安全升級存取點，避免造成開機回圈的影像損毀

目錄

簡介

某些思科存取點(AP)可能會透過CAPWAP從9800系列控制器下載損壞的映像。 根據AP的軟體版本，AP可能會嘗試引導損壞的映像，從而導致引導循環。 本文說明哪些AP型號和哪些網路路徑容易出現映像損壞，以及如何安全地升級。

如果AP此時由於此問題處於引導環路中，請參閱從由Wave 2和11ax存取點上的映像損壞引起的引導環路恢復(CSCvx32806)一文以獲取有關恢復步驟的指導。

如何判斷升級是否容易發生映像損壞

如果以下情況與您的部署有關，則您的AP可能容易下載損壞的軟體，然後嘗試啟動該軟體：

未受影響的產品

- 無線區域網控制器(WLC)：從AireOS無線區域網控制器下載的存取點不受影響
- Mobility Express、嵌入式無線控制器

- AP - Aironet 1800/1540/1100AC系列Wave 2 11ac和Wave1 11ac存取點(1700/2700/3700/1570/IW3700)不受影響（即使這些AP註冊到9800 WLC，它們也不受影響）
- 自2023年起推出的Wi-Fi 6E AP：IW9167、IW9165、C9163

受影響的產品

- WLC：從Cisco Catalyst 9800系列無線區域網控制器下載的AP可能會受到影響
- AP：註冊到Cisco Catalyst 9800系列無線區域網控制器的以下AP型號受到影響：
  - Aironet Wave2 11ac存取點(2800/3800/4800/1560/IW6330/ESW6300)
  - Catalyst 9100系列Wi-Fi6存取點(9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
  - Catalyst 9100系列Wi-FI6E存取點(9136/9162/9164/9166)

受影響的版本：啟動不良映像綜合症

AP嘗試引導已知已損壞的映象時遇到的此問題由以下Cisco漏洞ID解決：CSCvx32806、CSCwc72021、CSCwd90081，已在以下版本中修復：

- 8.10.185.0及更高版本
- 17.3.7及以上
- 17.6.6及以上
- 17.9.3及以上
- 17.11.1及以上

一旦存取點升級至具有上述修正程式的軟體，仍可能下載損毀的映像；不過，它不會嘗試啟動該映像，而是會繼續重新嘗試下載，直到下載成功為止。

受影響的網路路徑

在9800和AP之間的LAN路徑中（即具有完整1500位元組IP MTU的路徑，具有低延遲和極低資料包丟失的路徑）未發現AP映像損壞問題。 該問題更有可能在WAN上的CAPWAP隧道上發生，具有以下路徑特徵：

- 高資料包丟失
- 低CAPWAP MTU（小於1485位元組） - MTU越小，風險越高
  - 低CAPWAP MTU可能是資料包丟失的症狀

如何判斷您的網路路徑是否處於風險中

- 在9800上，使用

```
<#root>

9800-L#show capwap detailed
```

```
Name         APMAC          SourceIP        SrcPort DestIP          DestPort
MTU
   Mode      McastIf
-------------------------------------------------------------------------------------------------
Capwap1      D4AD.BDA2.8240 192.168.203.203 5247    192.168.6.100   5248
1485
  multicast Mc1
Capwap2      084F.F983.4A40 192.168.203.203 5247    192.168.6.103   5253
1005
  multicast Mc1
```

    - 如果給定AP的MTU出現波動，則這是一個強烈的風險指標
- 或**show ap config general | include CAPWAP\ Path\ MTU** (在show tech-support wireless中)
    - 在9800的「show tech-support wireless」輸出上使用Wireless Config Analyzer Express (WCAE)檢視存取點的MTU（在Access Points > Configuration下）
- 在9800上，使用「show ap uptime」查詢具有較長「AP運行時間」和較短「關聯運行時間」的AP
    - 如果AP沒有理由具有較短的關聯運行時間（即沒有重新配置），則這可能表明存在風險的網路路徑

