

Prácticas recomendadas de actualización de ACI y solución de problemas

Contenido

[Introducción](#)

[Antes de la actualización](#)

[Aspectos que se deben hacer antes de la actualización de APIC](#)

[Aspectos que se deben hacer antes de la actualización del switch](#)

[Solución de problemas de actualización](#)

[Situación: ID de APIC 2 o posterior con un 75%](#)

[Cómo solucionar problemas](#)

Introducción

Este documento describe los pasos para solucionar los problemas de actualización de la infraestructura centrada en aplicaciones (ACI) y las prácticas recomendadas que deben seguirse antes y durante el proceso de actualización.

Una actualización de ACI implica la actualización del software y los switches de Application Policy Infrastructure Controller (APIC) (hoja y columna). Una actualización del switch suele ser muy sencilla, sin embargo, una actualización de APIC podría implicar algunos problemas de clúster. Estas son algunas comprobaciones previas que Cisco recomienda preparar antes de iniciar una actualización.

Antes de la actualización

Antes de iniciar la actualización de ACI, asegúrese de realizar algunas comprobaciones previas para evitar comportamientos inesperados.

Aspectos que se deben hacer antes de la actualización de APIC

1. Borrar todos los errores

Muchos fallos en el fabric ACI indican que hay políticas inválidas o conflictivas, o incluso interfaces desconectadas, etc. Entienda el disparador y borre el antes de iniciar la actualización. Tenga en cuenta los fallos, como `encap already been used` or `Routed port is in L2 mode` podría provocar una interrupción inesperada. Cuando actualiza el switch, descarga todas las políticas desde APIC desde cero. A consecuencia de ello, las políticas inesperadas podrían hacerse cargo de las políticas esperadas, lo que podría provocar una interrupción.

2. Despejar la Superposición del Conjunto de VLAN

La superposición del conjunto de VLAN significa que el mismo ID de VLAN forma parte de dos o más grupos de VLAN. Si el mismo ID de VLAN se implementa en varios switches de

hoja que forman parte de diferentes grupos de VLAN, tendría un ID de VXLAN diferente en estos switches. Dado que ACI utiliza el ID de VXLAN para el reenvío, el tráfico destinado a una VLAN determinada puede terminar en una VLAN diferente o caer. Puesto que la hoja descarga la configuración de APIC después de su actualización, el orden en el que se implementa la VLAN tiene una función principal. Por lo tanto, esto podría dar lugar a una interrupción o a una pérdida intermitente de conectividad con los terminales en algunas VLAN.

Es importante verificar si el ID de VLAN se superpone y corregirlo antes de iniciar la actualización. Se recomienda que un ID de VLAN sea parte de un conjunto de VLAN solamente y reutilice el conjunto de VLAN donde sea necesario.

3. Confirmar ruta de actualización admitida

La actualización de APIC implica la conversión de datos de una versión a otra que se realiza internamente. Para que la conversión de datos se realice correctamente, hay algunos problemas de compatibilidad de versiones que deben tenerse en cuenta. Asegúrese siempre de comprobar si Cisco admite la actualización directa de su versión ACI actual a la nueva versión de destino a la que está actualizando. A veces tendrá que atravesar varios saltos para alcanzar la versión de destino. Si actualiza a una versión no admitida, podría ocasionar problemas de clúster y de configuración.

Las trayectorias de actualización soportadas siempre se enumeran en la [Guía de Actualización de Cisco ACI](#).

4. Copia de seguridad de la configuración APIC

Asegúrese de exportar una copia de seguridad de la configuración a un servidor remoto antes de iniciar la actualización. Este archivo de copia de seguridad exportado se puede utilizar para recuperar la configuración en los APIC si pierde toda la configuración o si hay un daño de datos después de la actualización.

Nota: Si activa el cifrado para la copia de seguridad, asegúrese de guardar la clave de cifrado. De lo contrario, todas las contraseñas de la cuenta de usuario, incluida la contraseña **admin**, no se importarán correctamente.

5. Confirmar acceso CIMC APIC

Cisco Integrated Management Controller (CIMC) es la mejor forma de obtener acceso de consola remota al APIC. Si el APIC no se reinicia después de un reinicio o los procesos se atascan, es posible que no pueda conectarse al APIC a través de la administración fuera de banda o dentro de banda del APIC. En esta etapa, puede iniciar sesión en CIMC y conectarse a la consola KVM para que el APIC realice algunas comprobaciones y resuelva el problema.

6. Verifique y confirme la compatibilidad de la versión de CIMC

Asegúrese siempre de ejecutar la versión CIMC recomendada de Cisco compatible con la versión ACI de destino antes de iniciar la actualización de ACI. Consulte [APIC recomendado y versión CIMC](#).

7. Confirmar que el proceso APIC no está bloqueado

El proceso denominado Elemento de dispositivo (AE) que se ejecuta en el APIC es responsable de activar la actualización en el APIC. Existe un error conocido en la interfaz de gestión inteligente de la plataforma (IPMI) de CentOS que podría bloquear el proceso AE en APIC. Si el proceso AE está bloqueado, la actualización del firmware APIC no se iniciará. Este proceso consulta el IPMI del chasis cada 10 segundos. Si el proceso AE no ha consultado el IPMI del chasis en los últimos 10 segundos, esto podría significar que el proceso AE está bloqueado.

