

Catalyst 9800 WLCでのAP加入プロセスについて

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[CAPWAPセッションの確立](#)

[DTLSセッションの確立](#)

[ワイヤレスLANコントローラの検出方法](#)

[ワイヤレスLANコントローラを選択](#)

[CAPWAPステートマシン](#)

[CAPWAP状態：検出](#)

[CAPWAPの状態：DTLSのセットアップ。](#)

[CAPWAP状態：参加](#)

[CAPWAP状態：イメージデータ](#)

[CAPWAP状態：設定](#)

[CAPWAP状態：Run](#)

[設定](#)

[スタティックWLCの選択](#)

[APへのTelnet/SSHアクセスの有効化](#)

[データリンク暗号化](#)

[確認](#)

[トラブルシューティング](#)

[既知の問題](#)

[WLC GUIのチェック](#)

[コマンド](#)

[WLCから](#)

[Wave 2およびCatalyst 11ax APから](#)

[Wave 1 APから](#)

[放射性物質トレース](#)

はじめに

このドキュメントでは、Cisco Catalyst 9800 WLCを使用したAP加入プロセスについて詳しく説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Control and Provisioning Wireless Access Points(CAPWAP)の基本的な知識
- ワイヤレスLANコントローラ(WLC)の使用に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 9800-L WLC、Cisco IOS® XE Cupertino 17.9.3
- Catalyst 9120AXEアクセスポイント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

CAPWAPセッションの確立

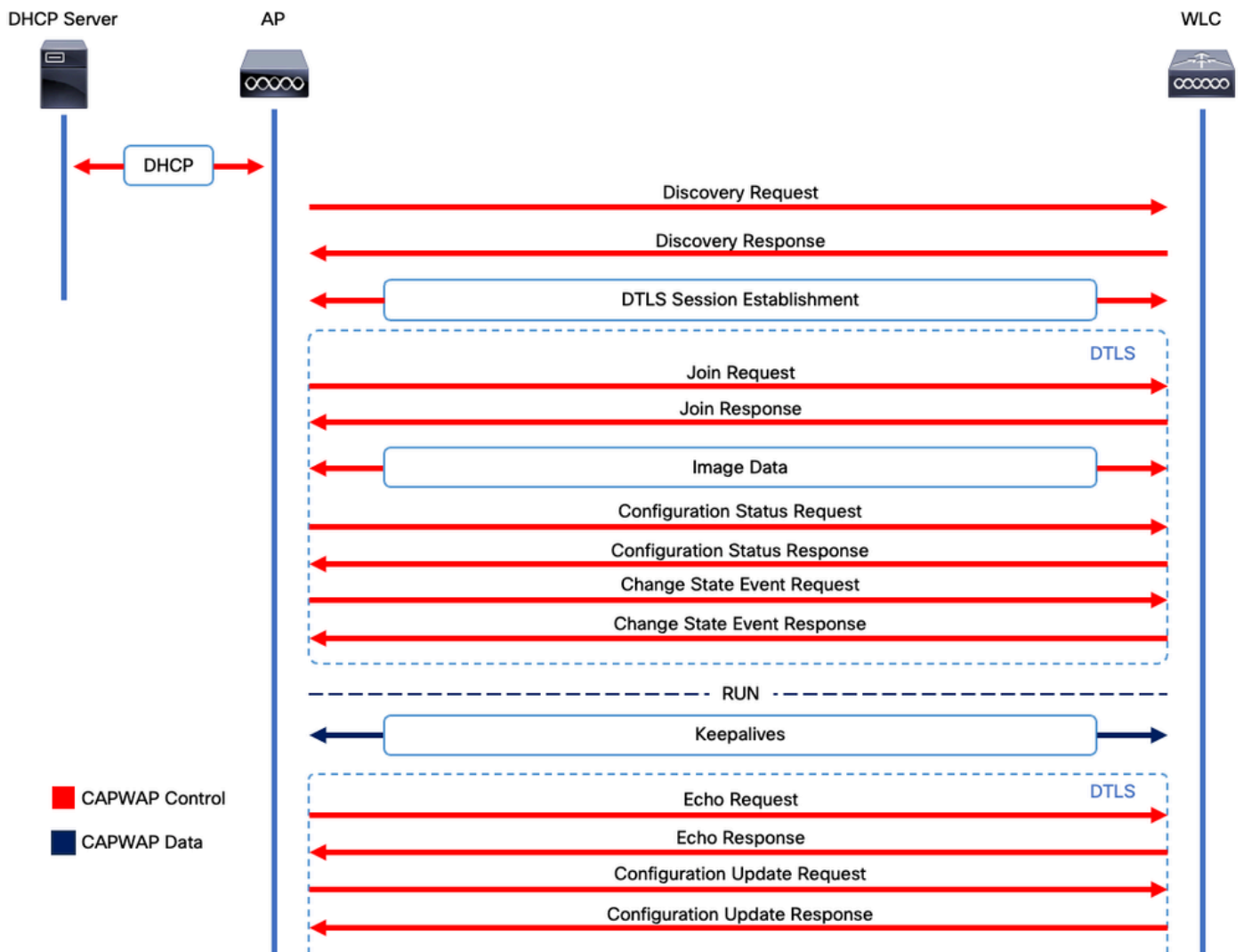
Control And Provisioning Wireless Access Point(CAPWAP)は、アクセスポイント(AP)とワイヤレスLANコントローラ(WLC)で使用される転送メカニズムを提供するプロトコルです。CAPWAP制御の場合は、安全な通信トンネルを介して制御およびデータプレーン情報を交換します。

AP加入プロセスを詳しく説明するには、Control And Provisioning Wireless Access Point(CAPWAP)セッションの確立プロセスを理解することが重要です。

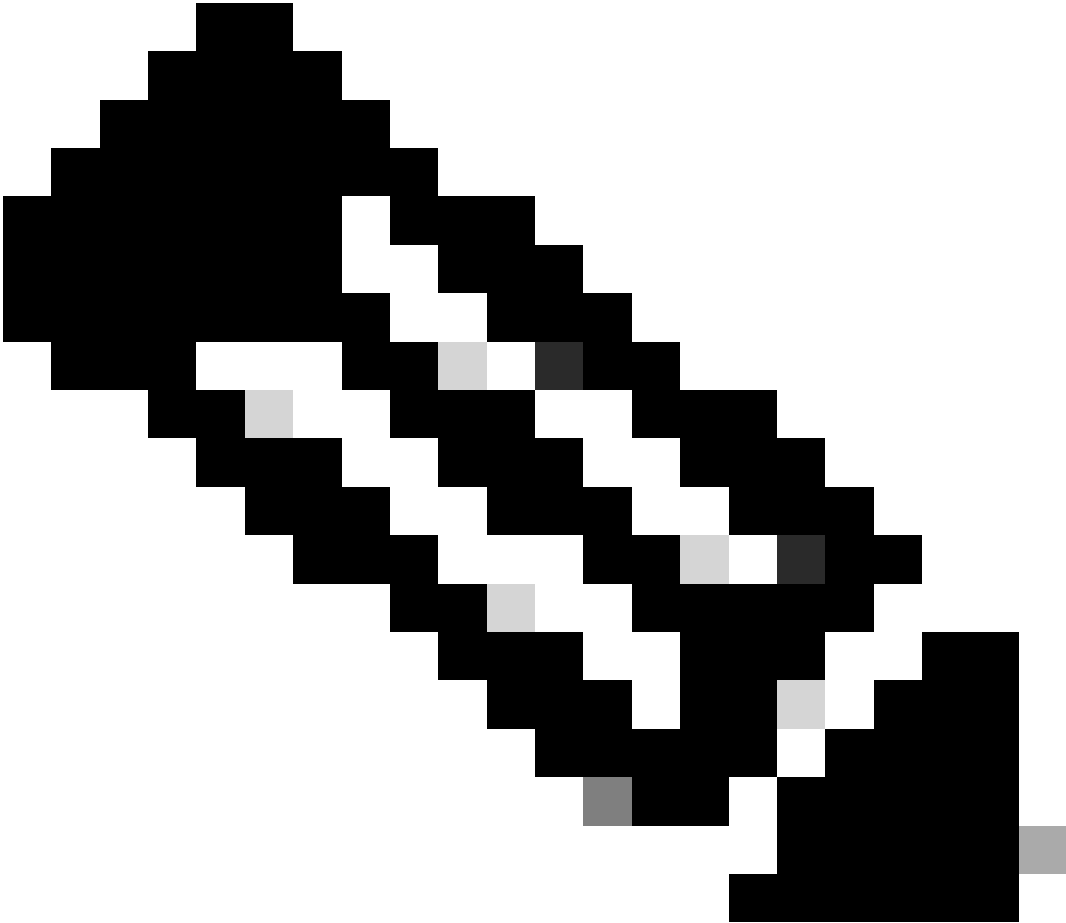
CAPWAPプロセスを開始する前に、APにIPアドレスが必要であることを注意してください。APにIPアドレスがない場合、APはCAPWAPセッション確立プロセスを開始しません。

