Convalida e ripristino dei punti di accesso Catalyst sulla versione 17.12 interessati dall'errore di aggiornamento

Sommario

Introduzione

Questo documento descrive la procedura di ripristino quando l'ID bug Cisco è CSCwf25731 e CSCwf37271

Access point interessati

Questo influisce sui modelli di Access Point. se non si utilizzano i modelli riportati di seguito, non si subisce alcun impatto e non sono necessarie ulteriori azioni:

- Catalyst 9124 (I/D/E)
- Catalyst 9130 (I/E)
- Catalyst 9136I
- Catalyst 9162I
- Catalyst 9163E

- Catalyst 9164I

- Catalyst 9166 (I/D1)
- Catalyst IW9167 (I/E)

Contesto

Gli aggiornamenti dai sistemi presenti sul sito 17.12.4/5/6a a qualsiasi versione possono causare l'ingresso di un loop di avvio in determinati modelli di punti di accesso in determinate condizioni, innescato da un errore di installazione dell'immagine a causa di spazio su disco insufficiente sullo storage del dispositivo di destinazione. Questo scenario si verifica solo durante un'operazione di aggiornamento che coinvolge punti di accesso, ad esempio ISSU, installazione dell'immagine del controller completo o APSP, e non influisce su qualsiasi normale servizio, operazioni quotidiane o installazioni SMU.

Prima di eseguire qualsiasi aggiornamento sui punti di accesso potenzialmente interessati, è necessario eseguire ulteriori passaggi. Questo problema non prevede soluzioni e non dipende dalla configurazione, dal tipo di distribuzione o dal modello del controller

Questo problema non influisce sulle versioni precedenti alla 17.12.4 o se sul punto di accesso è in esecuzione una versione successiva alla 17.12.6a, ad esempio 17.15.x, e non è mai stata installata alcuna delle versioni interessate.

È disponibile una correzione per Cisco IOS XE release 17.12.4, 17.12.5, 17.12.6a, sotto forma di rispettivi APSP. Inoltre, è disponibile un APSP di pulizia per le versioni 17.15.4d e 17.18.2, per recuperare lo spazio perso, per le distribuzioni che utilizzavano la release interessata e che sono già state aggiornate a una versione successiva.

Se la rete ha già utilizzato una delle versioni interessate o non si è certi che le versioni siano state utilizzate in precedenza, si consiglia di eseguire i controlli prima di eseguire qualsiasi aggiornamento come precauzione

Dettagli causa principale

I punti di accesso dei modelli interessati, che eseguono i codici da 17.12.4 a 17.12.6a, creano un file persistente "/storage/cnssdaemon.log", che può crescere fino a 5 MB al giorno, e utilizzano tutto lo spazio disponibile su quella partizione del disco. Il file non viene cancellato al riavvio. Una volta che la partizione è completamente utilizzata, gli aggiornamenti possono non riuscire, in quanto un passaggio critico per l'archiviazione della nuova versione del file non è completato.

Questo problema è stato introdotto da un aggiornamento della libreria che ha modificato la destinazione del log per un componente interno. Il file registro non è necessario per il funzionamento del dispositivo

L'errore di aggiornamento si verifica solo se l'access point è in esecuzione dalla partizione 1 e lo spazio della partizione 2 è esaurito. Se lo spazio è sufficiente o l'access point è stato avviato dalla partizione 2, l'aggiornamento è riuscito

Procedura di verifica dell'aggiornamento

Se il WLC è attualmente in data 17.12.4, 17.12.5, 17.12.6a, l'aggiornamento è obbligatorio per una versione del software con la correzione, seguendo i passaggi seguenti. Per tutte le altre versioni installate sul WLC, se si intende aggiornare,si consiglia di attenersi alle seguenti istruzioni:

Passaggio 1: Verificare se i punti di accesso sono potenzialmente interessati (fare riferimento alla tabella 1). Se l'operazione non ha alcun impatto, non è richiesto alcun processo di pre-controllo/recupero ed è possibile procedere direttamente all'aggiornamento a una delle release più recenti.

Passaggio 2: In caso di impatto, eseguire i controlli preliminari per identificare il numero di access point interessati nella sezione Controlli preliminari.

Passaggio 3: Sugli access point identificati, eseguire le operazioni di ripristino descritte nella sezione relativa.

Passaggio 4: Eseguire nuovamente la verifica preliminare per verificare che nessun altro access point sia interessato.

Passaggio 5: Procedere con l'aggiornamento alle rispettive versioni APSP o software indicate nella tabella delle versioni fisse.

