Ricetta di cottura: Configurazione minima CLI bootstrap per Catalyst 9800

Sommario

Introduzione

In questo documento vengono descritte diverse opzioni disponibili per il "bootstrap" (esecuzione della configurazione iniziale) su un Catalyst 9800 Wireless Lan Controller (WLC). Alcuni possono richiedere processi esterni (download PNP o TFTP), altri possono essere eseguiti parzialmente tramite CLI, quindi completati tramite GUI, ecc.

Questo documento si concentrerà su un formato "ricetta di cottura", con la minima serie di azioni semplificate, per avere un 9800 configurato per le operazioni di base, compresa l'amministrazione

remota, e le best practice, nel più breve tempo possibile.

Il modello fornito contiene commenti preceduti dal carattere "!" per spiegare punti specifici della configurazione. Inoltre, tutti i valori che devono essere forniti dall'utente sono contrassegnati nella tabella "ingredienti" qui di seguito

Questa versione è destinata alla versione 17.3 e successive

Prerequisiti

- Controller Catalyst 9800 "preconfigurato". Fondamentalmente, senza alcuna configurazione
- Informazioni di base sulla configurazione di IOS-XE
- Accedere alla porta console del controller. Può trattarsi della porta fisica CON dell'accessorio (9800-40, 9800-80, 9800-L) o del client di accesso remoto dell'hypervisor per 9800-CL
- Per l'accesso seriale, qualsiasi applicazione client terminale di vostra preferenza

Ingredienti

Ogni elemento in maiuscolo corrisponde a un'impostazione che è necessario modificare prima di utilizzare il modello di configurazione:

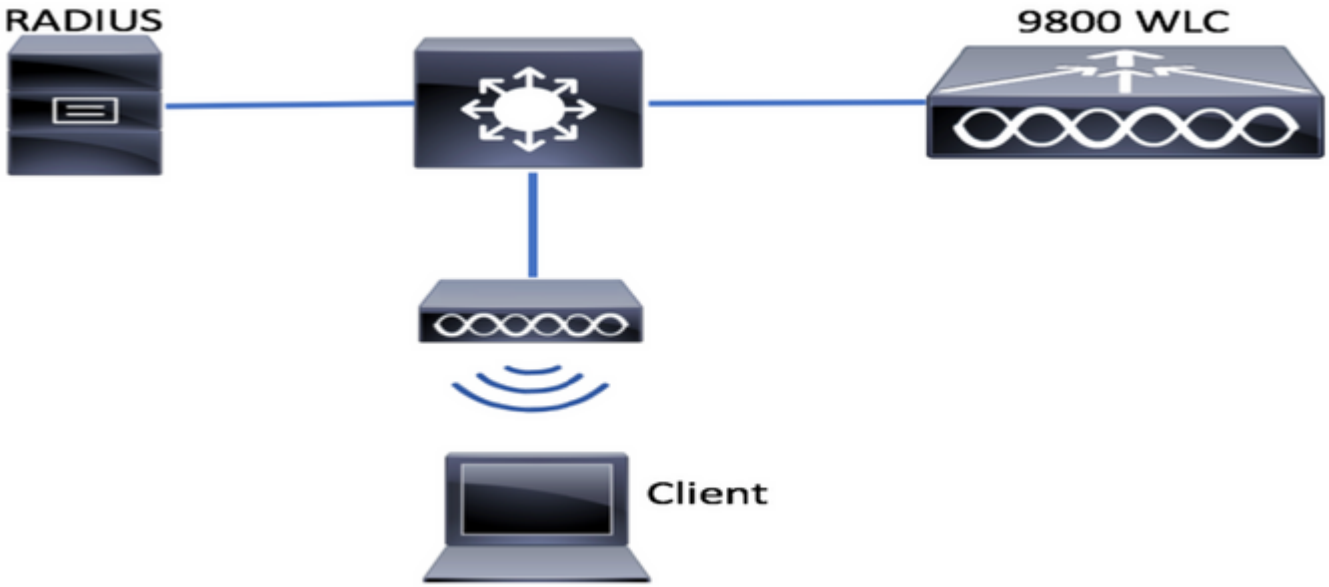
Valore obbligatorio	Nome nel modello	Esempio
IP gestione fuori banda	[OOM_IP]	192.168.0.25
Gateway predefinito di gestione fuori banda	[OOM_GW]	192.168.0.1
Nome utente amministratore	[AMMINISTRATORE]	admin
Password amministratore	[PASSWORD]	ah1-7k++a1
Nome utente amministratore AP	[AP_ADMIN]	admin
Password CLI AP	[AP_PASSWORD]	alkhb90jlih
Abilita segreto AP	[AP_SECRET]	kh20-9yjh
Nome host controller	[NOME_WLC]	9800-bcn-1
Nome dominio società	[NOME_DOMINIO]	company.com
ID VLAN client	[VLAN_CLIENT]	15
Nome VLAN client	[NOME_VLAN]	vlan_client
VLAN Wireless Management Interface	[VLAN_WMI]	25
IP interfaccia di gestione wireless	[IP_WMI]	192.168.25.10
Maschera dell'interfaccia di gestione wireless	[MASCHERA_WMI]	255.255.255.0
GW predefinito interfaccia di gestione wireless	[WMI_GW]	192.168.25.1
Server NTP	[IP_NTP]	192.168.1.2
IP server Radius	[IP_RAGGIO]	192.168.0.98

