調理法：Catalyst 9800の最小ブートストラップCLI設定

内容

概要

このドキュメントでは、Catalyst 9800ワイヤレスLANコントローラ(WLC)の「ブートストラップ」（初期設定の実行）に使用できるオプションについて説明します。 外部プロセス（PNPまたはTFTPのダウンロード）が必要なものもあれば、CLIを使用して部分的に実行し、GUIを使用して実行できるものもあります。

このドキュメントでは、最小限の合理化された一連のアクションを含む「料理のレシピ」形式に焦点を当て、可能な限り最短の時間でリモート管理やベストプラクティスなどの基本操作に

9800を設定します。

提供されたテンプレートには、「!」という文字で始まるコメントがあります。 を参照してください。また、ユーザーが提供する必要があるすべての値は、以下の「材料」の表に記載されています

これは、17.3以降のバージョンを対象としています

前提条件

- Catalyst 9800コントローラは「すぐに使える」状態です。 基本的に、設定は必要ありません
- IOS-XEの設定に関する基本的な知識
- コントローラのコンソールポートにアクセスします。これは、アプライアンスのCON物理ポート(9800-40、9800-80、9800-L)、または9800-CLのハイパーバイザリモートアクセスクライアント経由で実行できます
- シリアルアクセスの場合は、任意のターミナルクライアントアプリケーションのプリファレンス

材料

各大文字の項目は、設定テンプレートを使用する前に変更する必要がある設定に対応しています。

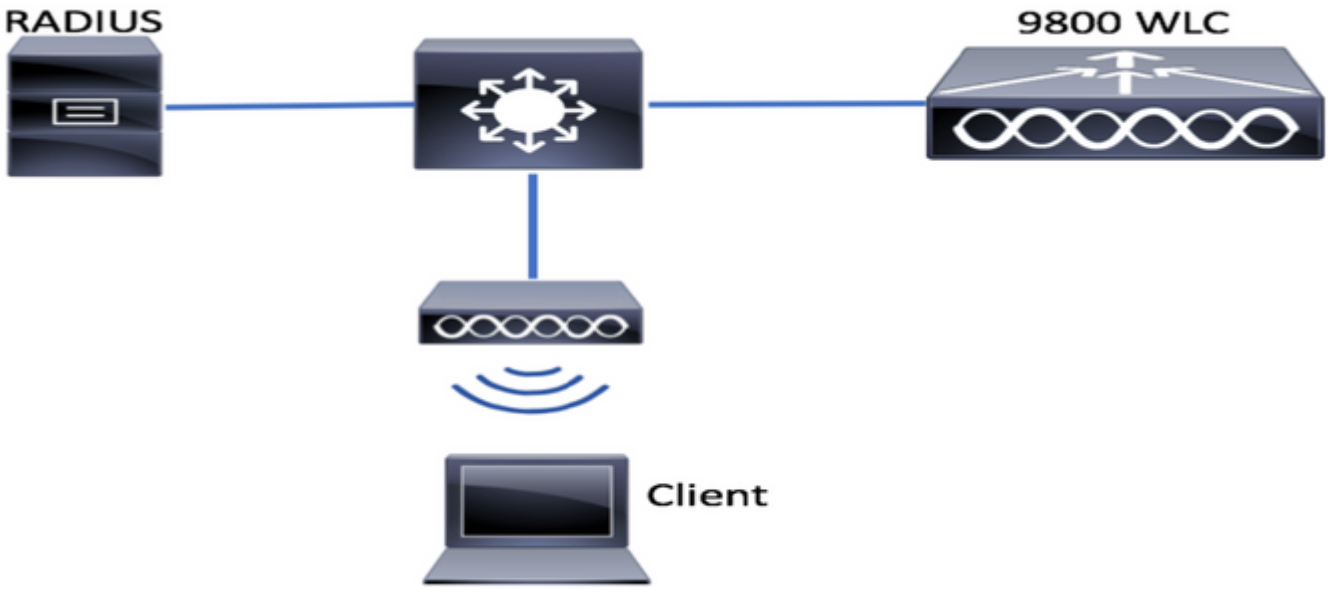
必要な値	テンプレート内の名前	例
アウトオブバンド管理IP	[OOM_IP]	192.168.0.25
アウトオブバンド管理デフォルトゲートウェイ	[OOM_GW]	192.168.0.1
管理者ユーザー名	[ADMIN]	admin
管理者パスワード	[PASSWORD]	ah1-7k++a1
AP管理者ユーザ名	[AP_ADMIN]	admin
AP CLIパスワード	[AP_PASSWORD]	alkhb90jlih
APイネーブルシークレット	[AP_SECRET]	kh20-9yjh
コントローラホスト名	[WLC_NAME]	9800-bcn-1
会社ドメイン名	[DOMAIN_NAME]	company.com
クライアントVLAN ID	[CLIENT_VLAN]	15
クライアントVLAN名	[VLAN_NAME]	client_vlan
ワイヤレス管理インターフェイスVLAN	[WMI_VLAN]	25
ワイヤレス管理インターフェイスIP	[WMI_IP]	192.168.25.10
Wireless Management Interface(WMI)マスク	[WMI_MASK]	255.255.255.0
Wireless Management Interface Default GW	[WMI_GW]	192.168.25.1
NTP サーバ	[NTP_IP]	192.168.1.2

RadiusサーバIP	[RADIUS_IP]	192.168.0.98
RADIUSキーまたは共有秘密	[RADIUS_KEY]	ThisIsASharedSecret
WLAN SSID WPA2事前共有キー名	[SSID-PSK]	個人
WLAN SSID WPA2 802.1x認証	[SSID-DOT1x]	companyname
WLAN SSIDゲストローカルWeb認証	[SSID-LWA]	guest1
WLAN SSIDゲストローカルWeb認証	[SSID-CWA]	ゲスト2

設定

ネットワーク図

このドキュメントは、非常に基本的なトポロジに従い、スイッチに接続されたCalatyst 9800コントローラと、テスト目的で同じVLAN上のアクセスポイントと、認証用のオプションのRADIUSサーバを使用します



オプション：コントローラを工場出荷時のデフォルトに戻す：ゼロデイ

コントローラがすでに設定されており、設定を行わずにデイゼロシナリオに戻す場合は、次のオプション手順を実行できます。

```
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
```

初期設定ウィザードのバイパス

コントローラのリロードが完了すると、基本的な初期設定を実行するためのCLI設定ウィザードが表示されます。このドキュメントでは、このオプションを省略し、次の手順で提供されるCLIテンプレートを使用してすべての値を設定します。

コントローラの起動が終了するまで待ちます。

```
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
```

「Enter」キーを押し、最初のダイアログに「no」と発音し、「yes」と発音して自動インストールプロセスを終了します。

```
% 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!
```

ブートストラップテンプレート：デバイスの基本設定

次の設定テンプレートを使用して、「成分」(Components)テーブルに示されている値を変更します。このドキュメントは、レビューを容易にするために異なるセクションに分割されています

すべてのセクションで、常にConfigモードから内容を貼り付け、「Enter」キーを押してプロンプトを表示し、enableコマンドとconfigコマンドを使用します。次に例を示します。

```
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
```

デバイスの初期設定とアウトオブバンド接続

設定モードで次のコマンドを使用します。ローカルキーを作成した後、SSHが有効になっていることを確認する設定の保存が終了します

```
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
```

オプション：CDPの有効化

設定モードに戻り、次のコマンドを使用します。9800-CLの場合、インターフェイスTe0/0/0およびTe0/0/1をGi1およびGi2に置き換えます

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

9800-CL – 自己署名証明書の作成

これは9800-CLコントローラでのみ実行できます。AP CAPWAP加入のアプライアンスモデル(9800-80、9800-40、9800-L)では**必要ありません**

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

VLAN の作成

設定モードから、必要な数のクライアントVLANと、ワイヤレス管理インターフェイス(WMI)に対応するVLANを作成します

ほとんどのシナリオでは、少なくとも2つのクライアントVLANが存在することが一般的です。1つは会社用で、もう1つはゲストアクセス用です。大規模なシナリオでは、必要に応じて数百の異なるVLANに分散できます

WMI vlanは、ほとんどの管理プロトコルとトポロジでコントローラにアクセスするためのポイントであり、アクセスポイントがCAPWAPトンネルを作成します

```
vlan [CLIENT_VLAN]
name [VLAN_NAME]

vlan [WMI_VLAN]
name [WIRELESS_MGMT_VLAN]
```

データインターフェイスの設定 – アプライアンス

9800-L、9800-40、9800-80では、コンフィギュレーションモードから次のコマンドを使用して、データプレーンインターフェイスの基本機能を設定できます。この例では、両方のポートでチャネルグループが作成されたLACPを提案しています。

