# Upgrade e downgrade dei controller Catalyst 9800: suggerimenti e consigli

## Sommario

# Introduzione

In questo documento vengono descritti gli aspetti da tenere in considerazione quando si aggiorna o si esegue il downgrade di un Catalyst 9800 Wireless LAN Controller (WLC).

# Prima di procedere

Questo documento non ha lo scopo di sostituire le note sulla versione, che devono sempre essere il documento di destinazione durante l'aggiornamento. L'obiettivo è quello di facilitare l'upgrade attraverso diverse release evidenziando i cambiamenti più impattanti tra le release.

Questo documento non sostituisce la lettura delle note sulla versione del software di destinazione. Eseguire il backup della configurazione e adottare tutte le precauzioni necessarie prima di procedere con l'aggiornamento.

Per impostazione predefinita, il server HTTP della 9800 non è mappato in modo statico a un certificato/trust point specifico che può comportare modifiche dopo l'aggiornamento. Impostare il server HTTP su un trust point statico (preferibilmente su un certificato rilasciato per lo scopo o sul certificato MIC in caso contrario) nella configurazione prima dell'aggiornamento.

## Il caso speciale delle versioni speciali di Engineering

Le build speciali di progettazione non supportano gli aggiornamenti di ISSU da tali build. Poiché questo documento è incentrato esclusivamente sulle release pubbliche pubblicate su Cisco.com, se si è su una build speciale di progettazione, consultare le note sulla release ricevute insieme a esse per ricevere supporto per tutte le domande relative all'aggiornamento.

# Aggiornamento

È possibile leggere direttamente le note nella versione del software di destinazione desiderata. I suggerimenti applicabili attraverso diverse versioni vengono ripetuti ogni volta per comodità. Non eseguire l'aggiornamento da più di tre release alla volta. Ad esempio, l'aggiornamento dalla versione 16.12.1 alla 17.3.2 è trattato nel presente documento, ma non comprende gli aggiornamenti dalla versione 16.12 alla 17.4. In uno scenario di questo tipo, passare alla versione 17.3 e controllare le note nella sezione 17.3, eseguire l'aggiornamento, quindi esaminare la

sezione 17.4 e preparare il secondo aggiornamento. In conclusione, i suggerimenti elencati non vengono più ripetuti dopo tre release principali, anche se ancora validi, poiché il documento presuppone che si proceda attraverso le release principali intermedie.

## Gibilterra

16.12.2

- Da Cisco IOS® XE Gibraltar 16.12.2s, il mapping WLAN automatico al profilo dei criteri predefinito sotto il tag dei criteri predefinito è stato rimosso. Se si sta eseguendo l'aggiornamento da una versione precedente a Cisco IOS XE Gibraltar 16.12.2s e la rete wireless utilizza il tag di criterio predefinito, il tag diventa inattivo a causa della modifica del mapping predefinito. Per ripristinare l'operazione di rete, aggiungere la WLAN richiesta ai mapping dei criteri sotto il tag dei criteri predefinito.
- Non utilizzare più di 31 caratteri per i nomi dei punti di accesso. Se il nome dell'access point è composto da almeno 32 caratteri, potrebbe verificarsi un arresto anomalo del controller.
- Non implementare i file OVA direttamente in VMware ESXi 6.5. Si consiglia di utilizzare uno strumento OVF per distribuire i file OVA.

16.12.3

- La versione 16.12.3 è la prima a imporre il supporto solo degli SFP elencati come supportati nella documentazione. Gli SFP non elencati causano un arresto della porta. Verificare l'elenco degli SFP supportati e accertarsi che gli SFP siano compatibili per evitare che le porte dati non siano attive dopo l'aggiornamento.
- Il file di aggiornamento per questa release può essere troppo grande per il caricamento HTTP (quando si esegue un aggiornamento dell'interfaccia utente Web) se si è nella release 16.12.1. Utilizzare un altro metodo di trasferimento o passare alla versione 16.12.2 che supporta il caricamento di file di dimensioni maggiori tramite l'interfaccia utente Web.
- Da Cisco IOS XE Gibraltar 16.12.2s, il mapping WLAN automatico al profilo dei criteri predefinito sotto il tag dei criteri predefinito è stato rimosso. Se si sta eseguendo l'aggiornamento da una versione precedente a Cisco IOS XE Gibraltar 16.12.2s e la rete wireless utilizza il tag di criterio predefinito, il tag diventa inattivo a causa della modifica del mapping predefinito. Per ripristinare l'operazione di rete, aggiungere la WLAN richiesta ai mapping dei criteri sotto il tag dei criteri predefinito.
- Non utilizzare più di 31 caratteri per i nomi dei punti di accesso. Se il nome dell'access point è composto da almeno 32 caratteri, potrebbe verificarsi un arresto anomalo del controller.
- Non implementare i file OVA direttamente in VMware ESXi 6.5. Si consiglia di utilizzare uno strumento OVF per distribuire i file OVA.

16.12.4

- Le versioni 16.12.3 e 17.2.1 sono le prime a implementare il supporto solo degli SFP

elencati come supportati nella documentazione. Gli SFP non elencati causano un arresto della porta. Verificare l'elenco degli SFP supportati e accertarsi che gli SFP siano compatibili per evitare che le porte dati non siano attive dopo l'aggiornamento.
- Il file di aggiornamento per questa release può essere troppo grande per il caricamento HTTP (quando si esegue un aggiornamento dell'interfaccia utente Web) se si è nella release 16.12.1. Utilizzare un altro metodo di trasferimento o passare alla versione 16.12.2 che supporta il caricamento di file di dimensioni maggiori tramite l'interfaccia utente Web.
- Da Cisco IOS XE Gibraltar 16.12.2s, il mapping WLAN automatico al profilo dei criteri predefinito sotto il tag dei criteri predefinito è stato rimosso. Se si sta eseguendo l'aggiornamento da una versione precedente a Cisco IOS XE Gibraltar 16.12.2s e la rete wireless utilizza un tag di criterio predefinito, il tag diventa inattivo a causa della modifica del mapping predefinito. Per ripristinare l'operazione di rete, aggiungere la WLAN richiesta ai mapping dei criteri sotto il tag dei criteri predefinito.

- Non utilizzare più di 31 caratteri per i nomi dei punti di accesso. Se il nome dell'access point è composto da almeno 32 caratteri, potrebbe verificarsi un arresto anomalo del controller.

- Non implementare i file OVA direttamente in VMware ESXi 6.5. Si consiglia di utilizzare uno strumento OVF per distribuire i file OVA.

16.12.5, 16.12.6a e 16.12.7

Identica alla release 16.12.4.

## Amsterdam

17.1.1

- Il file di aggiornamento per questa release può essere troppo grande per il caricamento HTTP (quando si esegue un aggiornamento dell'interfaccia utente Web) se si è nella release 16.12.1. Utilizzare un altro metodo di trasferimento o passare alla versione 16.12.2 che supporta il caricamento di file di dimensioni maggiori tramite l'interfaccia utente Web.
- Da Cisco IOS XE Gibraltar 16.12.2s, il mapping WLAN automatico al profilo dei criteri predefinito sotto il tag dei criteri predefinito è stato rimosso. Se si sta eseguendo l'aggiornamento da una versione precedente a Cisco IOS XE Gibraltar 16.12.2s e la rete wireless utilizza un tag di criterio predefinito, il tag diventa inattivo a causa della modifica del mapping predefinito. Per ripristinare l'operazione di rete, aggiungere la WLAN richiesta ai mapping dei criteri sotto il tag dei criteri predefinito.
- Da questa release, viene introdotto un nuovo controllo della raggiungibilità del gateway. Gli access point inviano richieste echo ICMP periodiche (ping) al gateway predefinito per verificare la connettività. È necessario verificare il filtro del traffico tra gli access point e il gateway predefinito (ad esempio, gli ACL) per consentire i ping ICMP tra l'access point e il gateway predefinito. Se i ping sono bloccati, anche se la connettività tra il controller e l'access point è attiva, gli access point vengono ricaricati a intervalli di 4 ore.

