

# Gestione Catalyst serie 9800 Wireless Controller con Prime Infrastructure con SNMP V2 y V3 y NetCONF

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Puertos utilizados](#)

[Configuración de SNMPv2 en el WLC Cat 9800](#)

[Configuración de SNMPv3 en el WLC Cat 9800](#)

[Configuración de Netconf en el WLC Cat 9800](#)

[Configuración \(Prime Infrastructure 3.5 y posterior\)](#)

[Verificación](#)

[Verificar estado de telemetría](#)

[Troubleshoot](#)

[Resolución de problemas en Prime Infrastructure](#)

[Resolución de problemas en Catalyst 9800 WLC](#)

[Eliminar toda la suscripción de telemetría de la configuración del WLC](#)

[Comprobar ID de suscripción para información de AP](#)

[Migración de PI a DNA-Center](#)

## Introducción

Este documento describe cómo integrar los controladores inalámbricos Catalyst serie 9800 (C9800 WLC) con Prime Infrastructure (3.x).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- WLC para C9800
- Prime Infrastructure (PI) versión 3.5
- Protocolo de administración de red simple (SNMP)

### Componentes Utilizados

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

- WLC para C9800
- Cisco IOS XE Gibraltar 16.10.1 a 17.3

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.

---

**Nota:** Prime Infra 3.8 sólo admite WLC 17.x 9800. Los clientes no aparecen en Prime Infrastructure si intenta administrar un WLC 16.12 con Prime Infra 3.8.

---

## Configurar

Para que Prime Infrastructure configure, administre y supervise los controladores de LAN inalámbrica de Catalyst serie 9800, debe poder acceder a C9800 a través de CLI, SNMP y Netconf. Al agregar C9800 a Prime Infrastructure, es necesario especificar las credenciales de Telnet/SSH, así como la cadena de comunidad SNMP, la versión, etc. PI utiliza esta información para verificar el alcance y para inventariar el WLC C9800. También utiliza SNMP para insertar plantillas de configuración y admitir capturas para eventos de cliente y puntos de acceso (AP). Sin embargo, para que PI recopile estadísticas de AP y clientes, Netconf es aprovechado. Netconf no está habilitado de forma predeterminada en el WLC C9800 y debe configurarse manualmente mediante CLI en la versión 16.10.1 (la GUI está disponible en 16.11.1).

## Puertos utilizados

La comunicación entre C9800 y Prime Infrastructure utiliza puertos diferentes.

- Todas las configuraciones y plantillas disponibles en Prime Infra se envían a través de SNMP y CLI. Utiliza el puerto UDP 161.
- Los datos operativos para el WLC C9800 se obtienen a través de SNMP. Utiliza el puerto UDP 162.
- Los datos operativos de AP y cliente aprovechan la telemetría de streaming.

Prime Infrastructure a WLC: puerto TCP 830. Prime Infra lo utiliza para enviar la configuración de telemetría a los dispositivos 9800 (mediante Netconf).

WLC a Prime Infrastructure: puerto TCP 20828 (para Cisco® IOS XE 16.10 y 16.11) o 20830 (para Cisco IOS XE 16.12, 17.x y versiones posteriores).

---

**Nota:** Las señales de mantenimiento se envían cada 5 segundos incluso cuando no hay telemetría para notificar.

---

**Nota:** en caso de que haya un firewall entre Prime Infrastructure y C9800, asegúrese de abrir estos puertos para establecer la comunicación.

---

## Configuración de SNMPv2 en el WLC Cat 9800

GUI:

Paso 1. Desplácese hasta **Administration > SNMP > Slide to Enable SNMP**.



Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

## SNMP

SNMP Mode

ENABLED



General

Community Strings

V3 Users

Hosts

System Location

System Contact

SNMP Traps

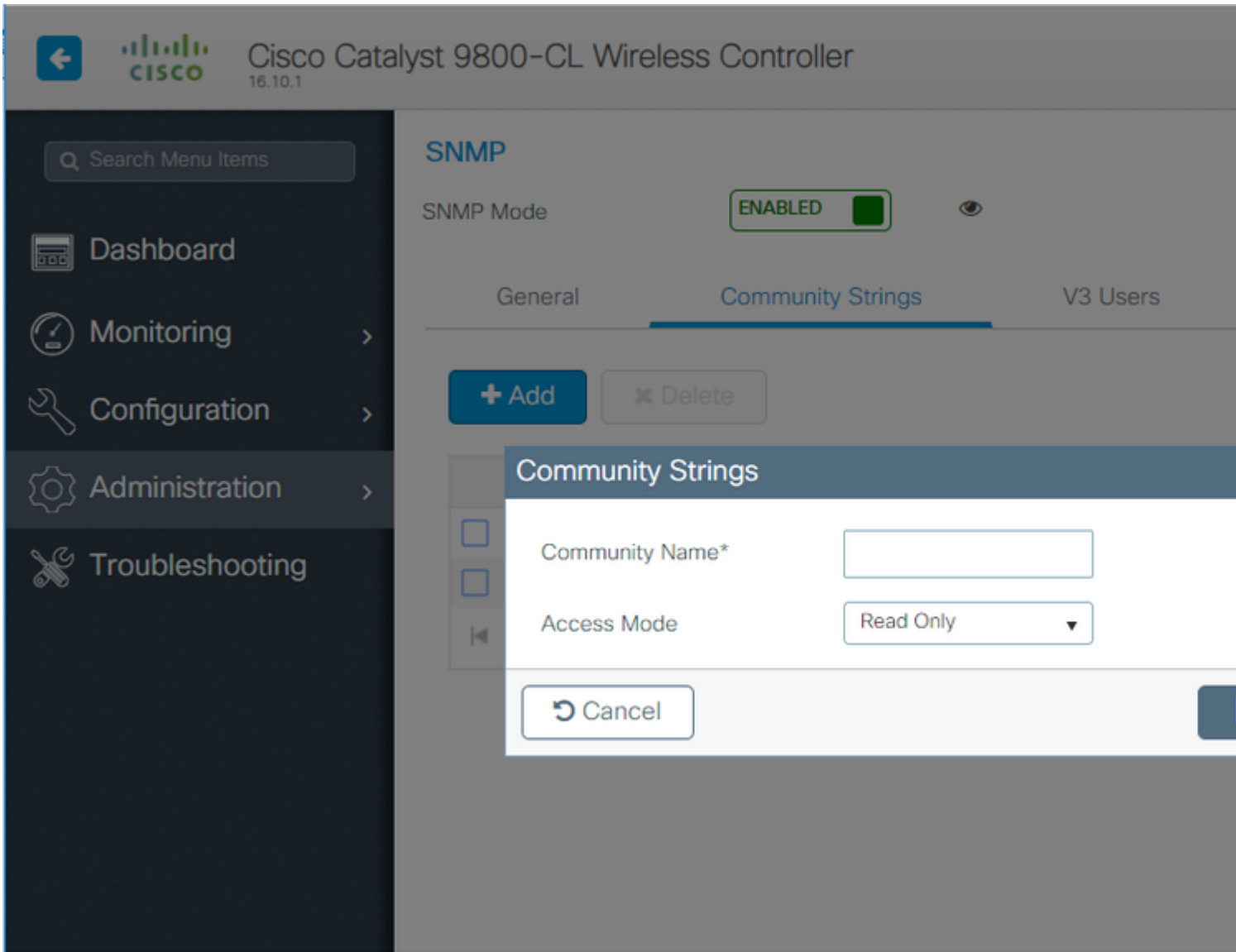
Available (82)

aaa_server	→
adslline	→
alarms	→
atm	→
auth-framework	→

Enabled (0)

Enable All

Paso 2. Haga clic en **Community Strings** y crear un nombre de comunidad de sólo lectura y de lectura y escritura.



CLI:

```
(config)#snmp-server community <snmpv2-community-name>  
(optional)(config)# snmp-server location <site-location>  
(optional)(config)# snmp-server contact <contact-number>
```

## Configuración de SNMPv3 en el WLC Cat 9800

GUI:

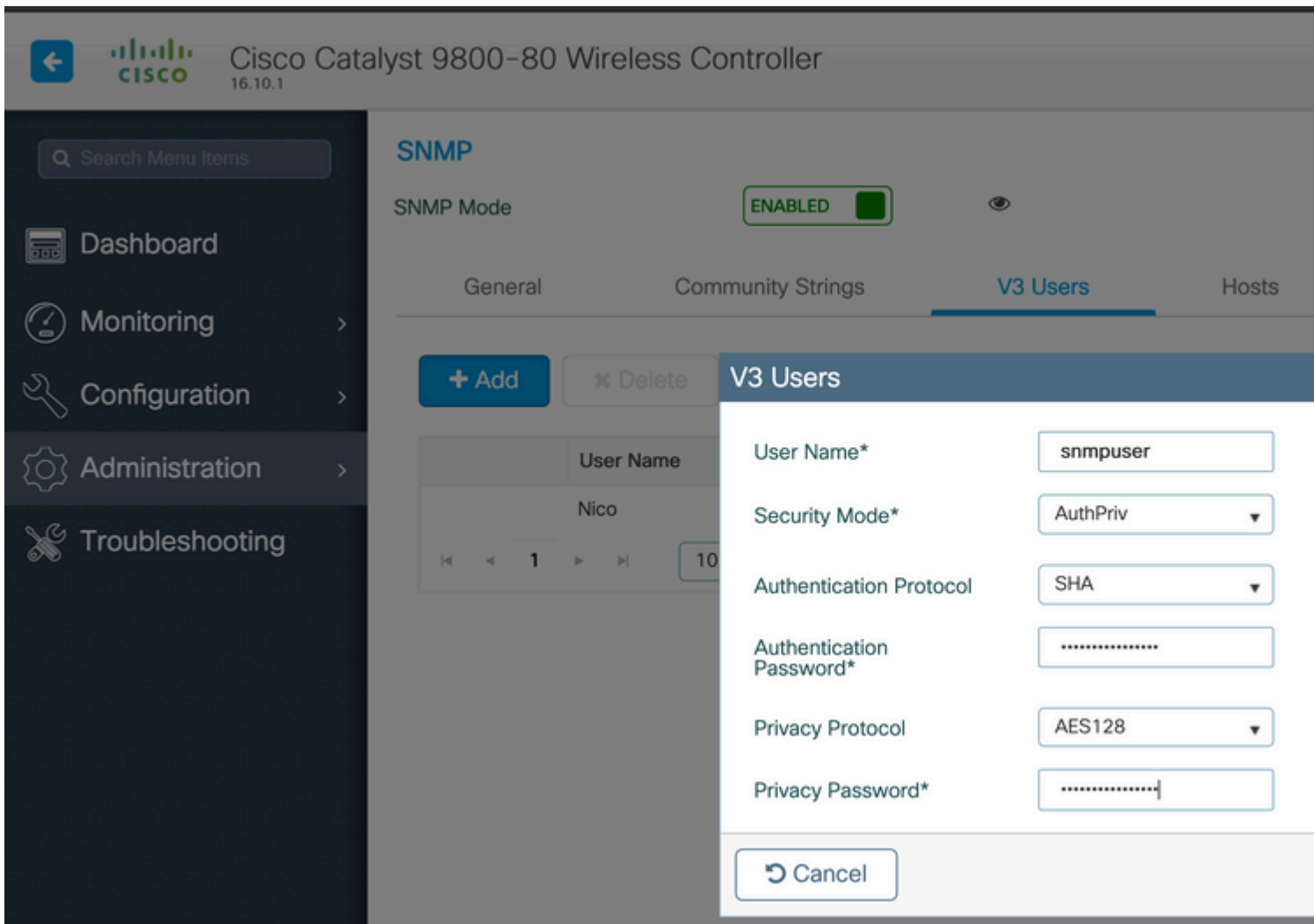
---

**Nota:** a partir de la versión 17.1 de Cisco IOS XE, la interfaz de usuario web solo permite crear usuarios v3 de solo lectura. Debe ejecutar el procedimiento CLI para crear un usuario v3 de lectura y escritura.

---

CLI:

Haga clic en **v3 users** y crear un usuario. Elegir **authPriv**, **SHA** y **AES** protocols y elija contraseñas largas. **MD5** y **DES/3DES** son protocolos inseguros y, aunque siguen siendo una opción en el 9800, no deben seleccionarse y ya no están completamente probados.



---

**Nota:** La configuración de usuario SNMPv3 no se refleja en la configuración en ejecución. Sólo se ve la configuración de grupo SNMPv3.

---

CLI:

```
(config)#snmp-server view primeview iso included
(config)#snmp-server group <v3-group-name> v3 auth write primeview
(config)#snmp-server user <v3username> <v3-group-name> v3 auth {md5 | sha} <AUTHPASSWORD> priv {3des | a
```

```
9800#show snmp user
```

```
User name: Nico
Engine ID: 800000090300706D1535998C
storage-type: nonvolatile active
Authentication Protocol: SHA
```

Privacy Protocol: AES128  
Group-name: SnmpAuthPrivGroup

## Configuración de Netconf en el WLC Cat 9800

GUI (a partir del 16.11):

Desplácese hasta **Administration > HTTP/HTTPS/Netconf**.

**Administration** ▾ > **Management** ▾ > **HTTP/HTTPS/Netconf**

### HTTP/HTTPS Access Configuration

HTTP Access

ENABLED

HTTP Port

80

HTTPS Access

ENABLED

HTTPS Port

443

Personal Identity  
Verification

DISABLED

### HTTP Trust Point Configuration

Enable Trust Point

DISABLED

### Netconf Yang Configuration

Status

ENABLED

SSH Port

830

CLI:

```
(config)#netconf-yang
```

---

**Precaución:** si aaa new-model está habilitado en C9800, también debe configurar:

(config)#aaa authorization exec default <local or radius/tacacs group>

(config)#aaa authentication login default <local or radius/tacacs group>

Netconf en C9800 utiliza el método predeterminado (y no puede cambiarlo) tanto para el login de autenticación aaa como para aaa authorization exec. En caso de que desee definir un método diferente para las conexiones SSH, puede hacerlo bajo el `line vty` línea de comandos. Netconf sigue utilizando los métodos predeterminados.

---

**Precaución:** la infraestructura Prime, al agregar un controlador 9800 a su inventario, sobrescribe los métodos predeterminados de autenticación de aaa y los métodos predeterminados de exec de autorización de aaa que configuró y los señala a la autenticación local solamente en caso de que Netconf no esté ya habilitado en el WLC. Si Prime Infrastructure puede iniciar sesión con Netconf, no cambia la configuración. Esto significa que, si estaba utilizando TACACS, perderá el acceso CLI después de agregar el 9800 a Prime. Puede revertir esos comandos de configuración después y hacer que apunten a TACACS si esa es su preferencia.

---

## Configuración (Prime Infrastructure 3.5 y posterior)

Paso 1. Capture la dirección IP de administración inalámbrica configurada en el WLC de Catalyst 9800.

GUI:

Desplácese hasta **Configuration > Interface: Wireless**.



Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Interface

Logical

Ethernet

Wireless

Layer2

VLAN

VTP

Radio Configurations

CleanAir

High Throughput

CLI:

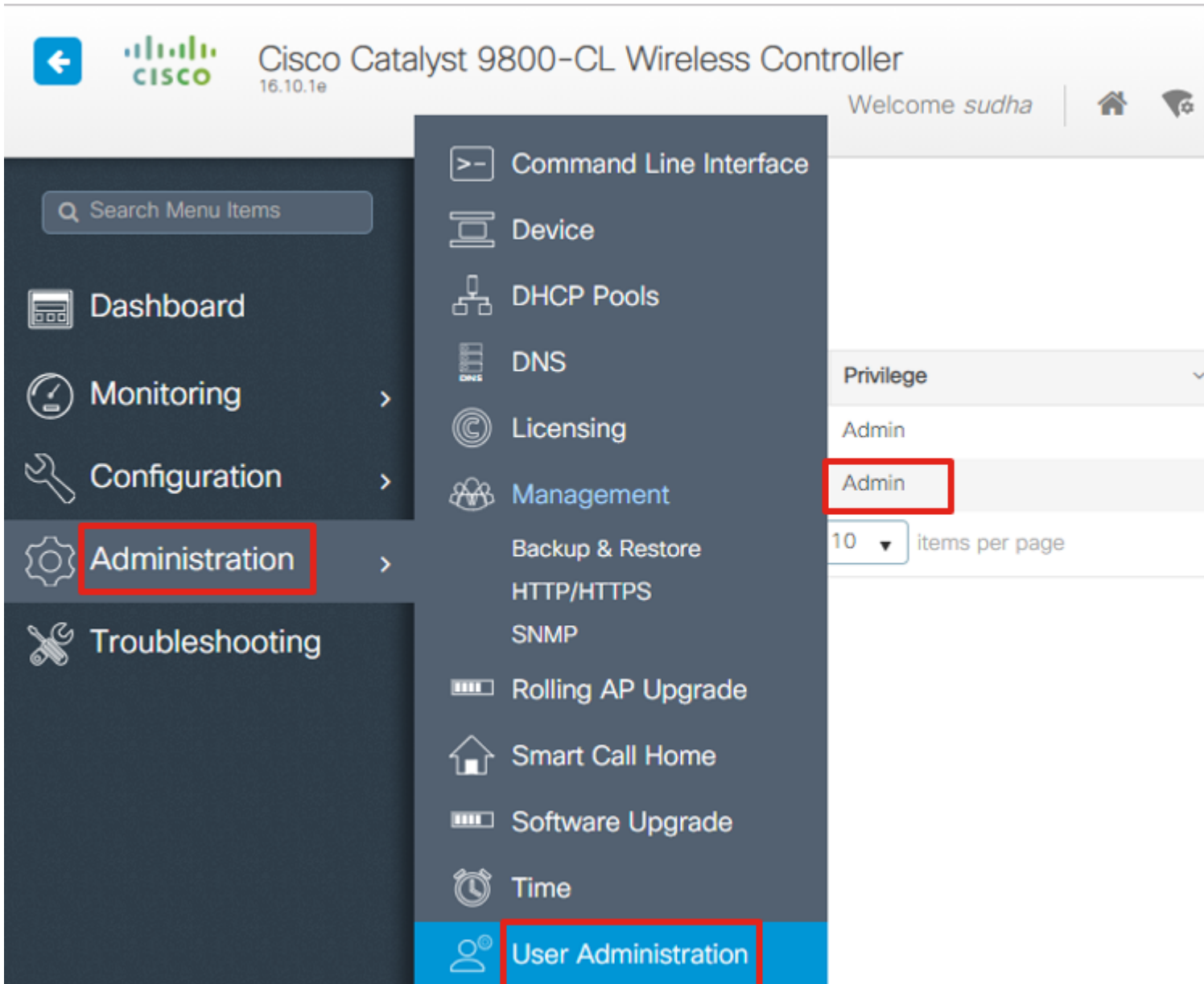
```
# show wireless interface summary
```

