Entender o processo de união de AP com o Catalyst 9800 WLC

Contents

Introdução

Este documento descreve em detalhes o processo de união do AP com o Cisco Catalyst 9800 WLC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entendimento básico do Control and Provisioning Wireless Access Points (CAPWAP)
- Compreensão básica do uso de um Wireless Lan Controller (WLC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 9800-L WLC, Cisco IOS® XE Cupertino 17.9.3
- Ponto de acesso Catalyst 9120AX

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Estabelecimento de sessão CAPWAP

O Ponto de Acesso Sem Fio de Controle e Provisionamento (CAPWAP) é o protocolo que fornece o mecanismo de transporte usado por Pontos de Acesso (APs) e Controladoras Wireless LAN (WLCs) para trocar informações de controle e plano de dados em um túnel de comunicação seguro (para Controle CAPWAP).

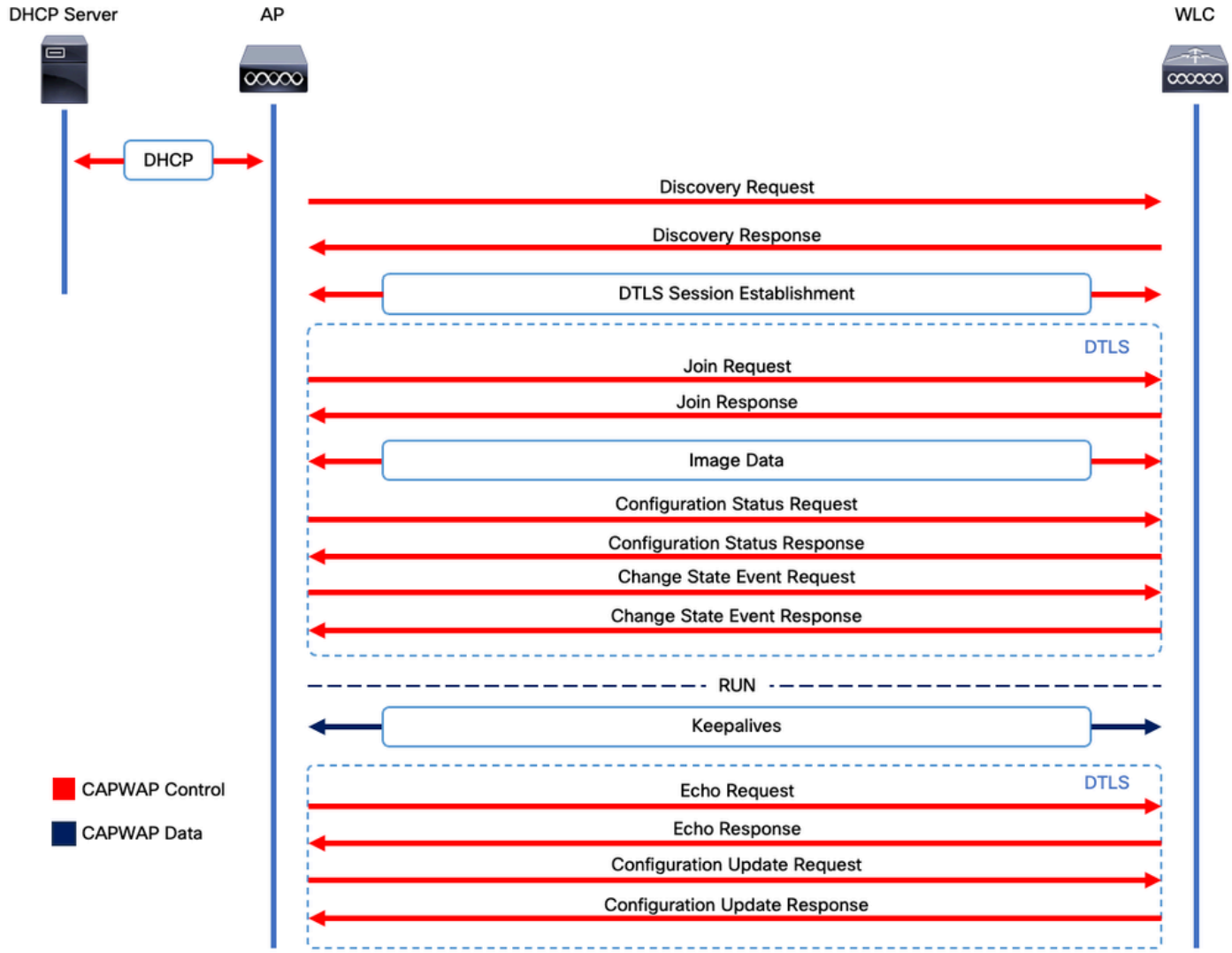
Para elaborar o processo de junção AP, é importante que você compreenda o processo de estabelecimento da sessão do ponto de acesso sem fio de controle e provisionamento (CAPWAP).

Lembre-se de que o AP precisa ter um endereço IP antes de poder iniciar o processo CAPWAP. Se o AP não tiver um endereço IP, ele não iniciará o processo de estabelecimento de sessão CAPWAP.

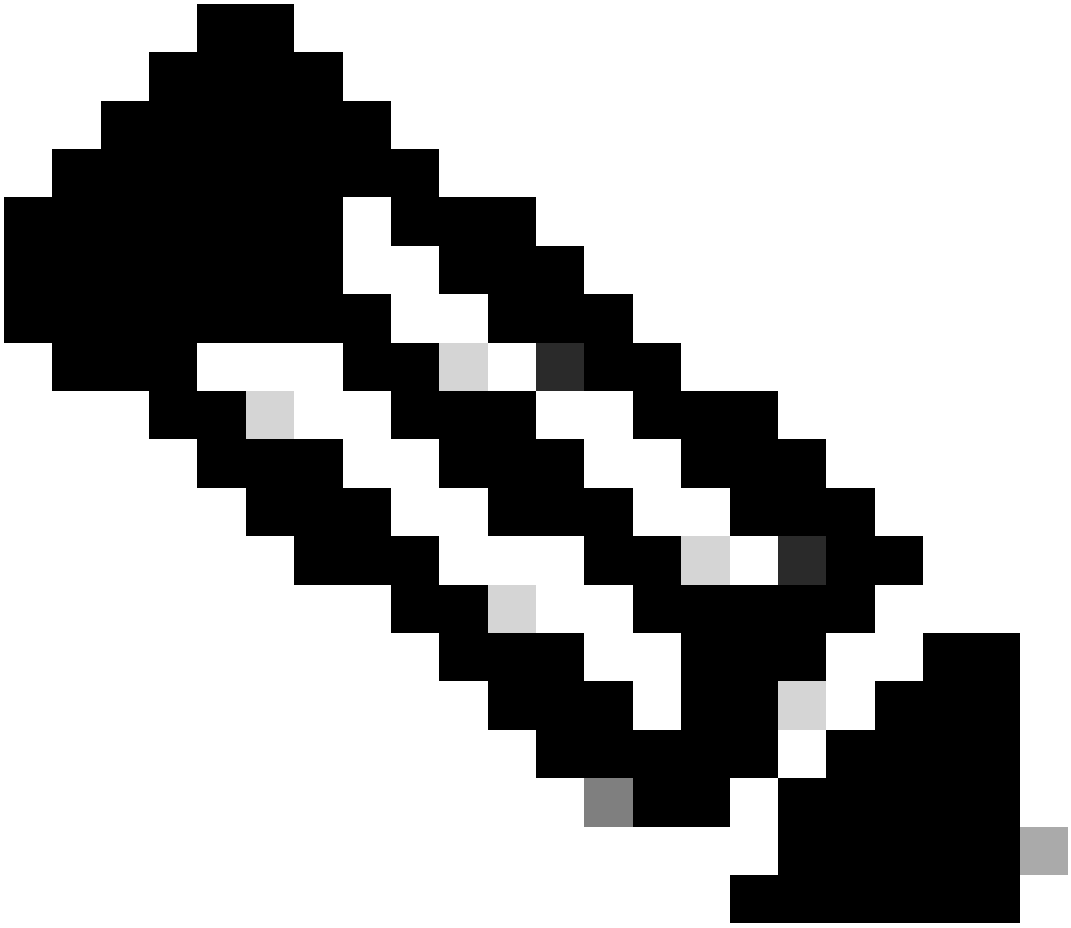
1. O Ponto de Acesso envia uma Solicitação de Descoberta. Consulte a seção Métodos de Descoberta de WLC para obter mais informações sobre isso
2. A WLC envia uma resposta de descoberta
3. Estabelecimento de sessão DTLS. Depois disso, todas as mensagens são criptografadas e exibidas como pacotes de dados de aplicativo DTLS em qualquer ferramenta de análise de pacotes.
4. O Ponto de Acesso envia uma Solicitação de Associação
5. A WLC envia uma resposta de união
6. O AP executa uma verificação de imagem. Se tiver a mesma versão de imagem que a WLC, ela continuará com a próxima etapa. Caso contrário, ele faz o download da imagem da WLC e a reinicializa para carregar a nova imagem. Nesse caso, ele repete o processo a partir da

etapa 1.

7. O ponto de acesso envia uma solicitação de status de configuração.
8. A WLC envia uma resposta de status de configuração
9. O ponto de acesso vai para o estado RUN
10. Durante o estado RUN, a Manutenção de Túnel CAPWAP é executada de duas maneiras:
    1. Os keepalives são trocados para manter o túnel CAPWAP Data
    2. O AP envia uma Solicitação de Eco para a WLC, que precisa ser respondida com sua respectiva Resposta de Eco. Isso serve para manter o túnel CAPWAP Control.



Processo de estabelecimento de sessão CAPWAP



Observação: de acordo com o RFC 5415, o CAPWAP usa as portas UDP 5246 (para controle CAPWAP) e 5247 (para dados CAPWAP).

Estabelecimento de Sessão DTLS

Quando o Ponto de acesso receber uma Resposta de descoberta válida da WLC, um túnel DTLS será estabelecido entre eles para transmitir todos os pacotes subsequentes por um túnel protegido. Este é o processo para estabelecer a sessão DTLS:

1. O AP envia uma mensagem Hello do cliente
2. A WLC envia uma mensagem HelloVerifyRequest com um cookie usado para validação.
3. O AP envia uma mensagem ClientHello com um cookie usado para validação.
4. A WLC envia esses pacotes na ordem:
    1. ServidorHello
    2. Certificado
    3. Troca de chave de servidor
    4. Certificate Request

    5. ServidorHelloDone
5. O AP envia estes pacotes na ordem:
    1. Certificado
    2. ClientKeyExchange
    3. Verificação de certificado
    4. AlterarEspecificaçãoDeCodificação
6. A WLC responde à ChangeCipherSpec do AP com sua própria ChangedCipherSpec:
    1. AlterarEspecificaçãoDeCodificação

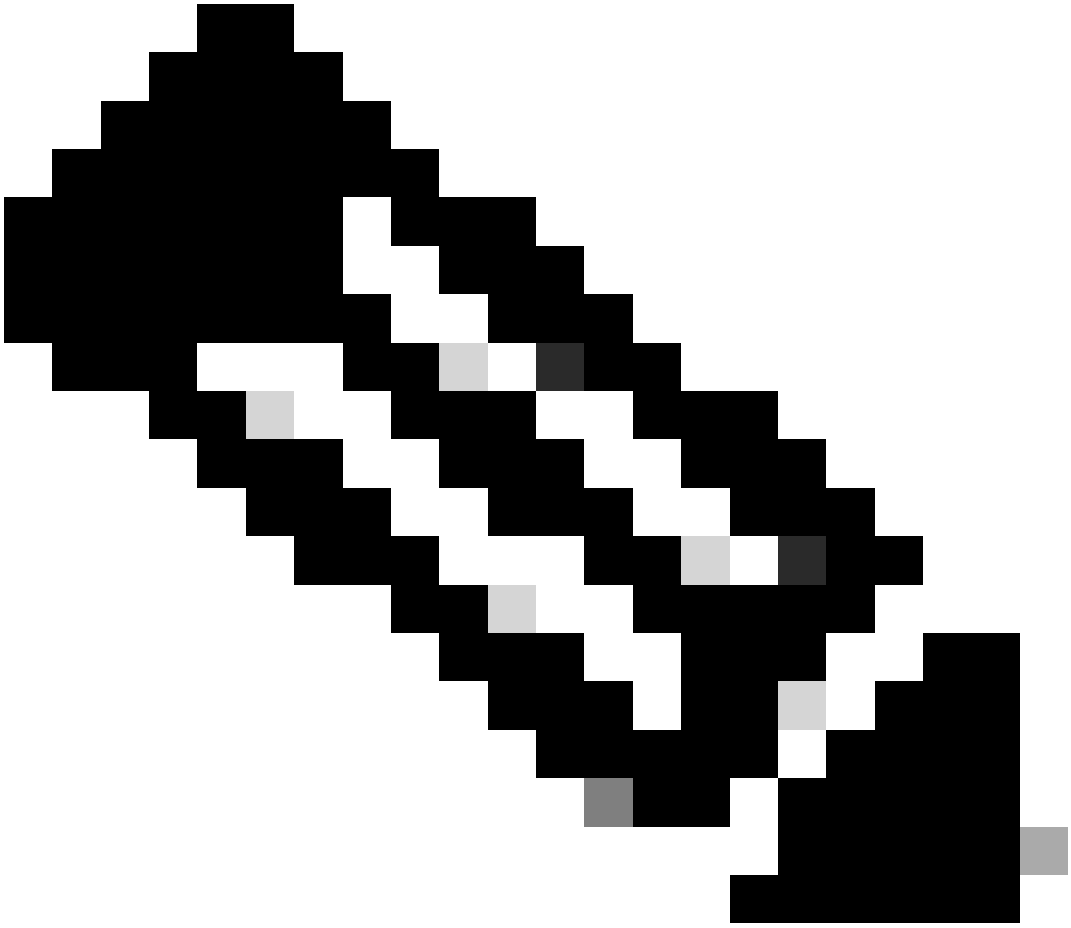
Após a última mensagem ChangedCipherSpec enviada pela WLC, o túnel seguro é estabelecido e todo o tráfego enviado em ambas as direções agora é criptografado.

Métodos de descoberta de controladores de LAN sem fio

Há várias opções para informar os Pontos de Acesso sobre a existência de uma WLC na rede:

- Opção de DHCP 43: essa opção fornece aos APs o endereço IPv4 da WLC a ser unida. Esse processo é conveniente para grandes implantações nas quais os APs e a WLC estão em locais diferentes.
- Opção de DHCP 52: essa opção fornece aos APs o endereço IPv6 da WLC para se unir. Seu uso é conveniente no mesmo cenário que a Opção de DHCP 43.
- Descoberta de DNS: os APs consultam o nome de domínio CISCO-CAPWAP-CONTROLLER.localdomain. Você deve configurar o servidor DNS para resolver o endereço IPv4 ou IPv6 da WLC para participar. Essa opção é conveniente para implantações nas quais as WLCs são armazenadas no mesmo site que os APs.
- Transmissão de Camada 3: os APs enviam automaticamente uma mensagem de broadcast para 255.255.255.255. Espera-se que qualquer WLC dentro da mesma sub-rede do AP responda a essa solicitação de descoberta.
- Configuração estática: você pode usar o comando capwap ap primary-base <wlc-hostname> <wlc-IP-address> para configurar uma entrada estática para uma WLC no AP.

    - **Descoberta de mobilidade**: se o AP tiver ingressado anteriormente em uma WLC que fazia parte de um grupo de mobilidade, o AP também salvará um registro das WLCs presentes nesse grupo de mobilidade.



Observação: os métodos de descoberta de WLC listados não têm nenhuma ordem de precedência.

Eleição do controlador de LAN sem fio

Uma vez que o AP tenha recebido uma **resposta de descoberta** de qualquer WLC usando qualquer um dos métodos de descoberta de WLC, ele seleciona um controlador para se unir com estes critérios:

- Controlador primário (configurado com o comando **capwap ap primary-base <wlc-hostname> <wlc-IP-address>**)
- Controlador secundário (configurado com o comando **capwap ap secondary-base <wlc-hostname> <wlc-IP-address>**)

- Controlador terciário (configurado com o comando **capwap ap tertiary-base <wlc-hostname> <wlc-IP-address>)**

- Se nenhuma WLC primária, secundária ou terciária tiver sido configurada anteriormente, o AP tentará se unir à primeira WLC que respondeu à solicitação de descoberta com sua própria **resposta de descoberta** que tem a capacidade máxima de **APs** disponíveis (ou seja, a **WLC** que pode suportar a maioria dos APs em um determinado momento).

Máquina de Estado CAPWAP

No console do AP, você pode controlar a máquina de estado CAPWAP, que passa pelas etapas descritas na seção Estabelecimento de sessão CAPWAP.