1. アクセスポイントがディスカバリ要求を送信します。詳細については、「WLCの検出方法」セクションを参照してください
2. WLCがディスカバリ応答を送信する
3. DTLSセッションの確立。この後、この後のすべてのメッセージは暗号化され、パケット分析ツールでDTLSアプリケーションデータパケットとして表示されます。
4. アクセスポイントが参加要求を送信
5. WLCが加入応答を送信する
6. APがイメージチェックを実行します。WLCと同じイメージバージョンの場合は、次の手順に進みます。存在しない場合は、WLCからイメージをダウンロードし、リブートして新しいイメージをロードします。この場合は、手順1からプロセスを繰り返します。
7. アクセスポイントが設定ステータス要求を送信します。
8. WLCが設定ステータス応答を送信する
9. アクセスポイントがRUN状態になる
10. RUN状態の間、CAPWAP Tunnel Maintenanceは2つの方法で実行されます。

1. キープアライブは、CAPWAPデータトンネルを維持するために交換されます
2. APがWLCにエコー要求を送信すると、WLCはそれぞれのエコー応答で応答される必要があります。これは、CAPWAP制御トンネルを維持するためです。



CAPWAPセッション確立プロセス



注：RFC 5415に従い、CAPWAPはUDPポート5246 (CAPWAP制御用) および5247 (CAPWAPデータ用) を使用します。

DTLSセッションの確立

アクセスポイントがWLCから有効なディスカバリ応答を受信すると、アクセスポイント間にDTLSトンネルが確立され、以降のすべてのパケットが安全なトンネルを介して送信されます。次に、DTLSセッションを確立するプロセスを示します。

1. APがClient Helloメッセージを送信する
2. WLCが検証に使用されるcookieを含むHelloVerifyRequestメッセージを送信します。
3. APが検証に使用されるcookieを含むClientHelloメッセージを送信します。
4. WLCは次のパケットを順に送信します。
 1. サーバHello
 2. 証明書
 3. サーバキー交換
 4. 証明書要求

5. サーバHelloDone
5. APは次のパケットを順に送信します。
 1. 証明書
 2. ClientKeyExchange (必須)
 3. 証明書の確認
 4. ChangeCipherSpec
6. WLCはAPのChangeCipherSpecに対し、独自のChangedCipherSpecで応答します。
 1. ChangeCipherSpec

WLCから最後のChangedCipherSpecメッセージが送信された後、セキュアトンネルが確立され、両方向で送信されるすべてのトラフィックが暗号化されます。

ワイヤレスLANコントローラの検出方法

アクセスポイントにネットワーク内の1つのWLCの存在を知らせる方法はいくつかあります。

- DHCPオプション43:このオプションは、加入するWLCのIPv4アドレスをAPに提供します。このプロセスは、APとWLCが異なるサイトにある大規模な導入に便利です。
- DHCPオプション52:このオプションは、加入するWLCのIPv6アドレスをAPに提供します。このコマンドは、DHCPオプション43と同じシナリオで便利に使用できます。
- DNSディスカバリ:APはドメイン名CISCO-CAPWAP-CONTROLLER.localdomainを照会します。参加するWLCのIPv4またはIPv6アドレスを解決するようにDNSサーバを設定する必要があります。このオプションは、WLCがAPと同じサイトに保存されている導入に便利です。
- レイヤ3ブロードキャスト:APは自動的にブロードキャストメッセージを255.255.255.255に送信します。APと同じサブネット内のすべてのWLCが、このディスカバリ要求に応答すると想定されます。
- スタティック設定 : `capwap ap primary-base <wlc-hostname> <wlc-IP-address>`コマンドを使用して、AP内のWLCのスタティックエントリを設定できます。
 - モビリティディスカバリ:APが以前、モビリティグループの一部であったWLCに加入していた場合、APはそのモビリティグループ内にあるWLCのレコードも保存します。



注：上記のWLCディスカバリ方式には優先順位はありません。

ワイヤレスLANコントローラの選択

いずれかのWLCディスカバリ方法を使用して任意のWLCからディスカバリ応答を受信したAPは、次の基準で加入するコントローラを1つ選択します。

- プライマリコントローラ(`capwap ap primary-base <wlc-hostname> <wlc-IP-address>`コマンドで設定)
- セカンダリコントローラ(`capwap ap secondary-base <wlc-hostname> <wlc-IP-address>`コマンドで設定)

- ターシャリコントローラ(capwap ap tertiary-base <wlc-hostname> <wlc-IP-address>コマンドで設定)
- プライマリ、セカンダリ、またはターシャリWLCが事前に設定されていない場合、APは、使用可能なAPの容量が最大である独自のディスカバリ応答を使用してディスカバリ要求に応答した最初のWLC(つまり、任意の時点で最も多くのAPをサポートできるWLC)への加入を試みます。

CAPWAPステートマシン

APコンソールでは、CAPWAPステートマシンを追跡できます。追跡は、「CAPWAPセッションの確立」セクションで説明する手順を実行します。

CAPWAP状態：検出

ここでは、ディスカバリ要求と応答を確認できます。APがDHCP (オプション43) を介してWLC IPを受信し、既知のWLCにディスカバリ要求を送信する方法を確認します。

<#root>

[*09/14/2023 04:12:09.7740]

CAPWAP State: Init

[*09/14/2023 04:12:09.7770]

[*09/14/2023 04:12:09.7770]

CAPWAP State: Discovery

[*09/14/2023 04:12:09.7790]

Discovery Request sent to 172.16.0.20, discovery type STATIC_CONFIG(1)

[*09/14/2023 04:12:09.7800]

Discovery Request

sent to 172.16.5.11, discovery type STATIC_CONFIG(1)

[*09/14/2023 04:12:09.7800]

Got WLC address 172.16.5.11 from DHCP.

[*09/14/2023 04:12:09.7820]

Discovery Request

sent to 172.16.0.20, discovery type STATIC_CONFIG(1)

[*09/14/2023 04:12:09.7830]

Discovery Request

sent to 172.16.5.11, discovery type STATIC_CONFIG(1)

[*09/14/2023 04:12:09.7840]

Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)

[*09/14/2023 04:12:09.7850]
[*09/14/2023 04:12:09.7850]

CAPWAP State: Discovery

[*09/14/2023 04:12:09.7850]

Discovery Response

from 172.16.0.20
[*09/14/2023 04:12:09.8030]

Discovery Response

from 172.16.5.11
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.0.20
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.11
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.11
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.0.20
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.169
[*09/14/2023 04:12:09.8060]

Discovery Response

from 172.16.5.169

このAPは、スタティックに設定されたWLC(172.16.0.20)とDHCPオプション43(172.16.5.11)で示されたWLCの両方からディスカバリ応答を受信した他に、ブロードキャストディスカバリメッセージを受信したために、同じサブネット内の別のWLC(172.16.5.169)からもディスカバリ応答を受信しました。

CAPWAPの状態 : DTLSのセットアップ。

ここでは、APとWLC間のDTLSセッションが交換されます。

<#root>

[*09/27/2023 21:50:41.0000]

CAPWAP State: DTLS Setup

[*09/27/2023 21:50:41.7140] sudi99_request_check_and_load: Use HARSA SUDI certificat

CAPWAP状態：参加

DTLSセッションを確立した後、WLCへの接続要求がセキュアセッション経由で送信されます。この要求がWLCからの加入応答でただちに応答される方法を確認します

<#root>

[*09/27/2023 21:50:41.9880]

CAPWAP State: Join

[*09/27/2023 21:50:41.9910]

Sending Join request to 172.16.5.11

through port 5270

[*09/27/2023 21:50:41.9950]

Join Response from 172.16.5.11

[*09/27/2023 21:50:41.9950]

AC accepted join request

with result code: 0

[*09/27/2023 21:50:41.9990] Received wlcType 0, timer 30

[*09/27/2023 21:50:41.9990] TLV ID 2216 not found

[*09/27/2023 21:50:41.9990] TLV-DEC-ERR-1: No proc for 2216

CAPWAP状態：イメージデータ

APは自身のイメージをWLCのイメージと比較します。この場合、APのアクティブパーティションとバックアップパーティションの両方ともWLCとは異なるイメージを持つため、**upgrade.sh**スクリプトを呼び出して、WLCに適切なイメージを要求し、現在の非アクティブパーティションにダウンロードするようにAPに指示します。

<#root>

[*09/27/2023 21:50:42.0430]

CAPWAP State: Image Data

[*09/27/2023 21:50:42.0430]

AP image version 8.10.185.0 backup 8.10.105.0, Controller 17.9.3.50

[*09/27/2023 21:50:42.0430]

Version does not match.

[*09/27/2023 21:50:42.0680]

upgrade.sh

: Script called with args:[PRECHECK]
[*09/27/2023 21:50:42.1060] do PRECHECK,

part2 is active part

[*09/27/2023 21:50:42.1240]

upgrade.sh

: /tmp space: OK available 101476, required 40000
[*09/27/2023 21:50:42.1250] wtpImgFileReadRequest: request ap1g7, local /tmp/part.tar
[*09/27/2023 21:50:42.1310]

Image Data Request sent to 172.16.5.11

, fileName [ap1g7], slaveStatus 0
[*09/27/2023 21:50:42.1340]

Image Data Response from 172.16.5.11

[*09/27/2023 21:50:42.1340] AC accepted join request with result code: 0
[*09/27/2023 21:50:42.1450] <.....
[*09/27/2023 21:50:55.4980]
[*09/27/2023 21:51:11.6290]Discarding msg CAPWAP_WTP_EVENT_REQUEST(type
[*09/27/2023 21:51:19.7220]
[*09/27/2023 21:51:24.6880]
[*09/27/2023 21:51:37.7790]
[*09/27/2023 21:51:50.9440]> 76738560 bytes, 57055 msgs, 930 last
[*09/27/2023 21:51:59.9160] Last block stored, IsPre 0, WriteTaskId 0
[*09/27/2023 21:51:59.9160]

Image transfer completed from WLC

, last 1

イメージ転送が完了すると、APはイメージ署名検証プロセスを開始して検証します。その後、upgrade.shスクリプトによって、そのイメージが現在の非アクティブパーティションにインストールされ、ブートに使用するパーティションがスワップされます。最後に、APはそれ自体をリロードし、プロセスを最初から繰り返します(CAPWAP State: Discover)。

<#root>

[*09/27/2023 21:52:01.1280]

Image signing verify success.

[*09/27/2023 21:52:01.1440]
[*09/27/2023 21:52:01.1440] [9/27/2023 21:53:2] : Shadow is now in-synced with master
[*09/27/2023 21:52:01.1440]
[*09/27/2023 21:52:01.1440] [9/27/2023 21:53:2] : Verifying against bundle image btldr.img...
[*09/27/2023 21:52:01.1570]

upgrade.sh

:

part to upgrade is part1

[*09/27/2023 21:52:01.1780]

upgrade.sh

: AP version1: part1 8.10.105.0, img 17.9.3.50

[*09/27/2023 21:52:01.1960]

upgrade.sh

: Extracting and verifying image in part1...

[*09/27/2023 21:52:01.2080]

upgrade.sh

: BOARD generic case execute

[*09/27/2023 21:52:01.5280]

upgrade.sh

: Untar /tmp/part.tar to /bootpart/part1...

[*09/27/2023 21:52:01.7890]

upgrade.sh

: Sync image to disk...

[*09/27/2023 21:52:31.4970]

upgrade.sh

: status '

Successfully verified image in part1.

'

[*09/27/2023 21:52:32.5270]

upgrade.sh

: AP version2: part1 17.9.3.50, img 17.9.3.50

[*09/27/2023 21:52:32.5540]

upgrade.sh

: AP backup version: 17.9.3.50

[*09/27/2023 21:52:32.5700]

upgrade.sh

:

Finished upgrade task.

[*09/27/2023 21:52:32.5840]

upgrade.sh

: Cleanup for do_upgrade...

[*09/27/2023 21:52:32.5970]

upgrade.sh

: /tmp/upgrade_in_progress cleaned

[*09/27/2023 21:52:32.6090]

upgrade.sh

: Cleanup tmp files ...
[*09/27/2023 21:52:32.6720]

upgrade.sh

: Script called with args:[ACTIVATE]
[*09/27/2023 21:52:32.7100] do ACTIVATE, part2 is active part
[*09/27/2023 21:52:32.7640]

upgrade.sh

: Verifying image signature in part1
[*09/27/2023 21:52:33.7730]

upgrade.sh

: status 'Successfully verified image in part1.'
[*09/27/2023 21:52:33.7850]

upgrade.sh

:
activate part1, set BOOT to part1

[*09/27/2023 21:52:34.2940]

upgrade.sh

:
AP primary version after reload: 17.9.3.50

[*09/27/2023 21:52:34.3070]

upgrade.sh

: AP backup version after reload: 8.10.185.0
[*09/27/2023 21:52:34.3190]

upgrade.sh

: Create after-upgrade.log
[*09/27/2023 21:52:37.3520]

AP Rebooting: Reset Reason - Image Upgrade



警告：証明書が期限切れのため、Wave 1アクセスポイントが新しいイメージのダウンロードに失敗する可能性があります。詳細については、[Field Notice 72524](#)を参照してください。影響とソリューションについては、『[2022年12月4日 \(CSCwd80290\)サポートドキュメント](#)』の「IOS APイメージのダウンロードが、イメージ署名証明書の期限切れにより失敗する」をよくお読みください。

APがリロードしてCAPWAP DiscoverおよびJoin状態に戻ると、Image Data状態の間に、適切なイメージが取得されたことを検出します。

<#root>

[*09/27/2023 21:56:13.7640]

CAPWAP State: Image Data

[*09/27/2023 21:56:13.7650]

AP image version 17.9.3.50 backup 8.10.185.0, Controller 17.9.3.50

[*09/27/2023 21:56:13.7650]

Version is the same, do not need update.

[*09/27/2023 21:56:13.7650] status '

upgrade.sh: Script called with args:[NO_UPGRADE]

,

[*09/27/2023 21:56:13.7850] do NO_UPGRADE, part1 is active part

CAPWAP状態 : 設定

APは、WLCと同じバージョンであることを確認した後、現在の設定をWLCに通知します。一般に、これは、APが設定を管理するように要求することを意味します (設定がWLCで使用可能な場合)。

<#root>

[*09/27/2023 21:56:14.8680]

CAPWAP State: Configure

[*09/27/2023 21:56:15.8890] Telnet is not supported by AP, should not encode this payload

[*09/27/2023 21:56:15.8890] Radio [1] Administrative state DISABLED change to ENABLED

[*09/27/2023 21:56:16.0650] Radio [0] Administrative state DISABLED change to ENABLED

[*09/27/2023 21:56:16.0750] DOT11_CFG[1]: Starting radio 1

[*09/27/2023 21:56:16.1150] DOT11_DRV[1]: Start Radio1

[*09/27/2023 21:56:16.1160] DOT11_DRV[1]: set_channel Channel set to 36/20

[*09/27/2023 21:56:16.4380] Started Radio 1

[*09/27/2023 21:56:16.4880] DOT11_CFG[0]: Starting radio 0

[*09/27/2023 21:56:17.5220] DOT11_DRV[0]: Start Radio0

[*09/27/2023 21:56:16.5650] DOT11_DRV[0]: set_channel Channel set to 1/20

[*09/27/2023 21:56:16.5650] Started Radio 0

[*09/27/2023 21:56:16.5890] sensord psage_base init: RHB Sage base ptr a1030000

CAPWAP状態 : Run

この時点で、APはコントローラに正常に加入しています。この状態の間、WLCは、APによって要求された設定を上書きするメカニズムをトリガーします。WLCにはAPに関する情報がなかったため、APの無線とクレデンシャルの設定がプッシュされ、APがデフォルトポリシータグに割り当てられることがわかります。

<#root>

[*09/27/2023 21:56:17.4870]

CAPWAP State: Run

[*09/27/2023 21:56:17.4870]

AP has joined controller

uwu-9800

[*09/27/2023 21:56:17.4940] DOT11_DRV[0]: set_channel Channel set to 1/20
[*09/27/2023 21:56:17.5440] sensord split_glue psage_base: RHB Sage base ptr a1030000
[*09/27/2023 21:56:17.6010] sensord split_glue sage_addr: RHB Sage base ptr a1030000
[*09/27/2023 21:56:17.6230] ptr a1030000
[*09/27/2023 21:56:17.6420]

DOT11_DRV[0]: set_channel Channel set to 1/20

[*09/27/2023 21:56:17.8120]

DOT11_DRV[1]: set_channel Channel set to 36/20

[*09/27/2023 21:56:17.9350] Previous AP mode is 0, change to 0
[*09/27/2023 21:56:18.0160] Current session mode: ssh, Configured: Telnet-No, SSH-Yes, Console-Yes
[*09/27/2023 21:56:18.1220] Current session mode: telnet, Configured: Telnet-No, SSH-Yes, Console-Yes
[*09/27/2023 21:56:18.1310] Current session mode: console, Configured: Telnet-No, SSH-Yes, Console-Yes
[*09/27/2023 21:56:18.1340]

chpasswd: password for user changed

[*09/27/2023 21:56:18.1350]

chpasswd: password for user changed

[*09/27/2023 21:56:18.1520] systemd[1]: Starting Cisco rsyslog client watcher...
[*09/27/2023 21:56:18.1610] Same LSC mode, no action needed
[*09/27/2023 21:56:18.1640] CLSM[00:00:00:00:00:00]: U3 Client RSSI Stats feature is deprecated; can no
[*09/27/2023 21:56:18.1720] systemd[1]: Stopping rsyslog client...
[*09/27/2023 21:56:18.2120] systemd[1]: Starting Cisco syslog service...
[*09/27/2023 21:56:18.2230] systemd[1]: Started Cisco syslog service.
[*09/27/2023 21:56:18.2410] systemd[1]: Started rsyslog client.
[*09/27/2023 21:56:18.2440] AP is in good condition, BLE is off
[*09/27/2023 21:56:18.2510] SET_SYS_COND_INTF: allow_usb state: 1 (up) condition
[*09/27/2023 21:56:18.2530] systemd[1]: Starting dhcpv6 client watcher...
[*09/27/2023 21:56:18.2530] systemd[1]: Stopping DHCPv6 client...
[*09/27/2023 21:56:18.2530] systemd[1]: Starting DHCPv6 client...
[*09/27/2023 21:56:18.2530] systemd[1]: Started DHCPv6 client.
[*09/27/2023 21:56:18.2530] systemd[1]: Started dhcpv6 client watcher.
[*09/27/2023 21:56:18.2560]

Set radio 0 power 4 antenna mask 15

[*09/27/2023 21:56:18.2530]

Set radio 1 power 4 antenna mask 15

[*09/27/2023 21:56:18.2530] Got WSA Server config TLVs
[*09/27/2023 21:56:18.2720]

AP tag change to default-policy-tag

[*09/27/2023 21:56:18.2780] Chip flash OK

設定

スタティックWLCの選択

GUIでは、**Configuration > Wireless > Access Points**の順に選択し、APを選択して、**High Availability**タブに移動します。ここでは、このドキュメントの「ワイヤレスLANコントローラの選択」セクションで説明されているように、プライマリ、セカンダリ、およびターシャリ WLCを設定できます。この設定は、アクセスポイントごとに行います。

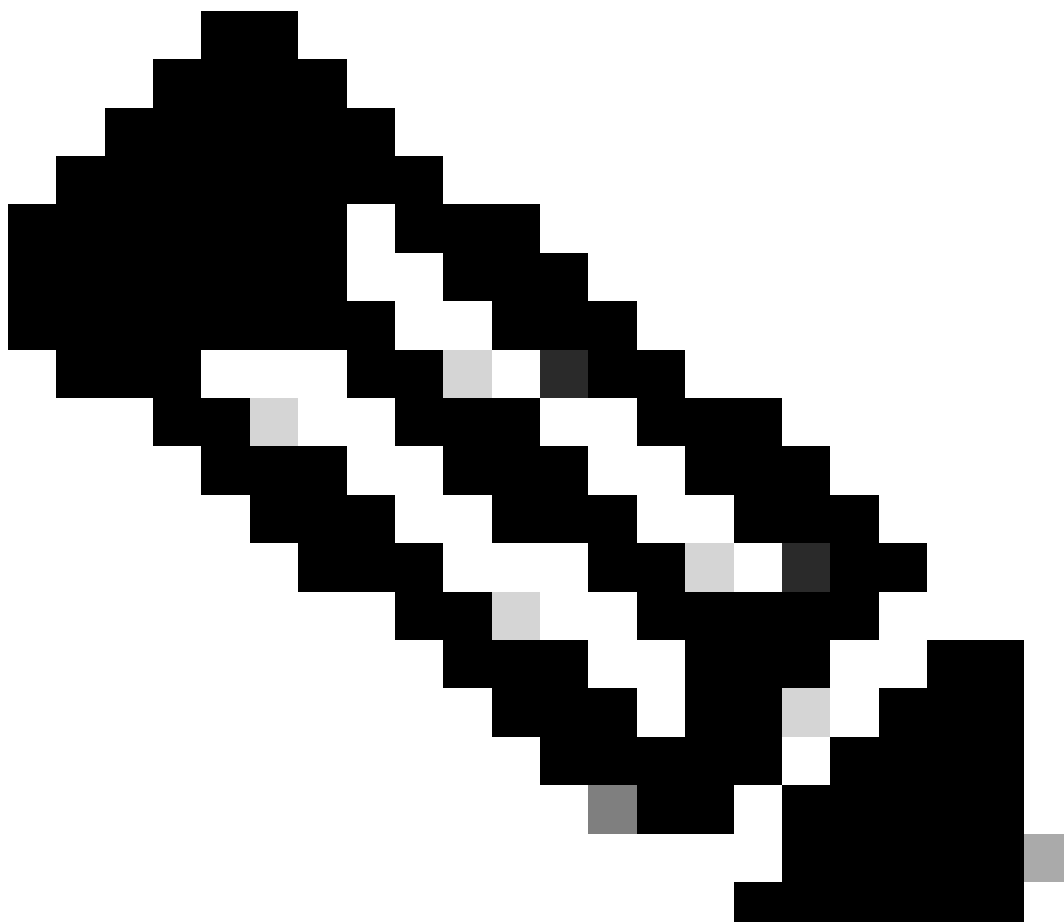
The screenshot displays the Cisco Catalyst 9800-L Wireless Controller GUI. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area is divided into two panels. The left panel, titled 'All Access Points', shows a table of APs with columns for AP Name, AP Model, and Slots. The right panel, titled 'Edit AP', shows the 'High Availability' configuration page with fields for Primary, Secondary, and Tertiary Controller, and a dropdown for AP failover priority.

AP Name	AP Model	Slots
AP70F0.967E.AFAC	C9120AXE-B	2
AP7c0e.ce14.8088	AIR-CAP3702I-N-K9	2
C9120AXI-EMORENOA	C9120AXI-A	2
AP9130AX-luisajim	C9130AXE-A	3
3802-emorenoa	AIR-AP3802I-B-K9	2

Name	Management IP Address (IPv4/IPv6)
Primary Controller	wlc-9800 172.16.5.11
Secondary Controller	
Tertiary Controller	

AP failover priority: Low

APのプライマリ、セカンダリ、ターシャリWLC。

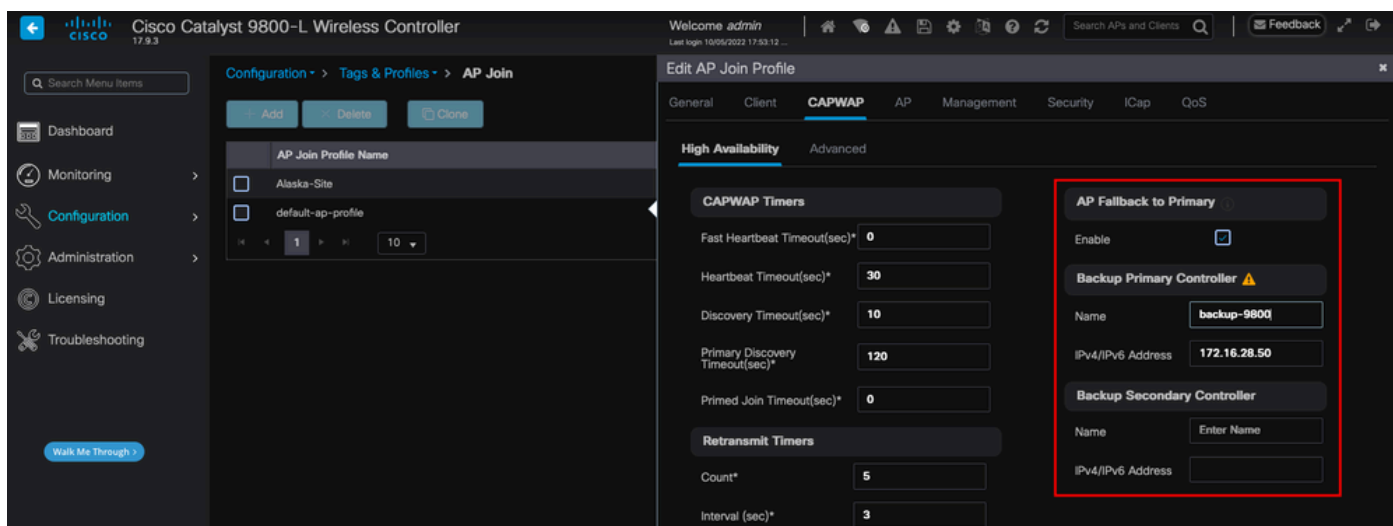


注: Cisco IOS XE 17.9.2以降では、プライミングプロファイルを使用して、正規表現(regex)に一致するAPグループまたは個々のAPに対して、プライマリ、セカンダリ、ターシャリコントローラを設定できます。詳細については、『[コンフィギュレーションガイド](#)』の「[APプライミングプロファイルで設定されたコントローラへのAPフォールバック](#)」セクションを参照してください。

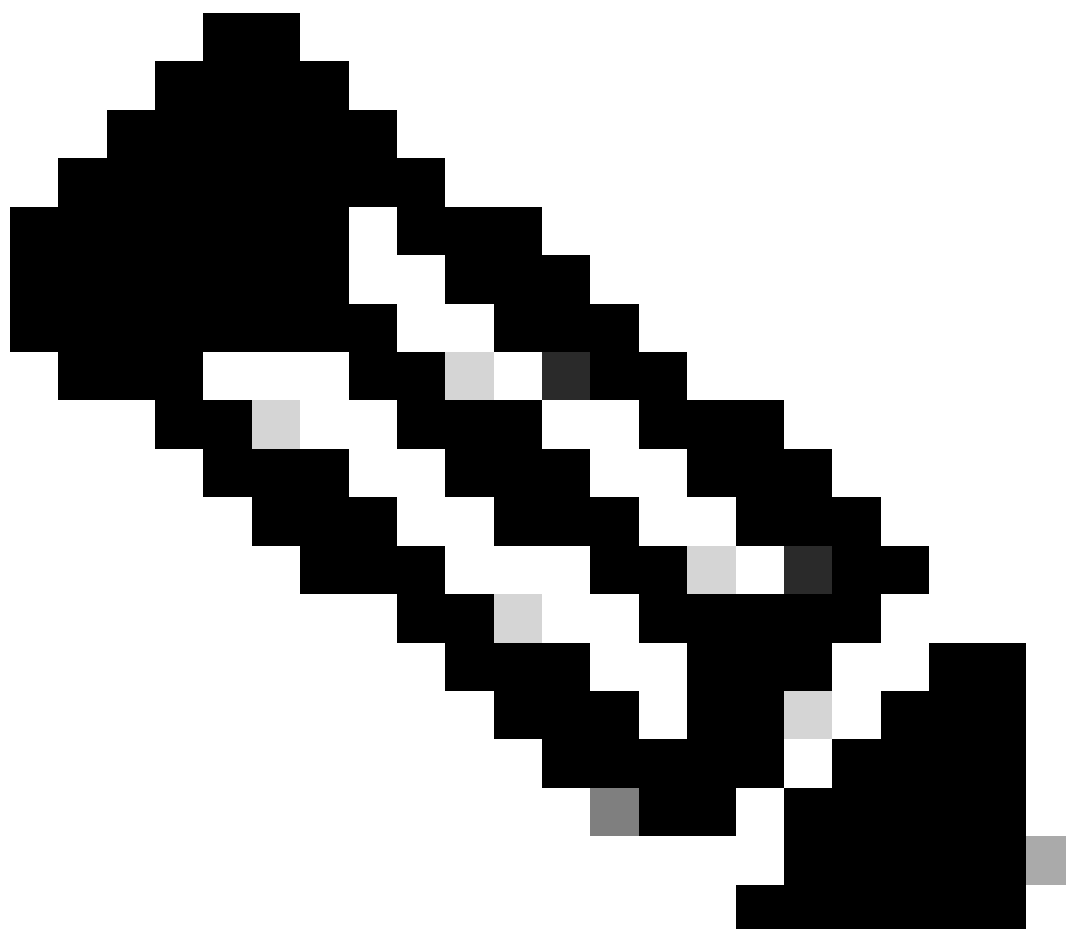
AP High Availabilityタブで設定するプライマリ、セカンダリ、ターシャリコントローラは、AP Join ProfileごとにCAPWAP > High Availabilityタブで設定できるバックアッププライマリおよびセカンダリ WLCとは異なることに注意してください。プライマリ、セカンダリ、ターシャリコントローラは、それぞれプライオリティ1、2、3のWLCと見なされ、バックアッププライマリおよびセカンダリは、プライオリティ4と5のWLCと見なされます。