Chiave Radius o segreto condiviso	[CHIAVE_RAGGIO]	SegretoCondiviso
Nome chiave già condivisa WLAN SSID WPA2	[SSID-PSK]	personale
Autenticazione WLAN SSID WPA2 802.1x	[SSID-DOT1x]	nomesocietà
Autenticazione Web locale guest SSID WLAN	[SSID-LWA]	guest1
Autenticazione Web locale guest SSID WLAN	[SSID-CWA	guest2

Configurazione

Esempio di rete

Questi documenti seguono una topologia di base, con un controller Catalyst 9800 collegato a uno switch e un punto di accesso sulla stessa vlan a scopo di test, con il server Radius opzionale per l'autenticazione



Facoltativo: Ripristino dei valori predefiniti del controller - Giorno zero

se il controller è già stato configurato e si desidera riportarlo allo scenario del giorno zero senza alcuna configurazione, è possibile eseguire la procedura facoltativa seguente:

```
DAO2#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Sep 7 10:09:31.141: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
DAO2#reload

System configuration has been modified. Save? [yes/no]: no
Reload command is being issued on Active unit, this will reload the whole stack
```

```
Proceed with reload? [confirm]

Sep 7 10:10:55.318: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
Chassis 1 reloading, reason - Reload command
```

Ignorare la Configurazione guidata iniziale

Al termine del ricaricamento, il controller presenterà una configurazione guidata CLI per eseguire una configurazione iniziale di base. In questo documento, questa opzione verrà ignorata e tutti i valori verranno configurati utilizzando il modello CLI fornito nei passaggi successivi.

