

Comprensión del proceso de unión de AP con el WLC Catalyst 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Establecimiento de sesión CAPWAP](#)

[Establecimiento de sesión DTLS](#)

[Métodos de detección del controlador de LAN inalámbrica](#)

[Elección del controlador de LAN inalámbrica](#)

[Máquina de estado CAPWAP](#)

[Estado CAPWAP: Descubrimiento](#)

[Estado CAPWAP: Configuración de DTLS.](#)

[Estado CAPWAP: Incorporarse](#)

[Estado CAPWAP: Datos de imagen](#)

[Estado CAPWAP: Configurar](#)

[Estado CAPWAP: Ejecute](#)

[Configurar](#)

[Elección estática del WLC](#)

[Habilitación del Acceso Telnet/SSH al AP](#)

[Cifrado de enlace de datos](#)

[Verificación](#)

[Troubleshoot](#)

[Problemas conocidos](#)

[Verificaciones GUI WLC](#)

[Comandos](#)

[Desde el WLC](#)

[Desde PA Wave 2 y Catalyst 11ax](#)

[Desde puntos de acceso Wave 1](#)

[Trazas radiactivas](#)

Introducción

En este documento se describe en detalle el proceso de unión de AP con el WLC de Cisco Catalyst 9800.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de los puntos de acceso inalámbricos de control y aprovisionamiento (CAPWAP)
- Comprensión básica del uso de un controlador de LAN inalámbrica (WLC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC Catalyst 9800-L, Cisco IOS® XE Cupertino 17.9.3
- Punto de acceso Catalyst 9120AX

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Establecimiento de sesión CAPWAP

El punto de acceso inalámbrico de control y aprovisionamiento (CAPWAP) es el protocolo que proporciona el mecanismo de transporte utilizado por los puntos de acceso (AP) y los controladores de LAN inalámbrica (WLC) para intercambiar información del plano de datos y control a través de un túnel de comunicación seguro (para el control CAPWAP).

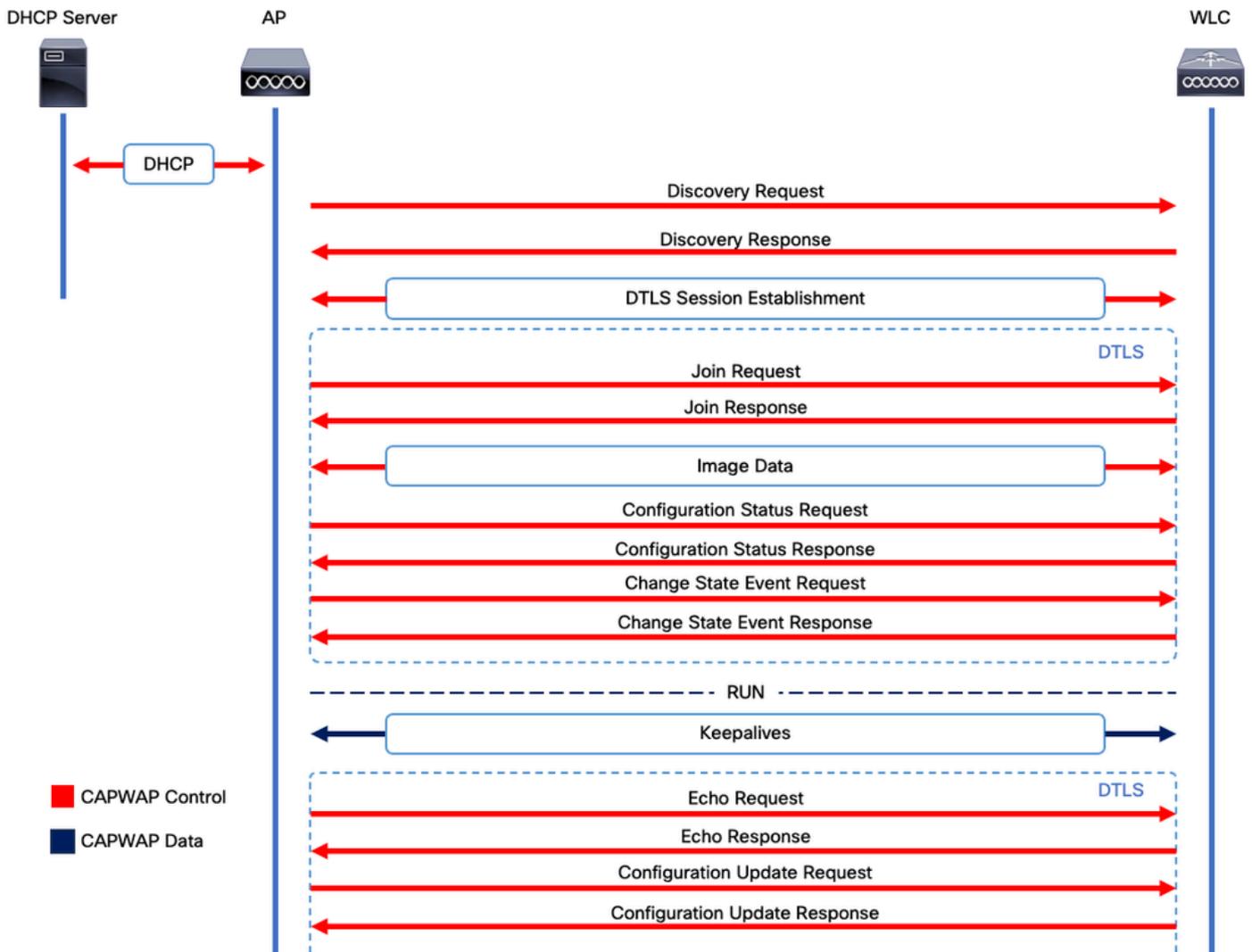
Para profundizar en el proceso de unión de PA, es importante que comprenda el proceso de establecimiento de sesión de control y aprovisionamiento de puntos de acceso inalámbricos (CAPWAP).

Tenga en cuenta que el AP necesita tener una dirección IP antes de poder iniciar el proceso CAPWAP. Si el AP no tiene una dirección IP, no inicia el Proceso de Establecimiento de Sesión CAPWAP.

1. El punto de acceso envía una solicitud de detección. Vea la sección Métodos de Detección de WLC para obtener más información sobre esto
2. El WLC envía una respuesta de detección
3. establecimiento de sesión DTLS. Después de esto, todos los mensajes posteriores se cifran y se muestran como paquetes de datos de aplicación DTLS en cualquier herramienta de análisis de paquetes.
4. El punto de acceso envía una solicitud de unión
5. El WLC envía una respuesta de unión
6. El AP realiza una verificación de la imagen. Si tiene la misma versión de imagen que el

WLC, entonces continúa con el siguiente paso. Si no lo hace, entonces descarga la imagen del WLC y se reinicia para cargar la nueva imagen. En tal caso, repite el proceso desde el paso 1.

7. El punto de acceso envía una solicitud de estado de configuración.
8. El WLC envía una respuesta del estado de la configuración
9. El punto de acceso pasa al estado RUN.
10. Durante el estado RUN, el Mantenimiento del Túnel CAPWAP se realiza de dos maneras:
 1. Se intercambian señales de mantenimiento para mantener el túnel de datos CAPWAP
 2. AP envía una solicitud de eco al WLC, que debe ser respondida con su respectiva respuesta de eco. Esto es para mantener el túnel de control CAPWAP.



Proceso de establecimiento de sesión CAPWAP



Nota: Según RFC 5415, CAPWAP utiliza los puertos UDP 5246 (para control CAPWAP) y 5247 (para datos CAPWAP).

Establecimiento de sesión DTLS

Una vez que el punto de acceso recibe una respuesta de detección válida del WLC, se establece un túnel DTLS entre ellos para transmitir todos los paquetes subsiguientes a través de un túnel seguro. Este es el proceso para establecer la sesión DTLS:

1. El AP envía un mensaje de saludo del cliente
2. El WLC envía un mensaje HelloVerifyRequest con una cookie utilizada para la validación.
3. El AP envía un mensaje ClientHello con una cookie utilizada para la validación.
4. El WLC envía estos paquetes en orden:
 1. ServerHello
 2. Certificado
 3. Intercambio de claves del servidor
 4. Solicitud de certificado

5. ServerHelloDone
5. AP envía estos paquetes en orden:
 1. Certificado
 2. IntercambioClavesCliente
 3. Verificación de certificado
 4. CambiarEspecCifrado
6. El WLC responde a los AP ChangeCypherSpec con su propio ChangedCypherSpec:
 1. CambiarEspecCifrado

Después del último mensaje ChangedCypherSpec enviado por el WLC, se establece el túnel seguro y todo el tráfico enviado en ambas direcciones se cifra ahora.

Métodos de detección del controlador de LAN inalámbrica

Hay varias opciones para que los puntos de acceso sepan de la existencia de un WLC en la red:

- Opción 43 de DHCP: Esta opción proporciona a los AP la dirección IPv4 del WLC a unirse. Este proceso es conveniente para las implementaciones grandes en las cuales los AP y el WLC están en sitios diferentes.
- Opción DHCP 52: Esta opción proporciona a los AP la dirección IPv6 del WLC a unirse. Su uso es conveniente en el mismo escenario que la opción DHCP 43.
- Detección de DNS: APs consulta el nombre de dominio CISCO-CAPWAP-CONTROLLER.localdomain. Debe configurar su servidor DNS para resolver la dirección IPv4 o IPv6 del WLC para unirse. Esta opción es conveniente para las implementaciones en las cuales los WLC se almacenan en el mismo sitio que los AP.
- Difusión de capa 3: Los AP envían automáticamente un mensaje de broadcast a 255.255.255.255. Se espera que cualquier WLC dentro de la misma subred que el AP responda a esta solicitud de detección.
- Configuración estática: Puede utilizar el comando capwap ap primary-base <wlc-hostname> <wlc-IP-address> para configurar una entrada estática para un WLC en el AP.
- Descubrimiento de movilidad: Si el AP se unió previamente a un WLC que era parte de un grupo de la movilidad, el AP también guarda un registro de los WLC presentes en ese grupo de la movilidad.



Nota: Los métodos de detección de WLC enumerados no tienen ningún orden de precedencia.

Elección del controlador de LAN inalámbrica

Una vez que el AP ha recibido una respuesta de detección de cualquier WLC que utiliza cualquiera de los métodos de detección del WLC, selecciona un controlador para unirse con este criterio:

1. Controlador principal (configurado con el comando `capwap ap primary-base <wlc-hostname> <wlc-IP-address>`)
2. Controlador secundario (configurado con el comando `capwap ap secondary-base <wlc-hostname> <wlc-IP-address>`)
3. Controlador terciario (configurado con el comando `capwap ap tertiary-base <wlc-hostname> <wlc-IP-address>`)
4. Si no se configuró previamente ningún WLC primario, secundario o terciario, entonces el AP intenta unirse al primer WLC que respondió a la petición de detección con su propia

respuesta de detección que tiene la capacidad máxima de los APs disponibles (es decir, el WLC que puede soportar la mayoría de los APs en un momento dado).

Máquina de estado CAPWAP

En la consola AP puede realizar un seguimiento de la máquina de estado CAPWAP, que recorre los pasos descritos en la sección Establecimiento de sesión CAPWAP.

Estado CAPWAP: Descubrimiento

Aquí puede ver las solicitudes de detección y las respuestas. Observe cómo el AP recibe una IP del WLC vía DHCP (opción 43), y también envía una petición de detección a los WLC previamente conocidos:

```
<#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

Además de recibir una respuesta de detección de un WLC configurado estáticamente (172.16.0.20) y del WLC indicado a través de la opción DHCP 43 (172.16.5.11), este AP también recibió una respuesta de detección de otro WLC (172.16.5.169) dentro de la misma subred porque recibió el mensaje de detección de difusión.

Estado CAPWAP: Configuración de DTLS.

Aquí, la sesión DTLS entre el AP y el WLC se intercambia.

<#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: Incorporarse

Después de establecer la sesión DTLS, una solicitud de unión al WLC se envía ahora sobre la sesión segura. Observe cómo esta solicitud se responde inmediatamente con una respuesta de unión del 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: Datos de imagen

El AP compara su imagen con la imagen del WLC. En este caso, tanto la partición activa de APs como su partición de respaldo tienen imágenes diferentes que el WLC, por lo que invoca la secuencia de comandos upgrade.sh, que indica al AP que solicite la imagen adecuada al WLC y la descargue en su partición no activa actual.

<#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

Una vez que se completa la transferencia de imagen, el AP inicia un proceso de verificación de firma de imagen para validarla. Después de hacerlo, la secuencia de comandos upgrade.sh instala la imagen en la partición no activa actual e intercambia la partición desde la que se inicia. Finalmente, el AP se recarga y repite el proceso desde el principio (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



Advertencia: Los puntos de acceso de la etapa 1 podrían no descargar una nueva imagen debido a un certificado caducado. Consulte [Aviso de campo 72524](#) para obtener más información y lea atentamente el [Documento de soporte de descarga de imagen de punto de acceso de Cisco IOS fallida debido a certificado de firma de imagen caducada el pasado 4 de diciembre de 2022 \(CSCwd80290\)](#) para comprender su impacto y solución.

Una vez que el AP se recarga y pasa otra vez a través de los estados CAPWAP Discover y Join, durante el estado Image Data detecta que ahora tiene la imagen adecuada.

