Procedure ottimali e risoluzione dei problemi di aggiornamento ACI

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi all'aggiornamento ACI (Application Centric Infrastructure) e vengono descritte le procedure ottimali da seguire prima e durante il processo di aggiornamento.

L'aggiornamento ACI comporta l'aggiornamento del software Application Policy Infrastructure Controller (APIC) e degli switch (foglia e dorso). Un aggiornamento dello switch è in genere molto semplice, ma un aggiornamento APIC può comportare alcuni problemi del cluster. Di seguito sono riportati alcuni controlli preliminari che Cisco consiglia di preparare prima di avviare un aggiornamento.

Prima dell'aggiornamento

Prima di avviare l'aggiornamento ACI, accertarsi di eseguire alcune verifiche preliminari per evitare comportamenti imprevisti.

Operazioni preliminari all'aggiornamento di APIC

1. **Cancella tutti gli errori**

   Molti errori nell'infrastruttura ACI indicano che sono presenti criteri non validi o in conflitto oppure interfacce disconnesse e così via. Comprendere il trigger e cancellarlo prima di avviare l'aggiornamento. Tenere presente che i difetti **encap already been used** O **Routed port is in L2 mode** potrebbe causare un'interruzione imprevista. Quando si aggiorna lo switch, vengono scaricate da zero tutte le policy dall'APIC. Di conseguenza, i criteri imprevisti potrebbero assumere il controllo dei criteri previsti e causare un'interruzione delle attività.

2. **Cancella sovrapposizione pool VLAN**

   La sovrapposizione del pool di VLAN indica che lo stesso ID VLAN fa parte di due o più pool di VLAN. Se lo stesso ID VLAN viene implementato su più switch foglia che fanno parte di

pool VLAN diversi, sugli switch verrà implementato un ID VXLAN diverso. Poiché ACI utilizza l'ID VXLAN per l'inoltro, il traffico destinato a una VLAN specifica potrebbe finire su una VLAN diversa o venire scartato. Poiché la foglia scarica la configurazione dall'APIC dopo l'aggiornamento, l'ordine in cui la VLAN viene distribuita ha un ruolo principale. Ciò potrebbe causare un'interruzione o una perdita intermittente della connettività agli endpoint in alcune VLAN.

Èimportante verificare la presenza di sovrapposizioni di ID VLAN e correggerli prima di avviare l'aggiornamento. Si consiglia di includere un ID VLAN in un solo pool di VLAN e riutilizzare il pool di VLAN, se necessario.

3. **Conferma percorso di aggiornamento supportato**

   L'aggiornamento di APIC comporta la conversione dei dati da una versione all'altra, che viene eseguita internamente. Affinché la conversione dei dati abbia esito positivo, è necessario risolvere alcuni problemi di compatibilità delle versioni. Verificare sempre che Cisco supporti l'aggiornamento diretto dalla versione ACI corrente alla nuova versione di destinazione a cui si sta eseguendo l'aggiornamento. A volte è necessario passare attraverso più hop per raggiungere la versione di destinazione. Se si esegue l'aggiornamento a una versione non supportata, potrebbero verificarsi problemi di configurazione e problemi relativi al cluster.

   I percorsi di aggiornamento supportati sono sempre elencati nella Guida all'aggiornamento di Cisco ACI.

4. **Backup configurazione APIC**

   Accertarsi di esportare un backup della configurazione in un server remoto prima di avviare l'aggiornamento. Questo file di backup esportato può essere utilizzato per ripristinare la configurazione sugli APIC se si perde tutta la configurazione o se i dati risultano danneggiati dopo l'aggiornamento.
   Nota: Se si abilita la crittografia per il backup, assicurarsi di salvare la chiave di crittografia. In caso contrario, tutte le password degli account utente, inclusa la password **admin**, non verrebbero importate correttamente.
5. **Conferma accesso CIMC APIC**

   Cisco Integrated Management Controller (CIMC) è il modo migliore per ottenere l'accesso da console remota all'APIC. Se l'APIC non viene riavviato dopo un riavvio o i processi sono bloccati, potrebbe non essere possibile connettersi all'APIC tramite la gestione fuori banda o in banda dell'APIC. In questa fase è possibile accedere a CIMC e collegarsi alla console KVM per l'APIC per eseguire alcuni controlli e risolvere il problema.

6. **Verifica e conferma della compatibilità delle versioni CIMC**

   Prima di avviare l'aggiornamento ACI, accertarsi sempre di eseguire la versione CIMC consigliata da Cisco compatibile con la versione ACI di destinazione. Fare riferimento alla versione APIC e CIMC consigliata.

7. **Confermare che il processo APIC non è bloccato**

   Il processo denominato Appliance Element (AE) in esecuzione nell'APIC è responsabile dell'attivazione dell'aggiornamento nell'APIC. Nell'interfaccia IPMI (Intelligent Platform Management Interface) di CentOS è presente un bug noto che potrebbe bloccare il processo AE nell'APIC. Se il processo AE è bloccato, l'aggiornamento del firmware APIC non viene eseguito. Questo processo interroga l'IPMI dello chassis ogni 10 secondi. Se il processo AE non ha interrogato l'IPMI dello chassis negli ultimi 10 secondi, il processo AE potrebbe essere bloccato.