Attendere il completamento dell'avvio del controller:

```
Installation mode is INSTALL

No startup-config, starting autoinstall/pnp/ztp...

Autoinstall will terminate if any input is detected on console

Autoinstall trying DHCPv4 on GigabitEthernet0

Autoinstall trying DHCPv6 on GigabitEthernet0


--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: CPU 0:
Machine Check: 0 Bank 9: ee2000000003110a
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: TSC 0
ADDR ff007f00 MISC 228aa040101086
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: PROCESSOR
0:50654 TIME 1631009693 SOCKET 0 APIC 0 microcode 2000049
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: CPU 0:
Machine Check: 0 Bank 10: ee2000000003110a
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: TSC 0
ADDR ff007fc0 MISC 228aa040101086
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: PROCESSOR
0:50654 TIME 1631009693 SOCKET 0 APIC 0 microcode 2000049
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: CPU 0:
Machine Check: 0 Bank 11: ee2000000003110a
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: TSC 0
ADDR ff007f80 MISC 228aa040101086
*Sep 7 10:15:01.936: %IOSXE-0-PLATFORM: Chassis 1 R0/0: kernel: mce: [Hardware Error]: PROCESSOR
0:50654 TIME 1631009693 SOCKET 0 APIC 0 microcode 2000049
Autoinstall trying DHCPv4 on GigabitEthernet0,Vlan1

Autoinstall trying DHCPv6 on GigabitEthernet0,Vlan1

Acquired IPv4 address 192.168.10.105 on Interface GigabitEthernet0
Received following DHCPv4 options:
domain-name : cisco.com
dns-server-ip : 192.168.0.21

OK to enter CLI now...

pnp-discovery can be monitored without entering enable mode

Entering enable mode will stop pnp-discovery
Guestshell destroyed successfully
```

Premere il tasto "Invio" e dire "no" alla finestra di dialogo iniziale, e "sì", per terminare il processo di installazione automatica:

```
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: yes


Press RETURN to get started!
```

Modello bootstrap - Impostazioni di base del dispositivo

Utilizzare i modelli di configurazione riportati di seguito e modificare i valori come indicato nella tabella Componenti. Questo documento è suddiviso in diverse sezioni per facilitarne la revisione

Per tutte le sezioni, incollare sempre il contenuto dalla modalità di configurazione, premendo il tasto "Enter" per ottenere il prompt, quindi utilizzando i comandi enable e config, ad esempio:

```
WLC>enable
WLC#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
WLC(config)#hostname controller-name
```

Configurazione iniziale del dispositivo e connettività fuori banda

Utilizzare i seguenti comandi in modalità di configurazione. Dopo la creazione della chiave locale, i comandi termineranno con il salvataggio della configurazione per verificare che SSH sia abilitato

```
hostname [WLC_NAME]

int gi0
ip add [OOM_IP] 255.255.255.0
exit
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 [OOM_GW]

no ip domain lookup

username [ADMIN] privilege 15 password 0 [PASSWORD]

ip domain name [DOMAIN_NAME]

aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authorization exec default local
aaa authorization network default local


line con 0
privilege level 15
login authentication CONSOLE
exit
crypto key generate rsa modulus 2048
ip ssh version 2
end
```

```
wr
```

Opzionale - Abilita CDP

Immettere nuovamente in modalità di configurazione e utilizzare i seguenti comandi. Per 9800-CL, sostituire le interfacce Te0/0/0 e Te0/0/1 con Gi1 e Gi2

```
cdp run
int te0/0/0
cdp ena
int te0/0/1
cdp ena
```

9800-CL - Crea certificato autofirmato

Questa operazione deve essere eseguita solo sui controller 9800-CL e **non** è richiesta sui modelli di accessorio (9800-80, 9800-40, 9800-L) per il join AP CAPWAP

```
wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 [CHANGEPASSWORD]
```

Creazione Di Vlan

In modalità configurazione, creare tutte le vlan client necessarie e la vlan corrispondente a WMI (Wireless Management Interface)

Nella maggior parte degli scenari, è comune avere almeno 2 vlan client, una per l'accesso aziendale e una per l'accesso guest. Scerari di grandi dimensioni possono estendersi su centinaia di VLAN diverse in base alle esigenze

La vlan WMI è il punto di accesso al controller per la maggior parte dei protocolli e delle topologie di gestione. Inoltre, i punti di accesso creeranno i propri tunnel CAPWAP

```
vlan [CLIENT_VLAN]
name [VLAN_NAME]

vlan [WMI_VLAN]
name [WIRELESS_MGMT_VLAN]
```

Configura interfacce dati - Accessori

Per 9800-L, 9800-40, 9800-80, dalla modalità di configurazione, è possibile utilizzare i seguenti comandi per impostare le funzionalità di base per le interfacce del piano dati. Nell'esempio, viene proposto il protocollo LACP, con un gruppo di canali creato su entrambe le porte.