如何從非固定AP軟體版本安全升級

注意：如果您的部署易受映像損壞的影響（即受影響的AP型號、運行的軟體未解決Boot a Bad Image Syndrome問題、具有風險的WAN特徵），則請勿透過簡單升級9800軟體進行升級，也不要讓AP重新加入和下載新軟體-它們可能會出現映像損壞並進入引導循環。 請改用下列其中一種方法：

使用AP的本地WLC進行升級

如果可能，在AP的LAN上放置暫存控制器-這可以是9800-CL，或（對於Wave 2 / Wi-Fi 6 AP）處於EWC模式的AP，然後將AP升級到目標版本。 然後，他們將能夠安全地加入生產控制器。

透過AireOS控制器升級

如果您的AireOS控制器運行的是8.10.190.0或更高版本，並且AireOS支援您的AP型號，請將AP加入該控制器。 這樣可以安全地將AP升級到固定軟體，然後它們就可以安全地加入生產控制器。

使用archive download-sw升級

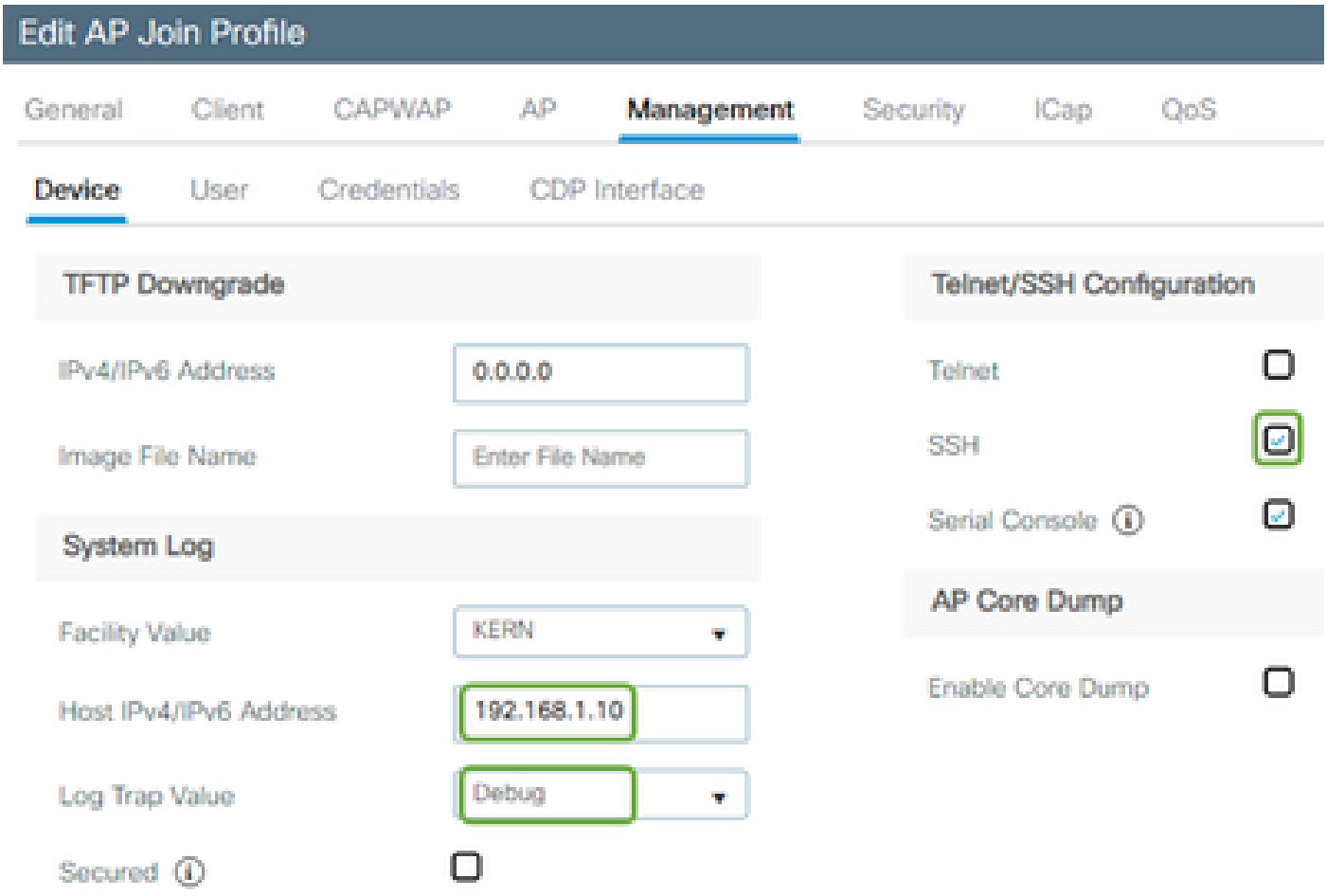
將目標AP映像暫存在升級AP可訪問的TFTP/SFTP伺服器上。 透過TFTP或SFTP進行AP映像升級時不存在映像損壞問題。 AP可以從AP CLI或從控制器CLI啟動映像下載請求（如果AP已加入控制器）。