17.2.1

- Le versioni 16.12.3 e 17.2.1 sono le prime a implementare il supporto solo degli SFP elencati come supportati nella documentazione. Gli SFP non elencati causano un arresto della porta. Verificare l'elenco degli SFP supportati e accertarsi che gli SFP siano compatibili per evitare che le porte dati non siano attive dopo l'aggiornamento.
- Il file di aggiornamento per questa release può essere troppo grande per il caricamento HTTP (quando si esegue un aggiornamento dell'interfaccia utente Web) se si è nella release 16.12.1. Utilizzare un altro metodo di trasferimento o passare alla versione 16.12.2 che supporta il caricamento di file di dimensioni maggiori tramite l'interfaccia utente Web.
- Da Cisco IOS XE Gibraltar 16.12.2s, il mapping WLAN automatico al profilo dei criteri predefinito sotto il tag dei criteri predefinito è stato rimosso. Se si sta eseguendo l'aggiornamento da una versione precedente a Cisco IOS XE Gibraltar 16.12.2s e la rete wireless utilizza un tag di criterio predefinito, è possibile che il tag non sia attivo a causa della modifica del mapping predefinito. Per ripristinare l'operazione di rete, aggiungere la WLAN richiesta ai mapping dei criteri sotto il tag dei criteri predefinito.
- a partire dalla versione 17.1, viene introdotto un nuovo controllo della raggiungibilità del gateway. Gli access point inviano richieste echo ICMP periodiche (ping) al gateway predefinito per verificare la connettività. È necessario verificare il filtro del traffico tra gli access point e il gateway predefinito (ad esempio, gli ACL) per consentire i ping ICMP tra l'access point e il gateway predefinito. Se i ping sono bloccati, anche se la connettività tra il controller e l'access point è attiva, gli access point vengono ricaricati a intervalli di 4 ore.

17.3.1

- Le versioni 16.12.3 e 17.2.1 sono le prime a garantire il supporto solo degli SFP elencati come supportati nella documentazione. Gli SFP non elencati causano un arresto della porta. Verificare l'elenco degli SFP supportati e accertarsi che gli SFP siano compatibili per evitare che le porte dati non siano attive dopo l'aggiornamento.
- Il file di aggiornamento per questa release può essere troppo grande per il caricamento HTTP (quando si esegue un aggiornamento dell'interfaccia utente Web) se si è nella release 16.12.1. Utilizzare un altro metodo di trasferimento o passare alla versione 16.12.2 che supporta il caricamento di file di dimensioni maggiori tramite l'interfaccia utente Web.
- Da Cisco IOS XE Gibraltar 16.12.2s, il mapping WLAN automatico al profilo dei criteri predefinito sotto il tag dei criteri predefinito è stato rimosso. Se si sta eseguendo l'aggiornamento da una versione precedente a Cisco IOS XE Gibraltar 16.12.2s e la rete wireless utilizza un tag di criterio predefinito, il tag diventa inattivo a causa della modifica del mapping predefinito. Per ripristinare l'operazione di rete, aggiungere la WLAN richiesta ai mapping dei criteri sotto il tag dei criteri predefinito.
- A partire dalla versione 17.1, viene introdotto un nuovo controllo della raggiungibilità del gateway. Gli access point inviano richieste echo ICMP periodiche (ping) al gateway predefinito per verificare la connettività. È necessario verificare il filtro del traffico tra gli access point e il gateway predefinito (ad esempio, gli ACL) per consentire i ping ICMP tra l'access point e il gateway predefinito. Se i ping sono bloccati, anche se la connettività tra il controller e l'access point è attiva, gli access point vengono ricaricati a intervalli di 4 ore.
- Se è stata configurata la modalità FIPS, assicurarsi di rimuovere la `security wpa wpa1 cipher tkip` prima di aggiornare Cisco IOS XE Amsterdam 17.3.x da una versione precedente. In caso contrario, la sicurezza WLAN viene impostata su TKIP, che non è supportato in

modalità FIPS. Dopo l'aggiornamento, è necessario riconfigurare la WLAN con AES.
- A partire da Cisco IOS XE Amsterdam 17.3.1, il controller wireless Cisco Catalyst 9800-CL richiede 16 GB di spazio su disco per le nuove implementazioni. È possibile aumentare le dimensioni dello spazio su disco solo tramite una reinstallazione con immagine 17.3.
- Cisco IOS XE Amsterdam 17.3.1 e versioni successive, il nome dell'access point può essere composto al massimo da 32 caratteri.
- Per l'autenticazione dell'indirizzo MAC locale (di client o access point), solo il formato `aaaabbbbcccc` (senza separatore) a partire dalla versione 17.3.1. Ciò significa che l'autenticazione non riesce se si aggiunge un indirizzo MAC con separatori nell'interfaccia utente Web o nella CLI.
- Da questa versione in poi, gli access point si ricaricano dopo 4 ore se non possono unirsi a un WLC, non possono eseguire il ping del loro gateway e ARP del loro gateway (tutte e tre le operazioni devono avere esito negativo per permettere il riavvio dell'access point). si tratta di un miglioramento (ID bug Cisco CSCvt89970) della precedente verifica del gateway solo ICMP delle versioni precedenti.
- A partire dalla versione 17.3.1, il nuovo modo di configurare i codici paese per gli access point è il `Wireless country <1 country code>` che è possibile ripetere più volte con diversi codici paese. Ciò consente di aumentare la quantità massima di codice paese oltre 20. I comandi `ap country` sono ancora presenti e continuano a funzionare, tuttavia, si `Wireless country` comandi come `ap country` i comandi sono obsoleti in una versione futura.

17.3.2

- Le versioni 16.12.3 e 17.2.1 sono le prime a implementare il supporto solo degli SFP elencati come supportati nella documentazione. Gli SFP non elencati causano un arresto della porta. Verificare l'elenco degli SFP supportati e accertarsi che gli SFP siano compatibili per evitare che le porte dati non siano attive dopo l'aggiornamento.
- Il file di aggiornamento per questa release può essere troppo grande per il caricamento HTTP (quando si esegue un aggiornamento dell'interfaccia utente Web) se si è nella release 16.12.1. Utilizzare un altro metodo di trasferimento o passare alla versione 16.12.2 che supporta il caricamento di file di dimensioni maggiori tramite l'interfaccia utente Web.
- Da Cisco IOS XE Gibraltar 16.12.2s, il mapping WLAN automatico al profilo dei criteri predefinito sotto il tag dei criteri predefinito è stato rimosso. Se si sta eseguendo l'aggiornamento da una versione precedente a Cisco IOS XE Gibraltar 16.12.2s e la rete wireless utilizza un tag di criterio predefinito, il tag diventa inattivo a causa della modifica del mapping predefinito. Per ripristinare l'operazione di rete, aggiungere la WLAN richiesta ai mapping dei criteri sotto il tag dei criteri predefinito.
- A partire dalla versione 17.1, viene introdotto un nuovo controllo della raggiungibilità del gateway. Gli access point inviano richieste echo ICMP periodiche (ping) al gateway predefinito per verificare la connettività. È necessario verificare il filtro del traffico tra gli access point e il gateway predefinito (ad esempio, gli ACL) per consentire i ping ICMP tra l'access point e il gateway predefinito. Se i ping sono bloccati, anche se la connettività tra il controller e l'access point è attiva, gli access point vengono ricaricati a intervalli di 4 ore.
- Se è stata configurata la modalità FIPS, assicurarsi di rimuovere la `security wpa wpa1 cipher tkip` prima di aggiornare Cisco IOS XE Amsterdam 17.3.x da una versione precedente. In caso contrario, la sicurezza WLAN viene impostata su TKIP, che non è supportato in

modalità FIPS. Dopo l'aggiornamento, è necessario riconfigurare la WLAN con AES.

- A partire da Cisco IOS XE Amsterdam 17.3.1, il controller wireless Cisco Catalyst 9800-CL richiede 16 GB di spazio su disco per le nuove implementazioni. È possibile aumentare le dimensioni dello spazio su disco solo tramite una reinstallazione con immagine 17.3.
- A partire da Cisco IOS XE Amsterdam 17.3.1, il nome dell'access point può essere composto al massimo da 32 caratteri.
- Per l'autenticazione dell'indirizzo MAC locale (di client o access point), solo il formato `aaaabbbbcccc` (senza separatore) a partire dalla versione 17.3.1. Ciò significa che l'autenticazione non riesce se si aggiunge un indirizzo MAC con separatori nell'interfaccia utente Web o nella CLI.
- A partire dalla versione 17.3.1, gli access point si ricaricano dopo 4 ore se non possono collegarsi a un WLC, non possono eseguire il ping del loro gateway e l'ARP del loro gateway (tutte e tre le opzioni devono avere esito negativo per permettere il riavvio dell'access point). si tratta di un miglioramento (ID bug Cisco CSCvt89970) alla verifica del gateway ICMP precedente alle versioni precedenti.
- A partire dalla versione 17.3.1, il nuovo modo di configurare i codici paese per gli access point è il `Wireless country <1 country code>` che è possibile ripetere più volte con diversi codici paese. Ciò consente di aumentare la quantità massima di codici paese di ben oltre 20. I comandi `ap country` sono ancora presenti e in corso, tuttavia, prendere in considerazione la possibilità di `Wireless country` comandi come `ap country` i comandi sono obsoleti in una versione futura.