Fare riferimento a questa tabella per verificare se la presente nota è applicabile:

Tabella 1 - Applicabilità del percorso di aggiornamento

Versione corrente	Destinazione	Applicabilità problema	Prima dell'aggiornamento, è necessaria la verifica preliminare	Percorso di destinazione/aggiornamento	Verifica preliminare aggiornamento
17,3 x 17,6 x 17,9 x	17.12.x	No	No	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	No
17,9 x	Any (Eccetto 17.12.4/5/6a)	No	No	Segui percorso di aggiornamento di destinazione	No

da 17.12.1 a 17.12.3	Any (Ad Eccezione Di 17.12.4/5/6a)	No	No	Segui percorso di aggiornamento di destinazione	Processo regolare
17.12.4/5/6a	17.12.x(4,5,6a ecc.), APSP	Sì	Sì	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	Sì
17.12.4/5/6a	17.15.x / 17.18.x	Sì	Sì	Aggiornare la versione 17.12.x dell'APSP, quindi aggiornare la versione 17.15.x + APSPx o 17.18.x + APSPx	Sì per il primo aggiornamento 17.12 APSP e No per gli aggiornamenti successivi.
Qualsiasi versione, l'immagine precedente era una di 17.12.4/5/6a	17.15 x	Sì	Sì	17.15.x + APSPx	Sì
Qualsiasi versione, l'immagine precedente era una di 17.12.4/5/6a	17,18 x	Sì	Sì	17.18.x + APSPx	Sì

17,15+ Nuova distribuzione	Qualsiasi	No	No	Qualsiasi	No
17.18. Nuova distribuzione	Qualsiasi	No	No	Qualsiasi	No

Nota: In generale, se la rete non è in esecuzione e non ha eseguito 17.12.4, 17.12.5, 17.12.6a in passato, il problema non è applicabile

Nota: Tutte le versioni non menzionate esplicitamente nella colonna "Current" seguono il percorso di aggiornamento consigliato.

Release fisse

Controller	Versione immagine AP
17.12.4 + APSP13	17.12.4.213
17.12.5 + APSP9	17.12.5.209
17.12.6a + APSP1	17.12.6.201
17.15.3 + APSP12	17.15.3.212
17,15,4 b + APSP6	17.15.4.206
17,15,4 d + APSP1	17.15.4.225
17.18.1 + APSP3	17.18.1.203
17.18.2 + APSP1	17.18.2.201

Controlli preliminari

Per valutare se la rete è suscettibile di questo problema, eseguire la procedura corrente. Questi passaggi forniscono una panoramica, ma per il rilevamento effettivo dei punti di accesso, utilizzare la sezione "Script di controllo preliminare" per automatizzare questo processo:

- Confermare se le immagini del punto di accesso sono una delle versioni interessate, nelle colonne Immagine primaria o Immagine di backup:

```
9800-l#show ap image
Total number of APs  : 4

Number of APs
        Initiated                 : 0
        Downloading               : 0
        Predownloading            : 0
        Completed downloading     : 0
        Completed predownloading  : 0
        Not Supported             : 0
        Failed to Predownload     : 0
        Predownload in progress   : No

AP Name             Primary Image          Backup Image            Predownload Status   Predownload Ver
-------------------------------------------------------------------------------------------------------
Ap1                 17.12.5.41        17.12.4.201               None                 0.0.0.0
Ap2                 17.12.5.41        17.12.4.201               None                 0.0.0.0
Ap3                 17.12.5.41        17.12.4.201               None                 0.0.0.0
Ap4                 17.12.5.41        17.12.4.201               None                 0.0.0.0
```

- Una verifica simile può essere eseguita nel punto di accesso:

```
AP# show version
AP Running Image     : 17.12.5.41
Primary Boot Image   : 17.12.5.41
Backup Boot Image    : 17.12.5.209
Primary Boot Image Hash: 93ef1e703a5e7c5a4f97b8f59b220f52d94dd17c527868582c0048caad6397a9f3526c644f94a5
Backup Boot Image Hash: 4bbe4a0d9edc3cad938a7de399d3c2e08634643a2623bae65973ef00deb154b8eb7c7917eeecdd4
1 Multigigabit Ethernet interfaces

Any Boot Image is one of the following:
- 17.12.4.0 to 17.12.4.212
- 17.12.5.0 to 17.12.5.208
- 17.12.6.0 to 17.12.6.200
```

- Verificare la partizione di avvio corrente:

```
AP# show boot
--- Boot Variable Table ---
BOOT path-list: part1
Console Baudrate: 9600 Enable Break:
```

```
The “BOOT path-list:” should be part1, suggesting that the Backup partition is running on part2.
```

- Verificare l'utilizzo corrente del file system:

```
AP# show filesystems
Filesystem                Size      Used Available Use% Mounted on
devtmpfs                880.9M         0    880.9M   0% /dev
/sysroot                883.8M    219.6M    664.1M  25% /
tmpfs                     1.0M     56.0K    968.0K   5% /dev/shm
tmpfs                   883.8M         0    883.8M   0% /run
tmpfs                   883.8M         0    883.8M   0% /sys/fs/cgroup
/dev/ubivol/part1       372.1M     79.7M    292.4M  21% /part1
/dev/ubivol/part2       520.1M    291.3M    228.9M  56% /part2

The “Use%” for “/dev/ubivol/part2” is close to 100%.
```

- Verificare l'integrità dell'immagine per entrambe le partizioni:

```
AP# show image integrity
/part1(Backup) 17.12.5.209
    part.bin : Good
    ramfs_data_cisco.squashfs : Good
    iox.tar.gz : Good
/part2(primary) 17.12.5.41
    part.bin : Good
    ramfs_data_cisco.squashfs : Good
    iox.tar.gz : Good

The image integrity should be “Good” for all fields in both the partitions. If not Good open a TAC case
```

Nella sezione successiva vengono illustrati gli script che automatizzano il processo di verifica preliminare per tutti gli access point.