1. 在AP可訪問的位置設定TFTP或SFTP伺服器。 請注意，TFTP效能受延遲限制，因此，如果TFTP伺服器與AP處於遠端狀態，下載速度會變慢。 由於SFTP使用TCP，因此如果使用高延遲路徑，其吞吐量將大大提高。 但是，無法從WLC觸發SFTP，因為它需要互動式通話方塊來輸入使用者名稱和密碼。
2. 在TFTP或SFTP伺服器上安裝所需的AP映像。 請參閱15.3(3)J* AP版本（對應至想要的IOS-XE版本）的相容性矩陣中的表4，然後從software.cisco.com下載適用於受影響之AP型號的輕量AP軟體映像。
    1. 例如，CW9162的17.9.5 AP映像isap1g6b-k9w8-tar.153-3.JPN4.tar。
3. 透過AP CLI升級：如果可以透過控制檯或SSH訪問AP的CLI：
    1. 輸入TFTP或SFTP命令：
       archive download-sw /no-reload tftp://<*ip-address*>/<*apimage*>
       或
       archive download-sw /no-reload sftp://<*ip-address*>/<*apimage*>
       使用者名稱：使用者
       密碼：*XXX*
       這將用有效映像覆蓋損壞的映像。
    2. 映像下載完成後，發出：
       test capwap restart
       這將重新啟動CAPWAP進程，以便AP能夠辨識新安裝的映像。
    3. 要透過「archive download-sw」升級大量AP，而不是在每個AP中單獨輸入命令，您可以使用指令碼編寫方法。 請參閱下面的透過WLAN輪詢器升級AP。
4. 如果AP已加入控制器，您可以從控制器CLI升級AP（僅限TFTP）：
    1. 在IOS-XE中：**ap nameAPNAMEtftp-*downgradeip.addr.of.server imagename.tar***
    2. 在AireOS中：**config ap tftp-downgradeip.addr.of.server imagename.*tarAPNAME***
        1. 雖然從AireOS下載的CAPWAP不易出現映像損壞，但如果您計畫將AP從AireOS遷移到9800，則應在將AP加入9800之前，先下載包含Alt-boot和Boot a Bad Image症候群（8.10.190.0或更高版本）修復的AP映像。
    3. 監控TFTP或SFTP伺服器日誌，驗證每個AP是否已成功下載映像。 下載完成後，每個AP將重新載入，運行新下載的映像。

透過Predownload升級AP，監控錯誤

在9800上載入目標映像，並使用AP預下載將新映像推入AP，同時監控AP映像損壞的例項。

步驟 1.驗證是否已在C9800 WLC上的AP加入配置檔案下啟用SSH。 在網路中設定系統日誌伺服器。在AP Join Profile for all sites下配置Syslog伺服器的IP地址，並將日誌陷阱值設定為Debug。驗證系統日誌伺服器是否正在從AP接收系統日誌。



步驟 2.將軟體映像下載到C9800 WLC以準備透過CLI進行預下載：

```
C9800# copy tftp://x.x.x.x/C9800-80-universalk9_wlc.17.03.07.SPA.bin bootflash:
C9800# install add file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
```

