Validation et récupération des points d'accès Catalyst sur 17.12 affectés par une défaillance de mise à niveau

Table des matières

Introduction

Ce document décrit la procédure de récupération quand vous êtes affecté par l'ID de bogue Cisco CSCwf25731 et CSCwf37271

Points d'accès affectés

Ces modèles de point d'accès sont affectés. si vous n'utilisez pas les modèles ci-dessous, vous n'êtes pas affecté et aucune autre action n'est requise :

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

- Catalyst 9164I

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

Contexte

Les mises à niveau de systèmes qui ont été disponibles sur 17.12.4/5/6a vers n'importe quelle version peuvent entraîner l'entrée d'une boucle de démarrage dans certaines conditions, déclenchée par un échec de l'installation de l'image en raison d'un espace disque insuffisant sur le stockage du périphérique cible. Ce scénario ne se produit que lors d'une opération de mise à niveau impliquant des points d'accès, par exemple ISSU, l'installation d'une image complète du contrôleur ou APSP, et n'a pas d'impact sur un service normal, les opérations quotidiennes ou les installations SMU.

Des étapes supplémentaires sont requises avant d'effectuer une mise à niveau sur les points d'accès éventuellement affectés. Ce problème n'a pas de solution de contournement et ne dépend pas de la configuration, du type de déploiement ou du modèle de contrôleur

Ce problème n'affecte pas les versions antérieures à 17.12.4, ou si le point d'accès exécute une version postérieure à 17.12.6a, par exemple 17.15.x et qu'il n'a jamais installé aucune des versions affectées.

Un correctif est disponible pour les versions 17.12.4, 17.12.5 et 17.12.6a de Cisco IOS XE, sous la forme de protocoles APSP respectifs. En outre, un APSP de nettoyage est disponible pour 17.15.4d et 17.18.2, pour récupérer l'espace perdu, pour les déploiements qui utilisaient la version concernée, et ont déjà mis à niveau vers une version ultérieure.

Si votre réseau a déjà été dans l'une des versions concernées ou si vous n'êtes pas sûr que le réseau ait utilisé ces versions précédemment, il est recommandé d'effectuer les vérifications avant toute mise à niveau par précaution

Détails de la cause première

Les points d'accès des modèles affectés, exécutant les codes 17.12.4 à 17.12.6a, créent un fichier persistant « /storage/cnssdaemon.log », qui peut atteindre 5 Mo par jour, et utilisent tout l'espace disponible sur cette partition de disque. Ce fichier n'est pas effacé au redémarrage. Une fois la partition entièrement utilisée, les mises à niveau peuvent échouer, car une étape critique du stockage de la nouvelle version du fichier n'est pas terminée.

Le problème a été introduit par une mise à jour de bibliothèque, qui a modifié la destination du journal pour un composant interne. Le fichier journal n'est pas nécessaire au fonctionnement du périphérique

L'échec de la mise à niveau ne se produit que si l'AP est exécuté à partir de la partition 1 et que l'espace de la partition 2 est épuisé. Si l'espace est suffisant ou si le point d'accès a démarré à partir de la partition 2, la mise à niveau est réussie

Procédure de vérification de mise à niveau

Si le WLC est actuellement sur 17.12.4, 17.12.5, 17.12.6a, la mise à niveau est obligatoire vers une version du logiciel avec le correctif tout en suivant les étapes ci-dessous. Pour toutes les autres versions installées sur le WLC, si vous prévoyez de mettre à niveau,il est fortement recommandé de suivre ces instructions :

Étape 1: Vérifiez si les points d'accès sont susceptibles d'être affectés (reportez-vous au tableau 1). S'il n'est pas affecté, aucun processus de vérification préalable/récupération n'est requis et vous pouvez procéder directement à la mise à niveau vers l'une des dernières versions.

Étape 2: Si vous êtes concerné, effectuez des vérifications préalables pour identifier le nombre de points d'accès affectés dans la section Prévérifications.

Étape 3: Sur les points d'accès identifiés, exécutez les étapes de récupération décrites dans la section de récupération.

Étape 4: Exécutez à nouveau la vérification préalable pour confirmer qu'aucun autre point d'accès n'est affecté.

Étape 5: Procédez à la mise à niveau vers les versions APSP ou logicielles respectives mentionnées dans le tableau Versions fixes.

Veuillez vous reporter à ce tableau pour vérifier si la présente note s'applique à vous :

Tableau 1 - Applicabilité du chemin de mise à niveau

Version actuelle	Target	Applicabilité du problème	Avant la mise à niveau Precheck requise	Chemin cible/mise à niveau	Prévérification de mise à niveau	Commentaires
17,3 x / 17,6 x / 17,9 x	17.12.x	Non	Non	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	Non	Vérifier la destination Notes de version
17.9.x.	Tout (sauf 17.12.4/5/6a)	Non	Non	Suivre le chemin de mise à	Non	17.9,1 à .5 ne prennent pas en charge la mise à

				niveau		niveau directe vers 17.15, utilisez 17.9.6 ou une version ultérieure Pour plus d'informations, consultez les notes de version
17.12.1 à 17.12.3	Tout (sauf 17.12.4/5/6a)	Non	Non	Suivre le chemin de mise à niveau	Processus régulier	Vérifier la destination Notes de version
17.12.4/5/6a	17.12.x(4,5,6a, etc.), APSP	Oui	Oui	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	Oui	Après l'installation d'un APSP fixe, aucune vérification supplémentaire n'est nécessaire pour les futures mises à niveau de la version 17.12
17.12.4/5/6a	17.15.x / 17.18.x	Oui	Oui	Mettre à niveau l'APSP 17.12.x respectif, puis mettre à niveau vers 17.15.x + APSPx ou 17.18.x + APSPx	Oui pour la première mise à niveau APSP 17.12 et Non pour les mises à niveau suivantes.	
Toute version,	17.15.x	Oui	Oui	17.15.x + APSPx	Oui	

image précédente était l'un de 17.12.4/5/6a						
Toute version, image précédente était l'un de 17.12.4/5/6a	17.18.x	Oui	Oui	17.18.x + APSPx	Oui	
+ de 17,15 Nouveau déploiement	tous les modèles	Non	Non	tous les modèles	Non	
17.18. Nouveau déploiement	tous les modèles	Non	Non	tous les modèles	Non	