```
<#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

Después de que el AP valida que tiene la misma versión que el WLC, notifica sus configuraciones actuales al WLC. En general, esto significa que el AP pide mantener sus configuraciones (si están disponibles en el 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: Ejecute

En este punto, el AP se ha unido con éxito al controlador. Durante este estado, el WLC dispara un mecanismo para invalidar la configuración solicitada por el AP. Puede ver que el AP consigue configuraciones de radio y de las credenciales empujadas, y también consigue asignado a la etiqueta de política predeterminada puesto que el WLC no tenía conocimiento previo de este 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]

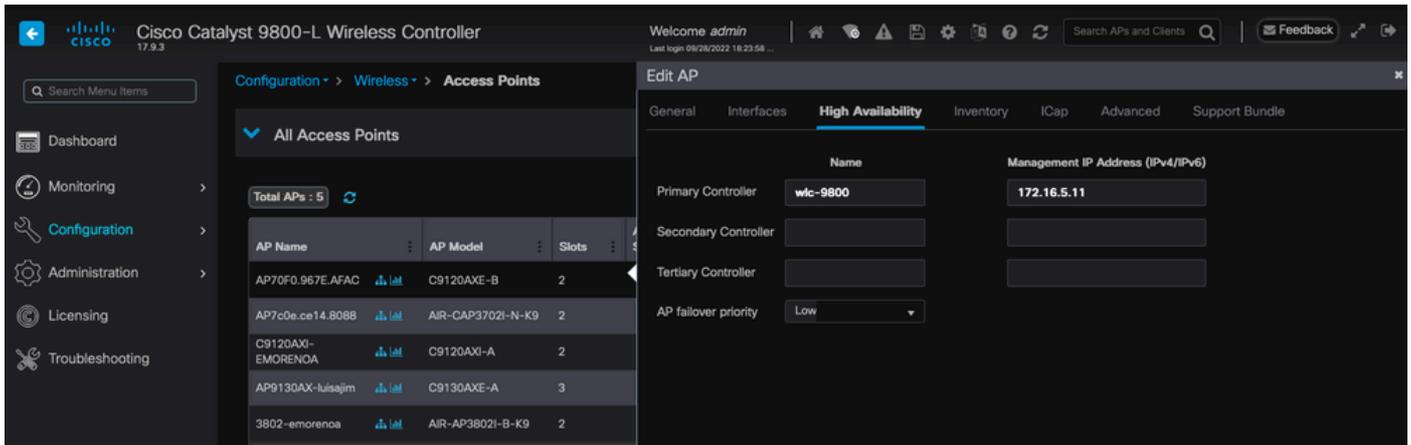
AP tag change to default-policy-tag

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

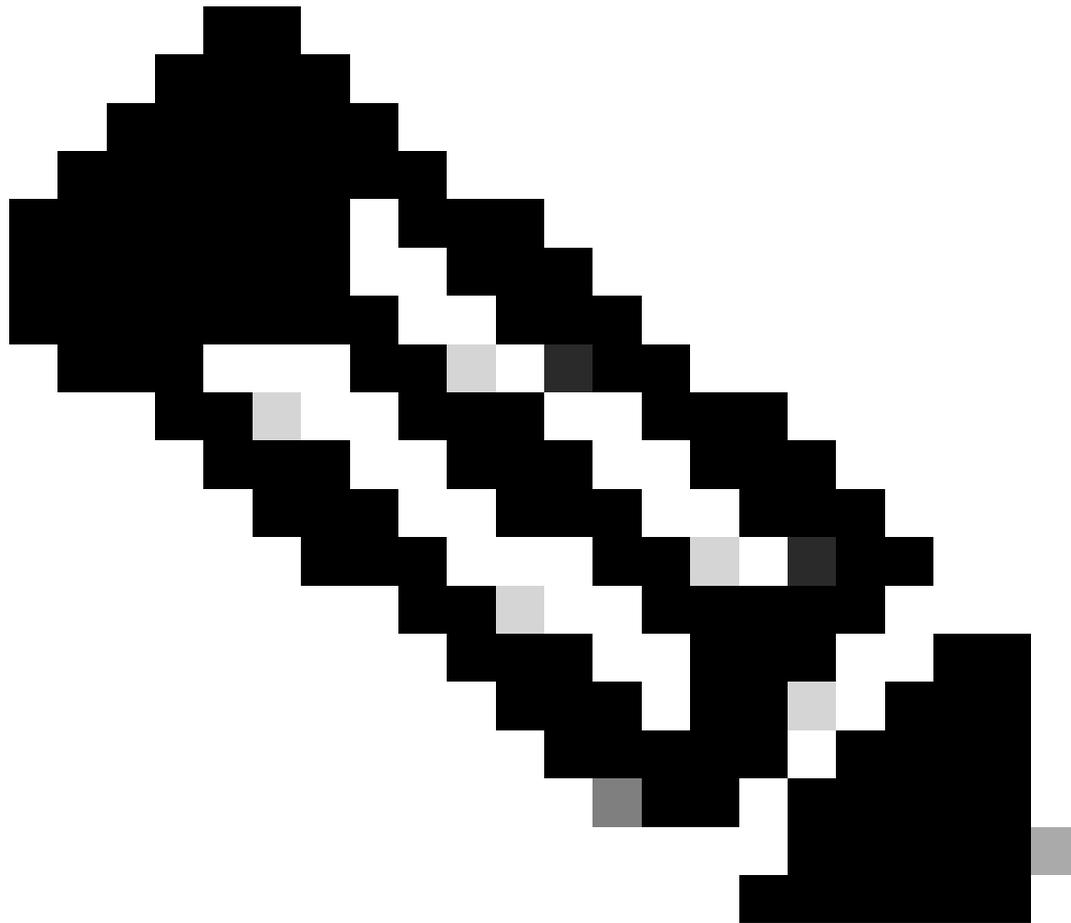
Configurar

Elección estática del WLC

En la GUI, puede ir a Configuration > Wireless > Access Points, seleccionar un AP y navegar a la pestaña High Availability. Aquí, puede configurar los WLC primario, secundario y terciario, como se describe en la sección Elección del controlador del Wireless LAN de este documento. Esta configuración se realiza por punto de acceso.



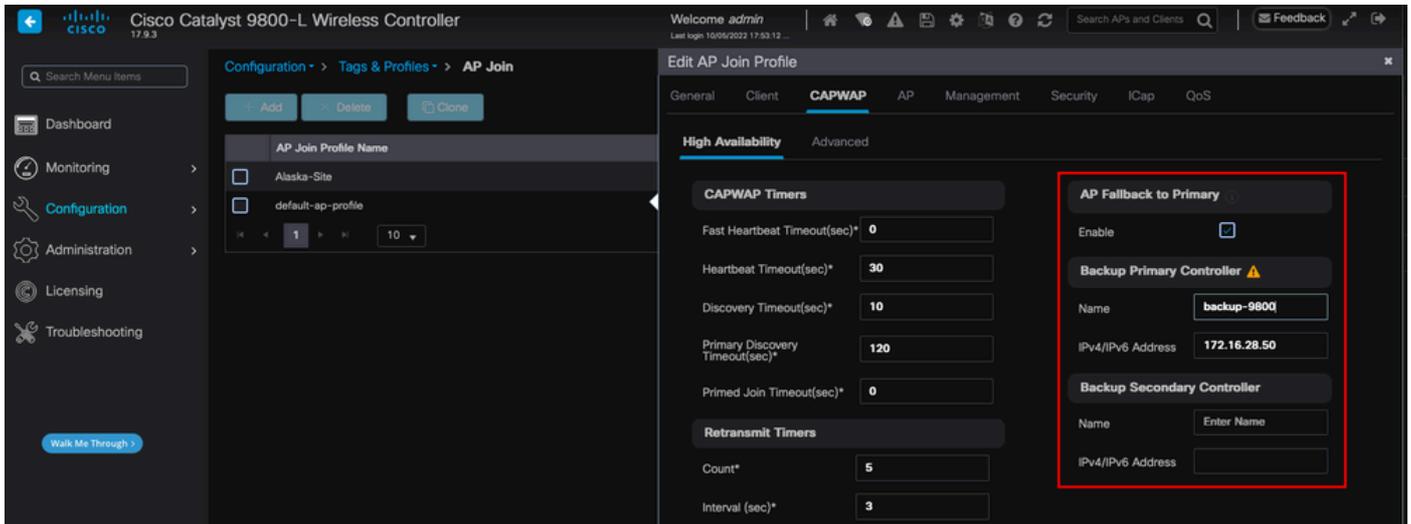
WLC primario, secundario y terciario para un AP.



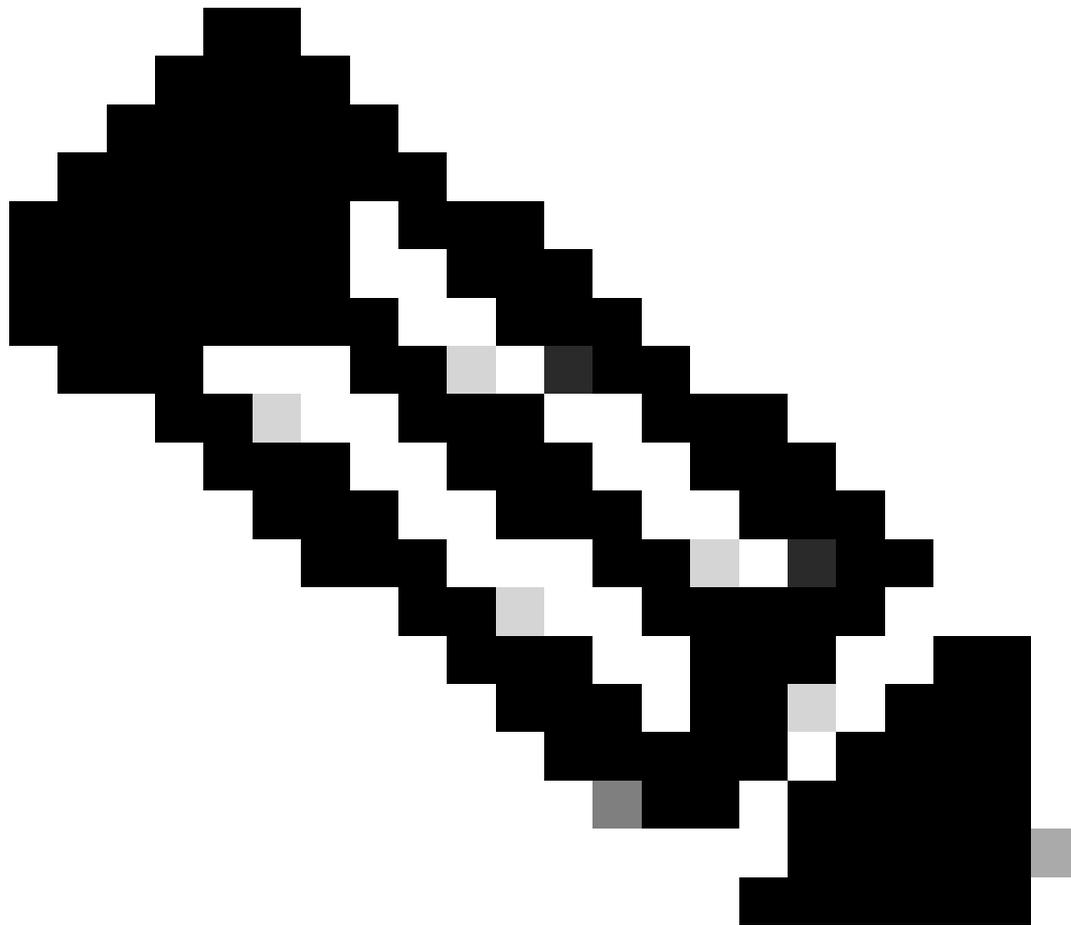
Nota: A partir de Cisco IOS XE 17.9.2, puede utilizar Perfiles de cebado para configurar controladores primarios, secundarios y terciarios para un grupo de AP que coincidan con una expresión regular (regex) o para un AP individual. Refiérase a la sección [Reserva de AP a los Controladores Configurados bajo el Perfil de Priming AP](#) de la [Guía de Configuración](#) para obtener más información.

Tenga en cuenta que los controladores primarios, secundarios y terciarios configurados en la pestaña de alta disponibilidad de AP difieren de los WLC primarios y secundarios de respaldo que se pueden configurar por perfil de unión de AP en la pestaña CAPWAP > High Availability. Los Controladores Primarios, Secundarios y Terciarios se consideran WLCs con las prioridades 1, 2 y 3, respectivamente, mientras que los Primarios y Secundarios de Respaldo se consideran WLCs con las prioridades 4 y 5.

Si se habilita AP Fallback, el AP busca activamente el controlador primario cuando se une a un WLC diferente. El AP solo busca los WLC con las prioridades 4 y 5 una vez que haya un evento CAPWAP Down y ninguno de los Controladores Primarios y Secundarios de Respaldo estén disponibles.



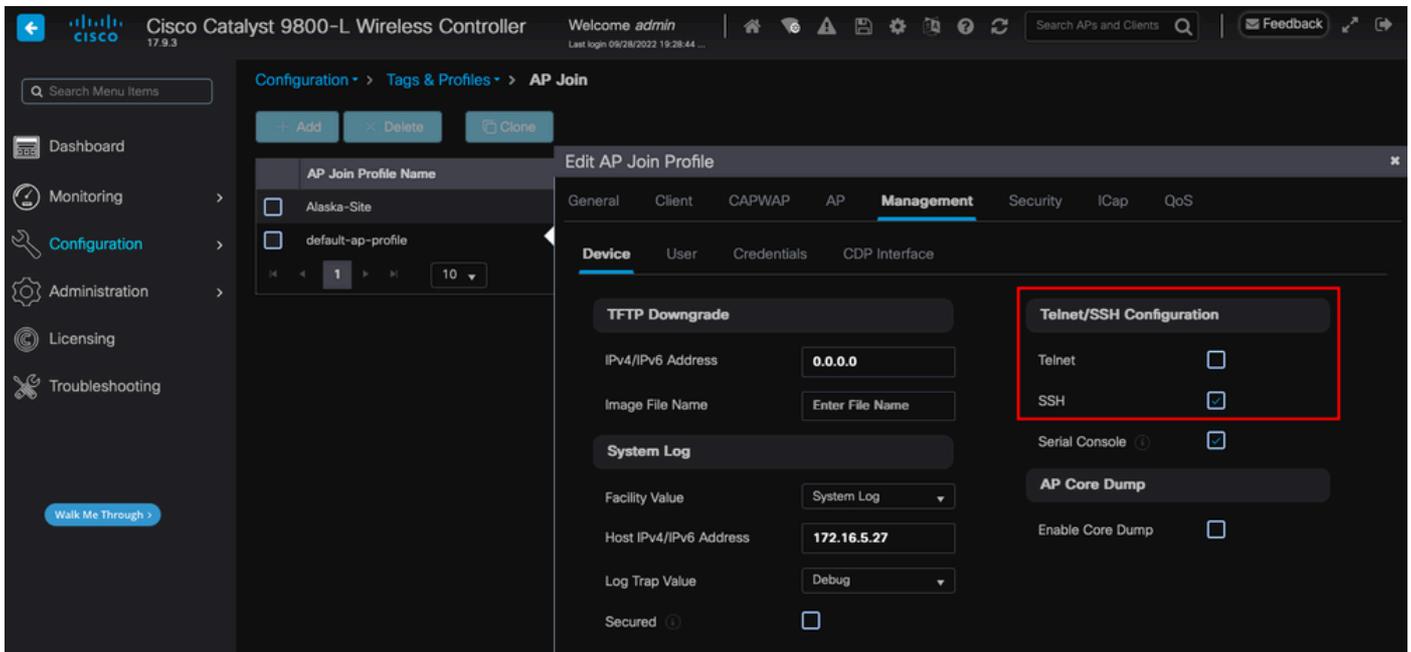
Opciones de alta disponibilidad en el perfil de unión de PA