   Èpossibile controllare lo stato del processo AE per conoscere l'ultima query IPMI. Dalla CLI di APIC, immettere il comando **date** per controllare l'ora di sistema corrente. Immettere il comando **grep "ipmi" /var/log/dme/log/svc_ifc_ae.bin.log | tail -5** e controllare l'ultima volta in cui il processo AE ha interrogato l'IPMI. Confrontare l'ora con l'ora di sistema per verificare se l'ultima query rientra nella finestra di 10 secondi dell'ora di sistema.

   Se il processo AE non è riuscito a eseguire una query sull'IPMI negli ultimi 10 secondi del tempo di sistema, è possibile riavviare l'APIC per ripristinare il processo AE prima di avviare l'aggiornamento.
   Nota: Non riavviare due o più APIC contemporaneamente per evitare problemi di cluster.
8. **Verifica e conferma della disponibilità NTP**

   Da ciascun APIC, eseguire il ping e confermare la raggiungibilità al server NTP per evitare problemi noti dovuti alla mancata corrispondenza del tempo dell'APIC. Per ulteriori informazioni, vedere la sezione Risoluzione dei problemi di questo articolo.

9. **Controllare lo stato di integrità di APIC**

   Verificare e confermare lo stato di integrità dell'APIC nel cluster prima di avviare l'aggiornamento. Il punteggio di 255 indica che l'APIC è sano. Immettere il comando **acidiag avread | grep id= | cut -d ' ' -f 9,10,20,26,46** da qualsiasi CLI APIC per controllare lo stato di integrità di APIC. Se il livello di integrità non è 255 per nessun APIC, non avviare l'aggiornamento.

10. **Valutazione dell'impatto di una nuova versione**

    Prima di avviare l'aggiornamento, consultare le note sulla versione per la versione ACI di destinazione e conoscere le modifiche comportamentali applicabili alla configurazione dell'infrastruttura per evitare risultati imprevisti dopo l'aggiornamento.

11. **Eseguire l'aggiornamento in laboratorio**

    Cisco consiglia di provare l'aggiornamento in un laboratorio o in un fabric di test prima del fabric di produzione effettivo per acquisire familiarità con l'aggiornamento e i comportamenti della nuova versione. Ciò consente inoltre di valutare eventuali problemi che possono verificarsi dopo l'aggiornamento.

Operazioni preliminari all'aggiornamento dello switch

1. **Posizionamento di vPC (Virtual Port Channel) e coppie di foglie ridondanti in diversi gruppi di manutenzione**

   ACI APIC ha un meccanismo per controllare e rimandare l'aggiornamento dei nodi foglia della coppia vPC da una determinata versione e successive. Tuttavia, è buona norma collocare gli switch vPC a coppie in gruppi di manutenzione diversi per evitare il riavvio simultaneo degli switch vPC.

   In caso di switch non vPC ridondanti, come ad esempio switch con terminale di confine, accertarsi di collocarli in gruppi di porte diversi per evitare interruzioni.

Risoluzione dei problemi relativi all'aggiornamento

Avviare sempre la risoluzione dei problemi di APIC1 se l'aggiornamento si blocca o non riesce. Se l'aggiornamento di APIC1 non è ancora stato completato, non eseguire alcuna operazione in APIC2 e APIC3. Il processo di aggiornamento di APIC è incrementale, pertanto APIC2 eseguirà l'aggiornamento solo dopo il completamento dell'aggiornamento e ne informerà APIC2 e così via. La violazione di questa condizione potrebbe pertanto compromettere il funzionamento del cluster, causando il danneggiamento del database e la ricostruzione del cluster.

Scenario: APIC ID 2 o successivo bloccato al 75%

In questo scenario, l'aggiornamento di APIC1 è riuscito, ma APIC2 è ancora bloccato al 75%. Questo problema si verifica se le informazioni sulla versione di aggiornamento di APIC1 non vengono propagate ad APIC2 o versione successiva. Si tenga presente che svc_ifc_appliance_director è responsabile della sincronizzazione della versione tra gli APIC.

Risoluzione dei problemi

Passaggio 1: Accertarsi che l'APIC1 possa eseguire il ping sul resto degli APIC con il relativo indirizzo IP TEP (Tunnel End Point), in modo da stabilire se è necessario risolvere il problema dallo switch foglia o continuare dall'APIC stesso. Se APIC1 non comunica con APIC2, è possibile chiamare il Technical Assistance Center (TAC) per risolvere il problema dello switch. Se APIC1 è in grado di eseguire il ping di APIC2, procedere con il secondo passaggio.

Passaggio 2: Poiché gli APIC possono eseguire il ping tra loro, le informazioni sulla versione APIC1 avrebbero dovuto essere replicate nel peer, ma in qualche modo non sono state accettate dal peer. Le informazioni sulla versione sono identificate da un timestamp della versione. È possibile confermare il timestamp della versione di APIC1 dalla CLI e dalla CLI di APIC2 che è in attesa al 75%.

Su 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)
```

Su 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)
```

Come si può vedere, il timestamp della versione di APIC2 (18:20:04) in esecuzione nella versione 2.0(1m) di questo esempio è superiore al timestamp della versione di APIC1 (18:01:04) in esecuzione nella versione 2.0(2f). Il processo di installazione di APIC2, pertanto, ritiene che l'aggiornamento di APIC1 non sia ancora completo e attende il 75%. L'aggiornamento di APIC2 ha inizio quando il timestamp della versione di APIC1 supera il timestamp della versione di APIC2. In base alla differenza di tempo, tuttavia, l'attesa potrebbe essere eccessiva. Per ripristinare il fabric da questo stato, è possibile aprire una richiesta TAC per ottenere assistenza nella risoluzione dei problemi e risolvere il problema da APIC1.