun wird das primäre vPC S1 ausgeschaltet oder neu geladen.
   - Bei diesem Ausfall wird auch die vPC Peer-Keepalive-Verbindung deaktiviert.
   - S2 wartet darauf, dass drei aufeinander folgende Peer-Keepalive-Nachrichten verloren gehen. Aus irgendeinem Grund wird entweder die vPC-Peer-Verbindung aktiviert oder S2 erhält eine Peer-Keepalive-Nachricht, und die automatische Wiederherstellung wird nicht aktiviert.
   - Wenn der Peer-Link jedoch deaktiviert bleibt und drei aufeinander folgende Peer-Keepalive-Nachrichten verloren gehen, aktiviert die automatische vPC-Wiederherstellung.
   - S2 übernimmt die Rolle des primären und aktiviert seinen lokalen vPC, der die Konsistenzprüfung umgeht.
   - Wenn S1 das Neuladen beendet, behält S2 seine primäre und S1 sekundäre Rolle, eine Konsistenzüberprüfung wird durchgeführt und geeignete Maßnahmen werden ergriffen.

   Hinweis: Wie in beiden Szenarien erläutert, ist der Switch, der seine vPC-Rolle bei der automatischen vPC-Wiederherstellung nicht unterbricht, auch nach dem Einschalten der Peer-Verbindung weiterhin primär. Der andere Peer übernimmt die Rolle des sekundären Peers und unterbricht seinen eigenen vPC, bis eine Konsistenzprüfung abgeschlossen ist.

Beispiel:

S1 ist ausgeschaltet. S2 wird erwartungsgemäß zur operativen Hauptkomponente. Peer-Link und Peer-Keepalive, und alle vPC-Verbindungen werden von S1 getrennt. S1 ist nicht eingeschaltet. Da S1 vollständig isoliert ist, wird der vPC aufgrund der automatischen Wiederherstellung eingeschaltet (obwohl die physischen Verbindungen ausgefallen sind) und übernimmt die Rolle des primären. Wenn nun Peer-Link oder Peer-Keepalive zwischen S1 und S2 verbunden sind, behält S1 die Rolle des primären und S2 wird sekundär. Diese Konfiguration veranlasst S2, seinen vPC so lange auszusetzen, bis sowohl der vPC Peer-Link als auch der Peer-Keepalive

eingeschaltet sind und die Konsistenzprüfung abgeschlossen ist. Dieses Szenario verursacht Datenverkehr in ein schwarzes Loch, da der S2 vPC sekundär ist und die physischen S1-Verbindungen deaktiviert sind.

Soll ich die automatische vPC-Wiederherstellung aktivieren?

Es empfiehlt sich, die automatische Wiederherstellung in Ihrer vPC-Umgebung zu aktivieren.

Es besteht eine geringe Wahrscheinlichkeit, dass die Funktion für die automatische vPC-Wiederherstellung ein Szenario mit doppelter Aktivität schafft. Wenn Sie zum Beispiel zunächst den Peer-Link verloren haben und dann den Peer-Keepalive verloren haben, wird ein Szenario mit doppelter Aktivität vorliegen.

In dieser Situation gibt jeder vPC-Teilnehmer-Port weiterhin dieselbe Link Aggregation Control Protocol-ID an wie vor dem Ausfall eines Dual-Active-Geräts.

Eine vPC-Topologie schützt im Falle von Szenarien mit zwei aktiven Geräten grundsätzlich vor Schleifen. Im schlimmsten Fall gibt es doppelte Frames. Dennoch leitet jeder Switch als Mechanismus zur Schleifenvermeidung Bridge Protocol Data Units (BPDUs) mit derselben BPDU Bridge-ID weiter wie vor dem Dual-Active-Ausfall von vPC.

Obwohl dies nicht intuitiv ist, ist es dennoch möglich und wünschenswert, den Datenverkehr vom Access Layer zum Aggregation Layer weiterzuleiten, ohne dass es bei den aktuellen Datenverkehrsflüssen zu Verlusten kommt, vorausgesetzt, die ARP-Tabellen (Address Resolution Protocol) werden bereits für alle erforderlichen Hosts auf beiden Cisco Nexus-Peers der Serie 7000 ausgefüllt.

Wenn neue MAC-Adressen von der ARP-Tabelle erfasst werden müssen, können Probleme auftreten. Die Probleme entstehen, weil die ARP-Antwort vom Server auf ein Gerät der Cisco Nexus 7000-Serie und nicht auf das andere gehasht wird, wodurch der Datenverkehr nicht korrekt fließen kann.

Angenommen, der Datenverkehr wurde vor dem eben beschriebenen Ausfall auf beide Geräte der Cisco Nexus 7000-Serie gleichmäßig über einen richtigen Port-Channel und eine Equal Cost Multipath (ECMP)-Konfiguration verteilt. In diesem Fall wird der Server-zu-Server- und Client-zu-Server-Datenverkehr mit dem Vorbehalt fortgesetzt, dass einzelne Hosts, die direkt mit der Cisco Nexus Serie 7000 verbunden sind, nicht kommunizieren können (da kein Peer-Link vorhanden ist). Darüber hinaus können neue MAC-Adressen, die bei einer Cisco Nexus 7000-Serie erfasst wurden, nicht auf dem Peer erfasst werden, da dies dazu führen würde, dass der auf dem Cisco Nexus 7000-Peer-Gerät eingehende Rückverkehr überflutet wird.

Weitere Informationen finden Sie auf Seite 19 des virtuellen PortChannel der Cisco NX-OS Software: Grundlegende Konzepte für weitere Informationen.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems