

Meilleures pratiques de mise à niveau ACI et dépannage

Contenu

[Introduction](#)

[Avant la mise à niveau](#)

[Choses à faire avant la mise à niveau APIC](#)

[Choses à faire avant la mise à niveau du commutateur](#)

[Dépannage des problèmes de mise à niveau](#)

[Scénario: ID APIC 2 ou ultérieur, 75 %](#)

[Dépannage](#)

Introduction

Ce document décrit les étapes à suivre pour résoudre les problèmes de mise à niveau de l'infrastructure axée sur les applications (ACI) et les meilleures pratiques à suivre avant et pendant le processus de mise à niveau.

Une mise à niveau ACI implique la mise à jour du logiciel et des commutateurs APIC (Application Policy Infrastructure Controller) (leaf et spine). Une mise à niveau de commutateur est généralement très simple, mais une mise à niveau APIC peut impliquer certains problèmes de cluster. Voici quelques prévérifications que Cisco recommande de préparer avant le démarrage d'une mise à niveau.

Avant la mise à niveau

Avant de commencer la mise à niveau de l'ACI, assurez-vous d'effectuer des prévérifications afin d'éviter tout comportement inattendu.

Choses à faire avant la mise à niveau APIC

1. Effacer toutes les erreurs

De nombreuses erreurs dans le fabric ACI indiquent qu'il existe des stratégies non valides ou conflictuelles, voire des interfaces déconnectées, etc. Comprenez le déclencheur et effacez-le avant de commencer la mise à niveau. Soyez conscient des défauts tels que `encap already been used` OU `Routed port is in L2 mode` peut entraîner une panne inattendue. Lorsque vous mettez à niveau le commutateur, il télécharge toutes les stratégies à partir du contrôleur APIC à partir de zéro. En conséquence, les politiques inattendues pourraient prendre le relais des politiques attendues qui pourraient provoquer une panne.

2. Effacer le chevauchement du pool VLAN

Le chevauchement de pools de VLAN signifie que le même ID de VLAN fait partie de deux

pools de VLAN ou plus. Si le même ID de VLAN est déployé sur plusieurs commutateurs Leaf qui font partie de différents pools de VLAN, il aura un ID VXLAN différent sur ces commutateurs. Puisque l'ACI utilise l'ID VXLAN pour le transfert, le trafic destiné à un VLAN particulier peut finir dans un VLAN différent ou être abandonné. Puisque la feuille télécharge la configuration à partir d'APIC après sa mise à niveau, l'ordre dans lequel le VLAN est déployé a un rôle majeur. Ainsi, cela peut entraîner une panne ou une perte de connectivité intermittente pour les points d'extrémité de certains VLAN.

Il est important de vérifier le chevauchement des ID de VLAN et de les corriger avant de commencer la mise à niveau. Il est recommandé de ne faire partie que d'un seul pool de VLAN et de réutiliser le pool de VLAN si nécessaire.

3. Confirmer le chemin de mise à niveau pris en charge

La mise à niveau du contrôleur APIC implique la conversion des données d'une version à l'autre qui est effectuée en interne. Pour que la conversion des données réussisse, il y a des problèmes de compatibilité de version qui doivent être traités. Veillez toujours à vérifier si Cisco prend en charge la mise à niveau directe de votre version ACI actuelle vers la nouvelle version cible vers laquelle vous effectuez la mise à niveau. Parfois, vous devrez passer par plusieurs sauts pour atteindre la version cible. Si vous effectuez une mise à niveau vers une version non prise en charge, cela peut entraîner des problèmes de cluster et de configuration.

Les chemins de mise à niveau pris en charge sont toujours répertoriés dans le [Guide de mise à niveau de Cisco ACI](#).

4. Configuration APIC de sauvegarde

Veillez à exporter une sauvegarde de configuration vers un serveur distant avant de commencer la mise à niveau. Ce fichier de sauvegarde exporté peut être utilisé pour récupérer la configuration sur les cartes APIC si vous perdez toute la configuration ou si des données sont endommagées après la mise à niveau.

