

Best Practices für ACI-Upgrades und Fehlerbehebung

Inhalt

[Einführung](#)

[Vor dem Upgrade](#)

[Aufgaben vor dem APIC-Upgrade](#)

[Dinge vor dem Switch-Upgrade](#)

[Beheben von Problemen mit Upgrades](#)

[Szenario: APIC-ID 2 oder höher bei 75 % festgehalten](#)

[Problembehebung](#)

Einführung

In diesem Dokument werden die Schritte zur Behebung von Problemen mit ACI-Upgrades (Application Centric Infrastructure) sowie die Best Practices beschrieben, die vor und während des Upgrade-Prozesses zu beachten sind.

Bei einem ACI-Upgrade werden Software und Switches (Leaf und Spine) des Application Policy Infrastructure Controller (APIC) aktualisiert. Ein Switch-Upgrade ist normalerweise sehr einfach, aber ein APIC-Upgrade kann einige Cluster-Probleme beinhalten. Cisco empfiehlt einige Vorabprüfungen, bevor ein Upgrade gestartet wird.

Vor dem Upgrade

Bevor Sie das ACI-Upgrade starten, sollten Sie einige Vorabprüfungen durchführen, um unerwartetes Verhalten zu vermeiden.

Aufgaben vor dem APIC-Upgrade

1. Beheben Sie alle Fehler.

Viele Fehler im ACI-Fabric-Status zeigen an, dass ungültige oder Konflikt-Richtlinien vorliegen oder sogar getrennte Schnittstellen usw. vorhanden sind. Verstehen Sie den Trigger, und löschen Sie ihn, bevor Sie das Upgrade starten. Beachten Sie die Fehler wie `encap already been used` Oder `Routed port is in L2 mode` kann zu einem unerwarteten Ausfall führen. Wenn Sie den Switch aktualisieren, werden alle Richtlinien vom APIC von Grund auf heruntergeladen. Infolgedessen könnten die unerwarteten Maßnahmen die erwarteten Richtlinien übernehmen, die zu einem Ausfall führen könnten.

2. Löschen der VLAN-Pool-Overlap

Überlappender VLAN-Pool bedeutet, dass dieselbe VLAN-ID Teil von zwei oder mehr VLAN-Pools ist. Wenn die gleiche VLAN-ID auf mehreren Leaf-Switches bereitgestellt wird, die Teil

verschiedener VLAN-Pools sind, wird auf diesen Switches eine andere VXLAN-ID verwendet. Da die ACI die VXLAN-ID für die Weiterleitung verwendet, kann der für ein bestimmtes VLAN bestimmte Datenverkehr in einem anderen VLAN landen oder fallen gelassen werden. Da das Leaf die Konfiguration nach dem Upgrade vom APIC herunterlädt, spielt die Reihenfolge, in der das VLAN bereitgestellt wird, eine wichtige Rolle. Dies kann in einigen VLANs zu einem Ausfall oder einem zeitweiligen Verbindungsverlust zu Endpunkten führen.

Es ist wichtig, vor dem Upgrade zu prüfen, ob sich die VLAN-ID überschneidet, und diese zu korrigieren. Es wird empfohlen, eine VLAN-ID nur aus einem VLAN-Pool zu erstellen und den VLAN-Pool ggf. wiederzuverwenden.

3. Unterstützten Upgrade-Pfad bestätigen

Das APIC-Upgrade beinhaltet die Datenkonvertierung von einer Version in eine andere, die intern durchgeführt wird. Damit die Datenkonvertierung erfolgreich ist, müssen einige Kompatibilitätsprobleme mit Versionen behoben werden. Überprüfen Sie immer, ob Cisco das direkte Upgrade Ihrer aktuellen ACI-Version auf die neue Zielversion unterstützt, auf die Sie aktualisieren. Manchmal müssen Sie mehrere Hops durchlaufen, um die Zielversion zu erreichen. Wenn Sie ein Upgrade auf eine nicht unterstützte Version durchführen, kann dies zu Problemen im Cluster und Konfigurationsproblemen führen.

Die unterstützten Upgrade-Pfade sind immer im [Cisco ACI Upgrade Guide](#) aufgeführt.

4. Backup-APIC-Konfiguration

Vergessen Sie nicht, eine Konfigurations-Sicherung auf einen Remote-Server zu exportieren, bevor Sie mit der Aktualisierung beginnen. Diese exportierte Sicherungsdatei kann verwendet werden, um die Konfiguration auf APICs wiederherzustellen, wenn Sie die gesamte Konfiguration verlieren oder nach dem Upgrade eine Datenbeschädigung vorliegt.

Hinweis: Wenn Sie die Verschlüsselung für die Sicherung aktivieren, müssen Sie den Verschlüsselungsschlüssel speichern. Andernfalls werden alle Kennwörter einschließlich des **Admin**-Kennworts nicht korrekt importiert.

5. APIC CIMC-Zugriff bestätigen

Der Cisco Integrated Management Controller (CIMC) ist die beste Lösung für den Remote-Konsolenzugriff auf den APIC. Wenn der APIC nach einem Neustart nicht wiederhergestellt wird oder die Prozesse festgefahren sind, können Sie möglicherweise keine Verbindung zum APIC über Out-of-Band- oder In-Band-Management des APIC herstellen. In dieser Phase können Sie sich beim CIMC anmelden und eine Verbindung zur KVM-Konsole herstellen, damit der APIC einige Überprüfungen durchführt und das Problem behebt.

6. Überprüfen und Bestätigen der Kompatibilität der CIMC-Version

Vergewissern Sie sich vor Beginn des ACI-Upgrades immer, dass die von Cisco empfohlene CIMC-Version, die mit der ACI-Zielversion kompatibel ist, ausgeführt wird. Siehe [Empfohlene APIC- und CIMC-Version](#).

7. Bestätigen Sie, dass der APIC-Prozess nicht gesperrt ist.

Der im APIC ausgeführte Prozess, das Appliance Element (AE), löst das Upgrade im APIC aus. Es gibt einen bekannten Fehler in CentOS Intelligent Platform Management Interface (IPMI), der den AE-Prozess im APIC sperren könnte. Wenn der AE-Prozess gesperrt ist, startet das APIC-Firmware-Upgrade nicht. Dieser Prozess fragt das Gehäuse IPMI alle 10 Sekunden ab. Wenn der AE-Prozess das Gehäuse IPMI in den letzten 10 Sekunden nicht abgefragt hat, kann dies bedeuten, dass der AE-Prozess gesperrt ist.

Sie können den Status des AE-Prozesses überprüfen, um die letzte IPMI-Abfrage zu ermitteln. Geben Sie in der APIC-CLI den Befehl ein `date` um die aktuelle Systemzeit zu überprüfen. Geben Sie jetzt den Befehl ein `grep "ipmi" /var/log/dme/log/svc_ifc_ae.bin.log | tail -5` und das letzte Mal überprüfen, wenn der AE-Prozess IPMI abgefragt hat. Vergleichen Sie die Zeit mit der Systemzeit, um zu überprüfen, ob die letzte Abfrage innerhalb des 10-Sekunden-Fensters der Systemzeit lag.

Wenn der AE-Prozess in den letzten 10 Sekunden der Systemzeit keine IPMI-Anfrage gesendet hat, können Sie den APIC neu starten, um den AE-Prozess wiederherzustellen, bevor Sie das Upgrade starten.

Hinweis: Führen Sie keinen gleichzeitigen Neustart von zwei oder mehr APICs durch, um Cluster-Probleme zu vermeiden.

8. NTP-Verfügbarkeit prüfen und bestätigen

Pingen Sie von jedem APIC aus die Erreichbarkeit an den NTP-Server, um bekannte Probleme aufgrund von APIC-Timer-Diskrepanzen zu vermeiden. Weitere Einzelheiten hierzu finden Sie im Abschnitt zur Fehlerbehebung in diesem Artikel.

9. Überprüfen Sie den APIC Health State.

Überprüfen und bestätigen Sie den Systemstatus des APIC im Cluster, bevor Sie das Upgrade starten. Der Gesundheitswert von 255 bedeutet, dass der APIC gesund ist. Geben Sie den Befehl ein `acidiaq avread | grep id= | cut -d ' ' -f 9,10,20,26,46` von jeder APIC-CLI aus, um den APIC-Systemstatus zu überprüfen. Wenn die Integritätsbewertung für einen APIC nicht 255 beträgt, starten Sie das Upgrade nicht.

10. Evaluierung der Auswirkungen einer neuen Version

Bevor Sie das Upgrade starten, lesen Sie die [Versionshinweise](#) für Ihre ACI-Zielversion und lernen alle Verhaltensänderungen kennen, die für Ihre Fabric-Konfiguration relevant sind, um unerwartete Ergebnisse nach dem Upgrade zu vermeiden.