AP Fallbackが有効な場合、APは別のWLCに加入するときにプライマリコントローラをアクティブに探します。CAPWAPダウンイベントが発生し、バックアッププライマリおよびセカンダリコントローラが使用できない場合、APはプライオリティ4および

5のWLCのみを検索します。



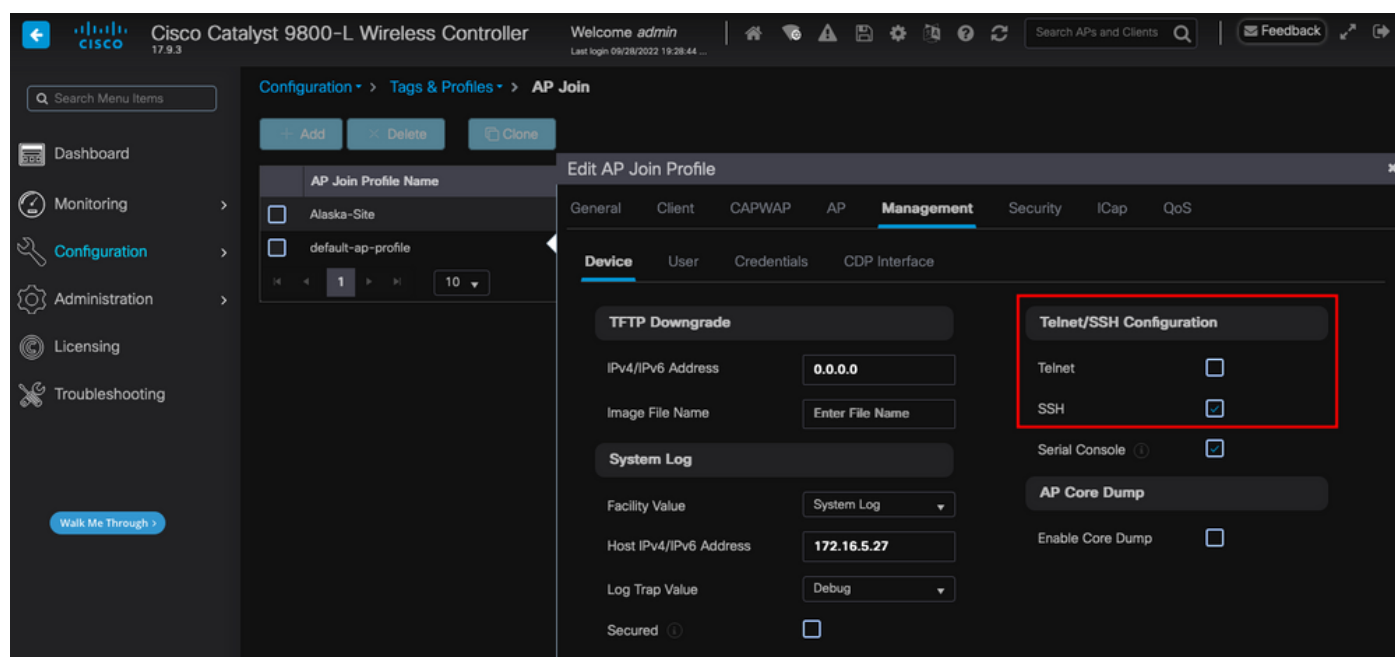
AP加入プロファイルのハイアベイラビリティオプション



注：AP Join プロファイルのバックアッププライマリおよびバックアップセカンダリWLCの設定では、アクセスポイントのHigh Availabilityタブに静的プライマリエントリと静的セカンダリエントリは入力されません。

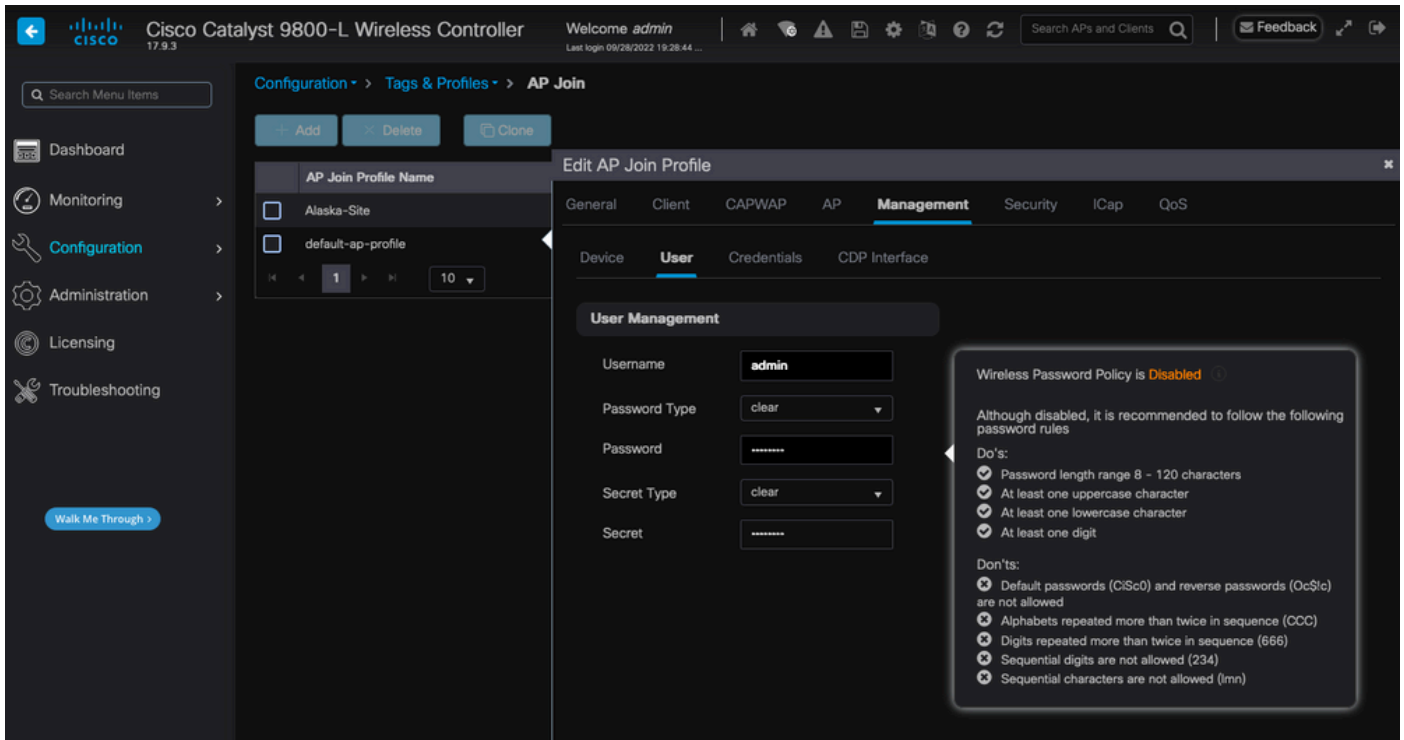
APへのTelnet/SSHアクセスの有効化

Configuration > Tags & Profiles > AP Join > Management > Deviceの順に選択し、SSHまたはTelnet、あるいはその両方を選択します。



