

Catalyst-AP's valideren en herstellen op 12.12 die zijn beïnvloed door een upgradefout

Inhoud

[Inleiding](#)

[Betrokken toegangspunten](#)

[context](#)

[Root Cause Details](#)

[Controleprocedure voor upgrade](#)

[Vaste releases](#)

[Controles vooraf](#)

[Vooraf controleren, script](#)

[WLAN Poller \(kan hier worden gedownload\)](#)

[Herstelproces:](#)

[Optie 1: Partitieswap](#)

[Optie 2: Open een TAC-geval om TAC de AP van de wortelschaal te laten opruimen \(na dit proces gaat u verder met de normale upgrade\)](#)

[Optie 3: Veilige status, maar AP heeft een fout-image in de back-uppartitie](#)

[Optie 4: Controle van de integriteit van het image is mislukt voor deze toegangspunten](#)

[Optie 5: Controle van de integriteit van het image is mislukt voor deze toegangspunten](#)

Inleiding

In dit document wordt de herstelprocedure beschreven wanneer u last hebt van Cisco-bug-ID [CSCwf25731](#)  en [CSCwf37271](#) .

Betrokken toegangspunten

Deze Access Point-modellen worden beïnvloed, als u de onderstaande modellen niet gebruikt, wordt u niet beïnvloed en zijn geen verdere acties vereist:

- Katalysator 9124 (I/D/E)
- Katalysator 9130 (I/E)
- Katalysator 9136I
- Katalysator 9162I
- Katalysator 9163E
- Katalysator 9164I

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

context

Upgrades van systemen die op 17.12.4/5/6a zijn geïnstalleerd naar elke release kunnen ertoe leiden dat specifieke Access Points-modellen onder bepaalde omstandigheden een opstartlus binnengaan, veroorzaakt door een fout bij de installatie van het image als gevolg van onvoldoende schijfruimte op de opslaglocatie van het doelapparaat. Dit scenario treedt alleen op tijdens een upgradebewerking met toegangspunten, bijvoorbeeld ISSU, installatie van een volledig controllerimage of APSP, en heeft geen invloed op een normale service, dagelijkse werking of SMU-installaties.

Extra stappen zijn vereist voordat u een upgrade uitvoert op de mogelijk getroffen toegangspunten. Dit probleem heeft geen oplossing en is niet afhankelijk van de configuratie, het implementatietype of het controllermodel

Dit probleem heeft geen invloed op versies vóór 17.12.4 of als het toegangspunt een release uitvoert na 17.12.6a, bijvoorbeeld 17.15.x en het nooit een van de getroffen versies heeft geïnstalleerd.

Er is een fix beschikbaar voor Cisco IOS XE releases 17.12.4, 17.12.5, 17.12.6a, in de vorm van respectieve APSP's. Daarnaast is er een opruimings-APSP beschikbaar voor 17.15.4d en 17.18.2, om de verloren ruimte te herstellen, voor die implementaties die de getroffen release gebruikten en al zijn geüpgraded naar een latere versie.

Als uw netwerk op een bepaald moment op een van de getroffen releases is geweest of als u niet zeker weet of het netwerk deze versies eerder heeft gebruikt, wordt het aanbevolen om de controles uit te voeren voordat een upgrade wordt uitgevoerd als voorzorgsmaatregel

Root Cause Details

Toegangspunten van de getroffen modellen, met de codes 17.12.4 tot 17.12.6a, maken een permanent bestand `"/storage/cnssdaemon.log"`, dat kan groeien tot 5 MB per dag, en gebruiken alle beschikbare ruimte op die schijfpartitie. Dit bestand is niet gewist bij het opnieuw opstarten. Zodra de partitie volledig is gebruikt, kunnen upgrades mislukken, omdat een kritieke stap voor het opslaan van de nieuwe bestandsversie niet is voltooid.