11. Upgrade im Labor

Cisco empfiehlt, das Upgrade vor der eigentlichen Produktionsstruktur in einem Labor oder in einer Teststruktur durchzuführen, um sich mit den Upgrades und dem Verhalten der neuen Version vertraut zu machen. Dies hilft auch bei der Bewertung möglicher Probleme, die nach dem Upgrade auftreten könnten.

Dinge vor dem Switch-Upgrade

1. Virtual Port Channel (vPC) und redundante Leaf-Paare in verschiedenen Wartungsgruppen platzieren

Der ACI APIC verfügt über einen Mechanismus zum Prüfen und Zurückstellen der Aktualisierung von vPC-Paar-Leaf-Knoten von einer bestimmten Version oder einer späteren Version. Es empfiehlt sich jedoch, vPC-Paare-Switches in verschiedene Wartungsgruppen zu verteilen, um einen gleichzeitigen Neustart beider vPC-Switches zu vermeiden.

Bei redundanten Nicht-vPC-Switches, z. B. Border Leaf, sollten Sie diese in verschiedene Portgruppen einteilen, um Ausfälle zu vermeiden.

Beheben von Problemen mit Upgrades

Führen Sie immer eine Fehlerbehebung für APIC1 durch, wenn das Upgrade nicht mehr durchgeführt werden kann oder fehlschlägt. Wenn das APIC1-Upgrade noch nicht abgeschlossen ist, führen Sie keine weiteren Schritte in APIC2 und APIC3 durch. Der APIC-Upgrade-Prozess ist inkrementell. Daher wird das APIC2 erst aktualisiert, nachdem APIC1 das Upgrade abgeschlossen und den APIC2 darüber usw. informiert hat. Eine Verletzung dieser Bestimmung kann den Cluster in einen defekten Zustand mit beschädigter Datenbank versetzen, und Sie müssen möglicherweise den Cluster neu erstellen.

Szenario: APIC-ID 2 oder höher bei 75 % festgehalten

In diesem Szenario ist zu sehen, dass das APIC1 erfolgreich aktualisiert wurde, der APIC2 jedoch bei 75 % feststeckt. Dieses Problem tritt auf, wenn die Informationen zur APIC1-Upgrade-Version nicht an APIC2 oder höher weitergegeben werden. Beachten Sie, dass `svc_ifc_appliance_director` ist für die Versionssynchronisierung zwischen APICs verantwortlich.

Problembefhebung

Schritt 1: Achten Sie darauf, dass APIC1 den Rest der APICs mit ihrer Tunnel End Point (TEP)-IP-Adresse pinggen kann, um zu bestimmen, ob eine Fehlerbehebung am Leaf-Switch durchgeführt werden muss oder ob der APIC selbst fortgesetzt werden muss. Wenn der APIC1 den APIC2 nicht pinggen kann, sollten Sie sich zur Fehlerbehebung an das Technical Assistance Center (TAC) wenden. Wenn der APIC1 den APIC2 pinggen könnte, fahren Sie mit dem zweiten Schritt fort.

Schritt 2: Da sich APICs gegenseitig pinggen können, hätten die APIC1-Versionsinformationen auf den Peer repliziert werden müssen, aber irgendwie vom Peer nicht akzeptiert werden. Die Versionsinformationen werden durch einen Versions-Timestamp identifiziert. Sie können den Zeitstempel der Version APIC1 aus der CLI und der APIC2-CLI bestätigen, die auf 75 % wartet.

Auf APIC1

```
apic1# acidiag avread | grep id=1 | cut -d ' ' -f20-21  
version=2.0(2f) lm(t):1(2018-07-25T18:01:04.907+11:00)
```

Auf APIC2

```
apic2# acidiag avread | grep id=1 | cut -d ' ' -f20-21  
version=2.0(1m) lm(t):1(2018-07-25T18:20:04.907+11:00)
```

Wie Sie sehen, ist der Versions-Timestamp von APIC2 (18:20:04), der Version 2.0(1m) in diesem Beispiel ausführt, höher als der Versions-Timestamp von APIC1 (18:01:04), der Version 2.0(2f) ausführt. Der APIC2-Installationsprozess geht also davon aus, dass das APIC1-Upgrade noch nicht abgeschlossen ist, und wartet mit 75 %. Das APIC2-Upgrade beginnt, wenn der Zeitstempel der Version APIC1 den Zeitstempel der Version APIC2 überschreitet. Dies kann jedoch aufgrund des Zeitunterschieds viel warten. Um das Fabric aus diesem Zustand wiederherzustellen, können Sie ein TAC-Ticket öffnen, um Unterstützung bei der Fehlerbehebung und Behebung des Problems im APIC1 zu erhalten.