Estado CAPWAP: descoberta

Aqui você pode ver as **solicitações de descoberta** e as respostas. Observe como o AP recebe um IP de WLC via **DHCP** (Opção 43) e também envia uma **Solicitação de Descoberta** para WLCs conhecidas anteriormente:

```
<#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

Além de receber uma **Resposta de Descoberta** de uma WLC configurada estaticamente (172.16.0.20) e da WLC indicada pela Opção de DHCP 43 (172.16.5.11), este AP também recebeu uma **Resposta de Descoberta** de outra WLC (172.16.5.169) dentro da mesma sub-rede porque recebeu a mensagem de Descoberta de broadcast.

Estado CAPWAP: configuração de DTLS.

Aqui, a sessão DTLS entre o AP e a WLC é trocada.

<#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
```

Estado CAPWAP: Ingressar

Depois de estabelecer a sessão DTLS, uma **solicitação de união** à WLC é enviada pela sessão segura. Observe como essa solicitação é imediatamente respondida com uma **Resposta de Junção** da WLC

<#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

Estado CAPWAP: dados da imagem

O AP compara sua imagem com a imagem da WLC. Nesse caso, a partição ativa do AP e sua partição de backup têm imagens diferentes da WLC, então ele chama o script **upgrade.sh**, que instrui o AP a solicitar a imagem adequada para a WLC e baixá-la em sua partição não ativa atual.

<#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

Uma vez concluída a transferência da imagem, o AP inicia um processo de verificação de assinatura da imagem para validá-la. Depois de fazer isso, o script **upgrade.sh** instala a imagem na partição não ativa atual e troca a partição da qual ela é inicializada. Por fim, o AP é recarregado e repete o processo desde o início (**Estado CAPWAP: 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

Aviso: os pontos de acesso Wave 1 podem falhar ao baixar uma nova imagem devido a um certificado expirado. Consulte o Field Notice 72524 para obter mais informações e leia atentamente o Documento de Suporte do IOS AP Image Download Fails Due to Expired Image Signing Certificate Past December 4th, 2022 (CSCwd80290) para entender seu impacto e sua solução.

Depois que o AP é recarregado e passa novamente pelos estados **CAPWAP Discover** e **Join**, durante o estado **Image Data** ele detecta que agora tem a imagem adequada.

<#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

Estado CAPWAP: Configurar

Depois que o AP validar que tem a mesma versão que a WLC, ele notificará suas configurações atuais à WLC. Em geral, isso significa que o AP pede para manter suas configurações (se estiverem disponíveis na WLC).

<#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

Estado CAPWAP: Executar

Neste ponto, o AP se uniu com êxito à controladora. Durante esse estado, a WLC aciona um mecanismo para substituir a configuração solicitada pelo AP. Você pode ver que o AP recebe **configurações de rádio e credenciais** e também é atribuído à **tag de política padrão**, já que a WLC não tinha conhecimento prévio desse 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]

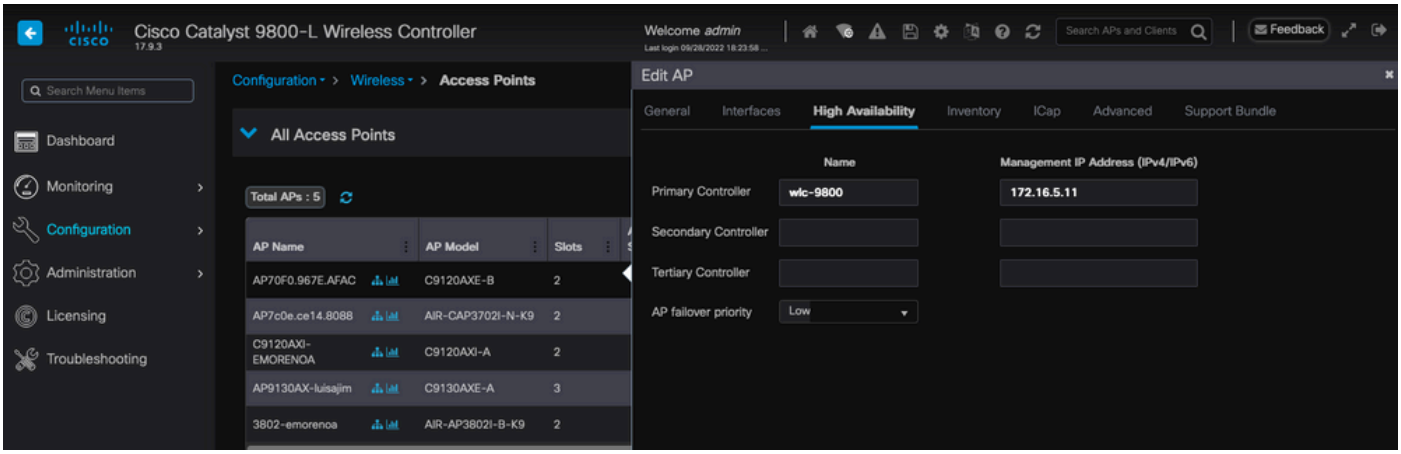
AP tag change to default-policy-tag

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

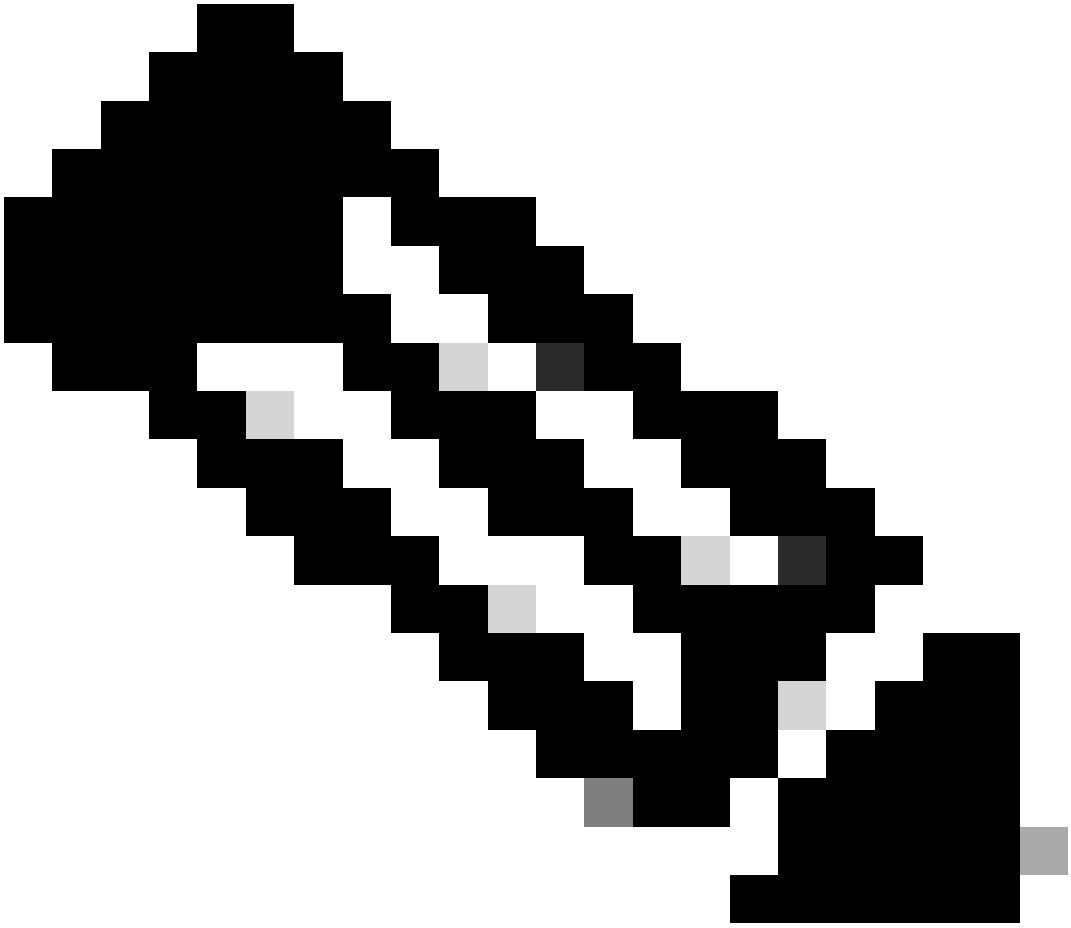
Configurar

Eleição estática de WLC

Na GUI, você pode ir para **Configuration > Wireless > Access Points**, selecionar um AP e navegar para a guia **High Availability**. Aqui, você pode configurar as WLCs **Primárias, Secundárias e Terciárias**, conforme descrito na seção Eleição da controladora Wireless LAN deste documento. Essa configuração é feita por Ponto de acesso.



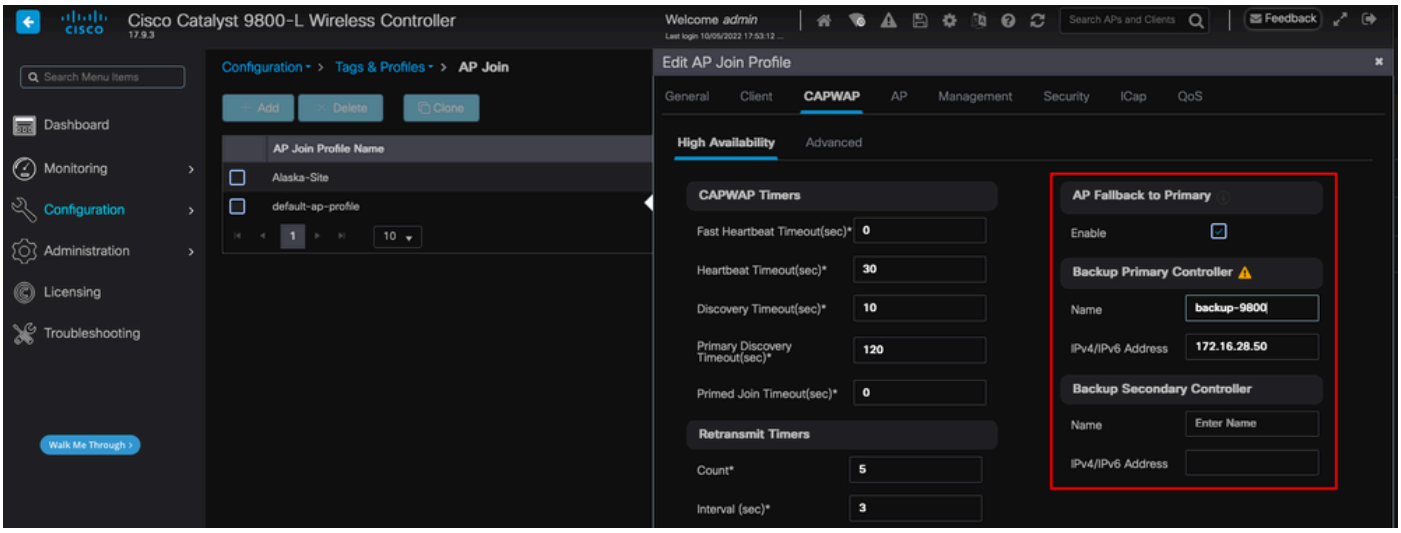
WLCs primárias, secundárias e terciárias para um AP.



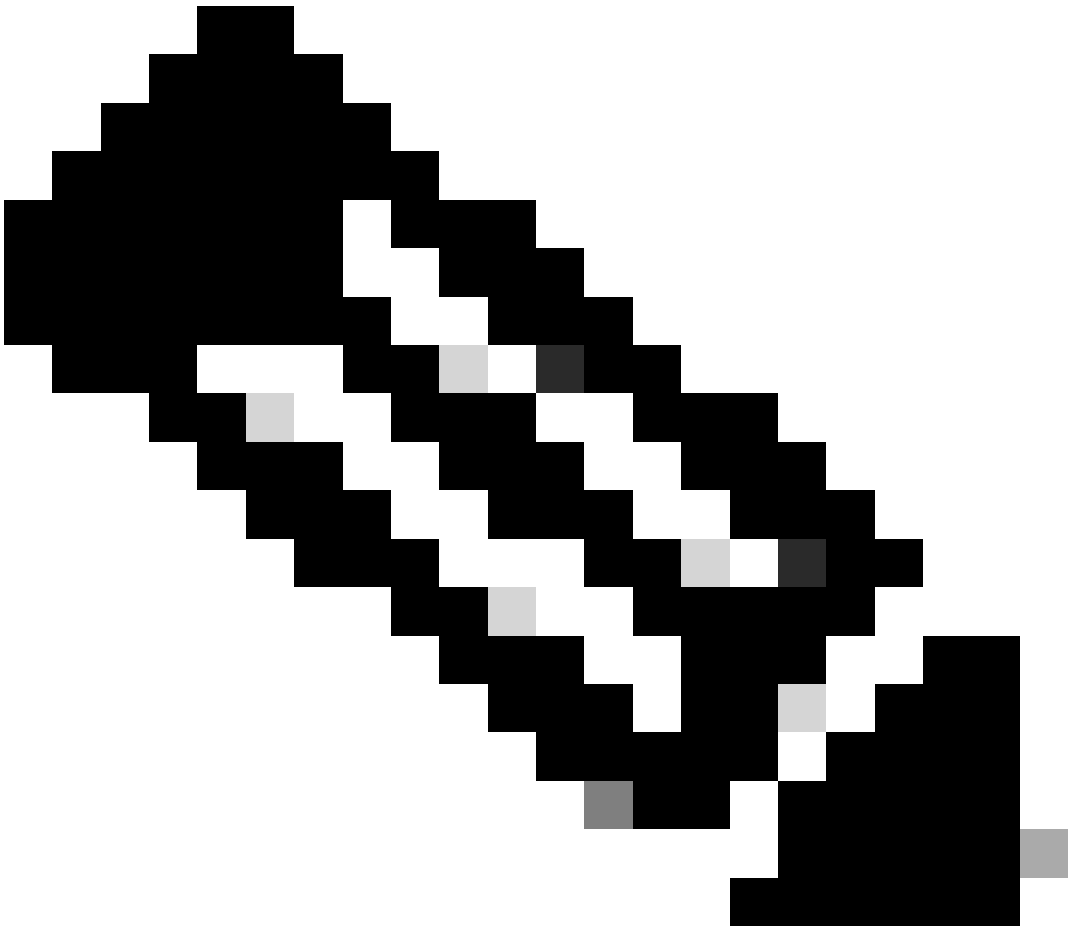
Observação: a partir do Cisco IOS XE 17.9.2, você pode usar Priming Profiles para configurar controladores primários, secundários e terciários para um grupo de APs que correspondam a expressão regular (regex) ou para um AP individual. Consulte a seção Fallback de AP para controladoras configuradas em AP Priming Profile do Guia de configuração para obter mais informações.

Observe que os Controladores Primário, Secundário e Terciário configurados na guia Alta Disponibilidade de AP diferem dos WLCs **Primário e Secundário de Backup** que podem ser configurados por **Perfil de Junção de AP** na **guia CAPWAP > Alta Disponibilidade. Os Controladores Primário, Secundário e Terciário** são considerados WLCs com prioridades 1, 2 e 3, respectivamente, enquanto os **Primário e Secundário de Backup** são considerados WLCs com prioridades 4 e 5.

Se o **Fallback de AP** estiver habilitado, o AP procurará ativamente o **Controlador primário** quando estiver unido a uma **WLC** diferente. O **AP** só procura **WLCs** com prioridades 4 e 5 quando houver um evento **CAPWAP Down** e nenhum dos **Controladores Primários e Secundários de Backup** estiver disponível.



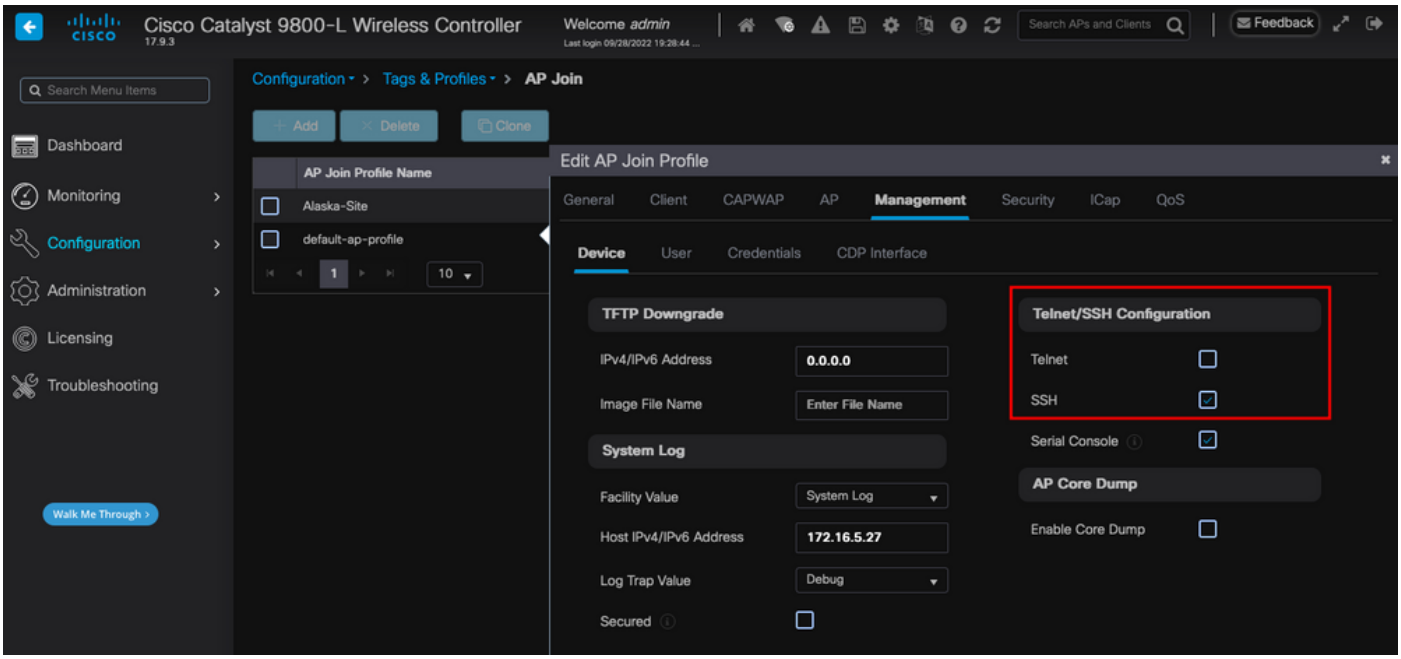
Opções de alta disponibilidade no perfil de ingresso no AP



Observação: a configuração das WLCs Backup Primary e Backup Secondary no AP Join Profile não preenche as entradas Static Primary e Secondary na guia High Availability do ponto de acesso.

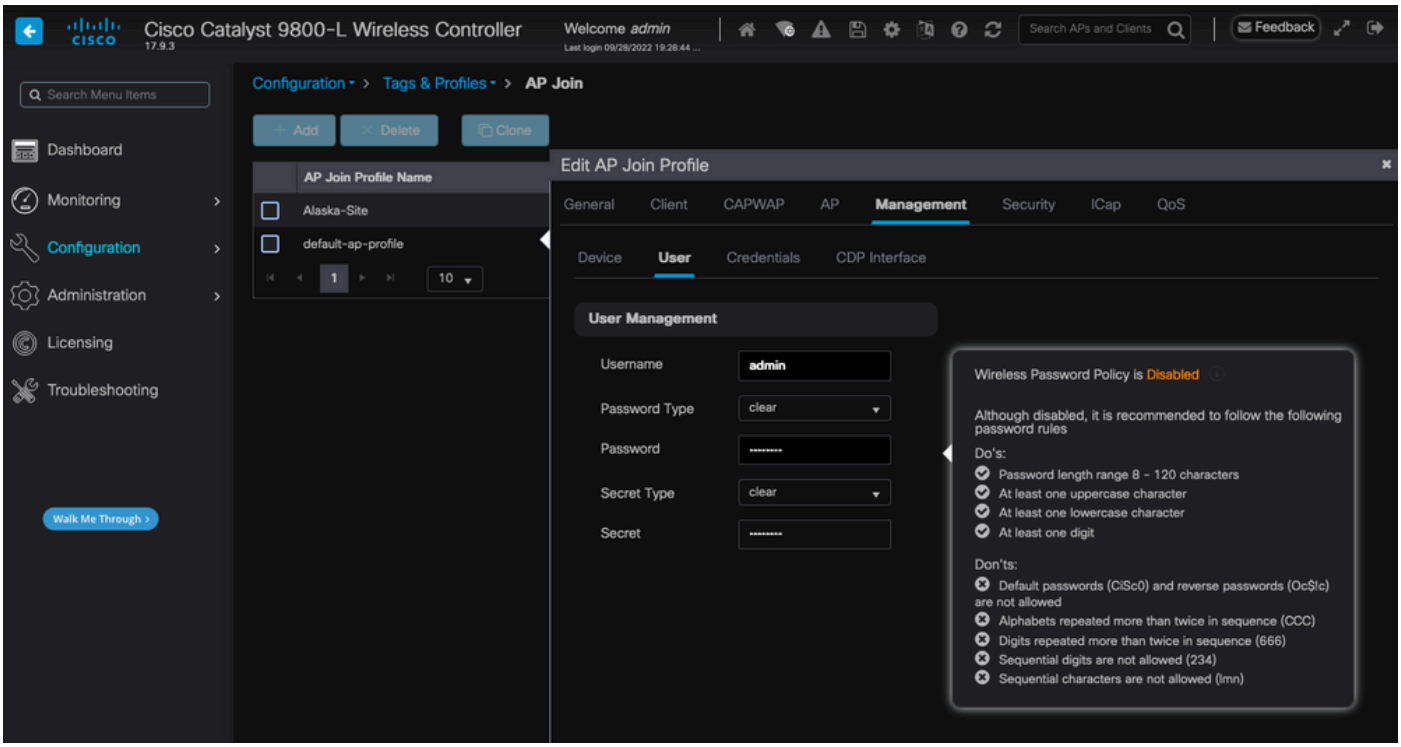
Habilitando o acesso Telnet/SSH para o AP

Vá para **Configuration > Tags & Profiles > AP Join > Management > Device** e selecione **SSH** e/ou **Telnet**.



Habilite o acesso Telnet/SSH no perfil de ingresso do AP

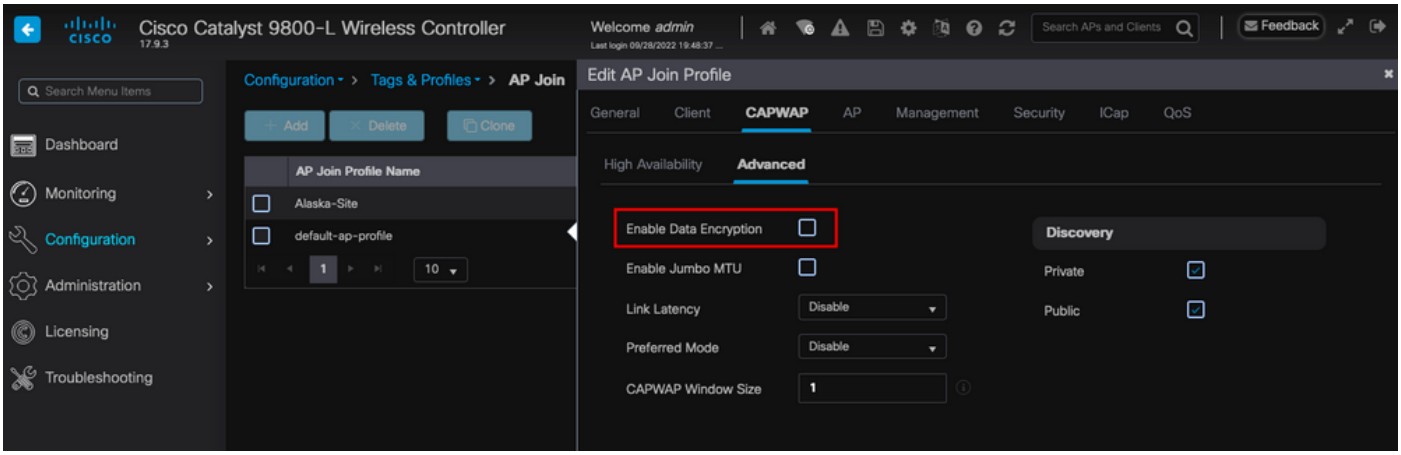
Para configurar as Credenciais SSH/Telnet, navegue até a guia **User** na mesma janela e defina o **Username, Password** e **Secret** para acessar o AP.



