烹飪食譜：Catalyst 9800最低啟動程式CLI配置

目錄

簡介

本檔案介紹Catalyst 9800無線Lan控制器(WLC)的「bootstrap」（執行初始組態）可用的多個選項。 某些進程可能需要外部進程（PNP或TFTP下載），某些進程可通過CLI部分完成，然後通過GUI完成等等。

本文檔將重點介紹「烹飪配方」格式，以及最簡單的操作集，以使9800配置在儘可能最短的時間內完成基本操作，包括遠端管理和最佳實踐。

提供的模板包含以字元「！」開頭的註釋 解釋配置的具體點。另外，您必須提供的所有值都將在下面的「成分」表中標籤

此版本面向17.3及更高版本

必要條件

- Catalyst 9800控制器「開箱即用」。 基本上，沒有任何配置
- 對IOS-XE配置的基本瞭解
- 存取控制器的主控台連線埠。這可以是裝置中的CON物理埠(9800-40、9800-80、9800-L)，也可以是通過適用於9800-CL的虛擬機器監控程式遠端訪問客戶端實現的
- 對於串列訪問，任何您喜歡的終端客戶端應用程式

配料

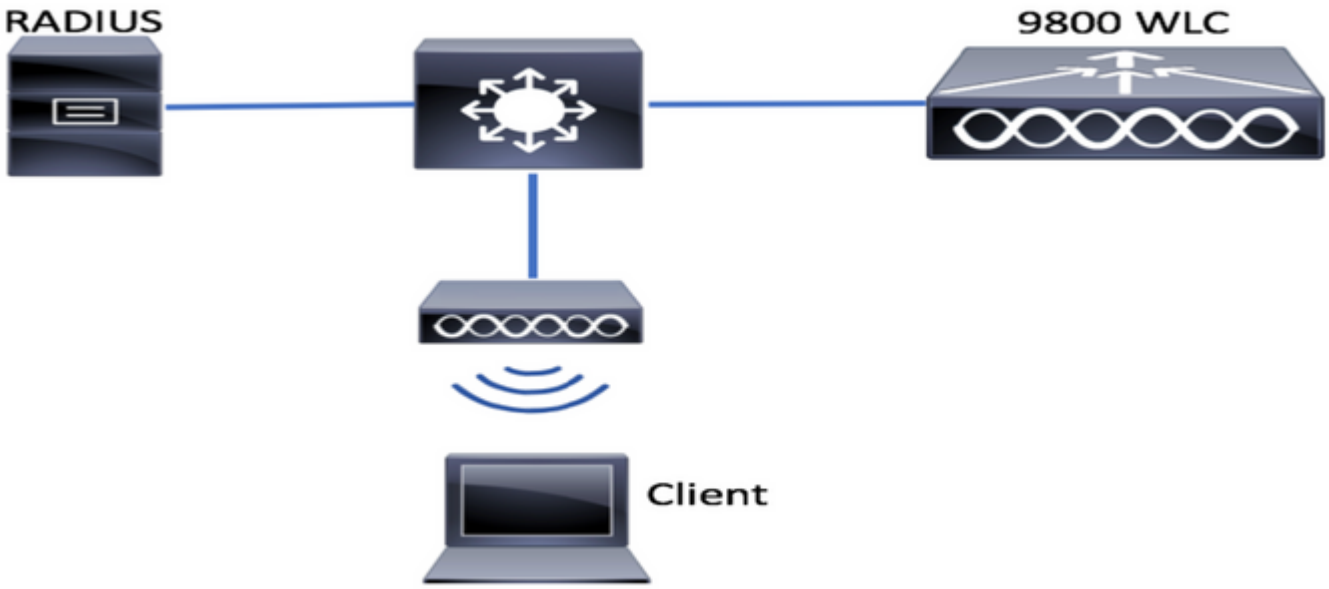
每個大寫專案對應於使用配置模板之前必須更改的設定：

需要值	模板中的名稱	範例
帶外管理IP	[OOM_IP]	192.168.0.25
帶外管理預設網關	[OOM_GW]	192.168.0.1
管理員使用者名稱	[ADMIN]	admin
管理員密碼	[密碼]	ah1-7k++a1
AP管理員使用者名稱	[AP_ADMIN]	admin
AP CLI密碼	[AP_PASSWORD]	alkhb90jlih
AP啟用密碼	[AP_SECRET]	kh20-9yjh
控制器主機名	[WLC_NAME]	9800-bcn-1
公司域名	[域名]	company.com
客戶端VLAN ID	[CLIENT_VLAN]	15
客戶端VLAN名稱	[VLAN名稱]	client_vlan
無線管理介面VLAN	[WMI_VLAN]	25
無線管理介面IP	[WMI_IP]	192.168.25.10
無線管理介面遮罩	[WMI_MASK]	255.255.255.0
無線管理介面預設GW	[WMI_GW]	192.168.25.1
NTP伺服器	[NTP_IP]	192.168.1.2
Radius伺服器IP	[RADIUS_IP]	192.168.0.98
Radius金鑰或共用金鑰	[RADIUS_KEY]	ThisIsASharedSecret
WLAN SSID WPA2預共用金鑰名稱	[SSID-PSK]	個人
WLAN SSID WPA2 802.1x驗證	[SSID-DOT1x]	公司名稱
WLAN SSID訪客本地Web驗證	[SSID-LWA]	guest1
WLAN SSID訪客本地Web驗證	[SSID-CWA	guest2

設定

網路圖表

本文遵循一個非常基本的拓撲，將Calatyst 9800控制器連線到交換機，並且使用同一個vlan上的接入點進行測試，使用可選的Radius伺服器進行身份驗證



可選：將控制器還原為出廠預設設定 — 零天

如果控制器已經過配置，並且您想將其移回零日場景，而不進行任何配置，您可以執行以下可選步驟：

```
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
```

繞過初始配置嚮導

控制器完成重新載入後，它將顯示CLI配置嚮導以執行基本初始配置。在本檔案中，我們將跳過此選項，並使用後續步驟中提供的CLI模板配置所有值。

等待控制器完成啟動：

```
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
```

按「Enter」鍵，對初始對話方塊說「no」，然後按下「yes」以終止自動安裝過程：

```
% 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!
```

載入程式模板 — 基本裝置設定

採用以下配置模板，並修改在「配料」(Infements)表格中指示的值。本文檔在不同的部分進行拆分，以便於檢視

對於所有部分，始終貼上來自配置模式的內容，按"Enter"鍵獲取提示，然後使用enable和config命令，例如：

```
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
```

初始裝置配置和帶外連線

在配置模式下使用以下命令。建立本地金鑰後，這些命令將結束儲存配置以確保SSH已啟用

```
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
```

可選 — 啟用CDP

在Config（配置）模式下再次輸入，然後使用以下命令。對於9800-CL，將介面Te0/0/0和Te0/0/1替換為Gi1和Gi2

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

9800-CL — 建立自簽名證書

這僅能在9800-CL控制器上執行，對於AP CAPWAP連線，裝置型號(9800-80、9800-40、9800-L)不需要**執行**

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

建立Vlan

在配置模式下，根據需要建立多個客戶端VLAN，以及與無線管理介面(WMI)對應的VLAN

在大多數情況下，通常至少有兩個客戶端vlan，一個用於企業vlan，一個用於訪客接入。大型系統可以根據需要跨越數百個不同的VLAN

對於大多數管理協定和拓撲，WMI VLAN是訪問控制器的點，此外接入點將在此建立其CAPWAP隧道

```
vlan [CLIENT_VLAN]
name [VLAN_NAME]

vlan [WMI_VLAN]
name [WIRELESS_MGMT_VLAN]
```

配置資料介面 — 裝置

對於9800-L、9800-40、9800-80，在配置模式下，可以使用以下命令設定資料平面介面的基本功能。本示例建議在兩個埠上建立通道組的LACP。

必須在交換機側配置匹配的拓撲。

根據您的拓撲結構以及是否使用埠通道，此部分可能會從提供的示例明顯改變為真正需要的內容。請仔細檢視。

```
!!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
```

配置無線管理介面

在配置模式下使用以下命令建立WMI。這是關鍵的一步

```
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]
```

配置時區和NTP同步

NTP對多種無線功能至關重要。在配置模式下使用以下命令進行設定：

```
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
```

VTY訪問和其他本地服務

按照最佳實踐，這將建立額外的VTY線路，以避免GUI訪問問題，並啟用基本服務來改善管理介面的TCP會話處理

```
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
```

Radius組態

這將建立基本設定，以啟用與ISE伺服器的RADIUS通訊

```
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
```

可選 — 每日配置備份

出於安全原因，您可以啟用到遠端TFTP伺服器的自動日常配置備份：

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

無線配置

本節將介紹不同WLAN型別的範例，包括WPA2與預共用金鑰、WPA2與802.1x/radius、中央Webauth和本地Webauth的最常見組合。預計您的部署不會具有所有這些功能，因此應根據需要刪除和修改

必須設定國家/地區命令，以確保控制器將配置標籤為「完成」。 您應該修改國家/地區清單以匹配您的部署位置：

```
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
```

可選 — 最佳實踐

這將確保網路符合基本的最佳做法：

- 接入點啟用了SSH、非預設憑證和系統日誌，以改善故障排除體驗。這是使用預設的AP加入配置檔案，如果新增新條目，應該對其應用類似的更改
- 啟用裝置分類，以跟蹤連線到網路的客戶端型別

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

device classifier
```

建立WLAN - WPA2-PSK

用所需的設定替換變數。這種型別的WLAN主要用於個人網路、簡單場景或支援沒有802.1x功能的IOT裝置

對於大多數企業方案而言，這是可選的

```
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
```

建立WLAN - WPA2 — 企業

採用Radius驗證的WPA2 WLAN的最常見情況。用於企業環境

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

建立WLAN — 使用本地Web驗證的訪客

用於更簡單的訪客接入，無ISE訪客支援

根據版本的不同，在建立第一個引數對映時可能會收到警告，請回答「是」以繼續

```
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
```

建立WLAN — 使用中央Web驗證的訪客

用於ISE訪客支援

```
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
```

為本地模式AP建立策略

本地模式AP是指與Catalyst 9800控制器位於同一物理位置的AP，通常位於同一網路中。

現在，我們擁有了具有基本裝置配置的控制器，並且建立了不同的WLAN配置檔案，現在應該將它與策略配置檔案粘在一起，通過標籤將它們應用到應該廣播這些SSID的接入點上

如需詳細資訊，請檢查瞭解Catalyst 9800無線控制器組態型號

```
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
```

為Flexconnect模式AP建立策略

當控制器與AP之間的連線通過WAN完成（因此它們之間的往返延遲增加）時，或者當出於拓撲原因，我們需要在AP埠本地交換客戶端流量，而不是通過CAPWAP在控制器介面上退出網路時，通常使用Flexconnect模式接入點

該配置類似於本地模式，但標籤為遠端端，具有本地交換流量

```
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
```

最終 — 將標籤應用於接入點

最後，我們需要將我們定義的標籤應用到每個接入點。必須將每個AP的乙太網MAC地址替換為裝置中的地址

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

如何獲取AP MAC地址清單

您可以使用命令show ap summary獲取當前加入的AP的清單

```
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
```

推薦閱讀

- Cisco Catalyst 9800系列配置最佳實踐
- 適用於Catalyst 9800無線LAN控制器的建議Cisco IOS XE版本
- 無線故障排除工具