Informazioni sugli aggiornamenti delle immagini dei punti di accesso per le distribuzioni remote

Sommario

Introduzione

Questo documento descrive i metodi per aggiornare in modo efficiente le immagini Cisco AP sulle WAN, risolvendo i problemi di latenza e affidabilità.

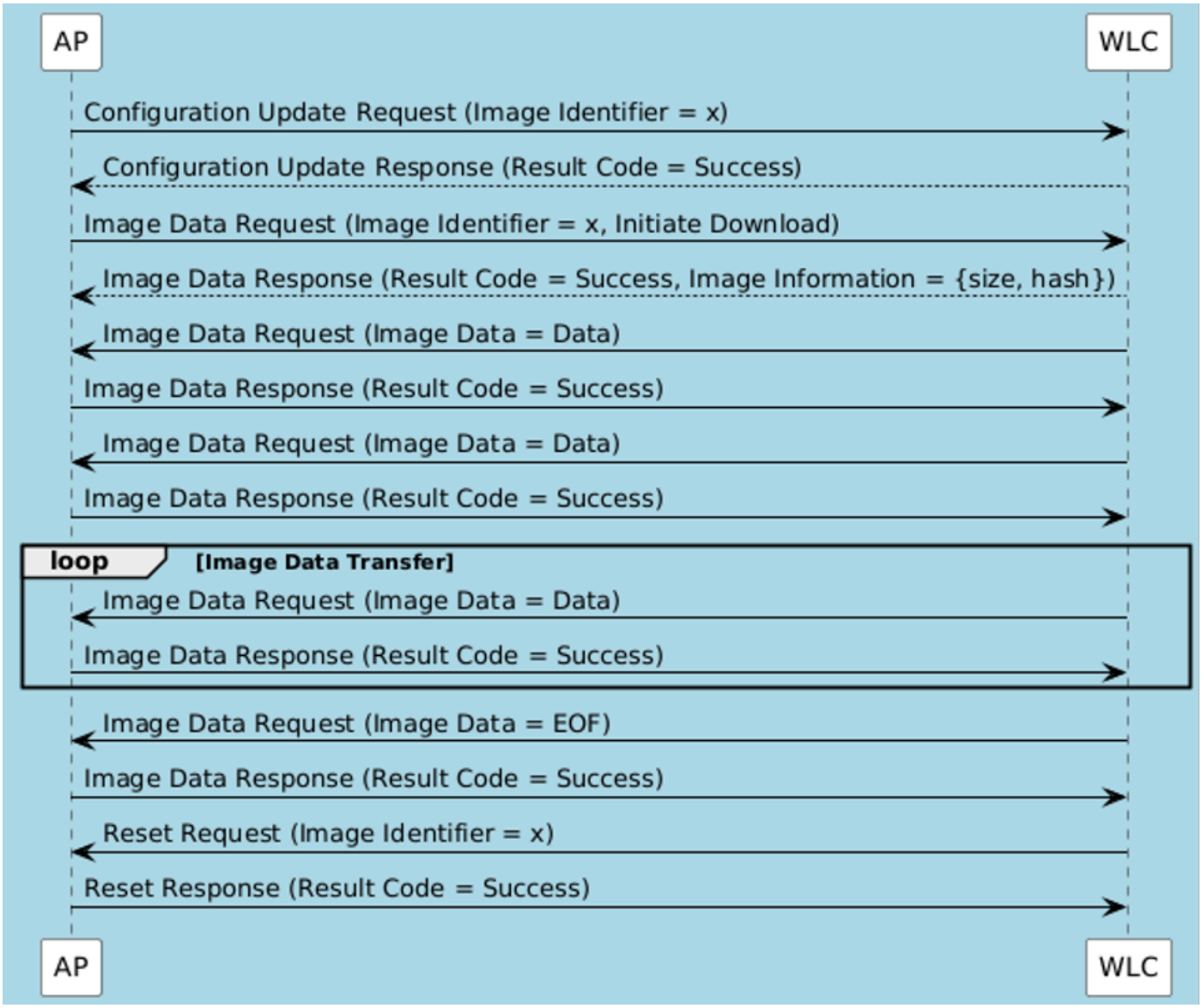
Metodi di aggiornamento delle immagini dei Cisco Access Point

Gli aggiornamenti regolari delle immagini sono essenziali per i Cisco Access Point (AP), ma l'esecuzione di tali aggiornamenti su collegamenti WAN (Wide Area Network) ad alta latenza a siti remoti può essere problematica. Il metodo standard di download delle immagini CAPWAP, sebbene efficace nelle reti locali, può essere lento e potenzialmente meno affidabile sulle WAN. In questa sezione vengono illustrati i motivi per cui ciò si verifica e vengono descritti metodi alternativi e avanzati progettati per aggiornamenti remoti efficienti.

La sfida: Download dell'immagine CAPWAP standard su WAN

Il processo fondamentale per l'aggiornamento dell'immagine AP tramite CAPWAP è definito nella RFC 5415, sezione 9.1. Questo meccanismo consente al controller WLC (Wireless LAN Controller) di servire la nuova immagine AP direttamente ai punti di accesso collegati tramite il tunnel CAPWAP. Per ogni messaggio Image Data Request (RFC 5415, sezione 9.1.1) contenente un blocco di dati del firmware, il WLC attende un riconoscimento Image Data Response (RFC 5415, sezione 9.1.2) corrispondente dall'access point prima di inviare il blocco successivo.

Nell'immagine è illustrato il processo di trasferimento dell'immagine tra l'access point e il WLC quando l'access point è in stato di esecuzione.



Flusso del processo di trasferimento delle immagini AP

Come osservato, il WLC invia messaggi Image Data Request contenenti blocchi di dati dell'immagine del firmware. L'access point conferma la ricezione di questi blocchi inviando messaggi Image Data Response. Questo scambio continua fino al trasferimento dell'intera immagine.

Per ogni messaggio Image Data Request, è previsto un messaggio Image Data Response corrispondente come conferma. Questo significa che l'access point deve attendere l'arrivo di ciascun pacchetto immagine, riconoscerlo e quindi attendere il pacchetto successivo. Questo comporta una lentezza nel download delle immagini negli ambienti WAN.

Prendiamo in considerazione un esempio: Se il tempo di andata e ritorno (RTT) tra l'access point e il WLC è 100 ms, la velocità di trasferimento viene limitata a circa 10 pacchetti al secondo. Se ogni pacchetto ha una dimensione di 1000 byte, il throughput è massimo di 10 KB/sec. Se l'immagine AP è 50 MB, il tempo minimo teorico per completare il trasferimento è di circa 5120 secondi. Ciò dimostra che, anche se la larghezza di banda è notevole, il download dell'immagine CAPWAP può essere lento a causa di questo meccanismo di riconoscimento dell'attesa e dell'interruzione. Questo effetto è meno evidente nei trasferimenti di immagini locali dove il WLC e

l'AP fanno parte della stessa rete del campus e la latenza è minima.