Script di preselezione

Controller WLAN (scaricabile da qui)

Passaggio 1: Estrarre il controller WLAN nel percorso file desiderato

Passaggio 2: Modificare questi valori nel file "config.ini":

```
wlc_type: 2
mode: ssh
ap_mode: ssh

; set global WLC credentials
```

```
wlc_user: username
wlc_pasw: password
wlc_enable: enable_password

; set global AP credentials
ap_user: ap_username
ap_pasw: ap_password
ap_enable: ap_enable_password

[WLC-1]
active: True
ipaddr:


mode: ssh
```

Passaggio 3: aggiungere ai file "cmdlist_cos" e "cmdlist_cos_qca" il commento del resto del contenuto predefinito e dell'elenco di comandi riportato di seguito.

```
show clock
show version
show flash
show flash | i cnssdaemon.log
show boot
show filesystems
show image integrity
```

Di seguito:

```
# snippet to download the Debug image on COS APs
# show version | in Compiled
# archive download-sw /reload tftp://


        /


#
show clock
show version
show flash
show flash | i cnssdaemon.log
show boot
show filesystems
show image integrity
```

Passaggio 4: eseguire wlanpoller utilizzando ".\wlanpoller.exe". Il poller WLAN viene eseguito, il protocollo SSH viene inviato a tutti gli access point e gli output di questi comandi vengono restituiti a tutti gli access point.

Passaggio 5: Dopo l'esecuzione, viene creata una cartella "dati". Immettere la cartella e andare fino alla fine dove si hanno più file creati per ciascuno dei punti di accesso.

Passaggio 6: Copiare/incollare il file "ap_detection_script.py" fornito separatamente in questa cartella ed eseguirlo. Lo script è disponibile nel seguente collegamento alla casella:

https://pubhub.devnetcloud.com/media/wireless-troubleshooting-tools/docs/9800-scripts/ap_detection_script.zip

In questo modo viene creato un file nella stessa cartella con il nome "Status_check_results.log". L'elenco contiene punti di accesso che potrebbero essere in uno stato di problema e che richiederebbero alcune operazioni di ripristino/extra prima di procedere con l'aggiornamento.

Processo di ripristino:

In base allo stato corrente di ciascun punto di accesso ritenuto problematico, lo script fornisce inoltre indicazioni su quale sia il modo più ottimizzato per ripristinare tali punti di accesso. Di seguito sono riportati i passaggi dettagliati che è necessario eseguire per ciascuna opzione.

Opzione 1: Scambio partizione

Passaggio 1: Verificare che l'access point non comunichi con il controller per evitare che l'access point torni alla partizione/versione precedente. A tal fine, è possibile usare un elenco degli accessi sul gateway del controller.

Passaggio 2: Dai punti di accesso potenzialmente interessati, configurare l'avvio per la partizione 2:

```
AP# config boot path 2
```

Passaggio 3: Riavviare l'access point per eseguirne l'avvio con l'immagine nella partizione 2:

```
AP# reset
```

Passaggio 4: Far sì che l'access point si unisca al controller al termine dell'aggiornamento. L'access point si unisce e scarica la nuova immagine.

NOTA: Se per qualsiasi motivo questa opzione non è disponibile, è sempre possibile aprire una

richiesta TAC e procedere con l'opzione 2 anche per questo gruppo di access point.

Opzione 2: Aprire una richiesta TAC per rimuovere TAC dalla shell radice nell'access point (dopo questa procedura, procedere con l'aggiornamento normale)

Opzione 3: stato sicuro ma l'access point ha un'immagine difettosa nella partizione di backup

Gli access point si trovano in questo stato soprattutto dopo il completamento dell'aggiornamento a una versione fissa. Questo stato suggerisce che l'access point sta eseguendo una versione fissa, ma la versione di backup è ancora in stato di bug. Per evitare ogni rischio, si consiglia di sostituire il backup degli access point con una buona immagine, ovvero con una versione in cui il problema non si verifica. A seconda del numero di punti di accesso in questione, è possibile che l'archivio scarichi un'immagine sull'access point o semplicemente esegua un pre-download senza attivarlo.

Opzione 4: Controllo integrità immagine non riuscito per questi punti di accesso

Aprire una richiesta TAC per chiedere al tecnico TAC di correggere gli access point prima di procedere con l'aggiornamento.

Opzione 5: Controllo integrità immagine non riuscito per questi punti di accesso

La partizione corrente non è suscettibile, ma la memoria flash è insufficiente. Si consiglia di aprire un TAC per pulire il file cnssdaemon.log dallo storage tramite devshell.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).