AP加入プロファイルでのTelnet/SSHアクセスの有効化

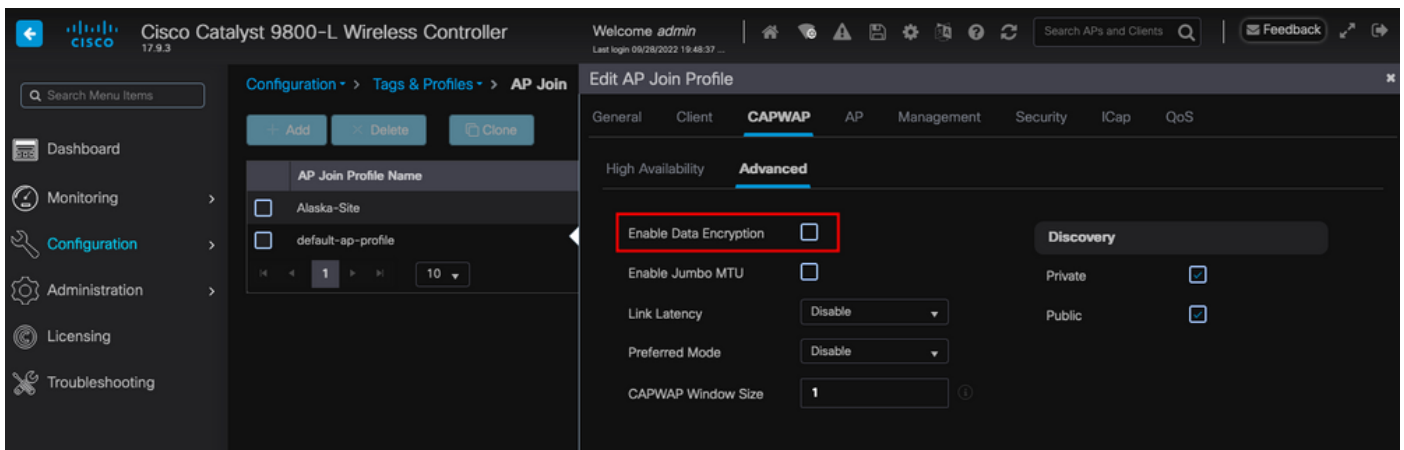
SSH/Telnetクレデンシャルを設定するには、同じウィンドウでUserタブに移動し、APにアクセスするためのUsername、Password、およびSecretを設定します。



APのSSHおよびTelnetクレデンシャル

データリンク暗号化

APのトラフィックのパケットキャプチャを実行する必要があるクライアントの問題をトラブルシューティングする必要がある場合は、**Configuration > Tags & Profiles > AP Join > CAPWAP > Advanced**で**Data Link Encryption**が無効になっていることを確認します。そうしないと、トラフィックは暗号化されます。



データリンク暗号化



注：データ暗号化では、CAPWAPデータトラフィックのみが暗号化されます。CAPWAP制御トラフィックはすでにDTLSで暗号化されています。

確認

APのコンソールでCAPWAP状態マシンを追跡することに加え、WLCで[組み込みパケットキャプチャ](#)を実行してAP加入プロセスを分析することもできます。

No.	Time	Time delta from Source	Destination	Protocol	Length	Destination Port	Info
886	12:58:41.288976	0.022802000	172.16.5.65	CAPWAP-Control	294	5246	CAPWAP-Control - Discovery Request
887	12:58:41.288976	0.000000000	172.16.5.11	CAPWAP-Control	147	5267	CAPWAP-Control - Discovery Response
888	12:58:41.388974	0.027998000	172.16.5.65	CAPWAP-Control	294	5246	CAPWAP-Control - Discovery Request
889	12:58:41.388974	0.000000000	172.16.5.11	CAPWAP-Control	147	5267	CAPWAP-Control - Discovery Response
1156	12:58:50.794957	0.195980000	172.16.5.65	DTLSv1.2	276	5246	Client Hello
1157	12:58:50.795948	0.000991000	172.16.5.11	DTLSv1.2	98	5267	Hello Verify Request
1158	12:58:50.796955	0.001007000	172.16.5.65	DTLSv1.2	296	5246	Client Hello
1159	12:58:50.798954	0.001999000	172.16.5.11	DTLSv1.2	562	5267	Server Hello, Certificate (Fragment)
1160	12:58:50.798954	0.000000000	172.16.5.11	DTLSv1.2	562	5267	Certificate (Fragment)
1161	12:58:50.798954	0.000000000	172.16.5.11	DTLSv1.2	562	5267	Certificate (Reassembled), Server Key Exchange (Fragment)
1162	12:58:50.798954	0.000000000	172.16.5.11	DTLSv1.2	349	5267	Server Key Exchange (Reassembled), Certificate Request, Server Hello Done
1163	12:58:50.859948	0.060980000	172.16.5.65	DTLSv1.2	594	5246	Certificate (Fragment)
1164	12:58:50.859948	0.000000000	172.16.5.11	DTLSv1.2	594	5246	Certificate (Reassembled), Client Key Exchange (Fragment)
1181	12:58:51.204975	0.066997000	172.16.5.65	DTLSv1.2	463	5246	Client Key Exchange (Reassembled), Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
1182	12:58:51.205984	0.001009000	172.16.5.11	DTLSv1.2	125	5267	Change Cipher Spec, Encrypted Handshake Message
1328	12:58:55.914945	0.016997000	172.16.5.11	DTLSv1.2	1487	5246	Application Data
1321	12:58:55.916944	0.001999000	172.16.5.11	DTLSv1.2	1484	5267	Application Data
1330	12:58:56.246981	0.109003000	172.16.5.65	DTLSv1.2	1439	5246	Application Data
1331	12:58:56.246981	0.000000000	172.16.5.11	DTLSv1.2	1439	5246	Application Data
1332	12:58:56.246981	0.000000000	172.16.5.11	DTLSv1.2	379	5246	Application Data
1333	12:58:56.247973	0.000992000	172.16.5.11	DTLSv1.2	354	5267	Application Data
1364	12:58:57.292984	0.040999000	172.16.5.65	DTLSv1.2	1439	5246	Application Data
1365	12:58:57.292984	0.000000000	172.16.5.11	DTLSv1.2	690	5246	Application Data
1366	12:58:57.293975	0.000991000	172.16.5.11	DTLSv1.2	354	5267	Application Data
1368	12:58:57.387965	0.069980000	172.16.5.65	DTLSv1.2	902	5246	Application Data
1369	12:58:57.388972	0.001007000	172.16.5.11	DTLSv1.2	402	5267	Application Data
1376	12:58:57.466961	0.001999000	172.16.5.65	DTLSv1.2	148	5246	Application Data
1377	12:58:57.466961	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1378	12:58:57.470968	0.001007000	172.16.5.11	CAPWAP-Data	104	5247	CAPWAP-Data Keep-Alive(Malformed Packet)
1379	12:58:57.474966	0.003998000	172.16.5.11	DTLSv1.2	133	5267	Application Data
1380	12:58:57.477972	0.003006000	172.16.5.11	CAPWAP-Data	104	5267	CAPWAP-Data Keep-Alive(Malformed Packet)
1400	12:58:57.546968	0.003997000	172.16.5.65	DTLSv1.2	148	5246	Application Data
1401	12:58:57.546968	0.000000000	172.16.5.11	DTLSv1.2	119	5246	Application Data
1402	12:58:57.547968	0.000992000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1403	12:58:57.547968	0.000000000	172.16.5.11	DTLSv1.2	121	5267	Application Data
1411	12:58:57.575958	0.002998000	172.16.5.65	DTLSv1.2	148	5246	Application Data
1412	12:58:57.575958	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1413	12:58:57.577957	0.001999000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1414	12:58:57.577957	0.000000000	172.16.5.11	DTLSv1.2	143	5246	Application Data
1415	12:58:57.577957	0.000000000	172.16.5.11	DTLSv1.2	1190	5267	Application Data
1416	12:58:57.577957	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1425	12:58:57.688959	0.078950000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1426	12:58:57.688959	0.000000000	172.16.5.11	DTLSv1.2	148	5246	Application Data
1427	12:58:57.688959	0.000000000	172.16.5.11	DTLSv1.2	119	5267	Application Data
1428	12:58:57.688959	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1429	12:58:57.688951	0.000992000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1430	12:58:57.688951	0.000000000	172.16.5.11	DTLSv1.2	222	5246	Application Data
1431	12:58:57.690958	0.001007000	172.16.5.11	DTLSv1.2	175	5267	Application Data
1432	12:58:57.690958	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1433	12:58:57.692957	0.001999000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1434	12:58:57.692957	0.000000000	172.16.5.11	DTLSv1.2	111	5246	Application Data