17.3.3

- Le versioni 16.12.3 e 17.2.1 sono le prime a implementare il supporto solo degli SFP elencati come supportati nella documentazione. Gli SFP non elencati causano un arresto della porta. Verificare l'elenco degli SFP supportati e accertarsi che gli SFP siano compatibili per evitare che le porte dati non siano attive dopo l'aggiornamento.
- Il file di aggiornamento per questa release può essere troppo grande per il caricamento HTTP (quando si esegue un aggiornamento dell'interfaccia utente Web) se si è nella release 16.12.1. Utilizzare un altro metodo di trasferimento o passare alla versione 16.12.2 che supporta il caricamento di file di dimensioni maggiori tramite l'interfaccia utente Web.
- Da Cisco IOS XE Gibraltar 16.12.2s, il mapping WLAN automatico al profilo dei criteri predefinito sotto il tag dei criteri predefinito è stato rimosso. Se si sta eseguendo l'aggiornamento da una versione precedente a Cisco IOS XE Gibraltar 16.12.2s e la rete wireless utilizza il tag di criterio predefinito, il tag diventa inattivo a causa della modifica del mapping predefinito. Per ripristinare l'operazione di rete, aggiungere la WLAN richiesta ai mapping dei criteri sotto il tag dei criteri predefinito.
- a partire dalla versione 17.1, viene introdotto un nuovo controllo della raggiungibilità del gateway. Gli access point inviano richieste echo ICMP periodiche (ping) al gateway predefinito per verificare la connettività. È necessario verificare il filtro del traffico tra gli access point e il gateway predefinito (ad esempio, gli ACL) per consentire i ping ICMP tra l'access point e il gateway predefinito. Se i ping sono bloccati, anche se la connettività tra il controller e l'access point è attiva, gli access point vengono ricaricati a intervalli di 4 ore.
- Se è stata configurata la modalità FIPS, assicurarsi di rimuovere la `security wpa wpa1 cipher tkip` prima di aggiornare Cisco IOS XE Amsterdam 17.3.x da una versione precedente. In caso contrario, la sicurezza WLAN viene impostata su TKIP, che non è supportato in

modalità FIPS. Dopo l'aggiornamento, è necessario riconfigurare la WLAN con AES.

- A partire da Cisco IOS XE Amsterdam 17.3.1, il controller wireless Cisco Catalyst 9800-CL richiede 16 GB di spazio su disco per le nuove implementazioni. È possibile aumentare le dimensioni dello spazio su disco solo tramite una reinstallazione con immagine 17.3.
- Cisco IOS XE Amsterdam 17.3.1 e versioni successive, il nome dell'access point può essere composto al massimo da 32 caratteri.
- Per l'autenticazione dell'indirizzo MAC locale (di client o access point), solo il formato aaaabbbbcccc (senza separatore) a partire dalla versione 17.3.1. Ciò significa che l'autenticazione non riesce se si aggiunge un indirizzo MAC con separatori nell'interfaccia utente Web o nella CLI.
- A partire dalla versione 17.3.1, gli access point si ricaricano dopo 4 ore se non possono collegarsi a un WLC, non possono eseguire il ping del loro gateway e l'ARP del loro gateway (tutte e tre le opzioni devono avere esito negativo per permettere il riavvio dell'access point). Questa è una versione migliorata (ID bug Cisco CSCvt89970) della verifica del gateway ICMP precedente alle versioni precedenti.
- A partire dalla versione 17.3.1, il nuovo modo di configurare i codici paese per gli access point è il Wireless country <1 country code> che è possibile ripetere più volte con diversi codici paese. Ciò consente di aumentare la quantità massima di codice paese oltre 20. I comandi ap country sono ancora presenti e stanno lavorando, tuttavia, valutano la possibilità di Wireless country comandi come ap country i comandi sono obsoleti in una versione futura.
- Il WLC può bloccarsi se i tuoi AP hanno nomi host più lunghi di 32 caratteri (ID bug Cisco CSCvy11981).

17.3.4

- Le versioni 16.12.3 e 17.2.1 sono le prime a garantire il supporto solo degli SFP elencati come supportati nella documentazione. Gli SFP non elencati causano un arresto della porta. Verificare l'elenco degli SFP supportati e accertarsi che gli SFP siano compatibili per evitare che le porte dati non siano attive dopo l'aggiornamento.
- Il file di aggiornamento per questa release può essere troppo grande per il caricamento HTTP (quando si esegue un aggiornamento dell'interfaccia utente Web) se si è nella release 16.12.1. Utilizzare un altro metodo di trasferimento o passare alla versione 16.12.2 che supporta il caricamento di file di dimensioni maggiori tramite l'interfaccia utente Web.
- Da Cisco IOS XE Gibraltar 16.12.2s, il mapping WLAN automatico al profilo dei criteri predefinito sotto il tag dei criteri predefinito è stato rimosso. Se si sta eseguendo l'aggiornamento da una versione precedente a Cisco IOS XE Gibraltar 16.12.2s e la rete wireless utilizza un tag di criterio predefinito, il tag diventa inattivo a causa della modifica del mapping predefinito. Per ripristinare l'operazione di rete, aggiungere la WLAN richiesta ai mapping dei criteri sotto il tag dei criteri predefinito.
- A partire dalla versione 17.1, viene introdotto un nuovo controllo della raggiungibilità del gateway. Gli access point inviano richieste echo ICMP periodiche (ping) al gateway predefinito per verificare la connettività. È necessario verificare il filtro del traffico tra gli access point e il gateway predefinito (ad esempio, gli ACL) per consentire i ping ICMP tra l'access point e il gateway predefinito. Se i ping sono bloccati, anche se la connettività tra il controller e l'access point è attiva, gli access point vengono ricaricati a intervalli di 4 ore.
- Se è stata configurata la modalità FIPS, assicurarsi di rimuovere la security wpa wpa1 cipher

tkip prima di aggiornare Cisco IOS XE Amsterdam 17.3.x da una versione precedente. In caso contrario, la sicurezza WLAN viene impostata su TKIP, che non è supportato in modalità FIPS. Dopo l'aggiornamento, è necessario riconfigurare la WLAN con AES.

- A partire da Cisco IOS XE Amsterdam 17.3.1, il controller wireless Cisco Catalyst 9800-CL richiede 16 GB di spazio su disco per le nuove implementazioni. È possibile aumentare le dimensioni dello spazio su disco solo tramite una reinstallazione con immagine 17.3.
- A partire da Cisco IOS XE Amsterdam 17.3.1, il nome dell'access point può essere composto al massimo da 32 caratteri.
- Per l'autenticazione dell'indirizzo MAC locale (di client o access point), solo il formato aaaabbbbcccc (senza separatore) a partire dalla versione 17.3.1. Ciò significa che l'autenticazione non riesce se si aggiunge un indirizzo MAC con separatori nell'interfaccia utente Web o nella CLI.
- A partire dalla versione 17.3.1, gli access point vengono ricaricati dopo 4 ore se non possono collegarsi a un WLC, non possono eseguire il ping del gateway e l'ARP del gateway (per riavviare l'access point, tutte e tre queste operazioni devono avere esito negativo). si tratta di un miglioramento (ID bug Cisco CSCvt89970) alla precedente verifica del gateway solo ICMP delle versioni precedenti.
- 17.3.1 in poi, il nuovo modo di configurare i codici paese per gli access point è il Wireless country <1 country code> che è possibile ripetere più volte con diversi codici paese. Ciò consente di aumentare la quantità massima di codice paese oltre 20. I comandi ap country sono ancora presenti e stanno lavorando, tuttavia, valutano la possibilità di Wireless country comandi come ap country i comandi saranno obsoleti in una versione futura.
- Quando si esegue l'aggiornamento alla versione 17.3.4 e successive, si consiglia di installare il bootloader/rommon 16.12.5r sui controller dove è applicabile (9800-80). (al momento, lo switch 9800-40 non dispone di un rommon 16.12.5r e non ha bisogno di un aggiornamento di rommon).
- L'aggiornamento del controller, da Cisco IOS XE Bengaluru 17.3.x a qualsiasi versione con ISSU, può non riuscire se il snmp-server enable traps hsrpè configurato. Accertarsi di rimuovere snmp-server enable traps hsrp dalla configurazione prima di avviare l'aggiornamento di un modulo ISSU perché snmp-server enable traps hsrp viene rimosso da Cisco IOS XE Bengaluru 17.4.x.