Note: Si vous activez le chiffrement pour la sauvegarde, veillez à enregistrer la clé de chiffrement. Sinon, tous les mots de passe du compte utilisateur, y compris le mot de passe **admin**, ne seront pas importés correctement.

5. Confirmer l'accès CIMC APIC

Le contrôleur de gestion intégré Cisco (CIMC) est le meilleur moyen d'obtenir l'accès à distance à la console APIC. Si le contrôleur APIC ne se réactive pas après un redémarrage ou si les processus sont bloqués, il se peut que vous ne puissiez pas vous connecter au contrôleur APIC via la gestion hors bande ou intrabande du contrôleur APIC. À ce stade, vous pouvez vous connecter à CIMC et vous connecter à la console KVM du contrôleur APIC pour effectuer des vérifications et résoudre le problème.

6. Vérifier et confirmer la compatibilité des versions CIMC

Veillez toujours à exécuter la version CIMC recommandée par Cisco compatible avec la version ACI cible avant de démarrer la mise à niveau ACI. Reportez-vous à [APIC et version](#)

[CIMC recommandées.](#)

7. Confirmer que le processus APIC n'est pas verrouillé

Le processus appelé Appliance Element (AE) qui s'exécute dans le contrôleur APIC est responsable de déclencher la mise à niveau dans le contrôleur APIC. Il y a un bogue connu dans l'interface de gestion de plate-forme intelligente (IPMI) de CentOS qui pourrait verrouiller le processus AE dans APIC. Si le processus AE est verrouillé, la mise à niveau du micrologiciel APIC ne démarrera pas. Ce processus interroge l'IPMI du châssis toutes les 10 secondes. Si le processus AE n'a pas interrogé l'IPMI du châssis au cours des 10 dernières secondes, cela peut signifier que le processus AE est verrouillé.

Vous pouvez vérifier l'état du processus AE pour connaître la dernière requête IPMI. À partir de l'interface de ligne de commande APIC, entrez la commande `date` afin de vérifier l'heure système actuelle. Entrez maintenant la commande `grep "ipmi" /var/log/dme/log/svc_ifc_ae.bin.log | tail -5` et vérifiez la dernière fois que le processus AE a interrogé l'IPMI. Comparez l'heure avec l'heure système afin de vérifier si la dernière requête se trouvait dans la fenêtre de 10 secondes de l'heure système.

Si le processus AE n'a pas pu interroger l'IPMI au cours des 10 dernières secondes du temps système, vous pouvez redémarrer l'APIC pour récupérer le processus AE avant de commencer la mise à niveau.

Note: Ne redémarrez pas deux ou plusieurs APIC simultanément pour éviter tout problème de cluster.

8. Vérifier et confirmer la disponibilité NTP

À partir de chaque module APIC, envoyez une requête ping et confirmez l'accessibilité au serveur NTP afin d'éviter les problèmes connus en raison d'une incompatibilité de temps APIC. Pour plus d'informations à ce sujet, reportez-vous à la section dépannage de cet article.

9. Vérifier l'état d'intégrité APIC

Vérifiez et confirmez l'état de santé de l'APIC dans le cluster avant de démarrer la mise à niveau. Le score de santé de 255 signifie que l'APIC est sain. Saisissez la commande `acidiag avread | grep id= | cut -d ' ' -f 9,10,20,26,46` de toute interface de ligne de commande APIC afin de vérifier l'état d'intégrité APIC. Si le score d'intégrité n'est pas 255 pour un module APIC, ne démarrez pas la mise à niveau.

10. Évaluer l'impact d'une nouvelle version

Avant de commencer la mise à niveau, consultez les [Notes de version](#) de votre version ACI cible et comprenez les changements de comportement applicables à votre configuration de fabric afin d'éviter tout résultat inattendu après la mise à niveau.