Attenzione: Un collegamento WAN con perdita di dati può potenzialmente portare al danneggiamento dell'immagine. Vedere bug Cisco IDCSCwf09053 per ulteriori informazioni.

Per ridurre queste limitazioni inerenti al meccanismo di trasferimento dei percorsi di controllo CAPWAP standard, in particolare in ambienti WAN con latenza elevata o larghezza di banda limitata, sono stati introdotti tre miglioramenti.

1. Le migliorie apportate alla finestra CAPWAP migliorano il percorso di controllo CAPWAP stesso implementando una finestra scorrevole a più pacchetti, consentendo l'invio di più pacchetti di dati prima della richiesta di conferma, aumentando la velocità di trasmissione sui collegamenti ad alta latenza all'interno del framework CAPWAP.
2. L'aggiornamento efficiente dell'immagine in modalità FlexConnect è un metodo ottimizzato appositamente progettato per i punti di accesso FlexConnect, spesso implementati nelle filiali con larghezza di banda WAN limitata. Questo metodo riduce al minimo il carico WAN distribuendo l'attività di download dell'immagine.
3. Il metodo di download dell'immagine AP basata su HTTP fuori banda si basa su un protocollo HTTP separato e più efficiente in esecuzione su un server Web dedicato sul controller per il trasferimento dell'immagine, spostandolo all'esterno del tunnel di controllo CAPWAP restrittivo.

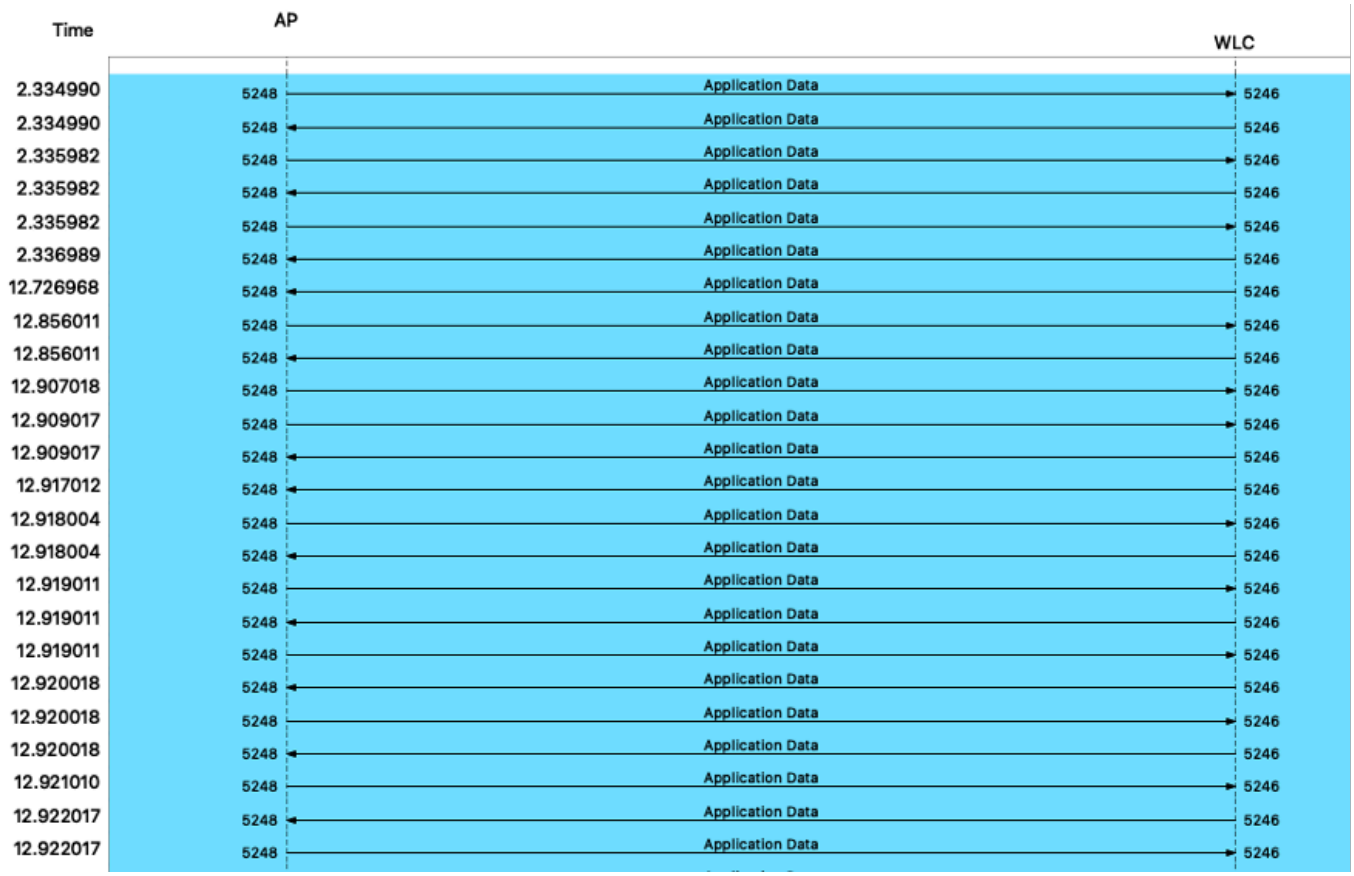
Miglioramenti della finestra di download dell'immagine CAPWAP

Questa funzione migliora la velocità di download delle immagini basate su CAPWAP in modo specifico per i punti di accesso Office Extend (OEAP) o Teleworker AP. Affronta il limite del canale di controllo CAPWAP standard con una singola finestra, che richiede la conferma per ogni pacchetto prima di inviare il successivo, rallentando i trasferimenti sui collegamenti ad alta latenza. Questo miglioramento aggiunge il supporto per più finestre scorrevoli per i pacchetti di controllo.