スイッチ側で一致するトポロジを設定することが重要です。

このセクションは、トポロジやポートチャネルを使用する場合に応じて、提示された例から実際に必要とされる内容に大幅な変更が加えられた可能性があります。慎重にレビューしてください。

```
!!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
```

ワイヤレス管理インターフェイスの設定

WMIを作成するには、設定モードから次のコマンドを使用します。これは重要なステップです

```
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]
```

タイムゾーンとNTP同期の設定

NTPは、いくつかのワイヤレス機能に不可欠です。設定するには、設定モードで次のコマンドを使用します。

```
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アクセスおよびその他のローカルサービス

ベストプラクティスに従って、これにより追加のVTY回線が作成され、GUIアクセスの問題が回避され、基本的なサービスが有効になり、管理インターフェイスのTCPセッション処理が向上します

```
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の設定

これにより、ISEサーバへのRADIUS通信を有効にするための基本設定が作成されます

```
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
```

オプション：毎日の設定バックアップ

セキュリティ上の理由から、リモートTFTPサーバへの毎日の自動バックアップを有効にできます。

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

ワイヤレス設定

このセクションでは、WPA2と事前共有キー、WPA2と802.1x/radius、中央Web認証、および口ーカルWeb認証の最も一般的な組み合わせを扱う、さまざまなWLANタイプの例について説明します。これらの機能がすべて導入されるとは限らないため、必要に応じて削除および変更する必要があります

コントローラが設定を「complete」としてマークするようにするには、countryコマンドを設定することが重要です。 展開場所に合わせて国リストを変更する必要があります。

```
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
```

オプション：ベストプラクティス

これにより、ネットワークが基本的なベストプラクティスを確実に満たすことができます。

- アクセスポイントでは、SSHが有効になっており、デフォルト以外のクレデンシャルとsyslogが使用され、トラブルシューティングのエクスペリエンスが向上します。これはデフォルトのAP加入プロファイルを使用しています。新しいエントリを追加する場合は、同様の変更を適用する必要があります
- デバイスの分類を有効にして、ネットワークに接続されているクライアントタイプを追跡する

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

device classifier
```

WLANの作成：WPA2-PSK

変数を必要な設定に置き換えます。このタイプのWLANは、主にパーソナルネットワーク、単純なシナリオ、または802.1x機能のないIOTデバイスをサポートするために使用されます

これは、ほとんどのエンタープライズシナリオでオプションです

```
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
```

WLANの作成：WPA2-Enterprise

RADIUS認証を使用するWPA2 WLANの最も一般的なシナリオ。エンタープライズ環境で使用

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

WLANの作成：ローカルWeb認証を使用したゲスト

ISEゲストサポートなしで、よりシンプルなゲストアクセスに使用

バージョンによっては、最初のパラメータマップを作成するときに警告が表示される場合があります。yesと答えて続行してください

```
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
```

WLANの作成：中央Web認証を使用したゲスト

ISEゲストサポートに使用

```
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
```

ローカルモードAPのポリシーの作成

ローカルモードAPは、通常、同じネットワーク上のCatalyst 9800コントローラと同じ物理的な場所にあるAPです。

基本的なデバイス設定のコントローラと異なるWLANプロファイルを作成したので、ポリシープロファイルと一緒にコントローラを接続し、SSIDをブロードキャストするアクセスポイントにタグを付けて適用します

詳細については、「Understanding Catalyst 9800 Wireless Controllers Configuration Model」を参照してください

```
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
```

FlexconnectモードAPのポリシーの作成

Flexconnectモードのアクセスポイントは、通常、コントローラとAP間の接続がWAN経由で行われる場合（ラウンドトリップ遅延が増加する場合）、またはトポロジ上の理由から、クライアントトラフィックをAPポートでローカルにスイッチングする必要があります

設定はローカルモードに似ていますが、ローカルでスイッチングされるトラフィックを使用して、リモート側としてフラグが付けられています

```
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 – アクセスポイントへのタグの適用

最後に、定義したタグを各アクセスポイントに適用する必要があります。各APのイーサネットMACアドレスは、デバイスに存在するMACアドレスに置き換える必要があります

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

AP MACアドレスのリストを取得する方法

show ap summaryコマンドを使用すると、現在加入しているAPのリストを取得できます

```
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
```

推奨書籍

- Cisco Catalyst 9800シリーズ設定のベストプラクティス
- Catalyst 9800ワイヤレスLANコントローラに推奨されるCisco IOS XEリリース
- ワイヤレストラブルシューティングツール