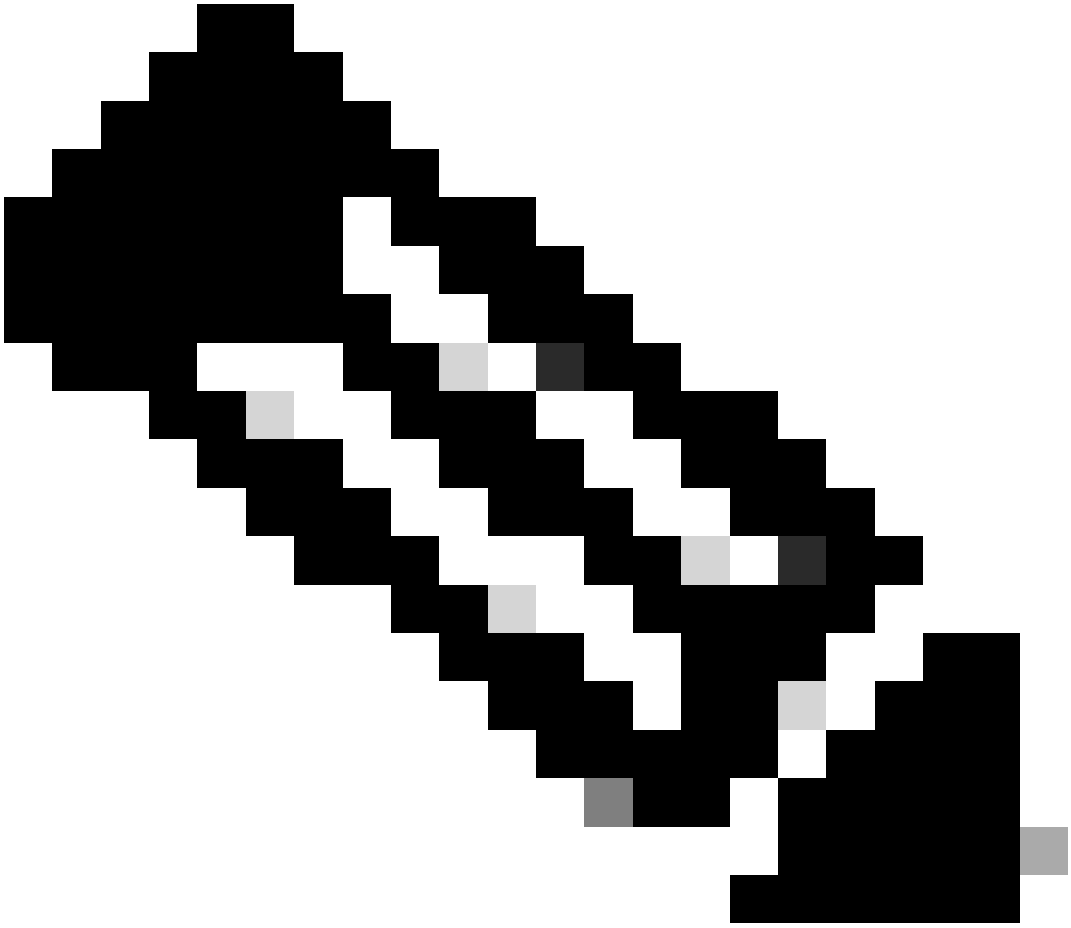
Credenciais SSH e Telnet para o AP

Criptografia de Enlace de Dados

Se você precisar solucionar qualquer problema de cliente que exija uma captura de pacote do tráfego do AP, certifique-se de que a **Criptografia de enlace de dados** não esteja habilitada em **Configuração > Marcas e perfis > AP Join > CAPWAP > Advanced**. Caso contrário, seu tráfego será criptografado.



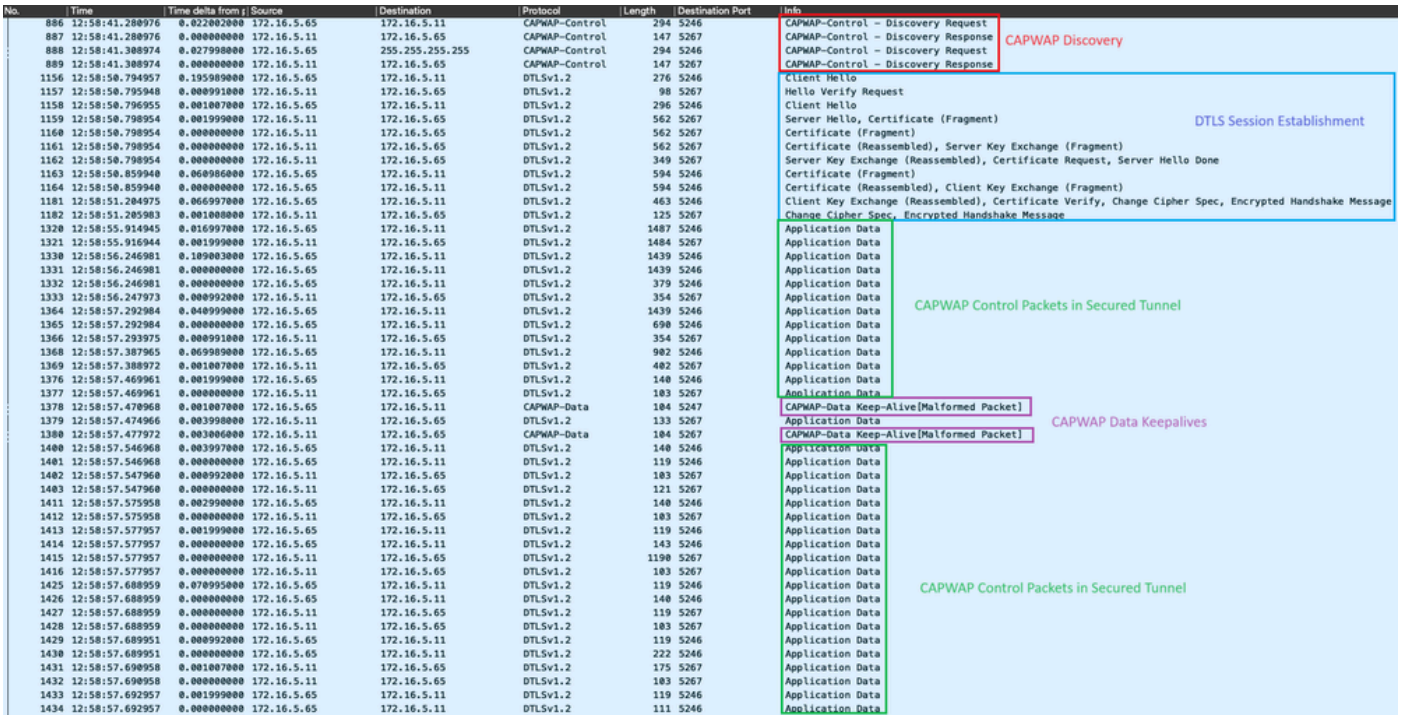
Criptografia de Enlace de Dados



Observação: a criptografia de dados criptografa apenas o tráfego de dados CAPWAP. O tráfego de controle CAPWAP já está criptografado via DTLS.

Verificar

Além de rastrear a máquina de estado CAPWAP no console do AP, você também pode usar uma Captura de pacote incorporada na WLC para analisar o processo de união do AP:



Processo de união de AP visto em uma captura de pacote incorporado na WLC

Observe como todo o tráfego após o pacote **Chance Cipher Spec** (Pacote No. 1182) é mostrado apenas como **Application Data** sobre **DTLSv1.2**. Esses são todos os dados criptografados após o **estabelecimento da sessão DTLS**.