Impatto delle dimensioni della finestra CAPWAP

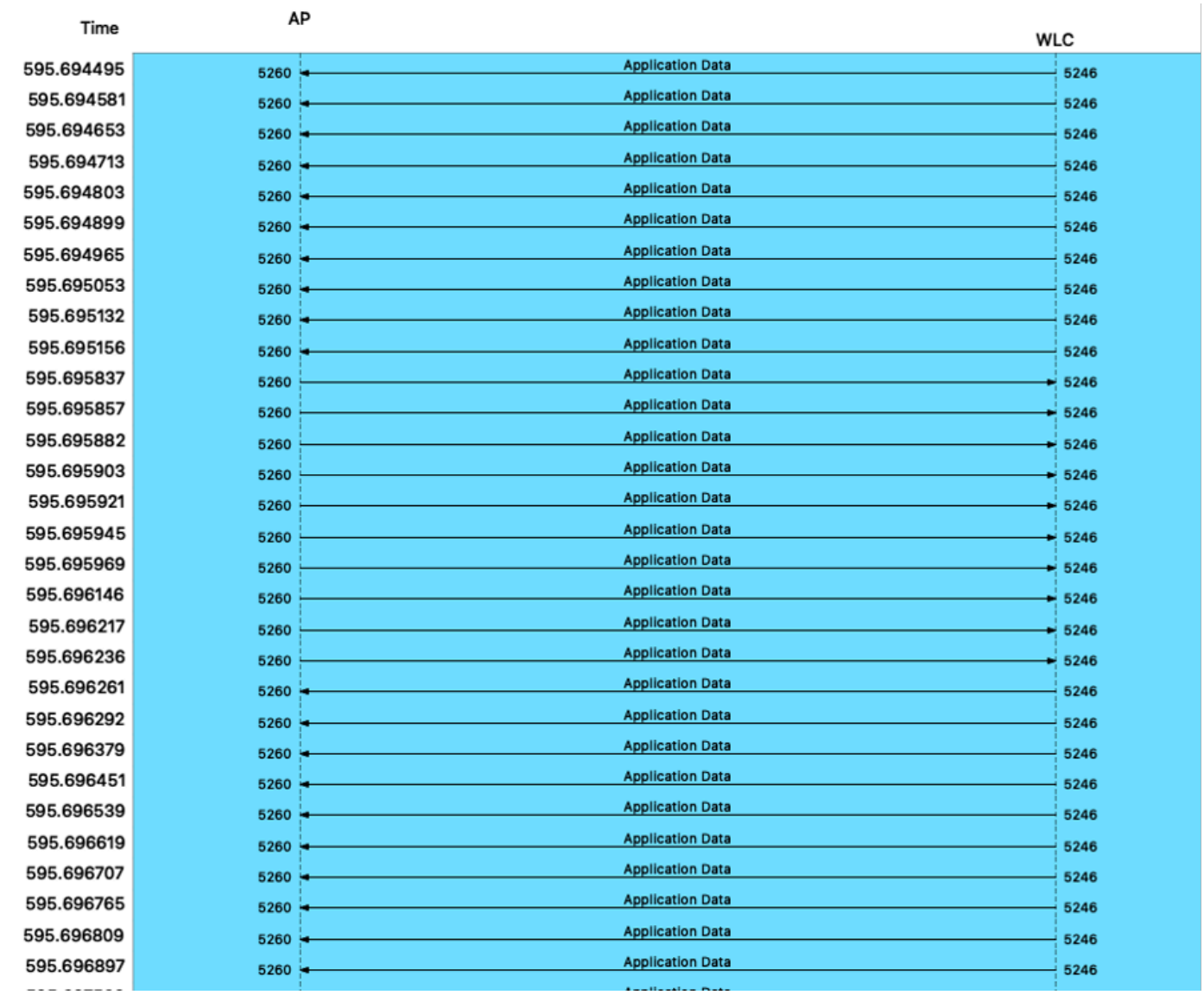
L'efficienza del processo di download delle immagini CAPWAP sul canale di controllo è influenzata in modo significativo dalle dimensioni configurate della finestra, in particolare sui collegamenti ad alta latenza.

Con CAPWAP Window Size = 1 (Predefinito/Standard): Il flusso del pacchetto mostra un comportamento "stop-and-wait" rigoroso. Per ogni pacchetto Image Data Request inviato dal WLC, il WLC si interrompe e attende una conferma di risposta dati dell'immagine dall'access point prima di inviare il pacchetto successivo.



Flusso di aggiornamento dell'immagine CAPWAP con finestra di dimensioni 1

Con CAPWAP Window Size = N (ad esempio, 20): Il flusso del pacchetto mostra un meccanismo a finestra scorrevole. Consentendo a più pacchetti di passare attraverso il collegamento prima di richiedere una conferma, la finestra scorrevole maschera efficacemente la latenza.



Flusso di aggiornamento dell'immagine CAPWAP con finestra di dimensioni 20

Panoramica del processo

1. Configurare un profilo AP specifico per i punti di accesso OEAP/Teleworker.
2. Impostare una dimensione della finestra CAPWAP maggiore di 1 all'interno di questo profilo.
3. Associare il profilo AP agli access point OEAP/Teleworker.
4. Durante il processo di aggiunta al punto di accesso, viene applicata la dimensione configurata della finestra.
5. I successivi download di immagini CAPWAP utilizzano le dimensioni maggiori della finestra, migliorando la velocità di trasmissione.

Configuration (CLI)

Configurare un profilo AP e impostare le dimensioni della finestra CAPWAP:

<#root>

```
configure terminal ap-profile capwap window size
  <- Between 3 to 20
end
```

Associare il profilo AP a un tag del sito e applicarlo agli access point (in modo simile ai passaggi 2 e 3 di Aggiornamento immagine efficiente, assicurandosi che il profilo AP corretto sia collegato tramite il tag del sito).