Èimportante configurare una topologia corrispondente sul lato dello switch.

Questa sezione può presentare cambiamenti significativi rispetto all'esempio fornito e alle reali esigenze, a seconda della topologia e dell'utilizzo dei canali delle porte. Rivedi attentamente.

```
!!Interfaces. LACP if standalone or static (channel-group 1 mode on) on if HA before 17.1.
interface TenGigabitEthernet0/0/0
```

```
description You should put here your switch name and port
switchport trunk allowed vlan [CLIENT_VLAN],[WMI_VLAN]
switchport mode trunk
no negotiation auto
channel-group 1 mode active

interface TenGigabitEthernet0/0/1
description You should put here your switch name and port
switchport trunk allowed vlan [CLIENT_VLAN],[WMI_VLAN]
switchport mode trunk
no negotiation auto
channel-group 1 mode active
no shut

int po1
switchport trunk allowed vlan [CLIENT_VLAN],[WMI_VLAN]
switchport mode trunk
no shut

!!Configure the same in switch and spanning-tree portfast trunk
port-channel load-balance src-dst-mixed-ip-port
```

Configura interfaccia di gestione wireless

Per creare WMI, utilizzare i comandi seguenti in modalità di configurazione. Questa è una fase critica

```
int vlan [WMI_VLAN]
ip add [WMI_IP] [WMI_MASK]
no shut

ip route 0.0.0.0 0.0.0.0 [WMI_GW]

!! The interface name will normally be somethng like Vlan25, depending on your WMI VLAN ID
wireless management interface Vlan[WMI_VLAN]
```

Configura sincronizzazione Fuso orario e NTP

L'NTP è fondamentale per diverse funzionalità wireless. Per impostare la modalità di configurazione, utilizzare i seguenti comandi:

```
ntp server [NTP_IP]
!!This is European Central Time, it should be adjusted to your local time zone
clock timezone CET 1 0
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
```

Accesso VTY e altri servizi locali

Seguendo le best practice, questo creerà linee VTY aggiuntive, per evitare problemi di accesso alla GUI e abilitare i servizi di base per migliorare la gestione delle sessioni TCP per le interfacce di gestione

```
service timestamps debug datetime msec
service timestamps log datetime msec
service tcp-keepalives-in
```

```
service tcp-keepalives-out
logging buffered 512000

line vty 0 15
transport input ssh

line vty 16 50
transport input ssh
```

Configurazione Radius

Verranno create le impostazioni di base per abilitare le comunicazioni Radius con il server ISE

```
radius server ISE
address ipv4 [RADIUS_IP] auth-port 1645 acct-port 1646
key [RADIUS_KEY]
automate-tester username dummy probe-on

aaa group server radius ISE_GROUP
server name ISE

aaa authentication dot1x ISE group ISE_GROUP

radius-server dead-criteria time 5 tries 3
radius-server deadtime 5
```

Opzionale - Backup giornaliero della configurazione

Per motivi di sicurezza, è possibile abilitare un backup automatico della configurazione giornaliera sul server TFTP remoto:

```
archive
path tftp://TFTP_IP/lab_configurations/9800-config.conf
time-period 1440
```

Configurazione wireless

In questa sezione viene illustrato un esempio di diversi tipi di WLAN, che include le combinazioni più comuni di WPA2 con Preshare Key, WPA2 con 802.1x/radius, Central Webauth e Local Webauth. Poiché non è previsto che la distribuzione disponga di tutti questi componenti, è consigliabile rimuovere e modificare in base alle esigenze

Èfondamentale impostare il comando country per assicurarsi che il controller contrassegni la configurazione come "completa". Modificare l'elenco dei paesi in modo che corrisponda al percorso di distribuzione:

```
ap dot11 24ghz cleanair
ap dot11 5ghz cleanair
no ap dot11 5ghz SI

!!Important: replace country list with to match your location
!!These commands are supported from 17.3 and higher
wireless country ES
wireless country US
```