Puede verificar el estado del proceso AE para conocer la última consulta IPMI. En la CLI de APIC, introduzca el comando `date` para verificar la hora actual del sistema. Ahora ingrese el comando `grep "ipmi" /var/log/dme/log/svc_ifc_ae.bin.log | tail -5` y verifique la última vez que el proceso AE consultó el IPMI. Compare el tiempo con el tiempo del sistema para verificar si la última consulta estuvo dentro de la ventana de 10 segundos del tiempo del sistema.

Si el proceso AE no ha podido consultar el IPMI en los últimos 10 segundos del tiempo del sistema, puede reiniciar el APIC para recuperar el proceso AE antes de iniciar la actualización.

Nota: No reinicie dos o más APIC al mismo tiempo para evitar cualquier problema de clúster.

8. Verifique y Confirme la Disponibilidad de NTP

Desde cada APIC, haga ping y confirme el alcance al servidor NTP para evitar problemas conocidos debido a la discordancia de tiempo de APIC. Puede encontrar más detalles sobre esto en la sección de solución de problemas de este artículo.

9. Compruebe el estado de mantenimiento de APIC

Verifique y confirme el estado de mantenimiento del APIC en el clúster antes de iniciar la actualización. La puntuación de salud de 255 significa que el APIC está sano. Introduzca el comando `acdiag avread | grep id= | cut -d ' ' -f 9,10,20,26,46` desde cualquier CLI APIC para verificar el estado de estado de APIC. Si la puntuación de estado no es 255 para ningún APIC, no inicie la actualización.

10. Evaluar el impacto de una nueva versión

Antes de iniciar la actualización, revise las [Release Notes](#) para su versión ACI de destino y comprenda cualquier cambio de comportamiento aplicable a su configuración de fabric para evitar cualquier resultado inesperado después de la actualización.

11. Etapa la actualización en el laboratorio

Cisco recomienda probar la actualización en un fabric de pruebas o de laboratorio antes del fabric de producción real para familiarizarse con la actualización y los comportamientos de la nueva versión. Esto también ayuda a evaluar los posibles problemas en los que podría ejecutarse después de la actualización.

Cosas que hacer antes de la actualización del switch

1. Colocar pares de hojas redundantes y de canal de puerto virtual (vPC) en diferentes grupos de mantenimiento

ACI APIC tiene un mecanismo para verificar y aplazar la actualización de nodos de hoja de par vPC desde una versión determinada y posterior. Sin embargo, es recomendable colocar switches de par vPC en diferentes grupos de mantenimiento para evitar que ambos se reinicien al mismo tiempo.

En el caso de los switches que no son vPC redundantes, como la hoja de borde, asegúrese de ponerlos en diferentes grupos de puertos para evitar interrupciones.

Solución de problemas de actualización

Comience siempre a resolver problemas de APIC1 si la actualización se atasca o falla. Si la actualización de APIC1 aún no ha finalizado, no haga nada en APIC2 y APIC3. El proceso de actualización de APIC es incremental y, por lo tanto, APIC2 se actualizará sólo después de que APIC1 complete la actualización y notifique al APIC2 sobre ello, etc. Por lo tanto, la violación de esto podría poner el clúster en un estado dañado con una base de datos dañada y podría ser necesario que reconstruyera el clúster.

Situación: ID de APIC 2 o posterior con un 75%

En esta situación, verá que APIC1 se actualiza correctamente, pero APIC2 sigue estancado en un 75%. Este problema ocurre si la información de la versión de actualización APIC1 no se propaga a APIC2 o posterior. Tenga en cuenta que `svc_ifc_appliance_director` está a cargo de la sincronización de la versión entre los APIC.

Cómo solucionar problemas

Paso 1: Asegúrese de que APIC1 pueda hacer ping al resto de los APIC con su dirección IP de punto final del túnel (TEP), ya que esto determinará si necesita resolver problemas desde el switch de hoja o continuar desde el APIC. Si APIC1 no puede hacer ping con APIC2, es posible que desee llamar al Technical Assistance Center (TAC) para resolver problemas del switch. Si APIC1 puede hacer ping con APIC2, continúe con el segundo paso.

Paso 2: Dado que los APIC pueden hacer ping entre sí, la información de la versión APIC1 se debería haber replicado al par, pero de alguna manera no fue aceptada por el par. La información de la versión se identifica mediante una marca de tiempo de la versión. Puede confirmar el sello de fecha y hora de la versión de APIC1 desde la CLI y la CLI de APIC2, que espera un 75%.

En 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)
```

En 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)
```

Como puede ver, la marca de tiempo de la versión de APIC2 (18:20:04) que ejecuta la versión 2.0(1m) en este ejemplo es mayor que la marca de tiempo de la versión de APIC1(18:01:04) que ejecuta la versión 2.0(2f). Por lo tanto, el proceso de instalación de APIC2 considera que la actualización de APIC1 aún no se ha completado y espera un 75%. La actualización de APIC2 se iniciará cuando la marca de tiempo de la versión de APIC1 supere la marca de hora de la versión de APIC2. Sin embargo, esto podría ser mucho esperar en función de la diferencia de tiempo. Para recuperar el fabric de este estado, puede abrir un caso del TAC para obtener ayuda para resolver problemas y solucionar el problema de APIC1.