Remarque : En général, si le réseau n'est pas en cours d'exécution et n'a pas exécuté 17.12.4, 17.12.5, 17.12.6a dans le passé, le problème n'est pas applicable

Remarque : Toute autre version qui n'est pas explicitement mentionnée dans la colonne « Actuel » suit le chemin de mise à niveau recommandé.

Versions fixes

Contrôleur	Version de l'image 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

17.15.4b + APSP6	17.15.4.206
17.15.4d + APSP1	17.15.4.225
17.18.1 + APSP3	17.18.1.203
17.18.2 + APSP1	17.18.2.201

Vérifications préalables

Pour déterminer si le réseau est susceptible de rencontrer ce problème, suivez les étapes en cours. Ces étapes aident à fournir une vue d'ensemble, mais pour la détection réelle des AP, veuillez utiliser la section "scripts de vérification préalable" pour automatiser ce processus :

- Vérifiez si les images de point d'accès sont identiques si les versions concernées, sous les colonnes Image principale ou Image de sauvegarde :

```
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
```

- Une vérification similaire peut être effectuée dans le point d'accès :

```
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
```

- Vérifiez la partition de démarrage actuelle :

```
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.
```

- Vérifier l'utilisation actuelle du système de fichiers :

```
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%.
```

- Vérifiez l'intégrité de l'image pour les deux partitions :

```
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
```

Dans la section suivante, nous vous guiderons à travers les scripts qui automatisent le processus de vérification préalable pour tous les AP.

Prévérifier le script

WLAN Poller(téléchargeable ici)

Étape 1: Extrayez le contrôleur WLAN à l'emplacement de fichier souhaité

Étape 2: Modifiez ces valeurs dans le fichier « 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
```

Étape 3 : Commentez le reste du contenu par défaut et la liste de commandes ci-dessous pour les fichiers « cmdlist_cos » et « cmdlist_cos_qca ».

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

Exemple ci-dessous :

```
# 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
```

Étape 4 : Exécutez wlanpoller à l'aide de « .\wlanpoller.exe ». L'interrogateur WLAN exécute SSH vers tous les AP et obtient les sorties de ces commandes pour chacun d'eux.

Étape 5: Après l'exécution, un dossier « données » est créé. Entrez le dossier et aller jusqu'à la fin où vous avez plusieurs fichiers créés pour chacun des AP.

Étape 6: Copiez/collez le fichier « ap_detection_script.py » fourni séparément dans ce dossier et exécutez-le. Vous trouverez le script à l'adresse ci-dessous :

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

Ceci crée un fichier dans le même dossier sous le nom « Status_check_results.log ». Ceci a la liste des AP qui pourraient être dans un état potentiellement problématique et nécessiteraient quelques étapes de récupération/supplémentaires avant de continuer avec votre mise à niveau.

Processus de récupération :

En fonction de l'état actuel de chaque point d'accès qui est jugé problématique, le script fournit en outre des indications sur la manière la plus optimisée de récupérer ces points d'accès. Voici les étapes détaillées que vous devez suivre pour chacune des options.

Option 1: Changement de partition

Étape 1: Assurez-vous que le point d'accès n'a pas de communication avec le contrôleur pour éviter que le point d'accès ne revienne à sa partition/version précédente. Ceci peut être réalisé par une liste d'accès sur la passerelle du contrôleur.

Étape 2: À partir des points d'accès potentiellement affectés, configurez le démarrage pour la partition 2 :

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

Étape 3: Redémarrez l'AP pour le faire démarrer avec l'image sur la partition 2 :

```
AP# reset
```

Étape 4: Demandez au point d'accès de joindre le contrôleur après la mise à niveau sur le contrôleur. L'AP se joint et télécharge la nouvelle image.

NOTE: Si cette option n'est pas viable pour une raison quelconque, vous pouvez toujours ouvrir un dossier TAC et continuer avec l'option 2 pour cet ensemble d'AP également.

Option 2: Ouvrez un dossier TAC pour que le TAC nettoie l'AP de l'interpréteur de commandes root (Après ce processus, vous allez de l'avant avec la mise à niveau normale)

Option 3 : état sûr mais AP a une image boguée dans la partition de sauvegarde

Les AP finissent dans cet état principalement après la mise à niveau vers une version fixe a été terminée. Cet état suggère que l'AP exécute une version fixe mais que la version de sauvegarde est toujours boguée. Pour se tromper sur le côté de la prudence, nous recommandons de remplacer la sauvegarde des AP par une bonne image ainsi que c'est-à-dire une version où ce problème n'est pas vu. Selon le nombre d'AP en question, soit archiver télécharger une image sur l'AP ou simplement faire un pré-téléchargement sans l'activer réellement.

Option 4: La vérification de l'intégrité de l'image a échoué pour ces AP

Ouvrez un dossier TAC pour demander à un ingénieur TAC de rectifier ces points d'accès avant de procéder à la mise à niveau.

Option 5: La vérification de l'intégrité de l'image a échoué pour ces AP

La partition actuelle n'est pas sensible, mais le stockage flash est faible. Recommandez d'ouvrir un TAC pour nettoyer le fichier cnssdaemon.log du stockage via le devshell.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.