- Durante l'aggiornamento a Cisco IOS XE 17.3.x e versioni successive, se ip http active-session-modules none è abilitato, non è possibile accedere alla GUI del controller utilizzando HTTPS. Per accedere alla GUI con HTTPS, eseguire questi comandi:

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

17.3.5

- A causa dell'ID bug Cisco CSCwb13784, se la MTU del percorso è inferiore a 1500 byte, i punti di accesso potrebbero non essere in grado di unirsi. Per risolvere il problema, scaricate la patch SMU disponibile per la versione 17.3.5.
- Le versioni 16.12.3 e 17.2.1 sono le prime a garantire il supporto solo degli SFP elencati come supportati nella documentazione. Gli SFP non elencati causano un arresto della porta. Verificare l'elenco degli SFP supportati e accertarsi che gli SFP siano compatibili per evitare

che le porte dati non siano attive dopo l'aggiornamento.

- Il file di aggiornamento per questa release può essere troppo grande per il caricamento HTTP (quando si esegue un aggiornamento dell'interfaccia utente Web) se si è nella release 16.12.1. Utilizzare un altro metodo di trasferimento o passare alla versione 16.12.2 che supporta il caricamento di file di dimensioni maggiori tramite l'interfaccia utente Web.
- Da Cisco IOS XE Gibraltar 16.12.2s, il mapping WLAN automatico al profilo dei criteri predefinito sotto il tag dei criteri predefinito è stato rimosso. Se si sta eseguendo l'aggiornamento da una versione precedente a Cisco IOS XE Gibraltar 16.12.2s e la rete wireless utilizza un tag di criterio predefinito, il tag diventa inattivo a causa della modifica del mapping predefinito. Per ripristinare l'operazione di rete, aggiungere la WLAN richiesta ai mapping dei criteri sotto il tag dei criteri predefinito.
- a partire dalla versione 17.1, viene introdotto un nuovo controllo della raggiungibilità del gateway. Gli access point inviano richieste echo ICMP periodiche (ping) al gateway predefinito per verificare la connettività. È necessario verificare il filtro del traffico tra gli access point e il gateway predefinito (ad esempio, gli ACL) per consentire i ping ICMP tra l'access point e il gateway predefinito. Se i ping sono bloccati, anche se la connettività tra il controller e l'access point è attiva, gli access point vengono ricaricati a intervalli di 4 ore.
- Se è stata configurata la modalità FIPS, assicurarsi di rimuovere la `security wpa wpa1 cipher tkip` prima di aggiornare Cisco IOS XE Amsterdam 17.3.x da una versione precedente. In caso contrario, la sicurezza WLAN viene impostata su TKIP, che non è supportato in modalità FIPS. Dopo l'aggiornamento, è necessario riconfigurare la WLAN con AES.
- Cisco IOS XE Amsterdam a partire dalla versione 17.3.1, il controller wireless Cisco Catalyst 9800-CL richiede 16 GB di spazio su disco per le nuove implementazioni. È possibile aumentare le dimensioni dello spazio su disco solo tramite una reinstallazione con immagine 17.3.
- Cisco IOS XE Amsterdam 17.3.1 e versioni successive, il nome dell'access point può essere composto al massimo da 32 caratteri.
- Per l'autenticazione dell'indirizzo MAC locale (di client o access point), solo il formato `aaaabbbbcccc` (senza separatore) a partire dalla versione 17.3.1. Ciò significa che l'autenticazione non riesce se si aggiunge un indirizzo MAC con separatori nell'interfaccia utente Web o nella CLI.
- A partire dalla versione 17.3.1, gli access point vengono ricaricati dopo 4 ore se non sono in grado di collegarsi a un WLC, non possono eseguire il ping del gateway e l'ARP del gateway (per riavviare l'access point, tutte e tre devono avere esito negativo). si tratta di un miglioramento (ID bug Cisco CSCvt89970) alla verifica del gateway ICMP precedente alle versioni precedenti.
- 17.3.1 in poi, il nuovo modo di configurare i codici paese per gli access point è il `Wireless country <1 country code>` che è possibile ripetere più volte con diversi codici paese. Ciò consente di aumentare la quantità massima di codice paese oltre 20. I comandi `ap country` sono ancora presenti e stanno lavorando, tuttavia, valutano la possibilità di `Wireless country` comandi come `ap country` i comandi saranno obsoleti in una versione futura.
- Quando si esegue l'aggiornamento alla versione 17.3.4 e successive, si consiglia di installare il bootloader/rommon 16.12.5r sui controller dove è applicabile (9800-80). (al momento, lo switch 9800-40 non dispone di un rommon 16.12.5r e non ha bisogno di un aggiornamento di rommon).
- L'aggiornamento del controller, da Cisco IOS XE Bengaluru 17.3.x a qualsiasi versione con

ISSU, può non riuscire se il snmp-server enable traps hsrpè configurato. Accertarsi di rimuovere snmp-server enable traps hsrp dalla configurazione prima di avviare l'aggiornamento di un modulo ISSU perché snmp-server enable traps hsrp viene rimosso da Cisco IOS XE Bengaluru 17.4.x.

- Durante l'aggiornamento a Cisco IOS XE 17.3.x e versioni successive, se ip http active-session-modules none è abilitato, non è possibile accedere alla GUI del controller utilizzando HTTPS. Per accedere alla GUI con HTTPS, eseguire questi comandi:
    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist

## Bengaluru

17.4.1

- a partire dalla versione 17.4.1, gli access point Cisco IOS della versione 1 non sono più supportati (1700,2700,3700,1570), ad eccezione di IW3700.
- Le WLAN possono essere arrestate dopo l'aggiornamento se non sono WPA (Guest, Open o CWA SSID) e se hanno FT adattivo configurato. La soluzione è rimuovere la configurazione FT adattiva prima dell'aggiornamento (ID bug Cisco CSCvx34349). La configurazione Adaptive FT non ha alcun senso su SSID non WPA, quindi non vi è alcuna perdita di dati rimuovendoli.
- Il WLC può bloccarsi se i tuoi AP hanno nomi host più lunghi di 32 caratteri (ID bug Cisco CSCvy11981).

17.5.1

- a partire dalla versione 17.4.1, gli access point Cisco IOS della versione 1 non sono più supportati (1700,2700,3700,1570), ad eccezione di IW3700.
- A partire da Cisco IOS XE Bengaluru versione 17.4.1, la soluzione di telemetria fornisce un nome per l'indirizzo del destinatario anziché l'indirizzo IP per i dati di telemetria. Si tratta di un'opzione aggiuntiva. Durante il downgrade del controller e il successivo aggiornamento, è probabile che si verifichi un problema con la versione di aggiornamento che utilizza i nuovi ricevitori e questi non vengono riconosciuti nel downgrade. La nuova configurazione viene rifiutata e non riesce nel successivo aggiornamento. È possibile evitare la perdita di configurazione quando si esegue l'aggiornamento o il downgrade da Cisco DNA Center.
- Le WLAN possono essere arrestate dopo l'aggiornamento se non sono WPA (Guest, Open o CWA SSID) e se hanno FT adattivo configurato. La soluzione è rimuovere la configurazione FT adattiva prima dell'aggiornamento (ID bug Cisco CSCvx34349). La configurazione Adaptive FT non ha alcun senso su SSID non WPA, quindi non vi è alcuna perdita di dati rimuovendoli.
- Il WLC può bloccarsi se i tuoi AP hanno nomi host più lunghi di 32 caratteri (ID bug Cisco CSCvy11981).
- Quando si aggiorna la GUI da una versione a un'altra, si consiglia di cancellare la cache del browser per ricaricare correttamente tutte le pagine della GUI.

- Durante l'aggiornamento a Cisco IOS XE 17.3.x e versioni successive, se ip http active-session-modules none è abilitato, non è possibile accedere alla GUI utilizzando HTTPS. Per accedere alla GUI con HTTPS, eseguire questi comandi:
    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist
- Se si verifica l'errore "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" dalla GUI dopo un riavvio o un arresto anomalo del sistema, si consiglia di rigenerare il certificato del trust point.
- La procedura per generare un nuovo trust firmato è la seguente:

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http authentic
```

```
! use local or aaa as applicable.
```

17.6.1

- a partire dalla versione 17.4.1, gli access point Cisco IOS della versione 1 non sono più supportati (1700,2700,3700,1570), ad eccezione di IW3700.
- A partire da Cisco IOS XE Bengaluru versione 17.4.1, la soluzione di telemetria fornisce un nome per l'indirizzo del destinatario anziché l'indirizzo IP per i dati di telemetria. Si tratta di un'opzione aggiuntiva. Durante il downgrade del controller e il successivo aggiornamento, è probabile che si verifichi un problema con la versione di aggiornamento che utilizza i nuovi ricevitori e questi non vengono riconosciuti nel downgrade. La nuova configurazione viene rifiutata e non riesce nel successivo aggiornamento. È possibile evitare la perdita di configurazione quando si esegue l'aggiornamento o il downgrade da Cisco DNA Center.
- Le WLAN possono essere arrestate dopo l'aggiornamento se non sono WPA (Guest, Open o CWA SSID) e se hanno FT adattivo configurato. La soluzione è rimuovere la configurazione FT adattiva prima dell'aggiornamento (ID bug Cisco CSCvx34349). La configurazione

Adaptive FT non ha alcun senso su SSID non WPA, quindi non vi è alcuna perdita di dati rimuovendoli.

- Quando si aggiorna la GUI da una versione a un'altra, si consiglia di cancellare la cache del browser per ricaricare correttamente tutte le pagine della GUI.
- Un access point che si è unito a un WLC della versione 17.6.1 o successive non può più unirsi a un WLC di AireOS a meno che non esegua il codice 8.10.162 e versioni successive o il codice 8.5.176.2 e versioni successive.
- Con l'aggiornamento alla versione 17.6,1 e successive, si consiglia di installare il bootloader/rommon 16.12.5r sui controller dove è applicabile (9800-80). (al momento, lo switch 9800-40 non dispone di un rommon 16.12.5r e non ha bisogno di un aggiornamento di rommon).
- L'aggiornamento del controller, da Cisco IOS XE Bengaluru 17.3.x a qualsiasi versione con ISSU, può non riuscire se il `snmp-server enable traps hsrp`è configurato. Accertarsi di rimuovere `snmp-server enable traps hsrp` dalla configurazione prima di avviare l'aggiornamento di un modulo ISSU perché `snmp-server enable traps hsrp` viene rimosso da Cisco IOS XE Bengaluru 17.4.x.
- Durante l'aggiornamento a Cisco IOS XE 17.3.x e versioni successive, se `ip http active-session-modules none` è abilitato, l'accesso HTTPS alla GUI del controller non funziona. Per accedere alla GUI con HTTPS, eseguire questi comandi:
    - ip http session-module-list pkilist OPENRESTY_PKI
    - ip http active-session-modules pkilist
- Se si verifica l'errore "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" dalla GUI dopo un riavvio o un arresto anomalo del sistema, si consiglia di rigenerare il certificato del trust point.
- La procedura per generare un nuovo trust firmato è la seguente:

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http securffwe-server ip http server ip http secure-server ip http authen
```

```
! use local or aaa as applicable.
```

17.6.2

- a partire dalla versione 17.4.1, gli access point Cisco IOS della versione 1 non sono più supportati (1700,2700,3700,1570), ad eccezione di IW3700.
- A partire da Cisco IOS XE Bengaluru versione 17.4.1, la soluzione di telemetria fornisce un nome per l'indirizzo del destinatario anziché l'indirizzo IP per i dati di telemetria. Si tratta di un'opzione aggiuntiva. Durante il downgrade del controller e il successivo aggiornamento, è probabile che si verifichi un problema con la versione di aggiornamento che utilizza i nuovi ricevitori e questi non vengono riconosciuti nel downgrade. La nuova configurazione viene rifiutata e non riesce nel successivo aggiornamento. È possibile evitare la perdita di configurazione quando si esegue l'aggiornamento o il downgrade da Cisco DNA Center.
- Le WLAN possono essere arrestate dopo l'aggiornamento se non sono WPA (Guest, Open o CWA SSID) e se hanno FT adattivo configurato. La soluzione è rimuovere la configurazione FT adattiva prima dell'aggiornamento (ID bug Cisco CSCvx34349). La configurazione Adaptive FT non ha alcun senso su SSID non WPA, quindi non vi è alcuna perdita di dati rimuovendoli.
- Quando si aggiorna la GUI da una versione a un'altra, si consiglia di cancellare la cache del browser per ricaricare correttamente tutte le pagine della GUI.
- Un access point che si è unito a un WLC della versione 17.6.1 o successive non può più unirsi a un WLC di AireOS a meno che non esegua il codice 8.10.162 e versioni successive o il codice 8.5.176.2 e versioni successive.
- Con l'aggiornamento alla versione 17.6,1 e successive, si consiglia di installare il bootloader/rommon 16.12.5r sui controller dove è applicabile (9800-80). (al momento, lo switch 9800-40 non dispone di un rommong 16.12.5r e non richiede un aggiornamento a rommon).
- L'aggiornamento del controller, da Cisco IOS XE Bengaluru 17.3.x a qualsiasi versione con ISSU, può non riuscire se il `snmp-server enable traps hsrp`è configurato. Accertarsi di rimuovere `snmp-server enable traps hsrp` dalla configurazione prima di avviare l'aggiornamento di un modulo ISSU perché `snmp-server enable traps hsrp` viene rimosso da Cisco IOS XE Bengaluru 17.4.x.

- Durante l'aggiornamento a Cisco IOS XE 17.3.x e versioni successive, se `ip http active-session-modules none` è abilitato, l'accesso all'interfaccia utente del controller HTTPS non funziona. Per accedere alla GUI con HTTPS, eseguire questi comandi:

    - ip http session-module-list pkilist OPENRESTY_PKI

    - ip http active-session-modules pkilist

- Non utilizzare più di 31 caratteri per i nomi dei punti di accesso. Se il nome del punto di accesso è composto da almeno 32 caratteri, può verificarsi un arresto anomalo del controller.

- Se si verifica l'errore "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" dalla GUI dopo un riavvio o un arresto anomalo del sistema, si consiglia di rigenerare il certificato del trust point.

- La procedura per generare un nuovo trust firmato è la seguente:

```
configure terminal
no crypto pki trustpoint
```

```
no ip http server no ip http secure-server ip http server ip http secure-server ip http authentic
```

```
! use local or aaa as applicable.
```

## Cupertino

in questa sezione si presume che l'utente stia iniziando dalla versione 17.6.1 o successive e stia eseguendo l'aggiornamento a una release di Cupertino. Se si sta eseguendo l'aggiornamento direttamente da una release precedente (che può essere supportata, controllare le note sulla release per essere certi), leggere le avvertenze della sezione 17.3 e 17.6.

17.7.1

- Non utilizzare più di 31 caratteri per i nomi dei punti di accesso. Se il nome del punto di accesso è composto da almeno 32 caratteri, può verificarsi un arresto anomalo del controller.
- La versione 17.7.1 richiede che i codici dei paesi AP siano configurati nei profili di join AP.
- A causa dell'ID bug Cisco CSCvu22886, se si hanno 9130 o 9124 AP, è necessario passare alla versione 17.3.5a quando si esegue l'aggiornamento alla versione 17.7.1 o successive da una versione precedente alla 17.3.4.
- A partire da Cisco IOS XE Cupertino 17.7.1, per il controller wireless Cisco Catalyst 9800-CL, verificare di aver completato il report relativo alla misurazione dell'utilizzo delle risorse (RUM, Resource Utilization Measurement) e di aver reso disponibile l'ACK sull'istanza del prodotto almeno una volta. In questo modo, le informazioni sull'utilizzo corrette e aggiornate vengono riflesse in Cisco Smart Software Manager (CSSM). In caso contrario, un massimo di 50 access point può unirsi a uno switch 9800-CL finché non viene generato un report di licenza ACK.

17.8.1

- Non utilizzare più di 31 caratteri per i nomi dei punti di accesso. Se il nome del punto di

accesso è composto da almeno 32 caratteri, può verificarsi un arresto anomalo del controller.
- La versione 17.7.1 richiede che i codici dei paesi AP siano configurati nei profili di join AP.
- A causa dell'ID bug Cisco CSCvu22886, se si hanno 9130 o 9124 AP, è necessario passare alla versione 17.3.5a quando si esegue l'aggiornamento alla versione 17.7.1 o successive a partire da una versione precedente alla 17.3.4.
- Cisco IOS XE Cupertino versione 17.7.1 o successive, per il controller wireless Cisco Catalyst 9800-CL, verificare di aver completato il reporting RUM e di aver reso disponibile l'ACK sull'istanza del prodotto almeno una volta. In questo modo, le informazioni corrette e aggiornate sull'utilizzo vengono riflesse nel CSSM. In caso contrario, un massimo di 50 access point può unirsi a uno switch 9800-CL finché non viene generato un report di licenza ACK.

17,9 x

- I punti di accesso con Cisco IOS-XE 17.9.3 possono incontrare problemi durante il tentativo di aggiornare il software a causa di spazio insufficiente nel /tmp directory. Quando il /tmp lo spazio sull'access point si esaurisce, impedisce il download della nuova immagine. In questi casi, è consigliabile riavviare l'access point.