步驟 3.在Cisco C9800 WLC上運行AP映像預下載：

```
C9800# ap image predownload
```

注意：根據部署的規模和型別，這可能需要幾分鐘到幾小時不等。 在驗證控制器或AP的映像是否有效之前，請勿將其重新啟動！

步驟 4. 完成所有AP的預下載後，檢查系統日誌伺服器上是否出現以下兩種日誌消息之一：

- 映像簽名驗證成功。
- 映像簽名驗證失敗： -3

此外，請檢查**show ap image summary**命令的輸出，並檢查Failed to Download的所有例項。

如果計數器不為零，則透過show ap image查詢出現故障的AP | include Failed。

注意：如果任何AP記錄映像簽名驗證失敗，或者有任何AP下載失敗，則請勿繼續升級過程。如果所有AP都顯示了「Image signing verify success」消息，則所有AP都已正確下載該映像，您可以安全地繼續9800升級。

步驟5.如果任何AP顯示驗證失敗或下載失敗，則為避免引導循環，您需要使用以下過程用單獨的AP映像的存檔下載覆蓋AP的備份分割槽中的映像。

如果故障的AP數量很小，則只需透過SSH連線到每個AP並啟動以下步驟。

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

注意：需要「測試capwap重新啟動」，以便AP的CAPWAP進程能夠辨識備份分割槽中的映像已更新。 這會導致與9800的CAPWAP連線重新啟動時，服務短暫中斷。 如果這是操作問題，可將此步驟延遲到維護窗口。

使用WLAN輪詢器升級AP

如果要透過archive download-sw升級的AP數量較大，您可以使用WLAN輪詢器自動進程。

步驟1a.在Mac或Windows電腦上安裝WLAN輪詢器。

步驟1b.使用相關故障AP填充aplist csv檔案。

步驟1c.使用以下命令填充cmdlist檔案（您可以隨時自行決定增加更多內容）：

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

步驟1d.執行WLAN輪詢器。

步驟1e.執行完成後，請檢查每個AP的日誌檔案以驗證是否成功完成。

步驟 2.立即啟用C9800 WLC上的映像並重新載入。

```
C9800#install activate file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
- Confirm reload when prompted
```

步驟3.在C9800 WLC上提交映像。跳過此步驟將導致WLC回滾到以前的軟體映像

```
C9800#install commit
```

常見問題

問：幾天前我運行了一個預下載，但尚未重新啟動我的Cisco C9800 WLC和AP。我沒有系統日誌來驗證映像是否已損壞。如何驗證映像是否已損壞？

A.在AP/syslog上選中show logging。如果在show logging輸出中看不到成功或失敗消息，可以使用「show flash syslogs」命令在執行預下載時存檔中的系統日誌輸出。 如果您看到「Image signing verify success」消息，則表明此AP已成功下載映像。

問：我有一個使用本地模式的AP的集中部署。我是否仍需要執行「解決方法/解決方案」部分列出的步驟？

答：僅當透過WAN連線升級AP時，才會報告此問題。如果確信控制器與AP之間的資料包丟失非常少，則本地模式或本地網路上的AP極不可能遇到此問題，因此升級時不需要遵循此過程。

問：我擁有全新的開箱即用AP。如何部署它們而不遇到此問題？

答：除非在2023年12月以後生產，否則透過廣域網下載代碼的新開箱即用AP也容易出現此問題。

問：從9800下載的CAPWAP映像損壞後，思科長期採用什麼措施來解決此問題？

答：當AP已經運行17.11或更高版本時，它可以使用帶外映像下載功能使用HTTPS從控制器中提取映像。TCP使用滑動窗口可靠地傳輸資料，因此在WAN上傳輸資料的速度也比CAPWAP（或TFTP）快得多

問：我有AP現在處於引導環路中。 如何恢復它們？

答：請參閱文章「Recover from a boot loop caused by image corruption on Wave 2 and 11ax Access Points (CSCvx32806

)」。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。