

了解Catalyst 9800 WLC的AP加入过程

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[CAPWAP会话建立](#)

[DTLS会话建立](#)

[无线局域网控制器发现方法](#)

[无线局域网控制器选举](#)

[CAPWAP状态机](#)

[CAPWAP状态：发现](#)

[CAPWAP状态：DTLS设置。](#)

[CAPWAP状态：加入](#)

[CAPWAP状态：图像数据](#)

[CAPWAP状态：配置](#)

[CAPWAP状态：运行](#)

[配置](#)

[静态WLC选举](#)

[启用对无线接入点的Telnet/SSH访问](#)

[数据链路加密](#)

[验证](#)

[故障排除](#)

[已知问题](#)

[WLC GUI检查](#)

[命令](#)

[从WLC](#)

[来自Wave 2和Catalyst 11ax AP](#)

[从Wave 1 AP](#)

[放射性痕迹](#)

简介

本文档详细介绍使用Cisco Catalyst 9800 WLC的AP加入过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解控制和配置无线接入点(CAPWAP)
- 基本了解无线Lan控制器(WLC)的使用

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 9800-L WLC、Cisco IOS® XE Cupertino 17.9.3
- Catalyst 9120AX接入点

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

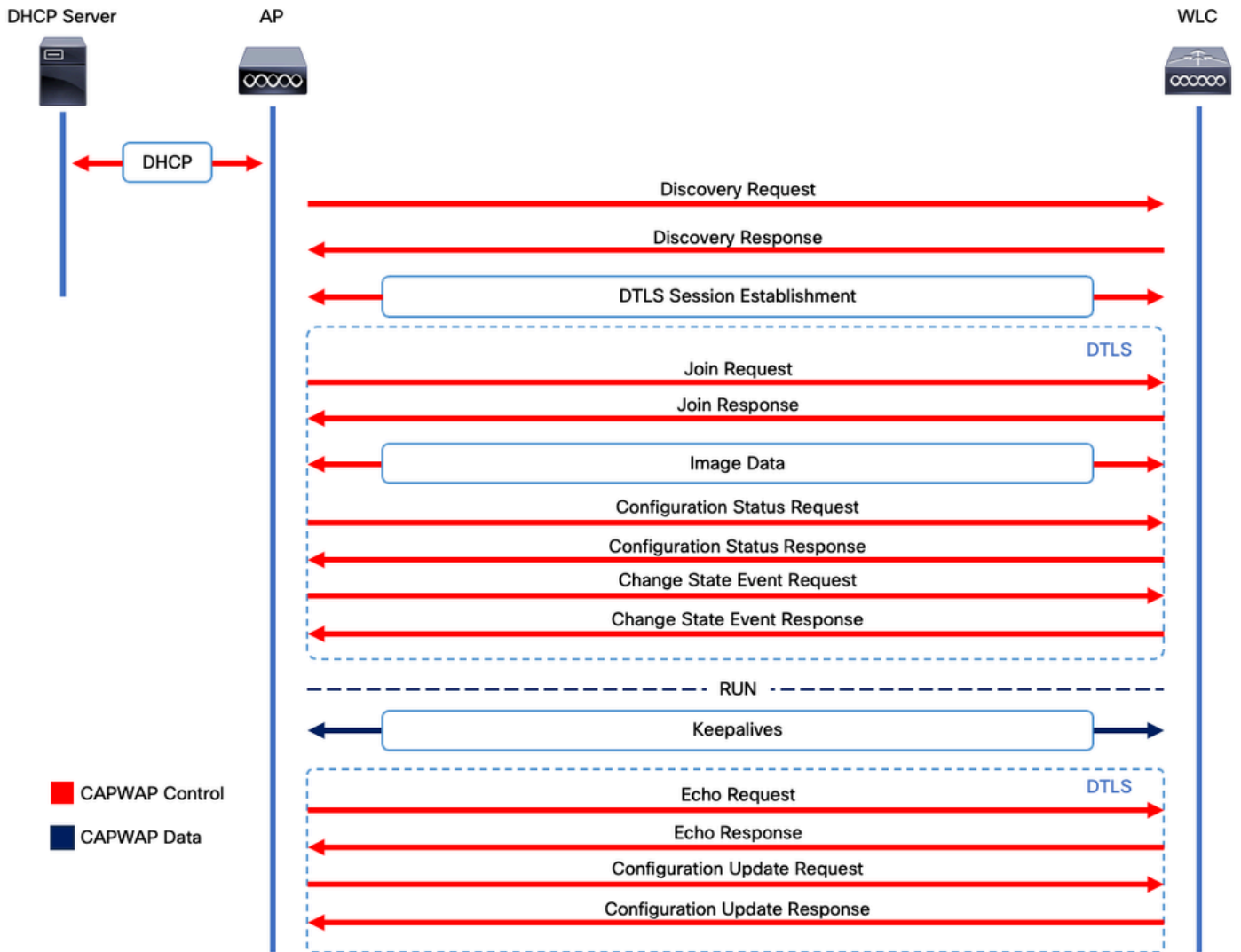
CAPWAP会话建立

控制和配置无线接入点(CAPWAP)是提供接入点(AP)和无线局域网控制器(WLC)使用的传输机制的协议，用于通过安全通信隧道（用于CAPWAP控制）交换控制和数据平面信息。

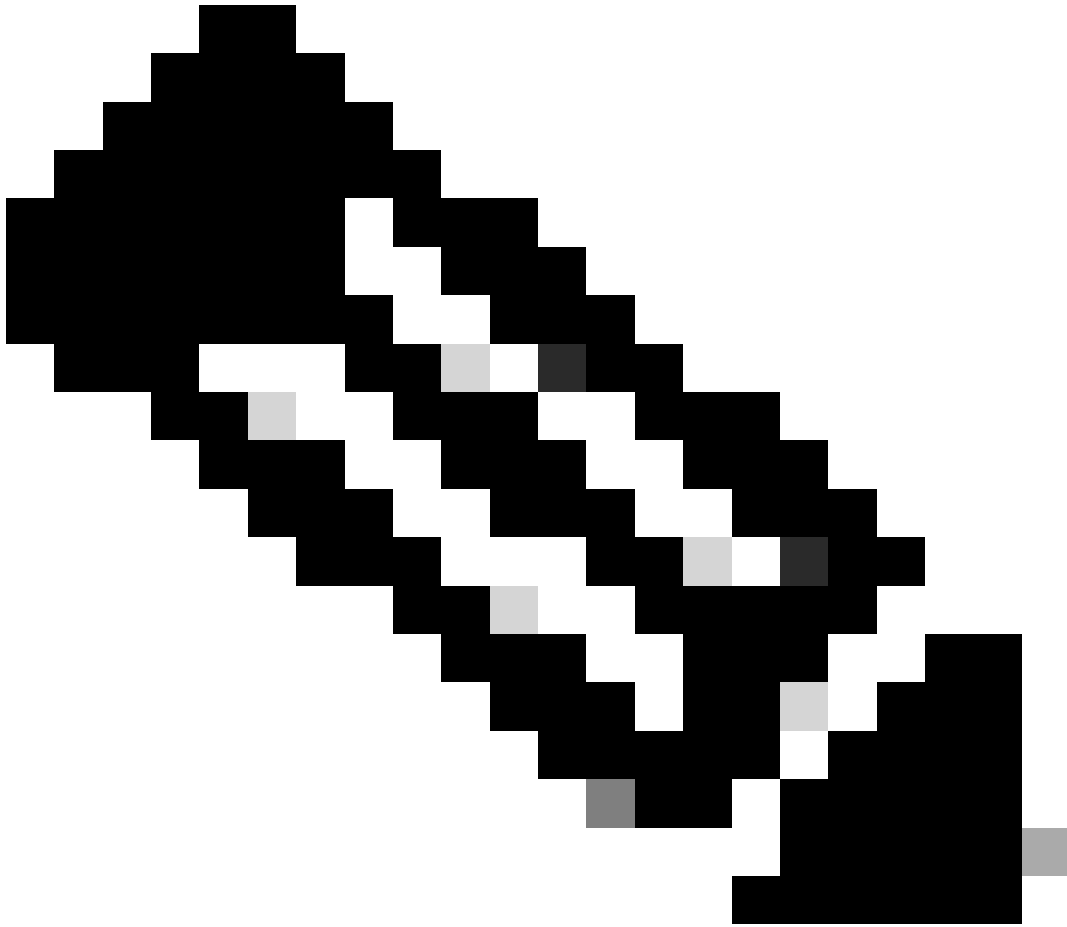
要详细说明AP加入过程，您必须了解控制和设置无线接入点(CAPWAP)会话建立过程。

请记住，AP需要有IP地址才能启动CAPWAP进程。如果AP没有IP地址，它不会启动CAPWAP会话建立过程。

1. 接入点发送发现请求。有关此过程的详细信息，请参阅WLC发现方法部分
2. WLC发送发现响应
3. DTLS会话建立。之后，所有消息都将加密，并在任何数据包分析工具中显示为DTLS应用数据包。
4. 接入点发送加入请求
5. WLC发送加入响应
6. AP执行映像检查。如果与WLC具有相同的映像版本，则继续执行下一步。如果没有，则从WLC下载映像并重新启动以加载新映像。在这种情况下，它会重复步骤1中的过程。
7. 接入点发送配置状态请求。
8. WLC发送配置状态响应
9. 接入点进入运行状态
10. 在RUN状态下，可以通过两种方式执行CAPWAP隧道维护：
 1. Keepalive交换以维护CAPWAP数据隧道
 2. AP向WLC发送Echo请求，WLC必须以其各自的Echo响应作为应答。这是为了维护CAPWAP控制隧道。



CAPWAP会话建立过程



注意：根据RFC 5415，CAPWAP使用UDP端口5246（用于CAPWAP控制）和5247（用于CAPWAP数据）。

DTLS会话建立

一旦接入点收到来自WLC的有效发现响应，即会在它们之间建立DTLS隧道，以通过安全隧道传输所有后续数据包。建立DTLS会话的过程如下：

1. AP发送客户端Hello消息
2. WLC发送HelloVerifyRequest消息，其中包含用于验证的cookie。
3. AP发送ClientHello消息，其中包含用于验证的cookie。
4. WLC按以下顺序发送这些数据包：
 1. ServerHello
 2. 证书
 3. 服务器密钥交换
 4. 证书请求
 5. ServerHelloDone