- 11AC I punti di accesso Wave 2 possono entrare in un loop di avvio quando si aggiorna il software su un collegamento WAN. Per ulteriori informazioni, visitare il sito Web all'indirizzo https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- la versione 17.9.3 e successive ripristinano il supporto per gli access point basati su Cisco IOS (serie x700 e 1570). Non sono stati supportati tra il 17.4 e il 17.9.2. Il supporto per questi AP non si estende oltre il normale supporto del ciclo di vita del prodotto. Fare riferimento ai singoli bollettini di fine supporto sul sito Cisco.com.
- L'aggiornamento del controller da Cisco IOS XE Bengaluru 17.3.x a Cisco IOS XE Bengaluru 17.6.x o Cisco IOS XE Cupertino 17.9.x e versioni successive con ISSU può avere esito negativo se è configurato il comando domain. Accertarsi di eseguire il comando no domain prima di avviare un aggiornamento di IOS perché il comando domain è stato rimosso da Cisco IOS XE Bengaluru 17.6.x.
- Cisco IOS XE Cupertino versione 17.7.1 o successive, per il controller wireless Cisco Catalyst 9800-CL, verificare di aver completato il reporting RUM e di aver reso disponibile l'ACK sull'istanza del prodotto almeno una volta. In questo modo, le informazioni corrette e aggiornate sull'utilizzo vengono riflesse nel CSSM. In caso contrario, un massimo di 50 access point può unirsi a uno switch 9800-CL finché non viene generato un report di licenza ACK.
- La frammentazione inferiore a 1500 non è supportata per i pacchetti RADIUS generati dai client wireless nell'interfaccia Gi0 (OOB).
- A partire dal 17.3, il modello 9800-CL richiede 16 GB di spazio su disco per funzionare correttamente. Non è possibile aumentare dinamicamente le dimensioni se l'istanza WLC è iniziata con un OAV da 8 GB (precedente alla versione 17.3). L'unico modo è creare un nuovo WLC da un OVA datato più tardi del 17.3.

- Il controller wireless Cisco Catalyst 9800-L può non rispondere ai segnali di interruzione ricevuti sulla porta della console durante il tempo di avvio, impedendo agli utenti di raggiungere il rommon. Questo problema viene osservato sui controller prodotti fino a novembre 2019, con l'impostazione predefinita del registro di configurazione 0x2102. Per evitare questo problema, impostare config-register su 0x2002. Questo problema è stato risolto nella versione 16.12(3r) rommon per il controller wireless Cisco Catalyst 9800-L. Per informazioni sull'aggiornamento di rommon, vedere la Upgrading rommon for Cisco Catalyst 9800-L Wireless Controllers del documento Aggiornamento dei dispositivi hardware programmabili per esterni per Cisco Catalyst serie 9800 Wireless Controller.

- Se questo messaggio di errore viene visualizzato dopo un riavvio o un arresto anomalo del sistema, è consigliabile rigenerare il certificato del punto di attendibilità:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

  Utilizzare questi comandi nell'ordine specificato per generare un nuovo certificato trust point autofirmato:

  1. device# configure terminal
  2. device(config)# no crypto pki trustpoint trustpoint_name
  3. device(config)# no ip http server
  4. device(config)# no ip http secure-server
  5. device(config)# ip http server
  6. device(config)# ip http secure-server
  7. device(config)# ip http authentication local/aaa

- Verificare che l'indirizzo MAC di mobilità sia impostato con wireless mobility mac-address
- Questi protocolli sono ora supportati tramite la porta di servizio nella versione 17.9:
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - GUI del controller
  - DNS

    - Trasferimento di file
    - GNMI
    - HTTP
    - HTTPS
    - LDAP
    - Gestione licenze per la funzionalità Smart Licensing per la comunicazione con CSM
    - Netconf
    - NetFlow
    - NTP
    - RADIUS (incluso CoA)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- L'immagine AP per la versione 17.9 è più grande del flash AP originariamente consentito. Se l'access point si lamenta di non avere spazio sufficiente per il download dell'immagine 17.9, è probabile che il percorso di aggiornamento alla versione 17.3.5 non sia stato rispettato, come indicato nelle note sulla versione, o che l'access point stia eseguendo un'immagine AireOS meno recente. Il passaggio da un WLC versione 17.3.5 o successive o l'aggiornamento dell'immagine AireOS alla versione più recente comporta il ridimensionamento del flash dell'access point per consentire il download dell'immagine 17.9.

## Dublino

17.10.1

- La funzionalità Cisco Centralized Key Management (CCKM) è stata deprecata da Cisco IOS XE Dublin 17.10.x.
- Smart Call Home sta diventando deprecato a favore di Smart Transport per le licenze.
- I punti di accesso con Cisco IOS-XE 17.9.3 o versioni successive possono incontrare problemi durante il tentativo di aggiornare il software a causa di spazio insufficiente nel `/tmp` directory. Quando il `/tmp` lo spazio sull'access point si esaurisce, impedisce il download della nuova immagine. In questi casi, è consigliabile riavviare l'access point.

I punti di accesso Wave 2 possono entrare in un loop di avvio quando si aggiorna il software su un collegamento WAN. Per ulteriori informazioni, visitare il sito Web all'indirizzo https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- A partire da Cisco IOS XE Cupertino 17.7.1, per il controller wireless Cisco Catalyst 9800-CL, verificare di aver completato il reporting RUM e di aver reso disponibile l'ACK sull'istanza del prodotto almeno una volta. In questo modo, le informazioni corrette e aggiornate sull'utilizzo vengono riflesse nel CSSM. In caso contrario, un massimo di 50 access point può unirsi a uno switch 9800-CL finché non viene generato un report di licenza ACK.
- La frammentazione inferiore a 1500 non è supportata per i pacchetti RADIUS generati dai client wireless nell'interfaccia Gi0 (OOB).
- A partire dal 17.3, il modello 9800-CL richiede 16 GB di spazio su disco per funzionare correttamente. Non è possibile aumentare dinamicamente le dimensioni se l'istanza WLC è iniziata con un OAV da 8 GB (precedente alla versione 17.3). L'unico modo è creare un nuovo WLC da un OVA datato più tardi del 17.3.
- Il controller wireless Cisco Catalyst 9800-L può non rispondere ai segnali BREAK ricevuti sulla porta della console durante il tempo di avvio, impedendo agli utenti di raggiungere il rommon. Questo problema viene osservato sui controller prodotti fino a novembre 2019, con l'impostazione predefinita del registro di configurazione 0x2102. Per evitare questo problema, impostare config-register su 0x2002. Il problema è stato risolto nella versione 16.12(3r) rommon per il controller wireless Cisco Catalyst 9800-L. Per informazioni su come aggiornare rommon, vedere la sezione Aggiornamento di rommon per Cisco Catalyst 9800-L Wireless Controller nel documento sull'aggiornamento dei dispositivi hardware programmabili per Cisco Catalyst serie 9800 Wireless Controller.

- Se questo messaggio di errore viene visualizzato dopo un riavvio o un arresto anomalo del sistema, è consigliabile rigenerare il certificato del punto di attendibilità:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Utilizzare questi comandi nell'ordine specificato per generare un nuovo certificato trust point autofirmato:

1. device# configure terminal
2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server

7. device(config)# ip http authentication local/aaa

- Verificare che l'indirizzo MAC di mobilità sia impostato con wireless mobility mac-address
- Questi protocolli sono ora supportati tramite la porta di servizio nella versione 17.9:
    - Cisco DNA Center
    - Cisco Smart Software Manager
    - Cisco Prime Infrastructure
    - Telnet
    - GUI del controller
    - DNS
    - Trasferimento di file
    - GNMI
    - HTTP
    - HTTPS
    - LDAP
    - Gestione licenze per la funzionalità Smart Licensing per la comunicazione con CSM
    - Netconf
    - NetFlow
    - NTP
    - RADIUS (incluso CoA)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+
- L'immagine AP per la versione 17.9 è più grande del flash AP originariamente consentito. Se l'access point si lamenta di non avere spazio sufficiente per il download dell'immagine 17.9, è probabile che il percorso di aggiornamento alla versione 17.3.5 non sia stato rispettato, come indicato nelle note sulla versione, o che l'access point stia eseguendo un'immagine AireOS meno recente. Il passaggio da un WLC versione 17.3.5 a una versione successiva o

l'aggiornamento dell'immagine AireOS alla versione più recente comporta il ridimensionamento del flash AP per consentire il download dell'immagine 17.9.

17.11.1

- La funzionalità CCKM è stata obsoleta da Cisco IOS XE Dublin 17.10.x.
- Smart Call Home sta diventando deprecato a favore di Smart Transport per le licenze

- I punti di accesso con Cisco IOS-XE 17.9.3 o versioni successive possono incontrare problemi durante il tentativo di aggiornare il software a causa di spazio insufficiente nel /tmp directory. Quando il /tmp lo spazio sull'access point si esaurisce, impedisce il download della nuova immagine. In questi casi, è consigliabile riavviare l'access point.