Opzionale - Procedure ottimali

Ciò garantirà che la rete rispetti le migliori pratiche di base:

- I punti di accesso dispongono di SSH abilitato, credenziali non predefinite e syslog per migliorare la risoluzione dei problemi. In questo modo viene utilizzato il profilo di join predefinito dell'access point. Se si aggiungono nuove voci, è necessario applicare modifiche simili
- Abilitare la classificazione dei dispositivi per tenere traccia dei tipi di client connessi alla rete

```
ap profile default-ap-profile
mgmtuser username [AP_ADMIN] password 0 [AP_PASSWORD] secret 0 [AP_SECRET]
ssh
syslog host [AP_SYSLOG]

device classifier
```

Creazione di WLAN - WPA2-PSK

Sostituire le variabili con le impostazioni necessarie. Questo tipo di WLAN viene utilizzato principalmente per reti personali, scenari semplici o per supportare dispositivi IOT senza funzionalità 802.1x

Opzionale per la maggior parte degli scenari aziendali

```
wlan wlan_psk 1 [SSID-PSK]
security wpa psk set-key ascii 0 [WLANPSK]
no security wpa akm dot1x
security wpa akm psk
no shutdown
```

Creazione di WLAN - WPA2-Enterprise

Scenario più comune di WPA2 WLAN con autenticazione Radius. Utilizzato in ambienti aziendali

```
wlan wlan_dot1x 2 [SSID-DOT1X]
security dot1x authentication-list ISE
no shutdown
```

Creazione di WLAN - Guest con autenticazione Web locale

Utilizzato per semplificare l'accesso Guest, senza il supporto di ISE Guest

A seconda della versione, è possibile che venga visualizzato un avviso durante la creazione della prima mappa dei parametri. Per continuare, rispondere Sì

```
parameter-map type webauth global
yes ! this may not be needed depending on the version
virtual-ip ipv4 192.0.2.1
virtual-ip ipv6 1001::1

aaa authentication login WEBAUTH local
aaa authorization network default local

wlan wlan_webauth 3 [SSID-WEBAUTH]
peer-blocking drop
```

```
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no security ft
no security wpa wpa2
security web-auth
security web-auth authentication-list WEBAUTH
security web-auth parameter-map global
no shu
```

Creazione di WLAN - Guest con autenticazione Web centrale

Utilizzato per il supporto guest ISE

```
aaa authentication network default local
aaa authorization network MACFILTER group ISE_GROUP
aaa accounting identity ISE start-stop group ISE_GROUP

aaa server radius dynamic-author
client [RADIUS_IP] server-key [RADIUS_KEY]

ip access-list extended REDIRECT
10 deny icmp any any
20 deny udp any any eq bootps
30 deny udp any any eq bootpc
40 deny udp any any eq domain
50 deny ip any host [RADIUS_IP]
55 deny ip host [RADIUS_IP] any
60 permit tcp any any eq www

wlan wlan_cwa 5 [SSID-CWA]
mac-filtering MACFILTER
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no security ft
no security wpa wpa2
no shutdown

!! we will create two policy profiles, to be used later depending if the APs are local or flex
mode
wireless profile policy local_vlanclients_cwa
aaa-override
accounting-list ISE
ipv4 dhcp required
nac
vlan [CLIENT_VLAN]
no shutdown

wireless profile policy policy_flex_cwa
no central association !!Ensure to disable central-assoc for flexconnect APs
no central dhcp
no central switching
aaa-override
accounting-list ISE
ipv4 dhcp required
nac
vlan [CLIENT_VLAN]
no shutdown
```

Creazione di criteri per i punti di accesso in modalità locale

I punti di accesso in modalità locale si trovano nella stessa posizione fisica del controller Catalyst 9800, generalmente sulla stessa rete.