5. AP按以下顺序发送这些数据包：

1. 证书
2. ClientKeyExchange
3. 证书验证
4. ChangeCipherSpec

6. WLC使用自己的ChangedCipherSpec响应AP的ChangeCipherSpec：

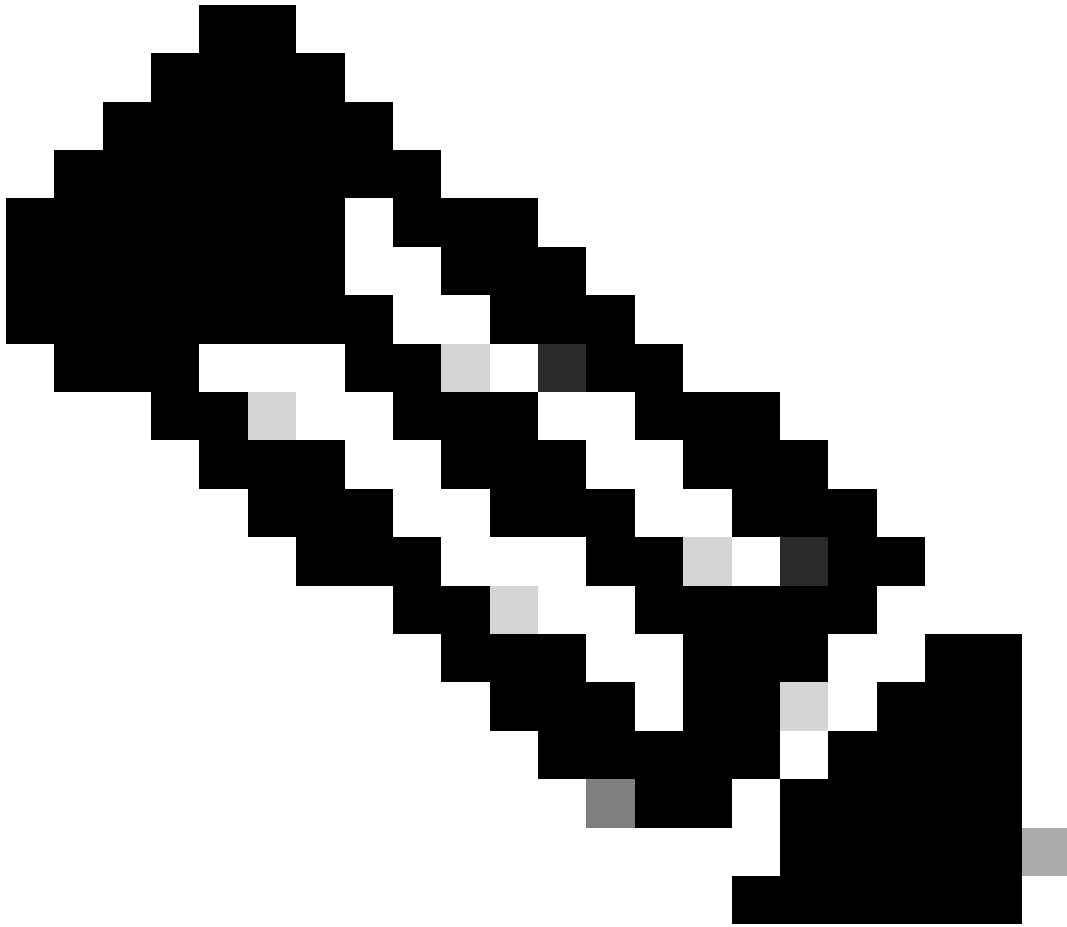
1. ChangeCipherSpec

在WLC发送最后一个ChangedCipherSpec消息之后，将建立安全隧道，并且现在将加密双向发送的所有流量。

无线局域网控制器发现方法

有多种选项可以让接入点知道网络中有一个WLC的存在：

- DHCP选项43：此选项为AP提供WLC的IPv4加入地址。对于AP和WLC位于不同站点的大型部署，此过程非常方便。
- DHCP选项52：此选项为AP提供要加入的WLC的IPv6地址。在与DHCP选项43相同的场景下，其使用非常方便。
- DNS发现：AP查询域名CISCO-CAPWAP-CONTROLLER.localdomain。您必须配置DNS服务器以解析WLC的IPv4或IPv6地址以加入。对于将WLC与AP存储在同一站点的部署，此选项比较方便。
- 第3层广播：AP自动向255.255.255.255发送广播消息。与AP位于同一子网的任何WLC都应响应此发现请求。
- 静态配置：可以使用 `capwap ap primary-base <wlc-hostname> <wlc-IP-address>`命令在AP中为WLC配置静态条目。
- 移动性发现：如果AP之前已加入作为移动组一部分的WLC，则AP还会保存该移动组中出现的WLC的记录。



注意：列出的WLC发现方法没有任何优先级顺序。

无线局域网控制器选举

一旦AP使用任何WLC发现方法从任何WLC收到发现响应，它将选择其中一个控制器以使用此条件加入：

- 主控制器(使用capwap ap primary-base <wlc-hostname> <wlc-IP-address> 命令配置)
- 辅助控制器(使用capwap ap secondary-base <wlc-hostname> <wlc-IP-address> 命令配置)
- 第三控制器(用capwap ap tertiary-base <wlc-hostname> <wlc-IP-address> 命令配置)

- 如果之前未配置任何主要、辅助或第三WLC，则AP尝试将响应发现请求的第一个WLC与具有最大可用AP容量的发现响应自己的发现响应(即在给定时间可支持最多AP的WLC)加入。

CAPWAP状态机

在AP控制台中，您可以跟踪CAPWAP状态机，该状态机将执行CAPWAP会话建立一节中介绍的步骤。

CAPWAP状态：发现

您可以在此处查看发现请求和响应。观察AP如何通过DHCP（选项43）接收WLC IP，以及如何将发现请求发送到先前已知的WLC：

```
<#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

除了从静态配置的WLC (172.16.0.20)和通过DHCP选项43 (172.16.5.11)指示的WLC接收发现响应外，该AP还从同一子网中的另一个WLC (172.16.5.169)接收发现响应，因为它获取了广播发现消息。

CAPWAP状态：DTLS设置。

在这里，AP和WLC之间的DTLS会话会交换。

<#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状态：加入

在建立DTLS会话之后，现在将通过安全会话向WLC发送加入请求。观察此请求如何从WLC立即响应加入响应

<#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状态：图像数据

AP将其映像与WLC映像进行比较。在这种情况下，AP的活动分区及其备份分区与WLC的映像不同，因此它会调用**upgrade.sh**脚本，该脚本会指示AP向WLC请求足够的映像，并将其下载到当前的非活动分区。

<#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

映像传输完成后，AP将启动映像签名验证过程以验证它。执行此操作后，upgrade.sh脚本会将映像安装到当前非活动分区中，并交换引导分区。最后，AP重新加载自身，并从头开始重复此过程(CAPWAP状态：发现)。

<#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：由于证书过期，Wave 1接入点可能无法下载新映像。请参阅[现场通知72524](#)获取详细信息，并仔细阅读[2022年12月4日之后由于映像签名证书过期，IOS AP映像下载失败\(CSCwd80290\)支持文档](#)以了解其影响和解决方案。

一旦AP重新加载并再次经历CAPWAP发现和加入状态，在图像数据状态期间，它将检测到现在已具有足够的映像。

<#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状态：配置

在AP验证其与WLC的版本相同后，它会将其当前配置通知给WLC。一般来说，这意味着AP会要求维护其配置（如果WLC中提供了这些配置）。

<#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状态：运行

此时，AP已成功加入控制器。在此状态下，WLC会触发一种机制以覆盖AP请求的配置。您可以看到，AP被推送了**Radio and Credentials configurations**，并且它还被分配到**default policy tag**，因为WLC之前不知道此AP。

<#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
```

配置

静态WLC选举

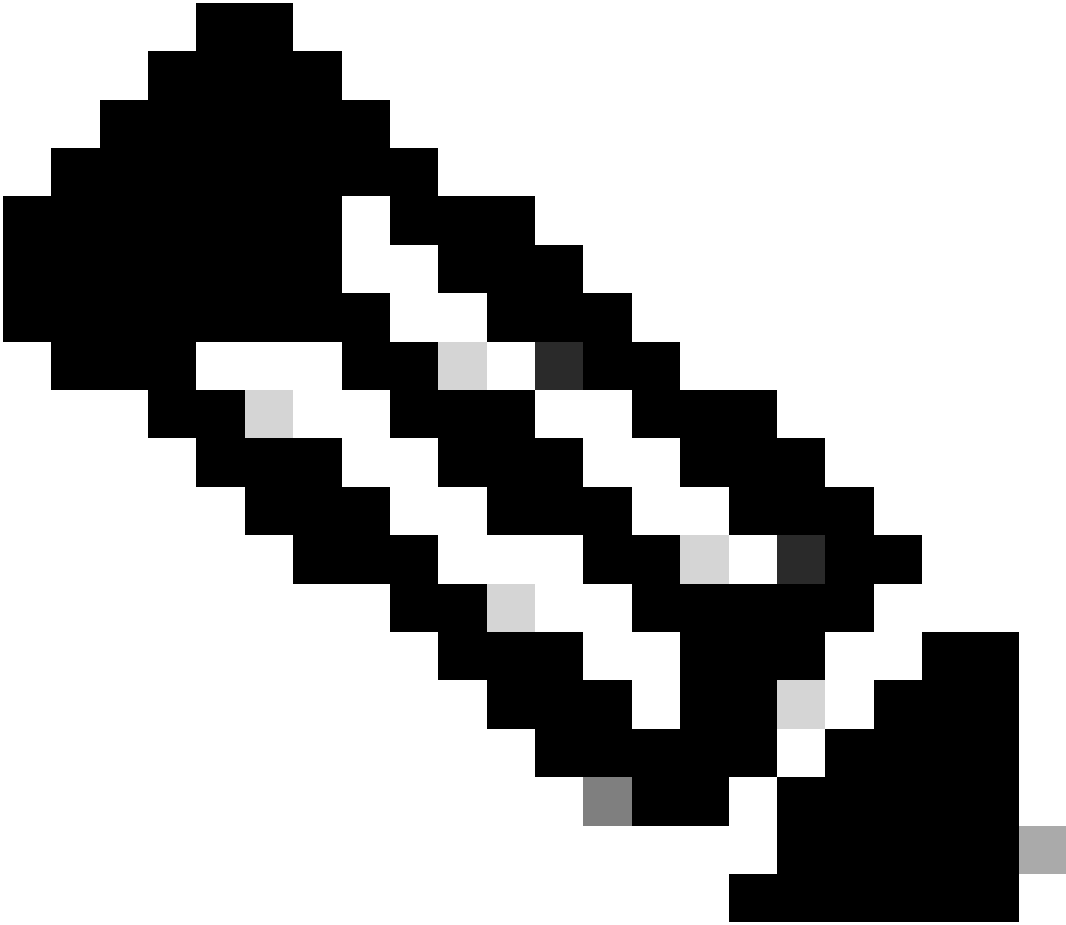
在GUI中，您可以转到**Configuration > Wireless > Access Points**，选择AP并转到**High Availability**选项卡。在此，您可以配置主WLC、辅助WLC和第三WLC，如本文档的无线LAN控制器选举部分所述。此配置按接入点执行。

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller GUI. The main navigation pane on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The central pane shows the 'All Access Points' list with columns for AP Name, AP Model, and Slots. The right pane is titled 'Edit AP' and has tabs for General, Interfaces, High Availability, Inventory, ICap, Advanced, and Support Bundle. The 'High Availability' tab is active, showing fields for Primary Controller (wlc-9800), Secondary Controller, Tertiary Controller, and AP failover priority (Low). The Management IP Address (IPv4/IPv6) is set to 172.16.5.11.

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

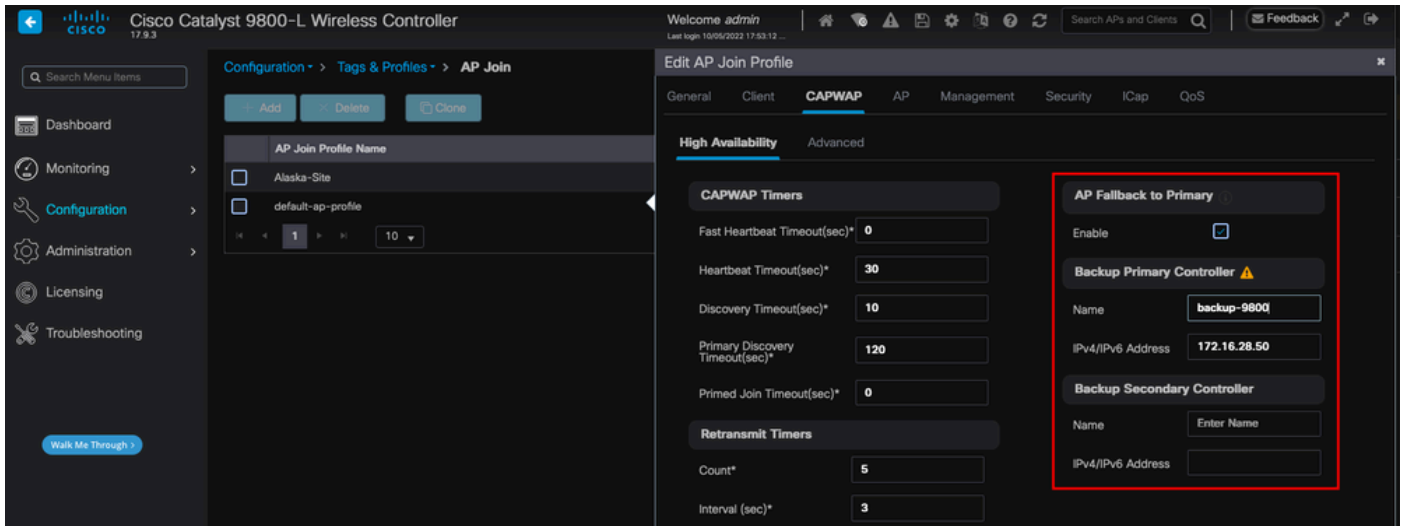
AP的主WLC、辅助WLC和第三WLC。



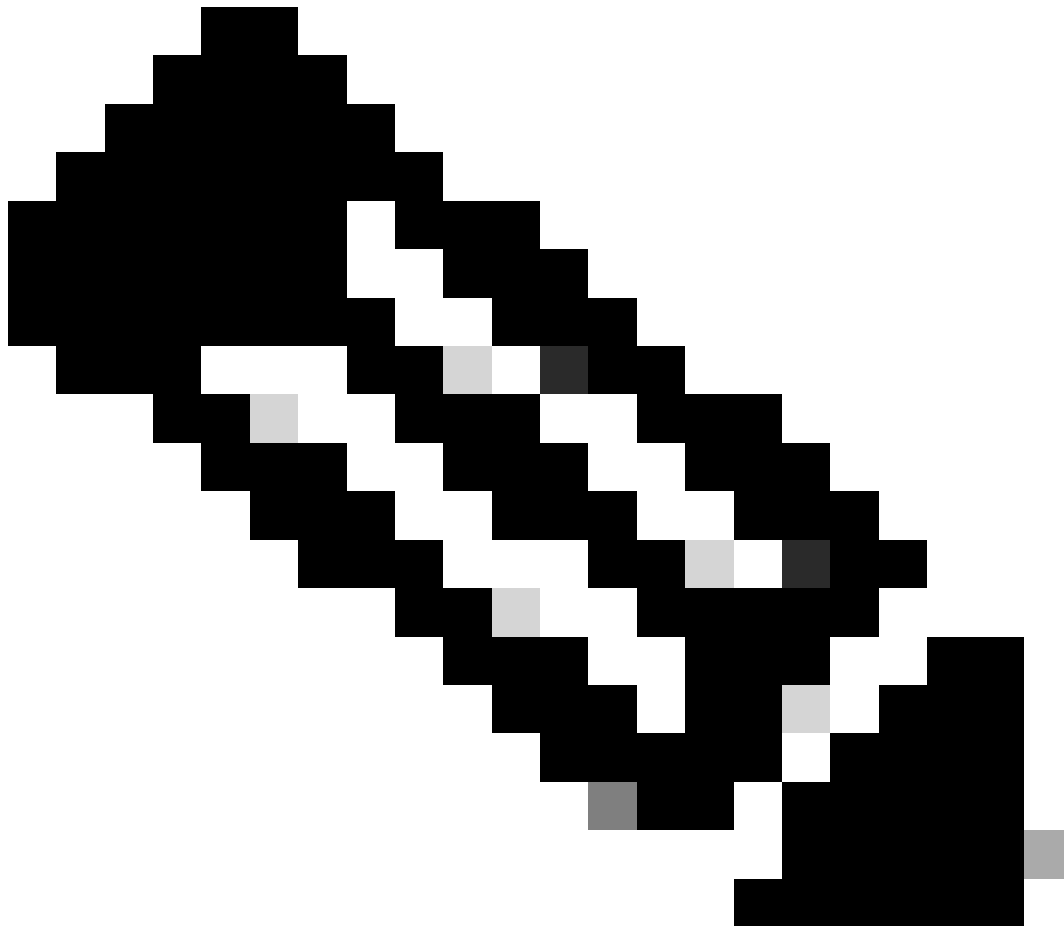
注意：从Cisco IOS XE 17.9.2开始，您可以使用启动配置文件为一组与正则表达式(regex)匹配的AP或单个AP配置主要、次要和第三控制器。有关详细信息，请参阅[配置指南](#)的[AP回退到在AP初始配置文件下配置的控制器](#)部分。

请注意，在AP High Availability选项卡中配置的主要、次要和第三控制器与Backup Primary and Secondary WLC不同，后者可在CAPWAP > High Availability选项卡下的AP Join Profile中进行配置。主控制器、辅助控制器和第三控制器分别被视为优先级为1、2和3的WLC，而备用主控制器和辅助控制器则被视为优先级为4和5的WLC。

如果启用了AP Fallback，则AP会在加入其他WLC时主动查找主控制器。发生CAPWAP Down事件并且没有可用的备用主控制器和辅助控制器时，AP只会查找优先级为4和5的WLC。



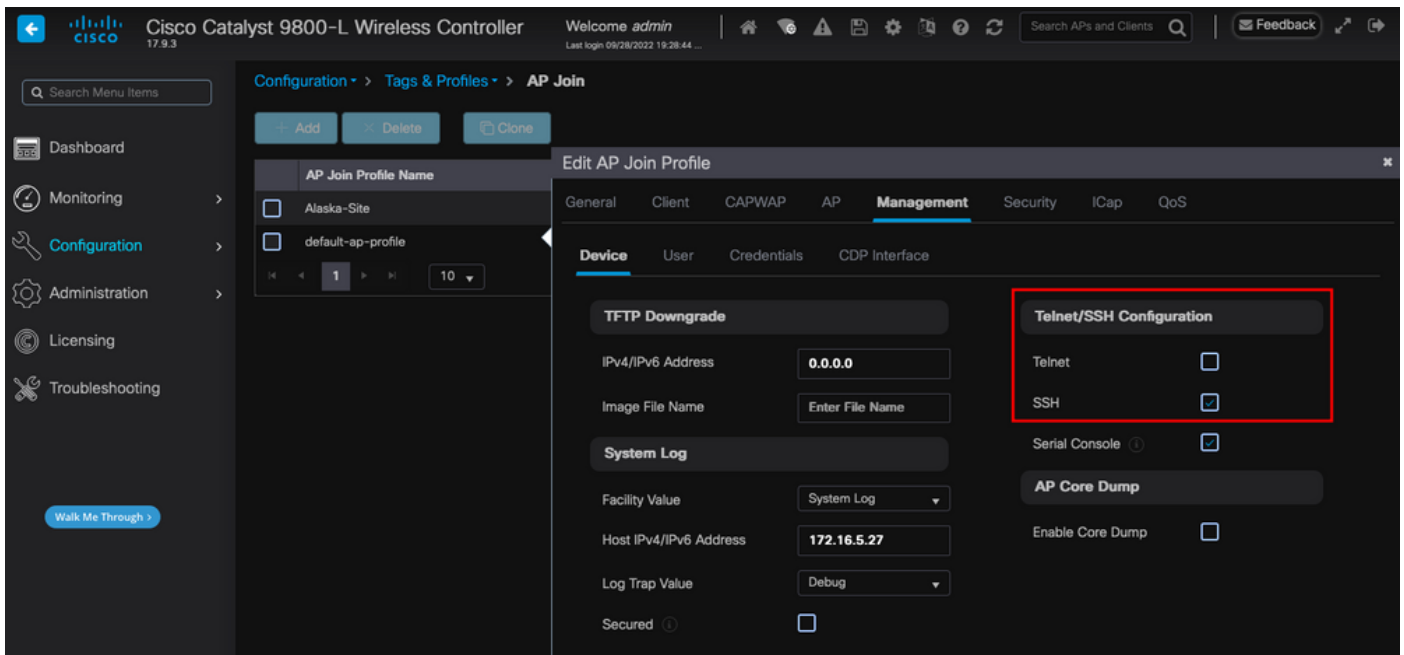
AP加入配置文件中的高可用性选项



注意：AP加入配置文件中备份主WLC和备份辅助WLC的配置不会填充接入点的High Availability选项卡中的Static Primary和Secondary条目。

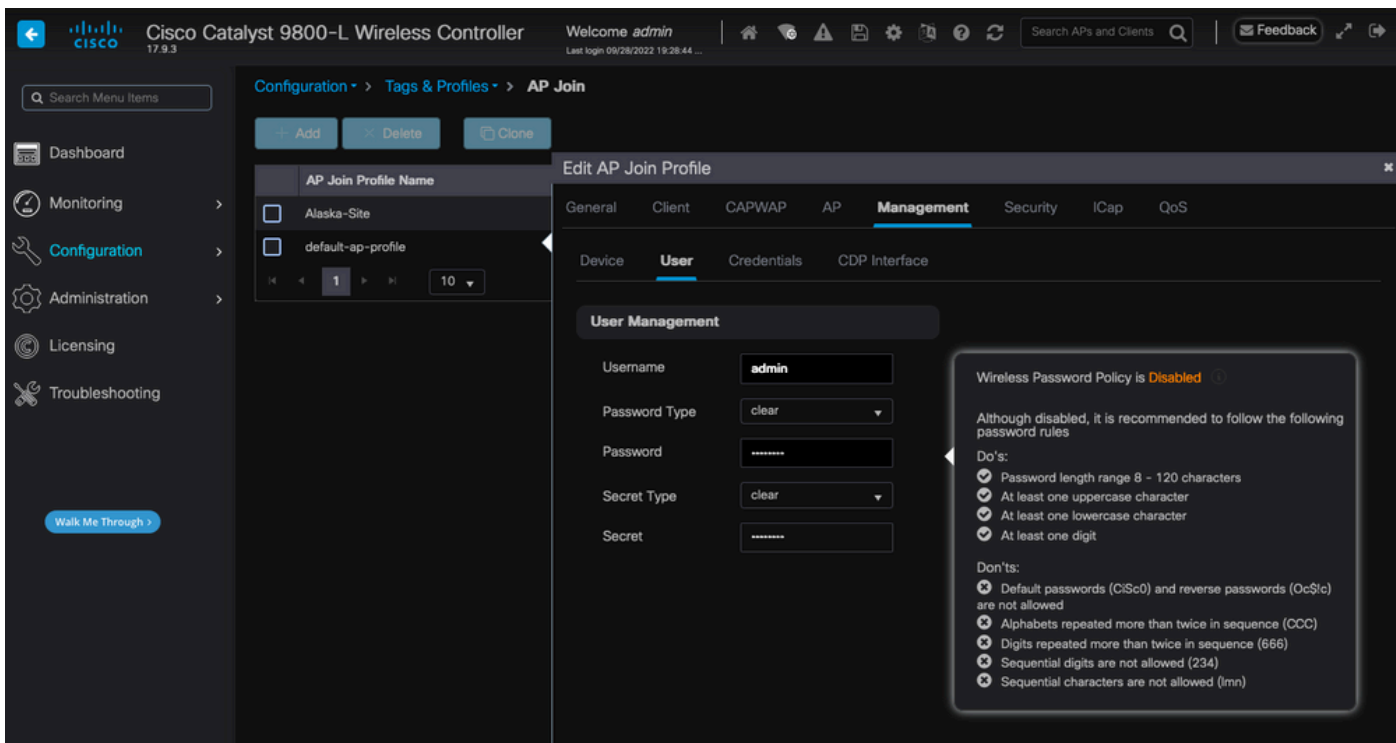
启用对无线接入点的Telnet/SSH访问

转至Configuration > Tags & Profiles > AP Join > Management > Device，然后选择SSH和/或Telnet。