Het probleem werd geïntroduceerd door een bibliotheekupdate die de logbestemming voor een interne component wijzigde. Het logbestand is niet nodig voor de werking van het apparaat

De upgradefout treedt alleen op als het toegangspunt vanaf partitie 1 wordt uitgevoerd en de partitie 2-ruimte is opgebruikt. Als er voldoende ruimte is of als AP is opgestart vanaf partitie 2, is de upgrade succesvol

Controleprocedure voor upgrade

Als de WLC momenteel op 17.12.4, 17.12.5, 01.12.6a staat, is een upgrade naar een softwareversie met de oplossing verplicht, terwijl de onderstaande stappen worden gevolgd. Voor alle andere versies die op de WLC zijn geïnstalleerd, als u van plan bent te upgraden, Het wordt ten zeerste aanbevolen om deze instructies te volgen:

Stap 1: Controleer of de toegangspunten mogelijk worden beïnvloed (zie tabel 1). Als dit niet wordt beïnvloed, is er geen pre-check / herstelproces vereist en kunt u direct doorgaan met upgraden naar een van de nieuwste releases.

Stap 2: Als u getroffen bent, voert u voorcontroles uit om het aantal AP's te identificeren dat getroffen is in het gedeelte Voorcontroles.

Stap 3: Voer op de geïdentificeerde toegangspunten de herstelstappen uit die in het gedeelte over herstel worden beschreven.

Stap 4: Voer de voorcontrole opnieuw uit om te bevestigen dat er geen ander toegangspunt is aangetast.

Stap 5: Ga door met het upgraden naar de respectieve APSP's of softwareversies die in de tabel met vaste versies worden genoemd.

Raadpleeg deze tabel om te controleren of deze kennisgeving op u van toepassing is:

Tabel 1 - Toepasselijkheid upgradepad

Huidige versie	doel	Toepasselijkheid van probleem	Voor upgrade is een precheck vereist	Doel-/upgradepad	Upgrade vooraf controleren	Opmerkingen
17,3,x / 17,6,x / 17,9 x	17,12 x	Nee	Nee	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	Nee	Releasebrieken bestemming controleren
17,9,x	Alle (behalve 17.12.4/5/6a)	Nee	Nee	Upgradepad voor bestemming volgen	Nee	17.9,1 tot en met .5 ondersteunen geen directe upgrade naar

						17.15, gebruik 17.9.6 of hoger Voor meer informatie zie release notes
17.12.1 tot en met 17.12.3	Alle (behalve 17.12.4/5/6a)	Nee	Nee	Upgradepad voor bestemming volgen	regulier proces	Releasebrieven bestemming controleren
17.12.4/5/6a	17.12.x (4,5,6a enz.), APSP	Ja	Ja	17.12.4 + APSPx 17.12.5 + APSPx 17.12.6a + APSPx 17.12.7	Ja	Na het installeren van een vaste APSP zijn er geen extra voorcontroles nodig voor toekomstige 10 .12 upgrades
17.12.4/5/6a	17,15 x / 17,18 x	Ja	Ja	Upgrade de respectieve 17.12.x APSP en upgrade vervolgens naar 17.15.x + APSPx of 17.18.x + APSPx	Ja voor de eerste 10 .12 APSP-upgrade en Nee voor de volgende upgrades.	
Elke release, vorige afbeelding was er een van 17.12.4/5/6a	17 15 x	Ja	Ja	17.15.x + APSPx	Ja	
Elke release, vorige afbeelding	17,18 x	Ja	Ja	17.18.x + APSPx	Ja	

was er een van 17.12.4/5/6a						
17,15+ Nieuwe implementatie	Alle	Nee	Nee	Alle	Nee	
17.18. Nieuwe implementatie	Alle	Nee	Nee	Alle	Nee	

Opmerking: in het algemeen geldt dat als het netwerk niet actief is en in het verleden niet 17.12.4, 17.12.5, 17.12.6a is uitgevoerd, het probleem niet van toepassing is

Opmerking: elke andere release die niet expliciet wordt vermeld in de kolom "Huidig" volgt het aanbevolen upgradepad.

Vaste releases

controleur	AP Image-versie
17 12,4 + APSP13	17.12.4.213
17 12,5 + APSP9	17.12.5.209
17 12,6 bis + APSP1	17.12.6.201
17 15,3 + APSP12	17.15.3.212
17,15,4 b + 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

Controles vooraf

Voer de huidige stappen uit om te evalueren of het netwerk gevoelig is voor dit probleem. Deze stappen helpen een overzicht te bieden, maar voor de daadwerkelijke detectie van toegangspunten kunt u de sectie "Precheck-scripts" gebruiken om dit proces te automatiseren:

- Bevestig onder Primaire of Back-upkoppen of de images van het toegangspunt er een zijn als de getroffen images vrijkomen:

```
9800-1#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

- Een soortgelijke verificatie kan worden uitgevoerd in het toegangspunt:

```
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

- Huidige opstartpartitie controleren:

```
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.

- Het huidige bestandssysteemgebruik controleren:

```
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%.