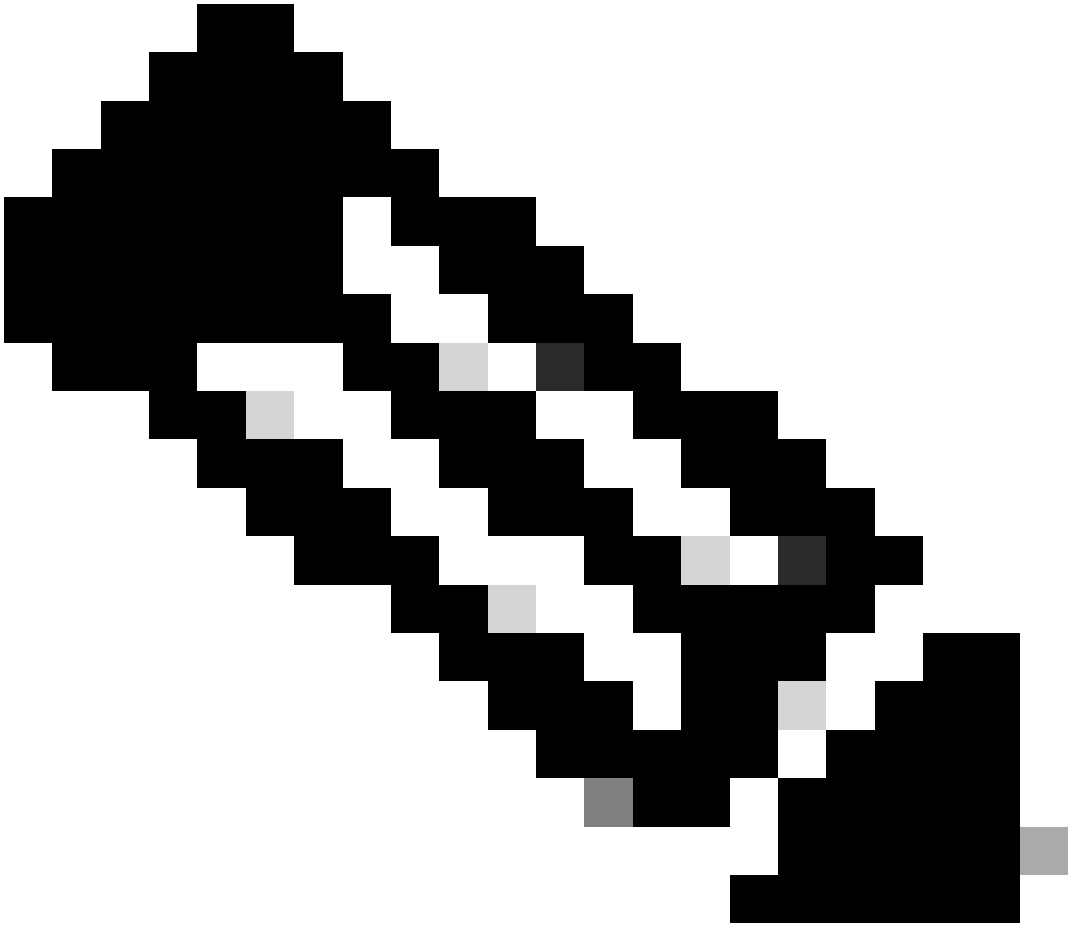
Verifica (CLI)

<#root>

```
show ap profile name detailed
 | in indo <- View CAPWAP window size in an AP profile
show capwap client rcb
 | in Window <- View CAPWAP status and modes for a specific AP(Look for CAPWAP Sliding Window and Activ
show ap config general
 | in indo <- View AP configuration details(Shows Capwap Active Window Size)
```

Limitazioni/Considerazioni

- Questa funzione è supportata solo sui profili OEAP.
- Le dimensioni della finestra vengono aggiornate nell'access point solo durante il processo di join.
- Il predownload non viene attivato se l'ultima immagine di aggiornamento è già presente nell'access point.



Nota: Benché sia documentato principalmente per OEAP, questo miglioramento è stato osservato anche per i FlexConnect AP standard. Tuttavia, questa funzionalità non è stata completamente testata/supportata per le distribuzioni FlexConnect.

Aggiornamento efficiente dell'immagine in modalità FlexConnect

L'aggiornamento efficiente dell'immagine è un metodo ottimizzato appositamente progettato per i punti di accesso FlexConnect, particolarmente utile nelle installazioni nelle filiali con larghezza di banda WAN limitata. Questo metodo riduce al minimo il carico della WAN designando un punto di accesso primario all'interno di un tag del sito per scaricare l'immagine dal controller, quindi consentendo ad altri punti di accesso subordinati nello stesso tag del sito di scaricare l'immagine dall'punto di accesso primario tramite TFTP. Il punto di accesso principale è un punto di accesso per modello per tag di sito.

Panoramica del processo

1. Una nuova immagine AP viene posizionata nell'area intermedia del WLC.
2. I punti di accesso FlexConnect vengono assegnati a un tag del sito configurato per l'aggiornamento efficiente dell'immagine.
3. Il WLC seleziona un punto di accesso per modello all'interno del tag del sito come punto di accesso primario.
4. L'access point principale scarica l'immagine dal WLC tramite il collegamento WAN (in genere tramite CAPWAP).
5. Una volta che l'access point primario ha l'immagine, gli access point subordinati nello stesso tag site scaricano l'immagine dall'access point primario tramite TFTP sulla rete locale.
6. Al massimo tre access point subordinati possono essere scaricati contemporaneamente da un access point primario.
7. Dopo il download, i punti di accesso si ricaricano per eseguire la nuova immagine.

Vantaggi

- Riduce il consumo di larghezza di banda della WAN consentendo solo al punto di accesso principale di scaricare l'immagine sulla WAN.
- Utilizzo di collegamenti di rete locali più veloci (tramite TFTP) per la distribuzione delle immagini agli access point subordinati.

Configuration (CLI)

<#root>

```
Enable Predownload in Flex Profile:

configure terminal
wireless profile flex




predownload



 <- Enables the Efficient Image Upgrade option.

end


Configure a Site Tag and Associate Flex Profile:

configure terminal
wireless tag site




flex-profile
```

<- Ensure 'no local-site' is configured if not already, for Flexconnect mode

end

Attach Policy Tag and Site Tag to AP(s):

configure terminal
ap

<- Use wired MAC address

policy-tag

site-tag

rf-tag

end

Trigger Predownload to a Site Tag:

enable

```
ap image predownload site-tag

          start
```

Verifica (CLI)

<#root>

```
show ap primary list
 <- Display list of primary APs
show ap image
 <- Display predownload status of APs: (Initially shows 'Predownloading', then 'Complete')
show ap name

          image

 <- Display image details for a specific AP
show capwap client rcb
 <- Check if Flex efficient image upgrade is enabled on the AP console
```

Limitazioni/Considerazioni

- I punti di accesso aggiunti tramite un codice di matricola del sito devono trovarsi nella stessa posizione fisica per un efficiente trasferimento TFTP locale.
- Utilizza la porta TCP 8443 per il servizio listener (utilizzata anche per altre funzioni come i bundle di debug del client e i file Clean Air). Questa porta rimane aperta anche se la funzione è disabilitata.
- Richiede che il WLC sia in modalità di installazione.

Download immagine punto di accesso basato su HTTP fuori

banda

Il download di immagini AP basate su HTTP OOB è un metodo migliorato introdotto in Cisco IOS® XE Dublin 17.11.1 per migliorare le prestazioni di aggiornamento delle immagini AP trasferendo le immagini al di fuori del percorso di controllo CAPWAP standard. Un vantaggio chiave e una rete di sicurezza è il fallback automatico al download CAPWAP in banda standard se il download del protocollo HTTP non riesce.

Il metodo HTTP OOB utilizza il protocollo TCP standard e il protocollo HTTP per il trasferimento delle immagini. A differenza del meccanismo di arresto e attesa del canale di controllo CAPWAP, il protocollo TCP utilizza per sua natura un meccanismo a finestra scorrevole che consente un trasferimento efficiente di grandi quantità di dati su collegamenti ad alta latenza.