Nota: La configuración de los WLCs Primario de Respaldo y Secundario de Respaldo en el AP Join Profile no rellena las entradas Primario Estático y Secundario en la pestaña de Alta Disponibilidad del Access Point.

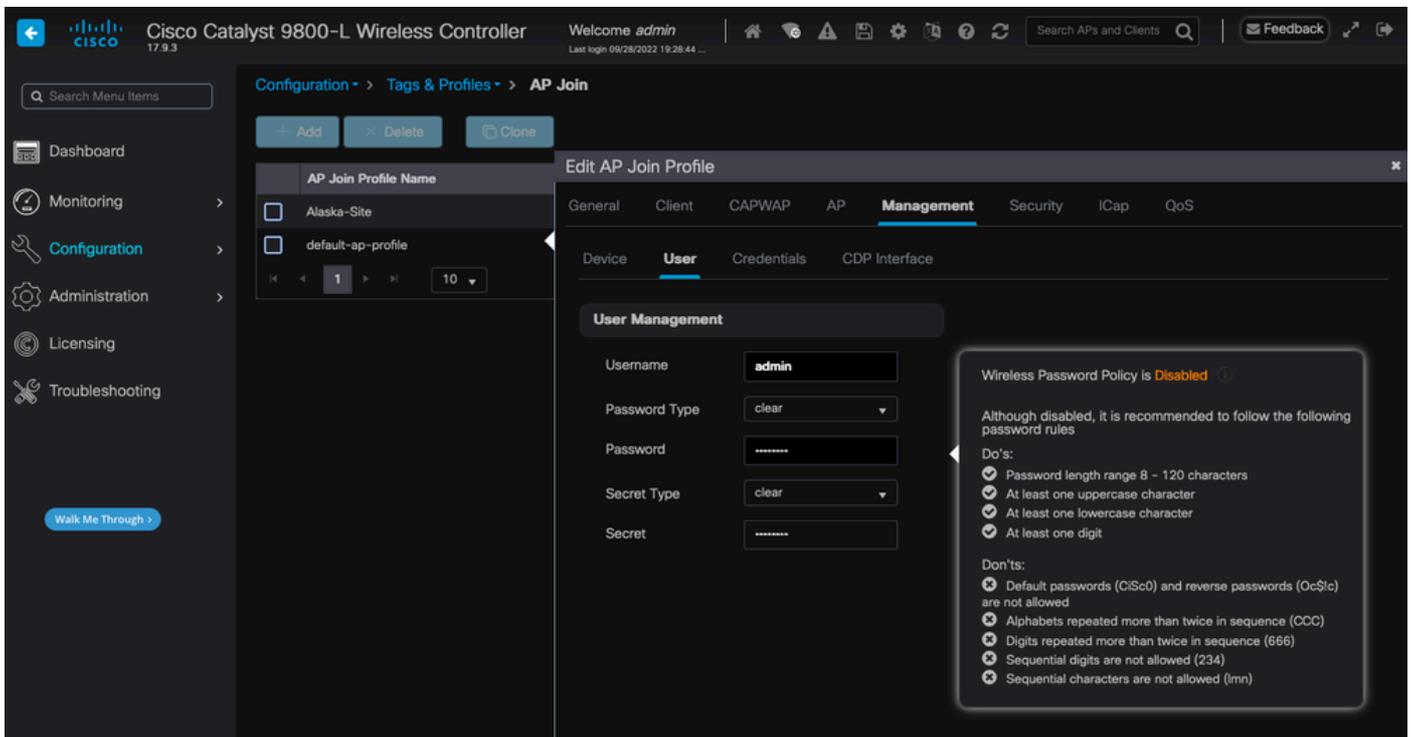
Habilitación del Acceso Telnet/SSH al AP

Vaya a Configuration > Tags & Profiles > AP Join > Management > Device y seleccione SSH y/o Telnet.



Habilitación del Acceso Telnet/SSH en el Perfil de Unión AP

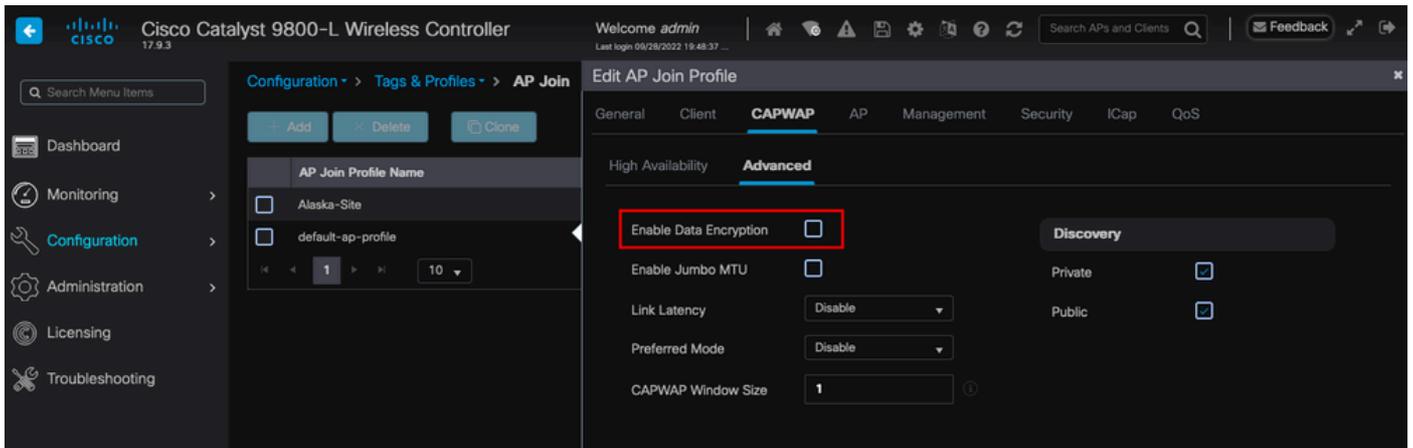
Para configurar las credenciales de SSH/Telnet, navegue hasta la pestaña User en la misma ventana y establezca el Username, Password y Secret para acceder al AP.



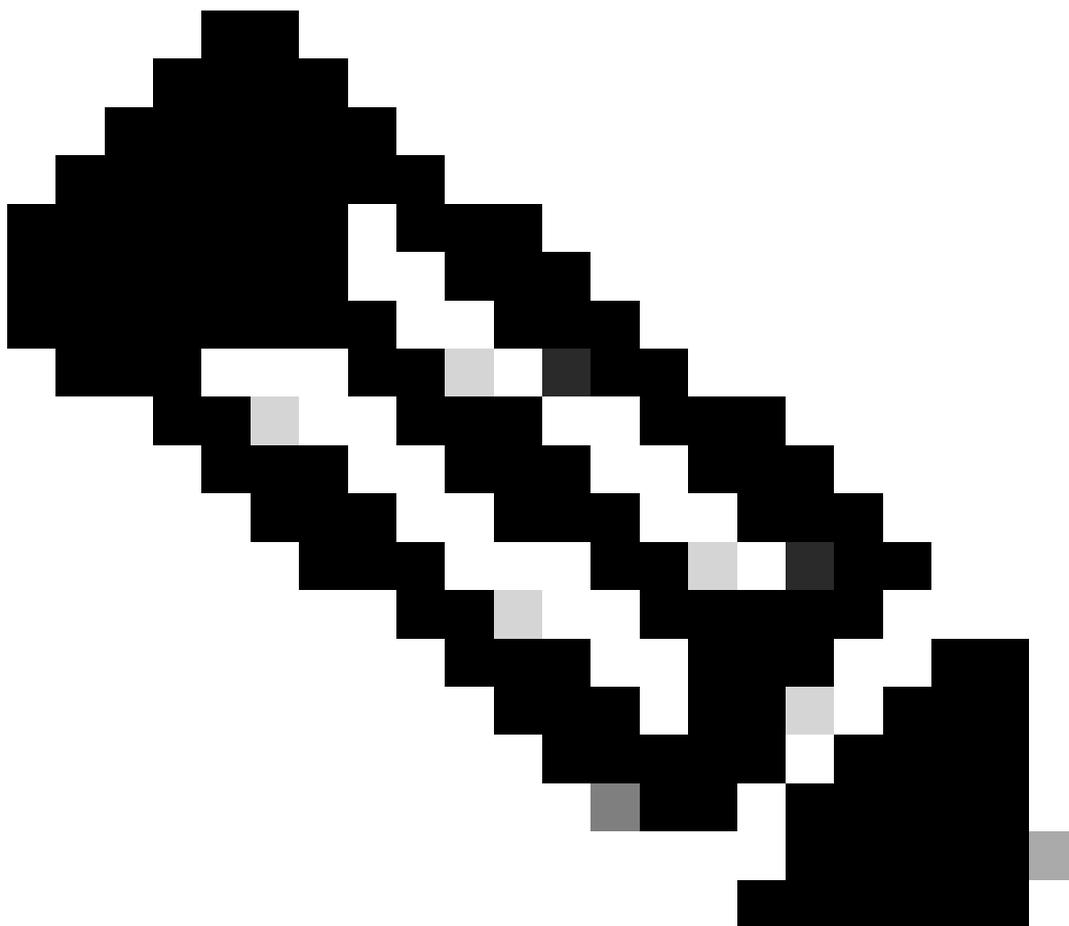
Credenciales de SSH y Telnet para el AP

Cifrado de enlace de datos

Si necesita resolver cualquier problema de cliente que requiera tomar una captura de paquetes del tráfico de APs, asegúrese de que Data Link Encryption no esté habilitado en Configuration > Tags & Profiles > AP Join > CAPWAP > Advanced. De lo contrario, el tráfico se cifrará.



Cifrado de enlace de datos



Nota: El cifrado de datos solo cifra el tráfico de datos CAPWAP. El tráfico de control

CAPWAP ya está cifrado mediante DTLS.

Verificación

Además de realizar un seguimiento de la máquina de estado CAPWAP en la consola de APs, también puede tomar una [captura de paquetes incrustada](#) en el WLC para analizar el proceso de unión de AP:

No.	Time	Time delta from [Source]	Destination	Protocol	Length	Destination Port	Info
886	12:58:41.288976	0.022002000	172.16.5.65	172.16.5.11	CAPWAP-Control	294 5246	CAPWAP-Control - Discovery Request
887	12:58:41.288976	0.000000000	172.16.5.11	172.16.5.65	CAPWAP-Control	147 5267	CAPWAP-Control - Discovery Response
888	12:58:41.388974	0.027998000	172.16.5.65	255.255.255.255	CAPWAP-Control	294 5246	CAPWAP-Control - Discovery Request
889	12:58:41.388974	0.000000000	172.16.5.11	172.16.5.65	CAPWAP-Control	147 5267	CAPWAP-Control - Discovery Response
1156	12:58:50.794957	0.195898000	172.16.5.65	172.16.5.11	DTLSv1.2	276 5246	Client Hello
1157	12:58:50.795948	0.000991000	172.16.5.11	172.16.5.65	DTLSv1.2	98 5267	Hello Verify Request
1158	12:58:50.796955	0.001007000	172.16.5.65	172.16.5.11	DTLSv1.2	296 5246	Client Hello
1159	12:58:50.798954	0.001999000	172.16.5.11	172.16.5.65	DTLSv1.2	562 5267	Server Hello, Certificate (Fragment)
1160	12:58:50.798954	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	562 5267	Certificate (Fragment)
1161	12:58:50.798954	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	562 5267	Certificate (Reassembled), Server Key Exchange (Fragment)
1162	12:58:50.798954	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	349 5267	Server Key Exchange (Reassembled), Certificate Request, Server Hello Done
1163	12:58:50.859940	0.060860000	172.16.5.65	172.16.5.11	DTLSv1.2	594 5246	Certificate (Fragment)
1164	12:58:50.859940	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	594 5246	Certificate (Reassembled), Client Key Exchange (Fragment)
1181	12:58:51.284975	0.066997000	172.16.5.65	172.16.5.11	DTLSv1.2	463 5246	Client Key Exchange (Reassembled), Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
1182	12:58:51.285983	0.001008000	172.16.5.11	172.16.5.65	DTLSv1.2	125 5267	Change Cipher Spec, Encrypted Handshake Message
1320	12:58:55.914945	0.016997000	172.16.5.65	172.16.5.11	DTLSv1.2	1487 5246	Application Data
1321	12:58:55.914944	0.001999000	172.16.5.11	172.16.5.65	DTLSv1.2	1484 5267	Application Data
1330	12:58:56.246981	0.109003000	172.16.5.65	172.16.5.11	DTLSv1.2	1439 5246	Application Data
1331	12:58:56.246981	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	1439 5246	Application Data
1332	12:58:56.246981	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	379 5246	Application Data
1333	12:58:56.247973	0.000992000	172.16.5.11	172.16.5.65	DTLSv1.2	354 5267	Application Data
1364	12:58:57.292984	0.040999000	172.16.5.65	172.16.5.11	DTLSv1.2	1439 5246	Application Data
1365	12:58:57.292984	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	698 5246	Application Data
1366	12:58:57.293975	0.000991000	172.16.5.11	172.16.5.65	DTLSv1.2	354 5267	Application Data
1368	12:58:57.387965	0.069898000	172.16.5.65	172.16.5.11	DTLSv1.2	982 5246	Application Data
1369	12:58:57.388972	0.001007000	172.16.5.11	172.16.5.65	DTLSv1.2	482 5267	Application Data
1376	12:58:57.469961	0.001999000	172.16.5.11	172.16.5.65	DTLSv1.2	148 5246	Application Data
1377	12:58:57.469961	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	103 5267	Application Data
1378	12:58:57.470968	0.001007000	172.16.5.65	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	172.16.5.65	DTLSv1.2	133 5267	Application Data
1380	12:58:57.477972	0.003000000	172.16.5.11	172.16.5.65	CAPWAP-Data	104 5267	CAPWAP-Data Keep-Alive[Malformed Packet]
1400	12:58:57.546968	0.003997000	172.16.5.65	172.16.5.11	DTLSv1.2	148 5246	Application Data
1401	12:58:57.546968	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	119 5246	Application Data
1402	12:58:57.547968	0.000992000	172.16.5.11	172.16.5.65	DTLSv1.2	183 5267	Application Data
1403	12:58:57.547968	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	121 5267	Application Data
1411	12:58:57.575958	0.002998000	172.16.5.65	172.16.5.11	DTLSv1.2	148 5246	Application Data
1412	12:58:57.575958	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	103 5267	Application Data
1413	12:58:57.577957	0.001999000	172.16.5.65	172.16.5.11	DTLSv1.2	119 5246	Application Data
1414	12:58:57.577957	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	143 5246	Application Data
1415	12:58:57.577957	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	1190 5267	Application Data
1416	12:58:57.577957	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	183 5267	Application Data
1425	12:58:57.688959	0.070955000	172.16.5.65	172.16.5.11	DTLSv1.2	119 5246	Application Data
1426	12:58:57.688959	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	148 5246	Application Data
1427	12:58:57.688959	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	119 5267	Application Data
1428	12:58:57.688959	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	103 5267	Application Data
1429	12:58:57.688951	0.000992000	172.16.5.65	172.16.5.11	DTLSv1.2	119 5246	Application Data
1430	12:58:57.688951	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	222 5246	Application Data
1431	12:58:57.690958	0.001007000	172.16.5.11	172.16.5.65	DTLSv1.2	175 5267	Application Data
1432	12:58:57.690958	0.000000000	172.16.5.11	172.16.5.65	DTLSv1.2	103 5267	Application Data
1433	12:58:57.692957	0.001999000	172.16.5.65	172.16.5.11	DTLSv1.2	119 5246	Application Data
1434	12:58:57.692957	0.000000000	172.16.5.65	172.16.5.11	DTLSv1.2	111 5246	Application Data