WLCの組み込みパケットキャプチャに見られるAP加入プロセス

Chance Cipher Specパケット (パケット番号1182) の後のすべてのトラフィックがDTLSv1.2を介してApplication Dataとしてのみ表示される点に注意してください。これは、DTLSセッションが確立された後のすべての暗号化データです。

トラブルシューティング

既知の問題

APがWLCに加入するのを妨げる可能性のある既知の問題を参照してください。

- [Wave 2およびCatalyst 11axアクセスポイント\(CSCvx32806\)での破損イメージによるブートループのAP](#)
- [フィールド通知72424: 2022年9月以降に製造されたC9105/C9120/C9130アクセスポイントは、ワイヤレスLANコントローラに加入するためにソフトウェアのアップグレードが必要な場合があります。](#)
- [フィールド通知72524: ソフトウェアのアップグレード/ダウングレード中に、証明書の期限切れのために2022年12月4日の後でCisco IOS APがダウンロード状態のままになる可能性 - ソフトウェアアップグレードを推奨](#)
- [Cisco Bug ID CSCwb13784: AP加入要求で無効なパスMTUが原因でAPが9800に加入できない](#)
- [Cisco Bug ID CSCvu22886: 17.7へのアップグレード時のC9130: メッセージ「unlzma: write: No space left on device」、/tmpの最大サイズを増やす](#)

アップグレードの前に、必ず各バージョンの『リリースノート』の「アップグレードパス」セクションを参照してください。



注：Cisco IOS XE Cupertino 17.7.1以降のCisco Catalyst 9800-CLワイヤレスコントローラは、スマートライセンスが接続されておらず、起動していない場合、50を超えるAPを受け入れません。

WLC GUIのチェック

WLCで、**Monitoring > Wireless > AP Statistics > Join Statistics** の順に選択すると、任意のAPから報告された**Last Reboot Reason**とWLCによって登録された**Last Disconnect Reason**を確認できます。

AP Name	AP Model	Status	IP Address	Base Radio MAC	Ethernet MAC	Last Reboot Reason (Reported by AP)	Last Disconnect Reason
9120AP	C9120AXI-A	Red	172.16.5.23	3c41.0a31.7700	6c41.0a16.e79c	No reboot reason	DTLS close alert from peer
josuhel9120	C9120AXI-B	Red	172.16.5.61	3c41.0a31.7780	6c41.0a16.e79c	No reboot reason	DTLS close alert from peer
AP19F9.2095.54F0	C9106AXI-B	Red	172.16.5.32	488b.0aa7.7940	1095.2090.54f0	No reboot reason	DTLS close alert from peer
AP72F9.9E76.AFAC	C9120AXI-B	Green	172.16.5.79	7090.9685.7980	7090.9676.afac	Controller reload command	Mesh AP role change
AP710e.ca14.8088	AR-CA93702I-N-K9	Green	172.16.5.31	710e.ca76.d800	710e.ca14.8088	Image upgrade successfully	NA
C9120AXI-EMORENCA	C9120AXI-A	Green	172.16.5.65	a49b.cd0a.1980	a49b.cd0a.1508	Image upgrade successfully	DTLS close alert from peer
BRCTAC0428	C9120AXI-B	Red	172.16.46.35	c884.a172.2600	c884.a165.8530	No reboot reason	DTLS close alert from peer
AP9130AXI-tulajim	C9130AXI-A	Green	172.16.5.67	011d.2d49.d840	7090.9606.4a44	Controller reload command	Mode change to sniffer
3802-emorenea	AR-AP9820I-B-K9	Green	172.16.5.25	802b.cba7.a5c0	286f.76f5.530e	Controller reload command	Mode change to sniffer

WLCのAP加入統計情報ページ

任意のAPをクリックして、AP加入統計情報の詳細を確認できます。ここでは、APが最後に加入してWLCの検出を試行した日時など、より詳細な情報を確認できます。

Access Point Statistics Summary

Is the AP currently connected to controller	NOT JOINED
Time at which the AP joined this controller last time	09/27/2022 09:45:49
Type of error that occurred last	Join
Time at which the last join error occurred	09/27/2022 09:46:01

Discovery Phase Statistics

Discovery requests received	106
Successful discovery responses sent	106
Unsuccessful discovery request processing	NA
Reason for last unsuccessful discovery attempt	None
Time at last successful discovery attempt	09/27/2022 09:52:27
Time at last unsuccessful discovery attempt	NA

Last AP Disconnect Details

Reason for last AP connection failure	DTLS close alert from peer
Last Reboot Reason (Reported by AP)	No reboot reason

Last AP message decryption failure details

Reason for last message decryption failure	NA
--	----

一般的なAP加入統計情報

詳細については、同じウィンドウの[統計情報]タブを参照してください。ここで、送信された参加応答の量と受信された参加要求の量、および送信された設定応答と受信された設定要求を比較できます。

Join Statistics

General

Statistics

Control DTLS Statistics

DTLS Session request received	8
Established DTLS session	8
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	09/27/2022 09:45:44
Time at last unsuccessful DTLS session	NA

Join phase statistics

Join requests received	8
Successful join responses sent	8
Unsuccessful join request processing	0
Reason for last unsuccessful join attempt	DTLS close alert from peer
Time at last successful join attempt	09/27/2022 09:45:49
Time at last unsuccessful join attempt	NA

Configuration phase statistics

Configuration requests received	15
Successful configuration responses sent	15
Unsuccessful configuration request processing	0
Reason for last unsuccessful configuration attempt	NA
Time at last successful configuration attempt	09/21/2022 01:39:07
Time at last unsuccessful configuration attempt	NA

Data DTLS Statistics

DTLS Session request received	0
Established DTLS session	0
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	NA
Time at last unsuccessful DTLS session	NA

詳細なAP加入統計情報

コマンド

次のコマンドは、APの加入に関する問題のトラブルシューティングに役立ちます。

WLCから

- show ap summary (WLCで実行)
- debug capwapエラー
- CAPWAPパケットのデバッグ

Wave 2およびCatalyst 11ax APから

- debug capwap client events
- debug capwap client error
- debug dtls clientエラー
- debug dtls clientイベント
- CAPWAPクライアントキープアライブのデバッグ
- capwap再起動のテスト
- CAPWAP AP Erase All (すべて消去)

Wave 1 APから

- debug capwap console cli
- debug capwap client no-reload
- show dtls stats (隠しコマンド)
- clear cawap ap all-config



注:TelnetまたはSSHを使用してAPに接続してトラブルシューティングを行う場合は、常にコマンド**terminal monitor**を発行し、APでデバッグを有効にした後で問題を再現してください。そうでない場合、デバッグからの出力は表示されません。

放射性物質トレース

AP加入の問題をトラブルシューティングする場合は、まず、加入に問題があるAPの無線とイーサネットの両方のMACアドレスの放射性トレースを取得することをお勧めします。これらのログを生成する方法の詳細は、『[Catalyst 9800 WLCでのデバッグとログの収集](#)』を参照してください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。