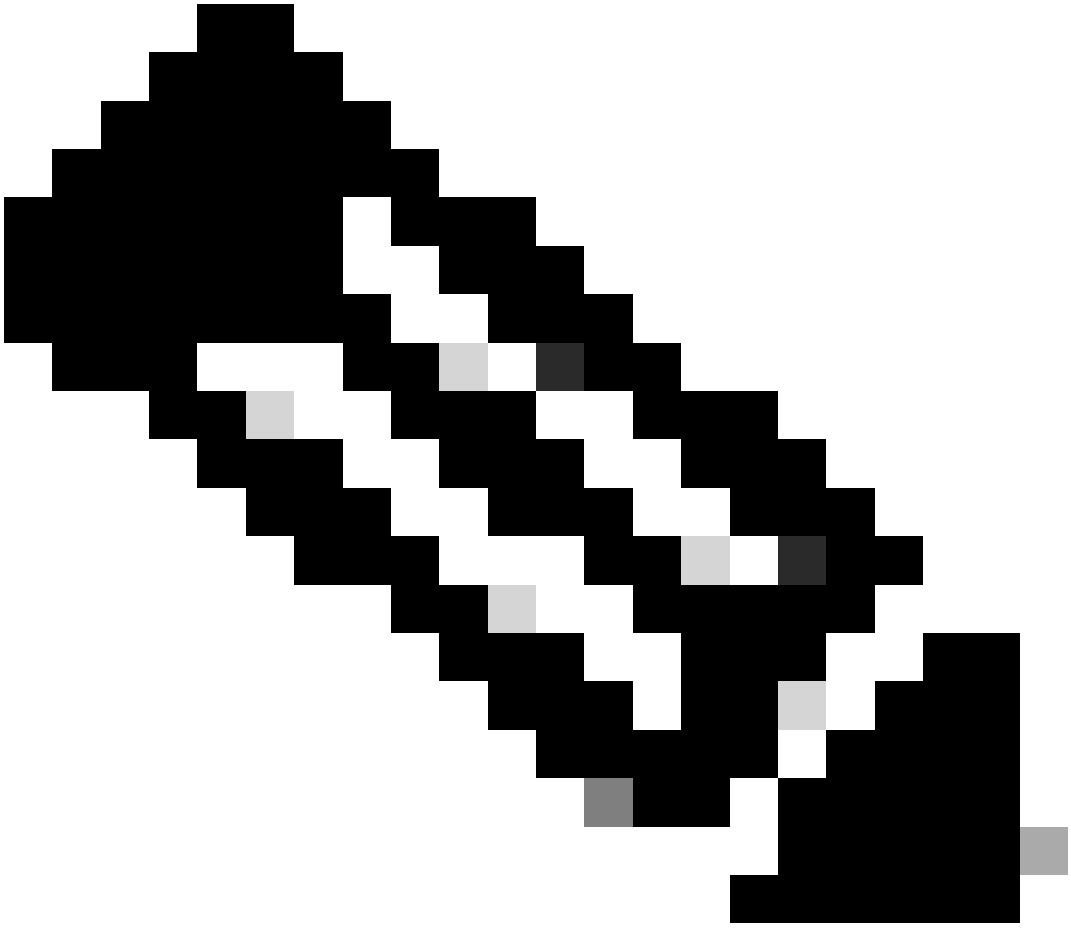
Troubleshooting

Problemas conhecidos

Consulte os problemas conhecidos que podem impedir que seus APs se juntem à WLC.

- APs em loop de inicialização devido à imagem corrompida no Wave 2 e nos Pontos de Acesso Catalyst 11ax (CSCvx32806)
- Aviso de campo 72424: os access points C9105/C9120/C9130 fabricados a partir de setembro de 2022 podem exigir atualizações de software para se unirem aos controladores de LAN sem fio.
- Aviso de campo 72524: durante a atualização/downgrade de software, os APs do Cisco IOS podem permanecer no estado de download após 4 de dezembro de 2022 devido à expiração do certificado - recomendada atualização de software
- ID de bug da Cisco CSCwb13784: APs não podem se unir ao 9800 devido a um caminho inválido de MTU na solicitação de ingresso do AP
- ID de bug Cisco CSCvu22886: C9130: mensagem "unlzma: write: No space left on device" na atualização para 17.7 Aumente o tamanho máximo de /tmp

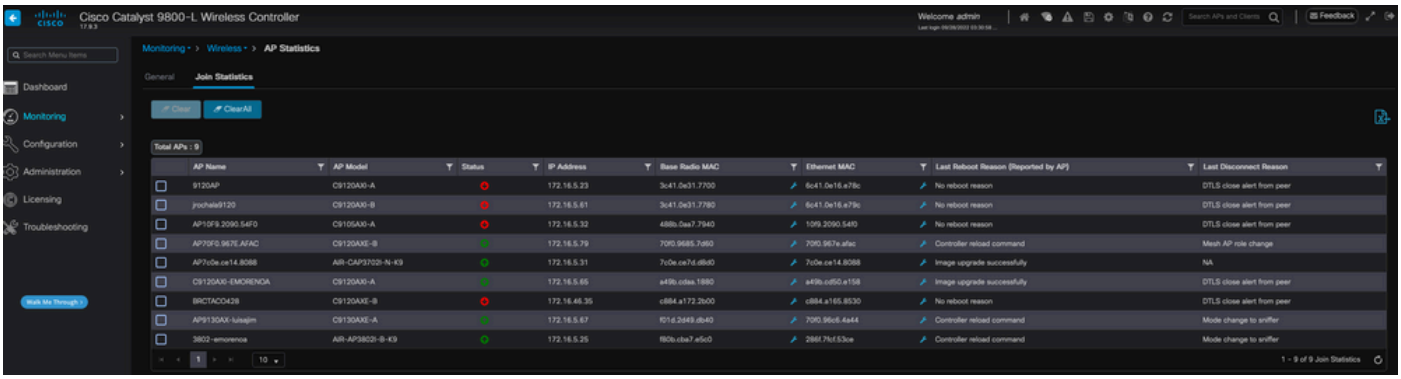
Consulte sempre a seção **Caminho de Upgrade** das Notas de Release de cada versão antes de fazer o upgrade.



Observação: a partir do Cisco IOS XE Cupertino 17.7.1, o Cisco Catalyst 9800-CL Wireless Controller não aceitará mais de 50 APs se o Smart Licensing não estiver conectado e ativado.

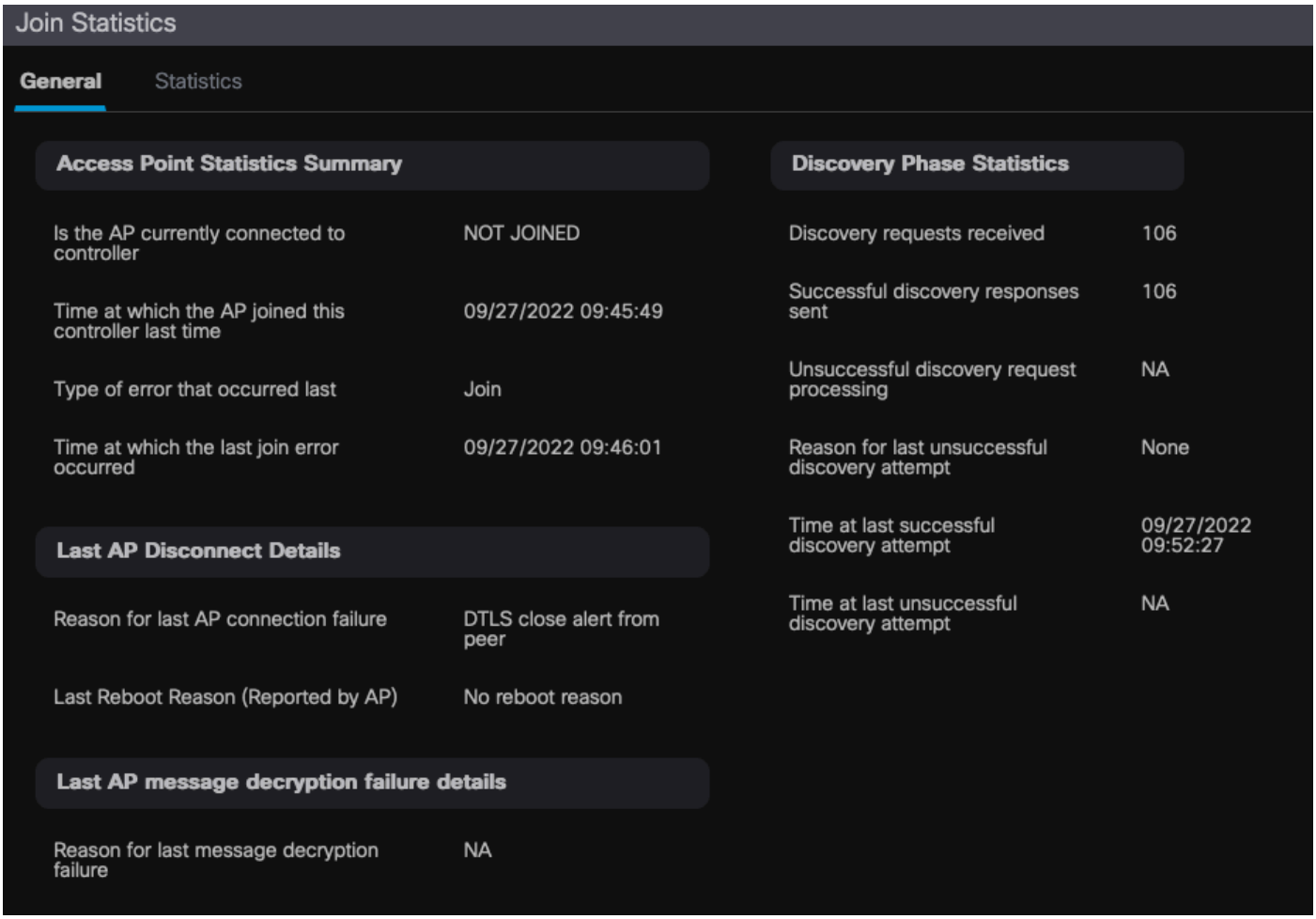
Verificações da GUI da WLC

Em sua WLC, vá para **Monitoring > Wireless > AP Statistics > Join Statistics** você pode ver o **Last Reboot Reason** relatado por qualquer AP e o **Last Disconnect Reason** registrado pela WLC.