Questo metodo utilizza un server Web (Inginx) in esecuzione sul controller per servire le immagini AP direttamente ai punti di accesso tramite HTTP. In questo modo vengono superate le limitazioni del percorso di controllo CAPWAP per i trasferimenti di file di grandi dimensioni, offrendo un meccanismo di download potenzialmente più veloce e flessibile.

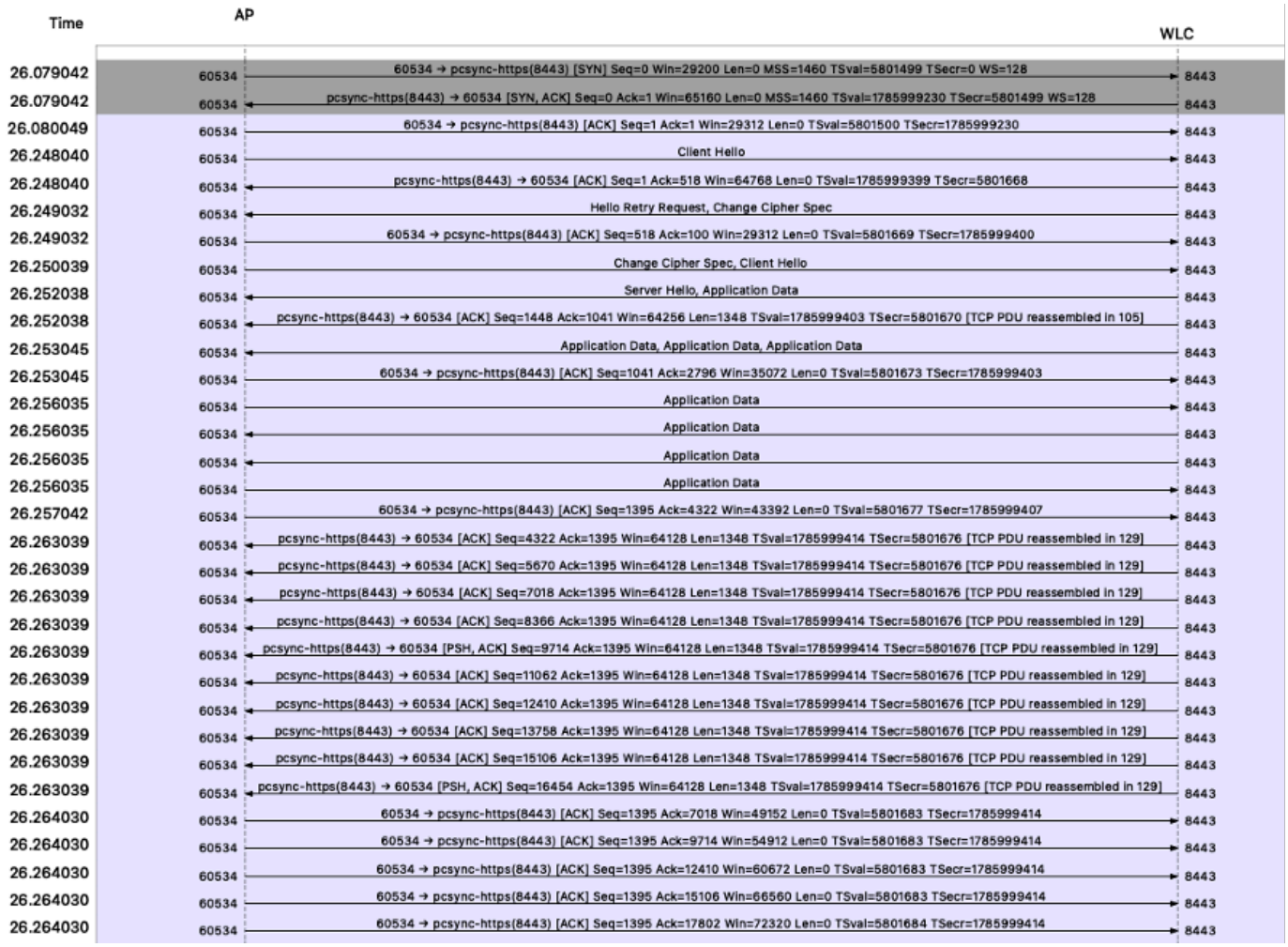
Scenario d'uso

Questo metodo è utile per accelerare gli aggiornamenti delle immagini AP, in particolare in installazioni di grandi dimensioni o in siti remoti dove le limitazioni di latenza e larghezza di banda del tunnel di controllo CAPWAP possono rendere i tradizionali download in banda estremamente lunghi.

Panoramica del processo

1. La nuova immagine AP viene posizionata nell'area intermedia del WLC.
2. Il metodo di aggiornamento HTTP fuori banda è abilitato e configurato nel controller.
3. L'access point, se supporta il metodo OOB, tenta di scaricare l'immagine richiesta dal server Web Inginx sul controller tramite HTTP sulla porta configurata.
4. Se il download del protocollo HTTP ha esito positivo, l'access point prosegue con il processo di aggiornamento.
5. Se il download del protocollo HTTP ha esito negativo, l'access point torna automaticamente al metodo di download CAPWAP in banda standard.

L'acquisizione del pacchetto mostra il WLC che agisce come server HTTP e l'AP come client HTTP che avvia una connessione TCP standard sulla porta 8443 e scarica il file.



Flusso del pacchetto di aggiornamento dell'immagine basato su HTTPS

Configuration (CLI)

<#root>

Enable the HTTPS upgrade method:

```
configure terminal
ap upgrade method https
end
```

Configure a custom HTTPS port (Optional - default is 8443):

```
configure terminal
ap file-transfer https port




end
```

GUI (Configuration)

1. Selezionare Configurazione > Wireless > Globale wireless.
2. Nella sezione Aggiornamento immagine AP, Abilitare il metodo HTTP.
3. (Facoltativo) Immettere i valori nel campo Porta HTTP.
4. Fare clic su Applica alla periferica.