Proceso de unión de AP visto en una captura de paquete incorporada en el WLC

Observe cómo todo el tráfico después del paquete Change Cipher Spec (Paquete No. 1182) se muestra solamente como Application Data sobre DTLSv1.2. Estos son todos los datos cifrados después del establecimiento de sesión DTLS.

Troubleshoot

Problemas conocidos

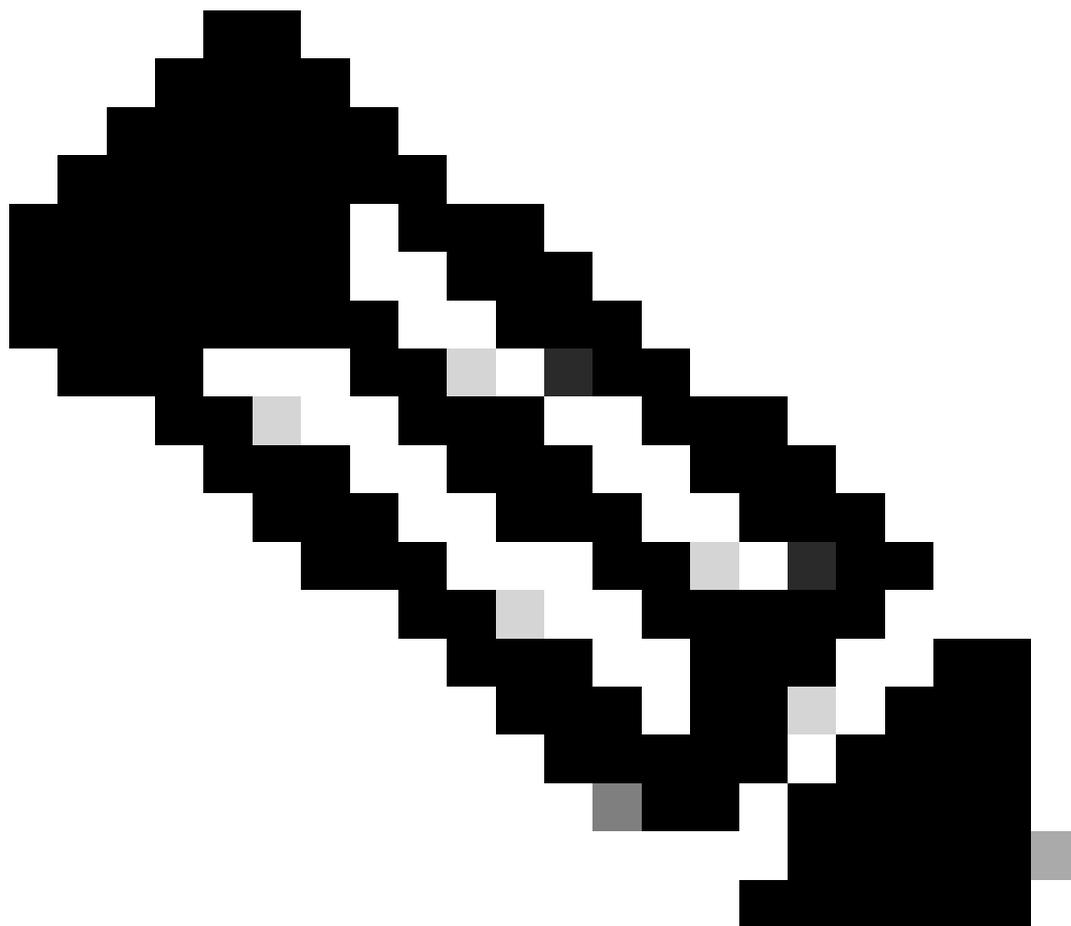
Por favor consulte los problemas conocidos que podrían impedir que sus AP se unan al WLC.