- Controleer de integriteit van het image voor beide partities:

```
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

In de volgende sectie doorlopen we de scripts die het voorcontroleproces voor alle toegangspunten automatiseren.

Vooraf controleren, script

WLAN Poller(Kan [hier](#) worden gedownload)

Stap 1: Pak de WLAN Poller uit naar de gewenste bestandslocatie

Stap 2: Wijzig deze waarden in het bestand "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
```

Stap 3: Geef commentaar op de rest van de standaardinhoud en de onderstaande lijst met opdrachten voor de bestanden "cmdlist_cos" en "cmdlist_cos_qca".

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

Steekproef hieronder:

```
# 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
```

Stap 4: Voer de wlanpoller uit met ".\wlanpoller.exe". De WLAN-poller draait SSH naar alle toegangspunten en krijgt de uitgangen van deze opdrachten voor alle toegangspunten.

Stap 5: Na de uitvoering wordt een "data" map aangemaakt. Voer de map in en ga helemaal tot het einde waar u meerdere bestanden hebt gemaakt voor elk van de toegangspunten.

Stap 6: Kopieer/plak de afzonderlijk verstrekte "ap_detection_script.py" in deze map en voer deze uit. U kunt het script vinden op de onderstaande Box link:

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

Hierdoor wordt een bestand in dezelfde map gemaakt met de naam "Status_check_results.log". Dit bevat de lijst met toegangspunten die mogelijk in een problematische staat verkeren en waarvoor een aantal herstel-/extra stappen nodig zijn voordat u doorgaat met uw upgrade.

Herstelproces:

Op basis van de huidige status van elk toegangspunt waarvan is vastgesteld dat deze problematisch is, zou het script verdere richtlijnen bieden over wat de meest geoptimaliseerde manier zou zijn om deze toegangspunten te herstellen. Hier zijn de gedetailleerde stappen die u zou moeten nemen voor elk van de opties.

Optie 1: Partitieswap

Stap 1: Zorg ervoor dat het toegangspunt geen communicatie heeft met de controller om te voorkomen dat het toegangspunt terugkeert naar de vorige partitie/versie. Dit kan worden bereikt door middel van een toegangslijst op de controllergateway.

Stap 2: Configureer vanaf de mogelijk getroffen toegangspunten het opstarten voor partitie 2:

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

Stap 3: Start het toegangspunt opnieuw op om het op te starten met het image op partitie 2:

```
AP# reset
```

Stap 4: Laat het toegangspunt lid worden van de controller nadat de upgrade op de controller is voltooid. Het toegangspunt wordt lid en downloadt het nieuwe image.

OPMERKING: Als u deze optie om welke reden dan ook niet kunt gebruiken, kunt u altijd een

TAC-kwestie openen en doorgaan met optie 2 voor deze set toegangspunten.

Optie 2: Open een TAC-geval om TAC de AP van de wortelschaal te laten opruimen (na dit proces gaat u verder met de normale upgrade)

Optie 3: Veilige status, maar AP heeft een fout-image in de back-uppartitie

De toegangspunten komen meestal in deze staat terecht nadat de upgrade naar een vaste versie is voltooid. Deze status suggereert dat het toegangspunt een vaste versie heeft, maar dat de back-upversie nog steeds buggy is. Als u de fout wilt maken, raden we u aan de back-up van toegangspunten ook te vervangen door een goed image, d.w.z. een versie waarin dit probleem niet wordt gezien. Afhankelijk van het aantal toegangspunten in kwestie, kunt u een afbeelding archiveren of downloaden naar het toegangspunt of gewoon een pre-download uitvoeren zonder deze daadwerkelijk te activeren.

Optie 4: Controle van de integriteit van het image is mislukt voor deze toegangspunten

Open een TAC-kwestie zodat de TAC-technicus deze AP's kan corrigeren voordat u doorgaat met de upgrade.

Optie 5: Controle van de integriteit van het image is mislukt voor deze toegangspunten

De huidige partitie is niet gevoelig, maar de flashopslag is laag. Aanbevolen om een TAC te openen om het bestand cnssdaemon.log uit de opslag op te ruimen via de devshell.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.