Verifica (CLI)

<#root>

show ap upgrade method

<- Check global HTTPS method status

show ap file-transfer https summary

<- View configured and operational HTTPS file transfer port

show ap name

config general | sec Upgrade

<- Check if a specific AP supports OOB capability (Look for "AP Upgrade Out-Of-Band Capability : Enabl

show wireless stats ap image-download

<- View the method used for recent downloads (Check the Method column)

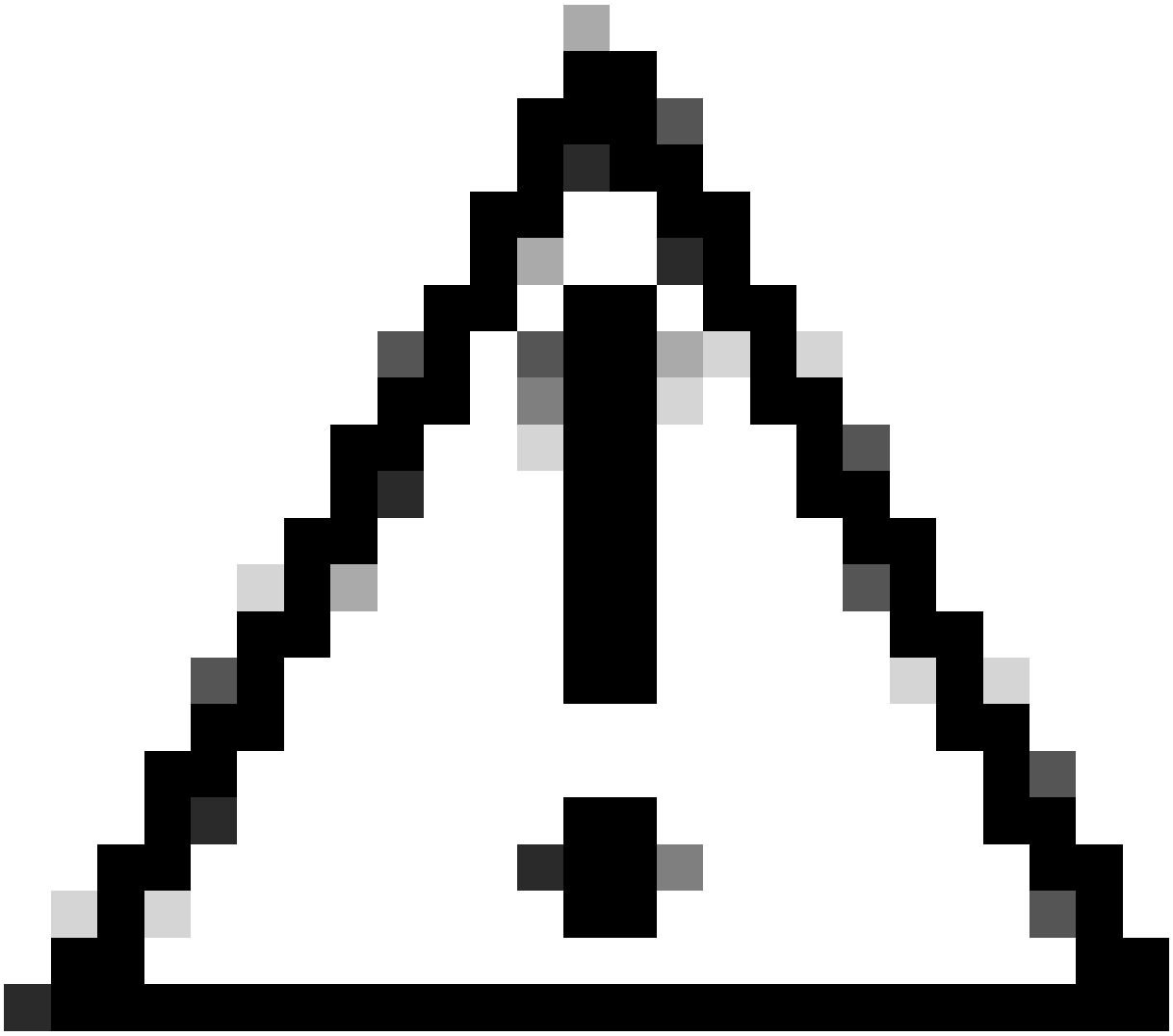
show platform software yang-management process

<- Verify nginx server status

Limitazioni/Considerazioni

- Richiede Cisco IOS® XE Dublin 17.11.1 o versioni successive.
- Non supportato sui Cisco Embedded Wireless Controller o sui Cisco Wave 1 Access Point.
- Richiede l'abilitazione della configurazione HTTPS globale nel controller.
- Il server UNIX deve essere in esecuzione sul controller.
- La porta configurata deve essere raggiungibile tra il controller e i punti di accesso.
- L'aggiornamento può avere esito negativo se il trust point del server HTTPS dispone di una catena di certificati CA.
- Deve essere disabilitato (nessun metodo di aggiornamento ap https) prima di eseguire il downgrade alle versioni precedenti a Cisco IOS® XE 17.11.1.

- La porta 443 è riservata. Evitare altre porte standard/conosciute.
- Conflitto predefinito della porta 8443: Se l'accesso HTTPS alla GUI del controller utilizza anche 8443, configurare una porta diversa per il trasferimento di file AP o l'accesso alla GUI.



Attenzione: È importante essere a conoscenza degli avvisi di sicurezza relativi al caricamento di file, come ad esempio il software Cisco IOS XE Wireless Controller Arbitrary File Upload Vulnerability. Accertarsi sempre che il software WLC sia aggiornato con le ultime patch di sicurezza.

Aggiornamento manuale di singoli punti di accesso tramite TFTP/SFTP

Questo metodo implica l'accesso diretto all'interfaccia CLI dell'access point tramite console o SSH e l'avvio del download dell'immagine da un server TFTP o SFTP. Questa opzione permette di risolvere i problemi di punti di accesso specifici, di aggiornare i punti di accesso che non sono attualmente collegati a un controller o di caricare un'immagine di debug fornita da TAC.

Trovare l'immagine PA:

Questo processo carica l'immagine dell'access point direttamente sull'access point. In caso di aggiornamento basato su WLC, il WLC si occupa di selezionare l'immagine corretta per l'AP dal bundle dell'immagine WLC. Qui è necessaria la selezione manuale.

La versione dell'immagine AP utilizza una convenzione di denominazione diversa dalla convenzione di denominazione dell'immagine WLC.