- [AP en el bucle de arranque debido a una imagen dañada en Wave 2 y puntos de acceso Catalyst 11ax \(CSCvx32806\)](#)
- [Aviso práctico 72424: Los puntos de acceso C9105/C9120/C9130 fabricados a partir de septiembre de 2022 pueden requerir actualizaciones de software para unirse a los controladores de LAN inalámbrica.](#)
- [Aviso práctico 72524: Durante la Actualización/Descarga de Software, los AP de Cisco IOS Podrían Permanecer en Estado de Descarga Después del 4 de Diciembre de 2022 Debido](#)

[al Vencimiento del Certificado - Actualización de Software Recomendada](#)

- [ID de bug de Cisco CSCwb13784: Los AP no pueden unirse a 9800 debido a la MTU de trayectoria inválida en la solicitud de unión a AP](#)
- [ID de bug de Cisco CSCvu22886: C9130: mensaje "unlzma: escribir: No queda espacio en el dispositivo" en la actualización a 17.7 Aumentar el tamaño máximo de /tmp](#)

Consulte siempre la sección Upgrade Path de las [Release Notes](#) de cada versión antes de actualizar.



Nota: A partir de Cisco IOS XE Cupertino 17.7.1, el controlador inalámbrico Cisco Catalyst 9800-CL no acepta más de 50 AP si la licencia inteligente no está conectada y activa.

Verificaciones GUI WLC

En su WLC, vaya a Monitoring > Wireless > AP Statistics > Join Statistics puede ver el último motivo de reinicio informado por cualquier AP y el último motivo de desconexión registrado por el

WLC.

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	3c41.0a31.7700	6c41.0a16.a75c	No reboot reason	DTLS close alert from peer
prohela120	C9120AXI-B	●	172.16.5.61	3c41.0a31.7780	6c41.0a16.a79c	No reboot reason	DTLS close alert from peer
AP15F9.2095.54F0	C9105AXI-A	●	172.16.5.32	480b.5aa7.7940	1099.2090.54D0	No reboot reason	DTLS close alert from peer
AP73F0.967E.AFAC	C9120AXI-B	●	172.16.5.79	7090.9685.7980	7090.967e.afac	Controller reload command	Mesh AP role change
AP730e.ca14.8068	AR-CAP3702N-N-K9	●	172.16.5.31	7c0e.ca7d.8b00	7c0e.ca14.8068	Image upgrade successfully	NA
C9120AXI-EMORENDA	C9120AXI-A	●	172.16.5.65	449b.cdaa.1980	449b.cda0.a158	Image upgrade successfully	DTLS close alert from peer
BRCTAC0428	C9120AXI-B	●	172.16.46.39	c884.a172.2600	c884.a165.8030	No reboot reason	DTLS close alert from peer
AP9130AX-tulajm	C9130AXI-A	●	172.16.5.67	8116.2449.d840	7090.9608.4444	Controller reload command	Mode change to sniffer
3802-emorenda	AR-AP9802I-B-K9	●	172.16.5.25	800c.cba7.a5c0	2866.7c13.30e	Controller reload command	Mode change to sniffer

Página Estadísticas de Unión de AP en el WLC

Puede hacer clic en cualquier AP y verificar los detalles de las estadísticas de unión a AP. Aquí, usted puede ver información más detallada, como la hora y la fecha en que el AP se unió por última vez e intentó descubrir el WLC.

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

Estadísticas generales de unión de PA

Para obtener información más detallada, vaya a la ficha Statistics (Estadísticas) de la misma ventana. Aquí puede comparar la cantidad de respuestas de unión enviadas con la cantidad de solicitudes de unión recibidas, así como las respuestas de configuración enviadas frente a las solicitudes de configuración recibidas.

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

Estadísticas detalladas de unión a PA

Comandos

Estos comandos son útiles para resolver problemas de unión de AP:

Desde el WLC

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

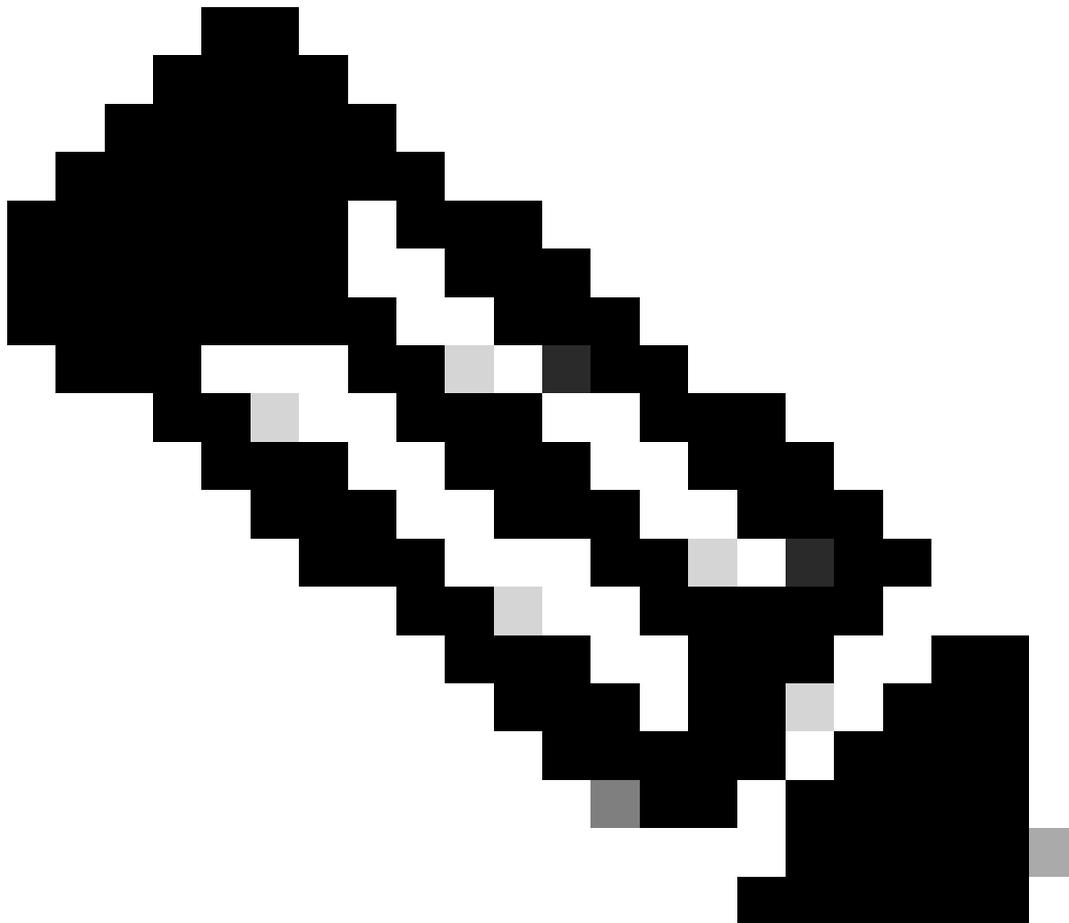
Desde PA Wave 2 y Catalyst 11ax

- 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

Desde puntos de acceso Wave 1

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



Nota: Cuando se conecta a los AP vía Telnet/SSH para resolver problemas, ejecute siempre el comando terminal monitor mientras reproduce el problema después de habilitar los debugs en los AP. De lo contrario, no podrá ver ningún resultado de las depuraciones.

Un buen punto de partida para resolver problemas de unión de AP es tomar rastros radiactivos de las direcciones MAC de radio y Ethernet de un AP que tiene problemas de unión. Consulte la [colección Debug & Log en el documento WLC de Catalyst 9800](#) para obtener detalles sobre la generación de estos registros.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).