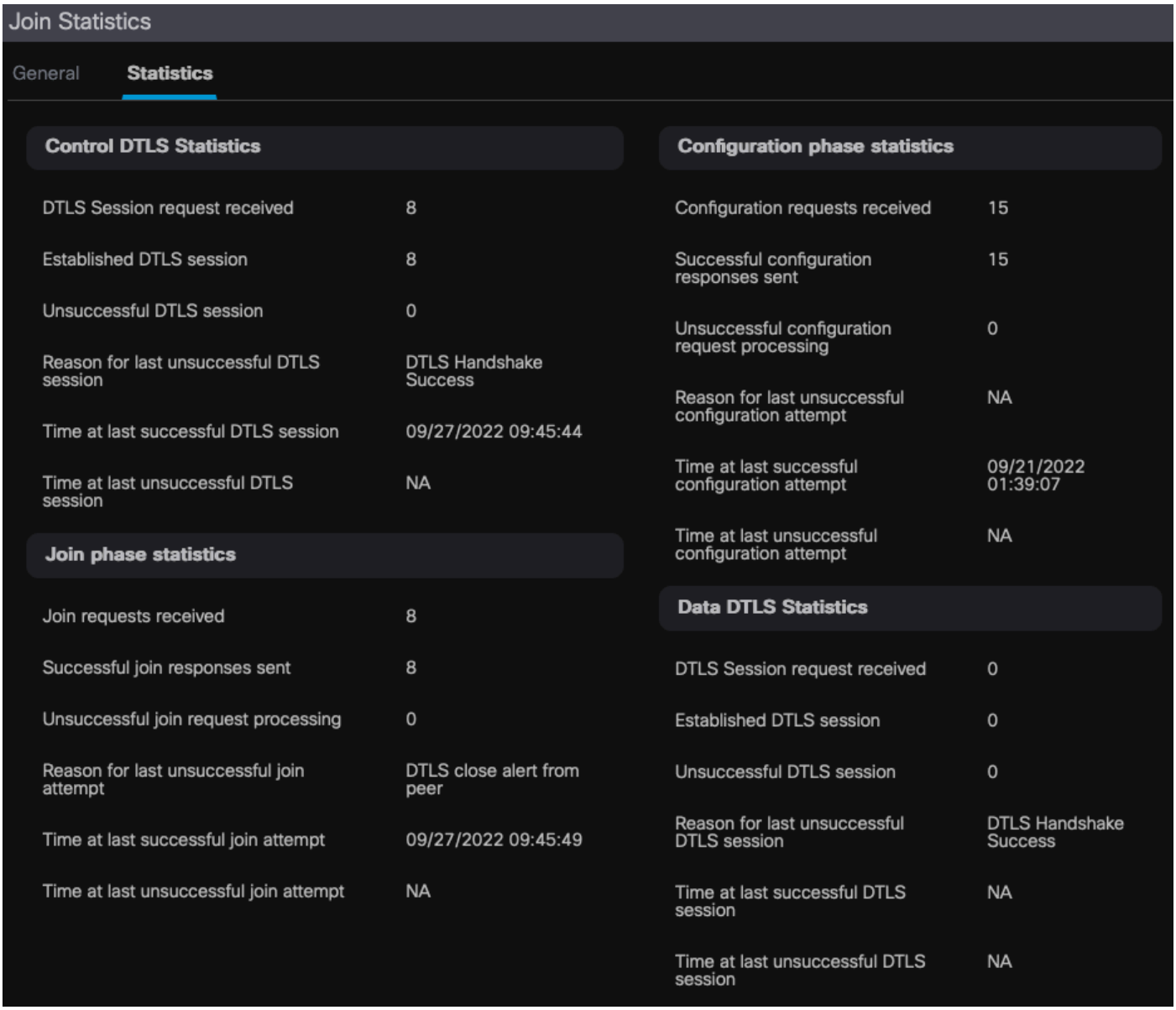
página Estatísticas de junção AP na WLC

Você pode clicar em qualquer AP e verificar os detalhes de Estatísticas de junção de AP. Aqui, você pode ver informações mais detalhadas, como a hora e a data em que o AP ingressou pela última vez e tentou descobrir a WLC.



Estatísticas Gerais de Junção AP

Para obter informações mais detalhadas, vá até a guia Estatísticas da mesma janela. Aqui você pode comparar a quantidade de **Respostas de Junção** Enviadas com a quantidade de Solicitações de Junção Recebidas**, bem como as** Respostas de Configuração Enviadas versus as Solicitações de Configuração Recebidas.



Estatísticas de Junção AP Detalhadas

Comandos

Estes comandos são úteis para solucionar problemas de AP Join:

Da WLC

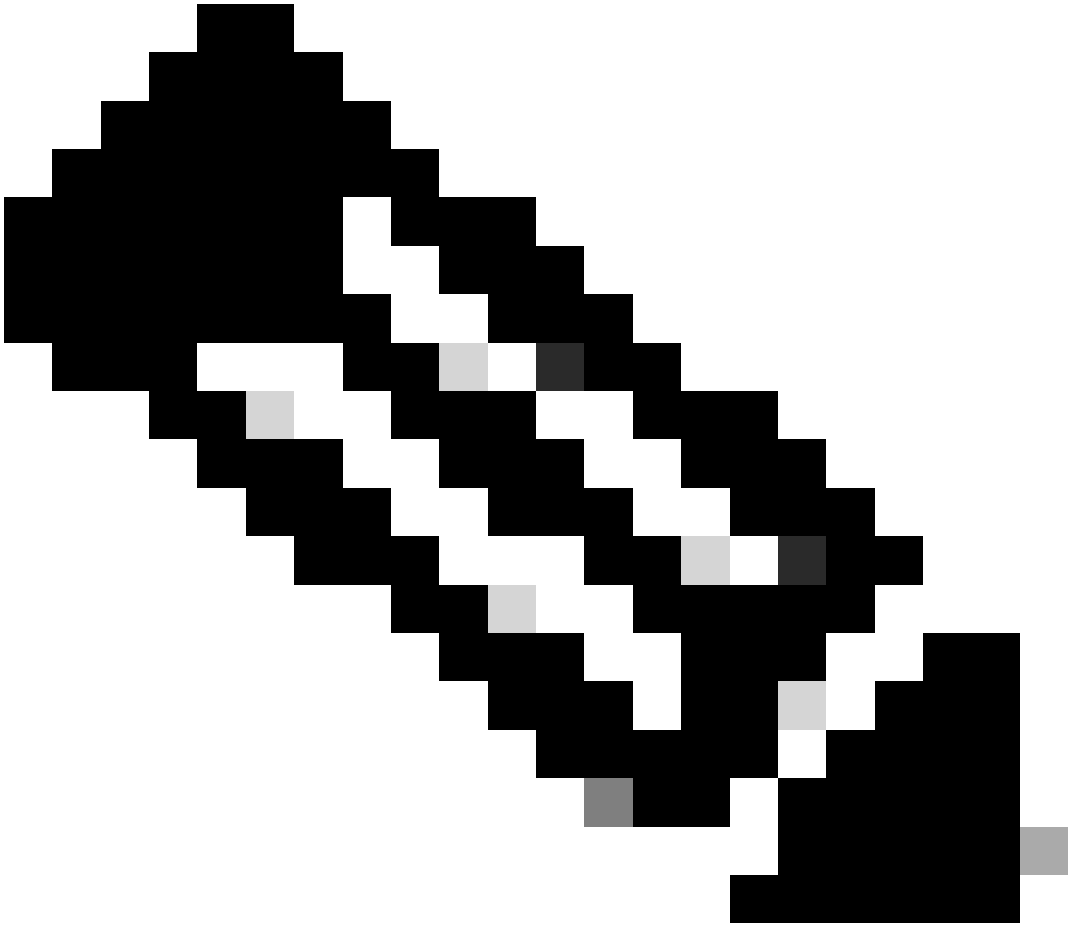
- show ap summary
- debug capwap error
- debug capwap packet

A partir de APs Wave 2 e Catalyst 11ax

    - 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

De APs da onda 1

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



Observação: quando você se conecta aos APs via Telnet/SSH para solucionar problemas, sempre emita o comando **terminal monitor** ao reproduzir o problema após habilitar as depurações nos APs. Caso contrário, você não poderá ver nenhuma saída das depurações.

Traços radioativos

Um bom ponto de partida para solucionar problemas de junção de AP é obter traços radioativos dos endereços MAC de rádio e Ethernet de um AP que tenha problemas de junção. Consulte a coleção Debug & Log no documento de WLC do Catalyst 9800 para obter detalhes sobre como gerar esses logs.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.