Passare al collegamento Supported Access Point in Cisco Catalyst serie 9800 Wireless Controller Software Releases

[Access point supportati nelle versioni software Cisco Catalyst serie 9800 Wireless Controller]

Cisco IOS XE 17.12.4	17.12.4.22	15.3(3)JPQ3	Cisco Catalyst APs: 9105AX (I/W), 9115AX (I/E), 9117AX (I), 9120AX (I/E/P), 9130AX (I/E), 9136 (I), 9162 (I), 9163 (E), 9164 (I), 9166 (I/D1) Cisco Aironet APs: 1815 (I/W/M/T), 1830 (I),1840 (I), 1852 (I/E), 1800 (I), 2800 (I/E), 3800 (I/E/P), 4800 (I) Outdoor and Industrial APs: 1542, 1560, 1570, and IW3702 Integrated Access Point in Cisco 1100 ISR (ISR-AP1100AC, ISR-AP1101AC, and ISR-AP1101AX) Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point, Cisco 6300 Series Embedded Services Access Point, Cisco Catalyst 9124AX (I/D/E) Access Points, Cisco Catalyst Industrial Wireless 9167 (I/E) Heavy Duty Access Points Sensors: Cisco Aironet 1800s Active Sensor Pluggable Modules: Wi-Fi 6 Pluggable Module for Industrial Routers

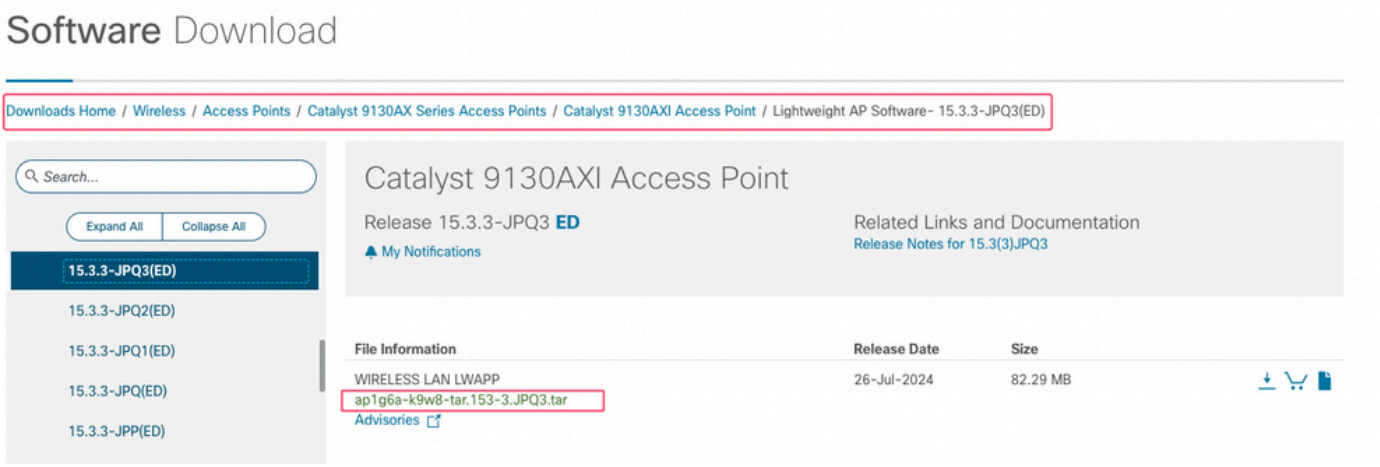
Matrice di compatibilità dei punti di accesso wireless

La prima colonna descrive l'immagine CCO del WLC 9800. La terza colonna elenca la rispettiva versione dell'immagine, mentre la quarta colonna elenca i punti di accesso supportati per tale versione. Si supponga che sia necessario installare l'immagine AP sull'access point 9130 versione 17.12.4. Se si controlla la tabella, il nome dell'immagine AP è 15.3(3)JPQ3 e il modello 9130 è supportato.

Il passaggio successivo è quello di passare a software.cisco.com e ottenere l'immagine dalla cartella di download del punto di accesso.

Download Home/ Wireless / Access Point / Access point Catalyst serie 9130AX / Access point Catalyst 9130AXI / Software Lightweight AP- 15.3.3-JPQ3(ED)

[Download del software - Access point Catalyst 9130AXI]



Posizione immagine AP

Avviso: Il percorso di download varia in base al modello AP e alla versione dell'immagine AP.

Panoramica del processo

1. Posizionare nell'area intermedia i file immagine PA di destinazione su un server TFTP o SFTP accessibile.
2. Accedere alla CLI dell'access point (console o SSH).
3. Eseguire il comando archive download-sw, specificando il server e il percorso del file di immagine.
4. L'access point scarica l'immagine.
5. Al termine del download, riavviare il processo CAPWAP o ricaricare il punto di accesso per rendere effettiva la nuova immagine.

Configurazione (AP CLI)

<#root>

archive download-sw /no-reload tftp:///

<- Using TFTP:

archive download-sw /no-reload sftp:/// Username:

Password:

<- Using SFTP:

reload

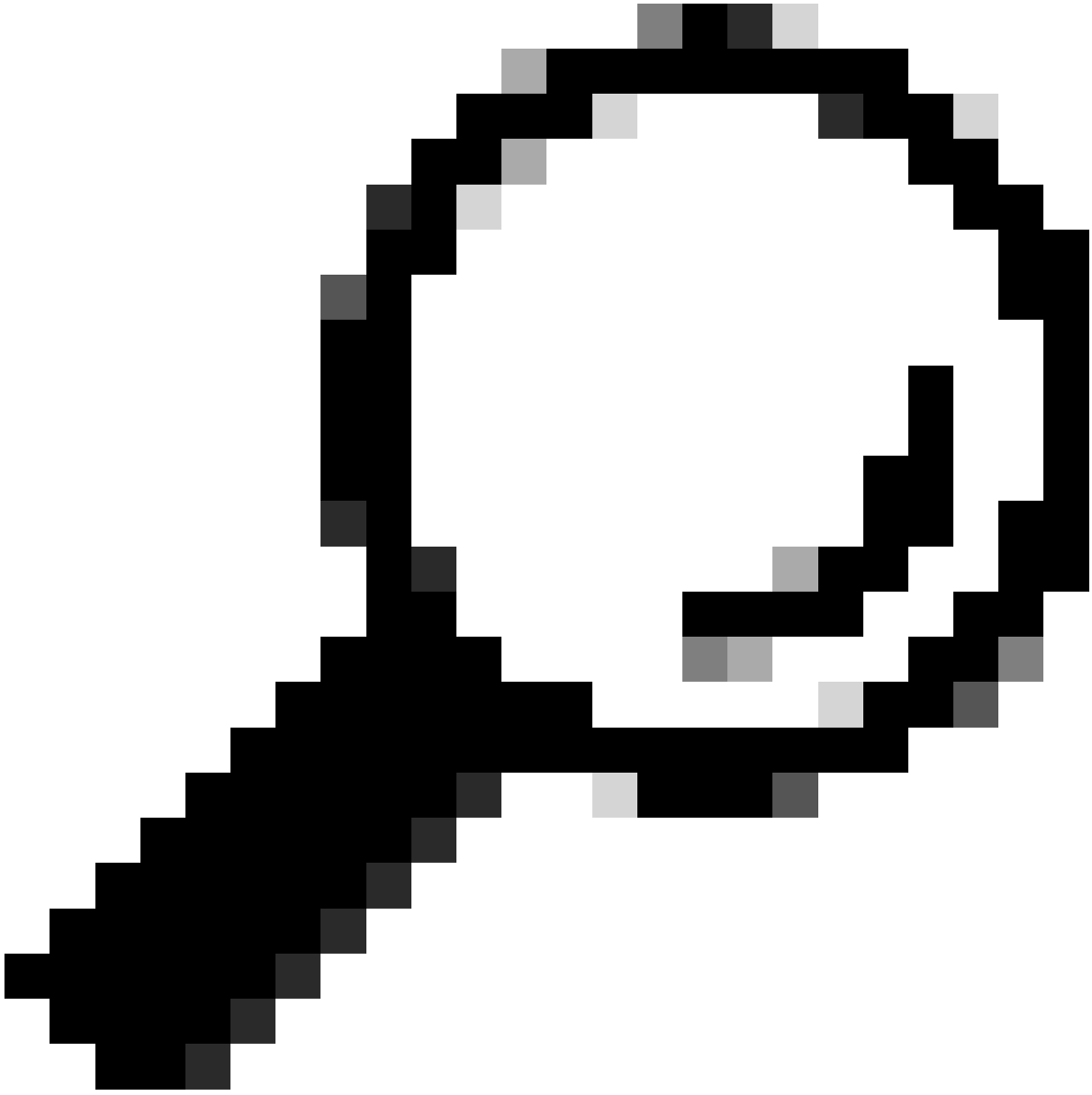
<- Restart CAPWAP process after download:

Verifica

- Monitorare i registri del server TFTP/SFTP per confermare il download.
- Osservare la console AP per verificare lo stato di avanzamento e il completamento del download.
- Dopo il riavvio/ricaricamento, verificare la nuova versione dell'immagine sulla CLI dell'access point o sul WLC.

Limitazioni/Considerazioni

- Richiede l'accesso diretto della CLI a ciascun access point.
- Non scalabile per l'aggiornamento di un numero elevato di access point singolarmente (la creazione di script è un'opzione).
- Le prestazioni TFTP sono sensibili alla latenza; SFTP (tramite TCP) offre prestazioni migliori rispetto ai percorsi ad alta latenza, ma richiede l'autenticazione interattiva (nome utente/password).
- L'opzione di riavvio/non ricaricamento impedisce al punto di accesso di ricaricarsi immediatamente dopo il download, consentendo il controllo manuale dei tempi di riavvio/ricaricamento.
- Se si esegue la migrazione degli access point da AireOS a 9800, si consiglia di aggiornare l'access point a una versione AireOS specifica (8.10.190.0 o successiva) con le correzioni prima di unirsi a 9800.



Suggerimento: Il controller WLAN è uno strumento che può essere utilizzato per creare

---

script per aggiornare manualmente più access point. Trovare il controller WLAN in questa posizione. Controller WLAN

Metodo da utilizzare su quale

- Per i punti di accesso OEAP o Teleworker su collegamenti ad alta latenza:
  Attivare l'opzione CAPWAP Image Download Time Enhanced. Questa funzionalità è stata appositamente progettata per migliorare le prestazioni di CAPWAP per questi tipi di distribuzione utilizzando una finestra scorrevole che consente di risolvere direttamente il problema di latenza all'interno del framework CAPWAP.
- Per i punti di accesso FlexConnect nelle filiali con larghezza di banda WAN limitata:
  Utilizzo dell'aggiornamento dell'immagine efficiente in modalità FlexConnect. Questo metodo è altamente consigliato in quanto riduce in modo significativo il carico della WAN utilizzando un punto di accesso primario per la distribuzione locale tramite TFTP, sfruttando velocità di rete interna più elevate.
- Per i punti di accesso in modalità locale (o FlexConnect/OEAP se i metodi descritti in precedenza non sono applicabili o sufficienti) sulle piattaforme supportate (Cisco IOS® XE 17.11.1+):
  Prendere in considerazione il download di immagini AP basate su HTTP fuori banda. Questo metodo utilizza i protocolli TCP/HTTP per il trasferimento bulk, più efficiente sui collegamenti ad alta latenza rispetto al protocollo CAPWAP standard. Fornisce inoltre un fallback al CAPWAP standard se il trasferimento OOB non riesce.
- Per risolvere i problemi di un singolo access point, aggiornare un access point non collegato a un WLC o in scenari di emergenza:
  Eseguire un aggiornamento manuale dei singoli punti di accesso tramite TFTP/SFTP. Ciò consente di controllare direttamente il processo di aggiornamento per un dispositivo specifico, ma non è pratico per installazioni su larga scala senza automazione. SFTP è generalmente preferito al TFTP per prestazioni migliori rispetto ai percorsi ad alta latenza, grazie all'uso del TCP.
- Aggiornamento CAPWAP standard: Sebbene sia il metodo predefinito, in genere non è consigliato come metodo principale per l'aggiornamento dei punti di accesso remoti su collegamenti WAN ad alta latenza, a causa del meccanismo di stop-and-wait che comporta trasferimenti lenti e potenziali problemi di affidabilità nelle versioni precedenti. Se possibile, utilizzare i metodi ottimizzati descritti per i siti remoti.

È possibile scegliere il metodo che meglio si allinea alla modalità operativa del punto di accesso, alle condizioni di rete, alla versione del software WLC e alla scalabilità delle operazioni di aggiornamento per garantire un processo uniforme ed efficiente per i punti di accesso remoti.

Conclusioni

Mentre il metodo standard di download delle immagini CAPWAP è adatto per le reti locali, le installazioni di punti di accesso remoti su collegamenti WAN traggono notevole vantaggio dalle tecniche di aggiornamento ottimizzate. Comprendere i limiti di CAPWAP standard su latenza elevata aiuta a scegliere l'approccio corretto. Il miglioramento dei tempi di download delle

immagini CAPWAP migliora le prestazioni dei punti di accesso OEAP/Teleworker, l'aggiornamento efficiente delle immagini ottimizza le installazioni FlexConnect riducendo il carico WAN e il protocollo HTTP fuori banda offre un'alternativa più veloce per le piattaforme supportate. Il metodo manuale TFTP/SFTP rimane uno strumento prezioso per la risoluzione dei problemi e per scenari specifici.

Riferimenti

Aggiornamento efficiente delle immagini

Download immagine punto di accesso fuori banda

Miglioramento tempo di download immagine AP (solo OEAP o Teleworker)

Access point Cisco supportati nelle versioni software della piattaforma Cisco Wireless Controller

Controller WLAN

Migrazione da AireOS WLC a Catalyst 9800 con WLAN Controller

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).