11. Étape de la mise à niveau dans les travaux pratiques

Cisco recommande d'essayer la mise à niveau dans un laboratoire ou un fabric de test

avant le fabric de production réel pour vous familiariser avec la mise à niveau et les comportements de la nouvelle version. Cela permet également d'évaluer tous les problèmes éventuels que vous pourriez rencontrer après la mise à niveau.

Choses à faire avant la mise à niveau du commutateur

1. Placer les paires vPC (Virtual Port Channel) et feuilles redondantes dans différents groupes de maintenance

L'ACI APIC dispose d'un mécanisme permettant de vérifier et de différer la mise à niveau des noeuds leaf de paire vPC à partir d'une certaine version et d'une version ultérieure. Cependant, il est recommandé de placer des commutateurs de paire vPC dans différents groupes de maintenance pour éviter que les deux commutateurs vPC redémarrent en même temps.

Dans le cas de commutateurs non vPC redondants, tels que les bordures Leaf, veillez à les placer dans différents groupes de ports afin d'éviter toute panne.

Dépannage des problèmes de mise à niveau

Commencez toujours à dépanner APIC1 si la mise à niveau est bloquée ou échoue. Si la mise à niveau APIC1 n'est pas encore terminée, ne faites rien dans APIC2 et APIC3. Le processus de mise à niveau du contrôleur APIC est incrémentiel et, par conséquent, le contrôleur APIC2 ne procédera à la mise à niveau qu'une fois que le contrôleur APIC1 aura terminé la mise à niveau et en aura informé le contrôleur APIC2, etc. Ainsi, une violation de cette règle peut mettre le cluster dans un état rompu avec une base de données corrompue et vous devrez peut-être reconstruire le cluster.

Scénario: ID APIC 2 ou ultérieur, 75 %

Dans ce scénario, vous verrez que le contrôleur APIC1 a été mis à niveau avec succès, mais le contrôleur APIC2 reste bloqué à 75 %. Ce problème se produit si les informations de version de mise à niveau APIC1 ne sont pas propagées vers APIC2 ou une version ultérieure. Sachez que `svc_ifc_appliance_director` est chargé de la synchronisation de version entre les APIC.

Dépannage

Étape 1 : Assurez-vous que l'APIC1 peut envoyer une requête ping aux autres APIC avec leur adresse IP de point de terminaison de tunnel (TEP), car cela déterminera si vous devez effectuer un dépannage à partir du commutateur Leaf ou continuer à partir de l'APIC lui-même. Si APIC1 ne peut pas envoyer de requête ping à APIC2, vous pouvez appeler le centre d'assistance technique (TAC) pour dépanner le commutateur. Si APIC1 peut envoyer une requête ping à APIC2, passez à la deuxième étape.

Étape 2 : Puisque les cartes APIC peuvent s'envoyer des requêtes ping, les informations de version APIC1 auraient dû être répliquées sur l'homologue, mais n'ont pas été acceptées par l'homologue. Les informations de version sont identifiées par un horodatage de version. Vous pouvez confirmer l'horodatage de version d'APIC1 à partir de l'interface CLI et de l'interface CLI

APIC2 qui attend à 75 %.

Sur APIC1

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

Sur APIC2

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

Comme vous le voyez, l'horodatage de version d'APIC2 (18:20:04) qui exécute la version 2.0(1m) dans cet exemple est supérieur à l'horodatage de version d'APIC1(18:01:04) qui exécute la version 2.0(2f). Ainsi, le processus d'installation d'APIC2 pense que la mise à niveau d'APIC1 n'est pas encore terminée et attend 75 %. La mise à niveau APIC2 démarre lorsque l'horodatage de version d'APIC1 dépasse l'horodatage de version d'APIC2. Cependant, cela pourrait être beaucoup d'attente en fonction de la différence de temps. Afin de récupérer le fabric à partir de cet état, vous pouvez ouvrir un dossier TAC pour obtenir de l'aide pour dépanner et résoudre le problème à partir d'APIC1.