  I punti di accesso Wave 2 possono entrare in un loop di avvio quando si aggiorna il software su un collegamento WAN. Per ulteriori informazioni, visitare il sito Web all'indirizzo https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- Cisco IOS XE Cupertino versione 17.7.1 o successive, per il controller wireless Cisco Catalyst 9800-CL, verificare di aver completato il reporting RUM e che l'ACK sia disponibile nell'istanza del prodotto almeno una volta. In questo modo, le informazioni corrette e aggiornate sull'utilizzo vengono riflesse nel CSSM. In caso contrario, un massimo di 50 access point può unirsi a uno switch 9800-CL finché non viene generato un report di licenza ACK.
- La frammentazione inferiore a 1500 non è supportata per i pacchetti RADIUS generati dai client wireless nell'interfaccia Gi0 (OOB).
- A partire dal 17.3, il modello 9800-CL richiede 16 GB di spazio su disco per funzionare correttamente. Non è possibile aumentare dinamicamente le dimensioni se l'istanza WLC è iniziata con un OAV da 8 GB (precedente alla versione 17.3). L'unico modo è creare un nuovo WLC da un OVA datato più tardi del 17.3.
- Il controller wireless Cisco Catalyst 9800-L può non rispondere ai segnali di interruzione ricevuti sulla porta della console durante il tempo di avvio, impedendo agli utenti di raggiungere il rommon. Questo problema viene osservato sui controller prodotti fino a novembre 2019, con l'impostazione predefinita del registro di configurazione 0x2102. Per evitare questo problema, impostare config-register su 0x2002. Questo problema è stato risolto nella versione 16.12(3r) rommon per il controller wireless Cisco Catalyst 9800-L. Per informazioni su come aggiornare rommon, vedere la sezione Aggiornamento di rommon per Cisco Catalyst 9800-L Wireless Controller nel documento sull'aggiornamento dei dispositivi hardware programmabili per Cisco Catalyst serie 9800 Wireless Controller.

- Se questo messaggio di errore viene visualizzato dopo un riavvio o un arresto anomalo del sistema, è consigliabile rigenerare il certificato del punto di attendibilità:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Utilizzare questi comandi nell'ordine specificato per generare un nuovo certificato trust point autofirmato:

1. device# configure terminal
2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server
7. device(config)# ip http authentication local/aaa

- Verificare che l'indirizzo MAC di mobilità sia impostato con wireless mobility mac-address
- Questi protocolli sono ora supportati tramite la porta di servizio nella versione 17.9:
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - GUI del controller
  - DNS
  - Trasferimento di file
  - GNMI
  - HTTP
  - HTTPS
  - LDAP
  - Gestione licenze per la funzionalità Smart Licensing per la comunicazione con CSM
  - Netconf
  - NetFlow
  - NTP

    - RADIUS (incluso CoA)
    - Restconf
    - SNMP
    - SSH
    - SYSLOG
    - TACACS+

- L'immagine AP per la versione 17.9 è più grande del flash AP originariamente consentito. Se l'access point si lamenta di non avere spazio sufficiente per il download dell'immagine 17.9, è probabile che il percorso di aggiornamento alla versione 17.3.5 non sia stato rispettato, come indicato nelle note sulla versione, o che l'access point stia eseguendo un'immagine AireOS meno recente. Il passaggio da un WLC versione 17.3.5 a una versione successiva o l'aggiornamento dell'immagine AireOS alla versione più recente comporta il ridimensionamento del flash AP per consentire il download dell'immagine 17.9.

17.12.1

- La funzionalità CCKM è stata obsoleta da Cisco IOS XE Dublin 17.10.x.
- Smart Call Home sta diventando deprecato a favore di Smart Transport per le licenze.

- I punti di accesso con Cisco IOS-XE 17.9.3 o versioni successive possono incontrare problemi durante il tentativo di aggiornare il software a causa di spazio insufficiente nel `/tmp` directory. Quando il `/tmp` lo spazio sull'access point si esaurisce, impedisce il download della nuova immagine. In questi casi, è consigliabile riavviare l'access point.

  I punti di accesso Wave 2 possono entrare in un loop di avvio quando si aggiorna il software su un collegamento WAN. Per ulteriori informazioni, visitare il sito Web all'indirizzo https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

- la versione 17.12.1 e successive ripristinano il supporto per gli access point basati su Cisco IOS (serie x700 e 1570). Non sono stati supportati tra il 17.4 e il 17.9.2. Il supporto per questi AP non si estende oltre il normale supporto del ciclo di vita del prodotto. Fare riferimento ai singoli bollettini di fine supporto sul sito Cisco.com.
- Cisco IOS XE Cupertino versione 17.7.1 o successive, per il controller wireless Cisco Catalyst 9800-CL, verificare di aver completato il reporting RUM e di aver reso disponibile l'ACK sull'istanza del prodotto almeno una volta. In questo modo, le informazioni corrette e aggiornate sull'utilizzo vengono riflesse nel CSSM. In caso contrario, un massimo di 50 access point può unirsi a uno switch 9800-CL finché non viene generato un report di licenza ACK.
- La frammentazione inferiore a 1500 non è supportata per i pacchetti RADIUS generati dai client wireless nell'interfaccia Gi0 (OOB).
- A partire dal 17.3, il modello 9800-CL richiede 16 GB di spazio su disco per funzionare

correttamente. Non è possibile aumentare dinamicamente le dimensioni se l'istanza WLC è iniziata con un OAV da 8 GB (precedente alla versione 17.3). L'unico modo è creare un nuovo WLC da un OVA datato più tardi del 17.3.

- Il controller wireless Cisco Catalyst 9800-L può non rispondere ai segnali di interruzione ricevuti sulla porta della console durante il tempo di avvio, impedendo agli utenti di raggiungere il rommon. Questo problema viene osservato sui controller prodotti fino a novembre 2019, con l'impostazione predefinita del registro di configurazione 0x2102. Per evitare questo problema, impostare config-register su 0x2002. Questo problema è stato risolto nella versione 16.12(3r) rommon per il controller wireless Cisco Catalyst 9800-L. Per informazioni su come aggiornare rommon, vedere la sezione Aggiornamento di rommon per Cisco Catalyst 9800-L Wireless Controller nel documento sull'aggiornamento dei dispositivi hardware programmabili per Cisco Catalyst serie 9800 Wireless Controller.

- Se questo messaggio di errore viene visualizzato dopo un riavvio o un arresto anomalo del sistema, è consigliabile rigenerare il certificato del punto di attendibilità:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

Utilizzare questi comandi nell'ordine specificato per generare un nuovo certificato trust point autofirmato:

1. device# configure terminal
2. device(config)# no crypto pki trustpoint trustpoint_name
3. device(config)# no ip http server
4. device(config)# no ip http secure-server
5. device(config)# ip http server
6. device(config)# ip http secure-server
7. device(config)# ip http authentication local/aaa

- Verificare che l'indirizzo MAC di mobilità sia impostato con wireless mobility mac-address
- Questi protocolli sono ora supportati tramite la porta di servizio nella versione 17.9:
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet

- GUI del controller
- DNS
- Trasferimento di file
- GNMI
- HTTP
- HTTPS
- LDAP
- Gestione licenze per la funzionalità Smart Licensing per la comunicazione con CSM
- Netconf
- NetFlow
- NTP
- RADIUS (incluso CoA)
- Restconf
- SNMP
- SSH
- SYSLOG
- TACACS+

- L'immagine AP per la versione 17.9 è più grande del flash AP originariamente consentito. Se l'access point si lamenta di non avere spazio sufficiente per il download dell'immagine 17.9, è probabile che il percorso di aggiornamento alla versione 17.3.5 non sia stato rispettato, come indicato nelle note sulla versione, o che l'access point stia eseguendo un'immagine AireOS meno recente. Mediante il passaggio da un WLC versione 17.3.5 e successive o l'aggiornamento dell'immagine AireOS alla versione più recente, il flash AP viene ridimensionato per consentire il download dell'immagine 17.9.

# Declassa

I downgrade non sono ufficialmente supportati e la configurazione può andare persa. Tuttavia, poiché il declassamento può avvenire nel mondo reale, questo documento elenca ancora le trappole più comuni per evitare il declassamento. Per trovare le informazioni necessarie, verificare la versione da cui si sta effettuando il downgrade (la versione precedente al downgrade).

## Gibilterra

16.12.2

- Non c'è niente da segnalare.

16.12.3

- Il ricaricamento continuo viene osservato quando si esegue il downgrade di Cisco Catalyst 9800 Wireless Controller da 17.x a 16.12.4a. Si consiglia di effettuare il downgrade a Cisco IOS XE Gibraltar 16.12.5 anziché 16.12.4a.