在AP加入配置文件中启用Telnet/SSH访问

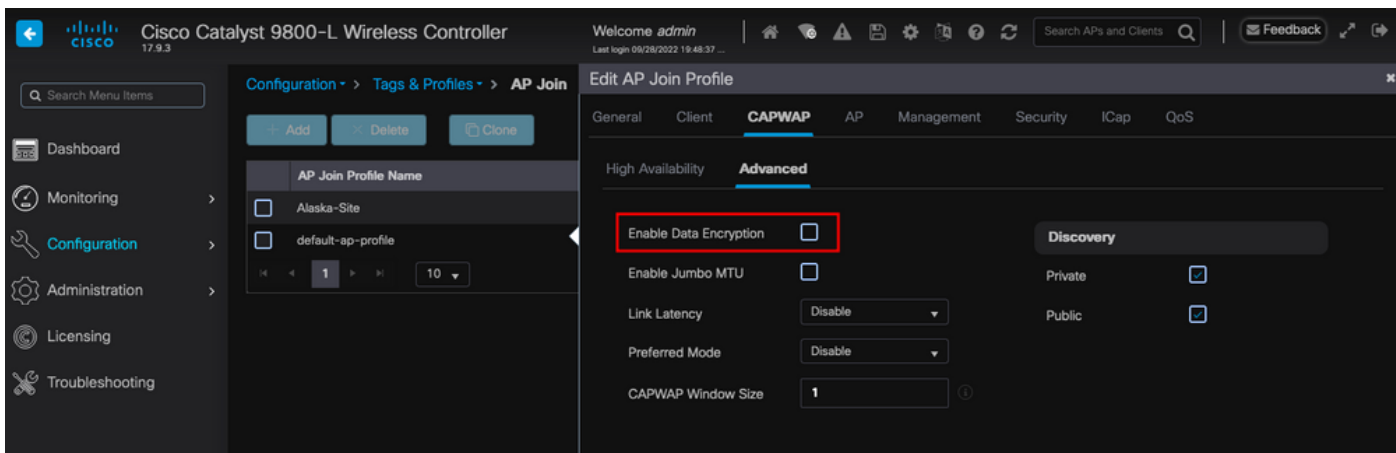
要配置SSH/Telnet凭证，请导航到同一窗口中的User选项卡，然后设置Username、Password和Secret以访问AP。



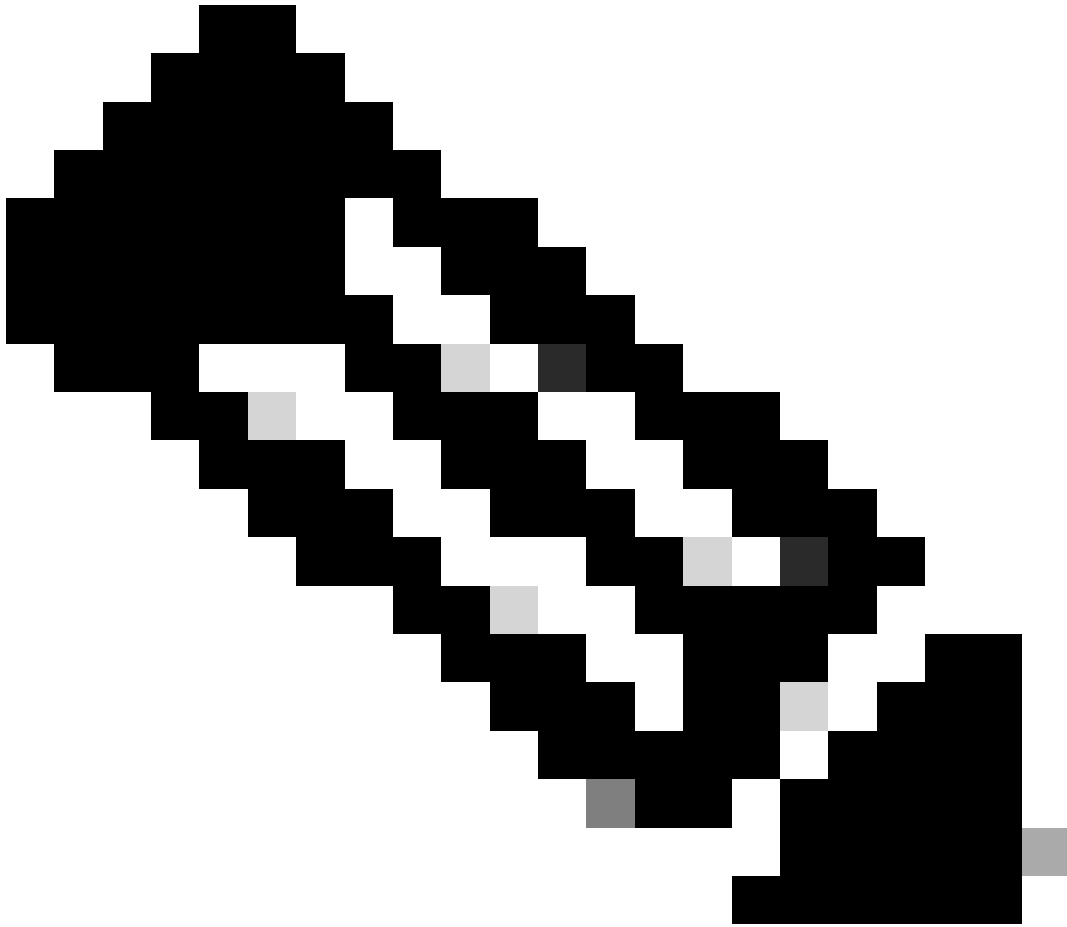
AP的SSH和Telnet凭证

数据链路加密

如果需要排除任何需要对AP数据流进行数据包捕获的客户端问题，请确保在Configuration > Tags & Profiles > AP Join > CAPWAP > Advanced下未启用Data Link Encryption。否则，您的流量将加密。