Ora che abbiamo il controller con la configurazione di base del dispositivo e i diversi profili WLAN creati, è il momento di associarli tutti ai profili delle policy e applicarli tramite tag ai punti di accesso che dovrebbero trasmettere questi SSID

Per ulteriori informazioni, vedere Informazioni sul modello di configurazione dei controller wireless Catalyst 9800

```
wireless profile policy policy_local_clients
description local_vlan
dhcp-tlv-caching
http-tlv-caching
radius-profiling
session-timeout 86400 !!Ensure to not use 0 since 0 means no pmk cache
idle-timeout 300
vlan [CLIENT_VLAN]
no shutdown

wireless tag site site_tag_local
description local

wireless tag policy policy_tag_local
description "Tag for APs on local mode"
!! Include here only the WLANs types from previous sections, that you have defined and are
interesting for your organization
!! For guest WLANS (CWA/LWA), it is common to use a different policy profile, to map to a
different VLAN
wlan wlan_psk policy policy policy_local_clients
wlan wlan_dot1x policy policy policy_local_clients
wlan wlan_webauth policy policy policy_local_clients
wlan wlan_cwa policy policy_local_clients
```

Creazione di criteri per i punti di accesso in modalità Flexconnect

I punti di accesso in modalità Flexconnect vengono generalmente utilizzati quando la connessione tra il controller e gli access point viene effettuata su una WAN (con un conseguente aumento del ritardo di andata e ritorno tra di essi) oppure quando, per motivi di topologia, è necessario che il traffico del client sia commutato localmente sulla porta dell'access point e non venga portato attraverso CAPWAP per uscire dalla rete alle interfacce del controller

La configurazione è simile alla modalità locale, ma contrassegnata come lato remoto, con traffico a commutazione locale

```
wireless profile flex flex_profile_native
acl-policy REDIRECT
central-webauth
arp-caching
!! Replace 25 with the VLAN native on your AP L2 topology
native-vlan-id 25
vlan-name [VLAN_NAME]
vlan-id [CLIENT_VLAN]

wireless tag site site_tag_flex
flex-profile flex_profile_native
no local-site
```

```
wireless profile policy policy_flex_clients
no central association !!Ensure to disable central-assoc for flexconnect APs
no central dhcp
no central switching
dhcp-tlv-caching
http-tlv-caching
idle-timeout 300
session-timeout 86400 !!Ensure to not use 0 since 0 means no pmk cache
vlan [CLIENT_VLAN]
no shutdown

wireless tag policy policy_tag_flex
description "Profile for Flex mode APs"
!! Include here only the WLANs types from previous sections, that you have defined and are
interesting for your organization
!! For guest WLANS (CWA/LWA), it is common to use a different policy profile, to map to a
different VLAN
wlan wlan_psk policy policy_flex_clients
wlan wlan_dot1x policy policy_flex_clients
wlan wlan_webauth policy policy_flex_clients
wlan wlan_cwa policy policy_flex_cwa
```

Finale - Applica tag agli access point

Per concludere, dobbiamo applicare le etichette che abbiamo definito a ciascun punto di accesso. È necessario sostituire l'indirizzo MAC Ethernet di ciascun access point con quello presente nel dispositivo

```
!!Tag assigment using static method. Replace mac with your device
ap F4DB.E683.74C0
policy-tag policy_tag_local
site-tag site_tag_local
```

Come ottenere un elenco di indirizzi MAC AP

Èpossibile ottenere un elenco degli access point attualmente collegati tramite il comando show ap summary

```
Gladius1#sh ap summ
Number of APs: 1

AP Name Slots AP Model Ethernet MAC Radio MAC Location Country IP Address State
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
9130E-r3-sw2-g1012 3 9130AXE 0c75.bdb6.28c0 0c75.bdb5.7e80 Test123 ES 192.168.25.139 Registered
```

Lettura consigliata

- Best practice per la configurazione di Cisco Catalyst serie 9800
- Versioni Cisco IOS XE consigliate per i controller LAN wireless Catalyst 9800
- Strumenti per la risoluzione dei problemi wireless