16.12.4

- Se si esegue il downgrade da questa versione a una precedente, il WLC può terminare in un loop di avvio se la telemetria è stata configurata a causa dell'ID bug Cisco CSCvt6990/ID bug Cisco CSCvv87417.
- Il controller wireless Cisco Catalyst 9800 può essere ricaricato se viene eseguito il downgrade da 17.x a 16.12.4a. Per evitare ciò, si consiglia di effettuare il downgrade a Cisco IOS XE Gibraltar 16.12.5 anziché 16.12.4a.

## Amsterdam

17.1.1

- Se si esegue il downgrade da questa versione a una precedente, il WLC può terminare in un loop di avvio se la telemetria è stata configurata a causa dell'ID bug Cisco CSCvt6990/CSCvv8741.
- Il ricaricamento continuo viene osservato quando si esegue il downgrade di Cisco Catalyst 9800 Wireless Controller da 17.x a 16.12.4a. Si consiglia di effettuare il downgrade a Cisco IOS XE Gibraltar 16.12.5 anziché 16.12.4a.

17.2.1

- Se si esegue il downgrade da questa versione a una precedente, il WLC può terminare in un loop di avvio se la telemetria è stata configurata a causa dell'ID bug Cisco CSCvt6990/ID bug Cisco CSCvv87417.
- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.3.1 a una versione precedente, i canali delle porte configurati con un intervallo superiore a quattro scompaiono.
- Il ricaricamento continuo viene osservato quando si esegue il downgrade di Cisco Catalyst 9800 Wireless Controller da 17.x a 16.12.4a. Si consiglia di effettuare il downgrade a Cisco IOS XE Gibraltar 16.12.5 anziché 16.12.4a.

17.3.1

- Se si esegue il downgrade da questa versione a una precedente, il WLC può terminare in un loop di avvio se la telemetria è stata configurata a causa dell'ID bug Cisco CSCvt6990

/CSCvv8741.

- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.3.1 a una versione precedente, i canali delle porte configurati con un intervallo più alto scompaiono.
- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.3.1 a una versione precedente, è possibile passare di nuovo alla procedura guidata del giorno 0 se il comando "wireless country" è stato configurato in quanto non esisteva prima della versione 17.3.
- Il ricaricamento continuo viene osservato quando si esegue il downgrade di Cisco Catalyst 9800 Wireless Controller da 17.x a 16.12.4a. Si consiglia di effettuare il downgrade a Cisco IOS XE Gibraltar 16.12.5 anziché 16.12.4a.
- Non è possibile arrestare il profilo della policy WLAN quando si esegue il downgrade da Cisco IOS XE Amsterdam 17.3.x (supporto della commutazione locale per IPv6 AVC) a Cisco IOS XE Gibraltar 16.12.x (dove la commutazione locale per IPv6 AVC non è supportata). In questi casi, è consigliabile eliminare il profilo dei criteri WLAN esistente e crearne uno nuovo.

17.3.2

- Se si effettua il downgrade da questa release a una precedente, il WLC termina in un loop di avvio se la telemetria è stata configurata a causa dell'ID bug Cisco CSCvt6990/ID bug Cisco CSCvv87417.
- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.3.1 a una versione precedente, i canali delle porte configurati con un intervallo più alto scompaiono.
- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.3.1 a una versione precedente, è possibile passare di nuovo alla procedura guidata del giorno 0 se il comando "wireless country" è stato configurato in quanto non esisteva prima della versione 17.3.
- Il ricaricamento continuo viene osservato quando si esegue il downgrade di Cisco Catalyst 9800 Wireless Controller da 17.x a 16.12.4a. Si consiglia di effettuare il downgrade a Cisco IOS XE Gibraltar 16.12.5 anziché 16.12.4a.
- Non è possibile arrestare il profilo della policy WLAN quando si esegue il downgrade da Cisco IOS XE Amsterdam 17.3.x (supporto della commutazione locale per IPv6 AVC) a Cisco IOS XE Gibraltar 16.12.x (dove la commutazione locale per IPv6 AVC non è supportata). In questi casi, è consigliabile eliminare il profilo dei criteri WLAN esistente e crearne uno nuovo.

17.3.3

- Se si esegue il downgrade da questa versione a una precedente, il WLC può terminare in un loop di avvio se la telemetria è stata configurata a causa dell'ID bug Cisco CSCvt6990/ID bug Cisco CSCvv87417.
- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.3.1 a una versione precedente, i canali delle porte configurati con un intervallo più alto scompaiono.
- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.3.1 a una versione precedente, è possibile passare di nuovo alla procedura guidata del giorno 0 se il comando "wireless country" è stato configurato in quanto non esisteva prima della versione 17.3.
- Il ricaricamento continuo viene osservato quando si esegue il downgrade di Cisco Catalyst

9800 Wireless Controller da 17.x a 16.12.4a. Si consiglia di effettuare il downgrade a Cisco IOS XE Gibraltar 16.12.5 anziché 16.12.4a.
- Non è possibile arrestare il profilo della policy WLAN quando si esegue il downgrade da Cisco IOS XE Amsterdam 17.3.x (supporto della commutazione locale per IPv6 AVC) a Cisco IOS XE Gibraltar 16.12.x (dove la commutazione locale per IPv6 AVC non è supportata). In questi casi, è consigliabile eliminare il profilo dei criteri WLAN esistente e crearne uno nuovo.

17.4.1

- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.4.1 a una versione precedente alla 17.3, è possibile eseguire di nuovo la procedura guidata del giorno 0 se il comando "wireless country" è stato configurato in quanto non esisteva prima della 17.3.
- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.4.1 a una versione precedente, la connessione di telemetria viene interrotta perché la versione 17.4 utilizza destinazioni di telemetria denominate che nelle versioni precedenti non erano supportate. È necessario ricreare la connessione di telemetria.
- Il ricaricamento continuo viene osservato quando si esegue il downgrade di Cisco Catalyst 9800 Wireless Controller da 17.x a 16.12.4a. Si consiglia di effettuare il downgrade a Cisco IOS XE Gibraltar 16.12.5 anziché 16.12.4a.

17.5.1

- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.4.1 a una versione precedente alla 17.3, è possibile eseguire di nuovo la procedura guidata del giorno 0 se il comando "wireless country" è stato configurato in quanto non esisteva prima della 17.3.
- Se si esegue il downgrade da Cisco IOS XE Amsterdam 17.4.1 a una versione precedente, la connessione di telemetria viene interrotta perché la versione 17.4 utilizza destinazioni di telemetria denominate che nelle versioni precedenti non erano supportate. È necessario ricreare la connessione di telemetria.
- Il ricaricamento continuo viene osservato quando si esegue il downgrade di Cisco Catalyst 9800 Wireless Controller da 17.x a 16.12.4a. Si consiglia di effettuare il downgrade a Cisco IOS XE Gibraltar 16.12.5 anziché 16.12.4a.

17,9 x

- In questa release non è possibile visualizzare le password 802.1x in testo non crittografato perché sono crittografate. Se si esegue il downgrade a un'immagine precedente che non supporta una password crittografata, gli access point rimangono bloccati e ripetutamente non riescono a eseguire l'autenticazione dot1x a causa di credenziali errate. È necessario disabilitare 802.1x sulla porta dello switch AP per consentire all'access point di collegarsi al controller prima di impostare la password non crittografata.

17.10.1

- Da questa release non è possibile visualizzare le password 802.1x in testo non crittografato

perché sono crittografate. Se si esegue il downgrade a un'immagine precedente che non supporta una password crittografata, gli access point rimangono bloccati e ripetutamente non riescono a eseguire l'autenticazione dot1x a causa di credenziali errate. È necessario disabilitare 802.1x sulla porta dello switch AP per consentire all'access point di collegarsi al controller prima di impostare la password non crittografata.

17.11.1

- Da questa release non è possibile visualizzare le password 802.1x in testo non crittografato perché sono crittografate. Se si esegue il downgrade a un'immagine precedente che non supporta una password crittografata, gli access point rimangono bloccati e ripetutamente non riescono a eseguire l'autenticazione dot1x a causa di credenziali errate. È necessario disabilitare 802.1x sulla porta dello switch AP per consentire all'access point di collegarsi al controller prima di impostare la password non crittografata.

17.12.x

- Da questa release non è possibile visualizzare le password 802.1x in testo non crittografato perché sono crittografate. Se si esegue il downgrade a un'immagine precedente che non supporta una password crittografata, gli access point rimangono bloccati e ripetutamente non riescono a eseguire l'autenticazione dot1x a causa di credenziali errate. È necessario disabilitare 802.1x sulla porta dello switch AP per consentire all'access point di collegarsi al controller prima di impostare la password non crittografata.

## Informazioni correlate

- 17.1 guida all'aggiornamento di AP in sequenza e patch a caldo
- 17.3 guida all'aggiornamento di IOS e patch a caldo.
- Supporto tecnico e download Cisco

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).