数据链路加密



注意：数据加密仅加密CAPWAP数据流量。CAPWAP控制流量已通过DTLS加密。

验证

除了在AP的控制台中跟踪CAPWAP状态机外，您还可以在WLC中执行[嵌入式数据包捕获](#)，以分析AP加入进程：

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	0.195998000	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	0.060986000	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	12:58:51.204975	0.000000000	172.16.5.11	DTLSv1.2	125	5246	Change Cipher Spec, Encrypted Handshake Message
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	0.069989000	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	12:58:57.469961	0.001999000	172.16.5.65	DTLSv1.2	148	5246	Application Data
1377	12:58:57.469961	0.000000000	172.16.5.11	DTLSv1.2	103	5267	Application Data
1378	12:58:57.470958	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	0.078995000	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	12:58:57.688959	0.000992000	172.16.5.65	DTLSv1.2	119	5246	Application Data
1430	12:58:57.688959	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	172.16.5.65	DTLSv1.2	111	5246	Application Data

在WLC的嵌入式数据包捕获中看到的AP加入过程

请注意，Chance Cipher Spec数据包（数据包1182）之后的所有流量如何仅显示为DTLSv1.2上的应用数据。这是DTLS会话建立后的所有加密数据。

故障排除

已知问题

请参阅可能阻止您的AP加入WLC的已知问题。

- [由于第二波和Catalyst 11ax无线接入点\(CSCvx32806\)中的图像损坏导致引导环路上的AP](#)
- [售后通知72424：自2022年9月起生产的C9105/C9120/C9130接入点可能需要软件升级才能加入无线LAN控制器。](#)
- [现场通知72524：在软件升级/降级期间，由于证书过期，思科IOS AP可能会在2022年12月4日后保持下载状态-建议进行软件升级](#)
- [思科漏洞ID CSCwb13784：由于无线接入点加入请求中的路径MTU无效，无线接入点无法加入9800](#)
- [思科漏洞ID CSCvu22886：C9130：升级到17.7时消息“unlzma：write：No space left on device”（unlzma：写入：设备上没有剩余空间）增加/tmp最大大小](#)

在升级之前，请始终参阅每个版本的[发行版本注释](#)的升级路径部分。



注意：从Cisco IOS XE Cupertino 17.7.1开始，如果智能许可未连接且未启用，则Cisco Catalyst 9800-CL无线控制器最多只能接受50个AP。

WLC GUI检查

在WLC上，转到**Monitoring > Wireless > AP Statistics > Join Statistics**，您可以看到任何AP报告的上次重新引导原因以及WLC注册的上次断开原因。

AP Name	AP Model	Status	IP Address	Base Radio MAC	Ethernet MAC	Last Reboot Reason (Reported by AP)	Last Disconnect Reason
9120AP	C9120AXI-A	●	172.16.5.23	3c41.0a31.7780	6c41.0a16.e79c	No reboot reason	DTLS close alert from peer
pschell9120	C9120AXI-B	●	172.16.5.61	3c41.0a31.7780	6c41.0a16.e79c	No reboot reason	DTLS close alert from peer
AP19F9.2096.94F0	C9106AXI-A	●	172.16.5.32	488b.0aa7.7940	1095.2090.54d0	No reboot reason	DTLS close alert from peer
AP72F9.9676.AFAC	C9120AXI-B	●	172.16.5.79	7090.9685.7980	7090.9676.afac	Controller reload command	Mesh AP role change
AP710e.ca14.8088	AR-CA93702I-N-K9	●	172.16.5.31	710e.ca14.8088	710e.ca14.8088	Image upgrade successfully	NA
C9120AXI-EMORENDA	C9120AXI-A	●	172.16.5.65	a49b.cdaa.1980	a49b.c050.4158	Image upgrade successfully	DTLS close alert from peer
BRCTAC0428	C9120AXI-B	●	172.16.46.35	c884.a172.2600	c884.a165.8530	No reboot reason	DTLS close alert from peer
AP9130AXI-tulajm	C9130AXI-A	●	172.16.5.67	011a.2a89.d840	7090.9606.4a44	Controller reload command	Mode change to sniffer
3802-emorenda	AR-AP9802I-B-K9	●	172.16.5.25	802b.caa7.a5c0	286f.7a15.53ae	Controller reload command	Mode change to sniffer

WLC上的AP Join Statistics页面

您可以点击任何AP并检查AP加入统计详细信息。在这里，您可以看到更详细的信息，例如AP上次加入并尝试发现WLC的时间和日期。

Join Statistics

General Statistics

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

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
--	----

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

常规AP加入统计信息

有关更多详细信息，请转到同一窗口的Statistics选项卡。在此，您可以比较发送的加入响应数与接收的加入请求数，以及发送的配置响应与接收的配置请求数。

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

详细的AP加入统计信息

命令

以下命令可用于排除AP加入问题：

从WLC

- show ap summary
- debug capwap error
- debug capwap packet

来自Wave 2和Catalyst 11ax AP

- debug capwap client events
- debug capwap client error
- debug dtls client error
- debug dtls client event
- debug capwap client keepalive
- test capwap restart
- capwap ap erase all

从Wave 1 AP

- debug capwap console cli
- debug capwap client no-reload
- show dtls stats
- clear cawap ap all-config



注意：当您通过Telnet/SSH连接到AP以进行故障排除时，请始终发出**terminal monitor**命令，同时在AP上启用调试后重现该问题。否则，您将无法看到来自调试的任何输出。

放射性痕迹

排除AP加入问题的一个好的起点是获取存在加入问题的AP的无线电和以太网MAC地址的放射性踪迹。有关生成这些日志的详细信息，请参阅[Catalyst 9800 WLC上的调试和日志收集](#)文档。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。