Paso 2. Capture las credenciales de privilegio de 15 usuarios y habilite la contraseña.

GUI:

Desplácese hasta **Administration > User Administration**.





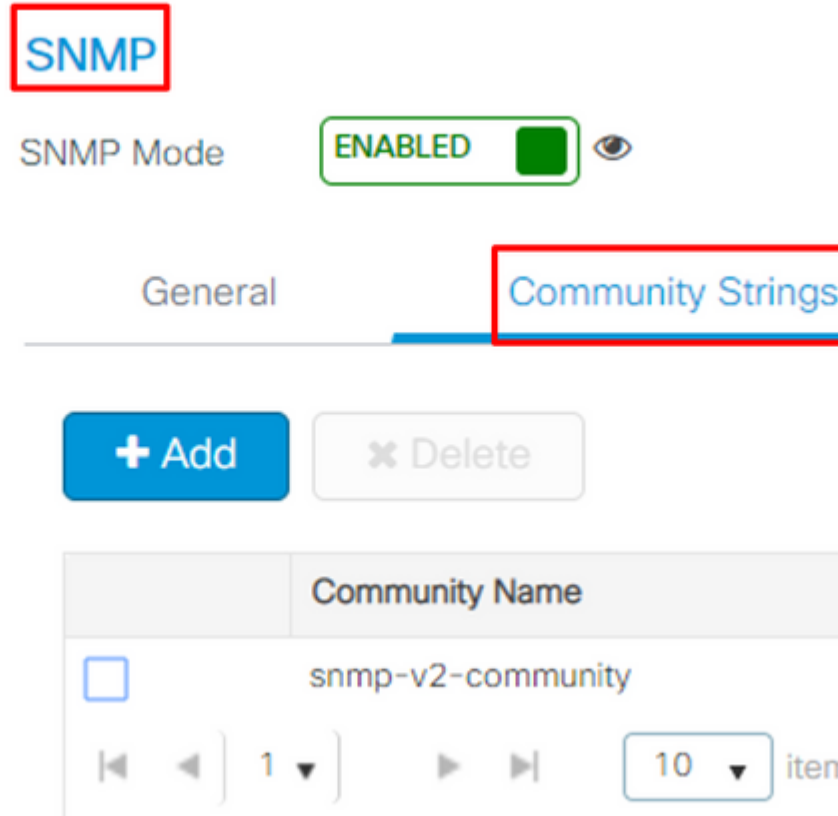
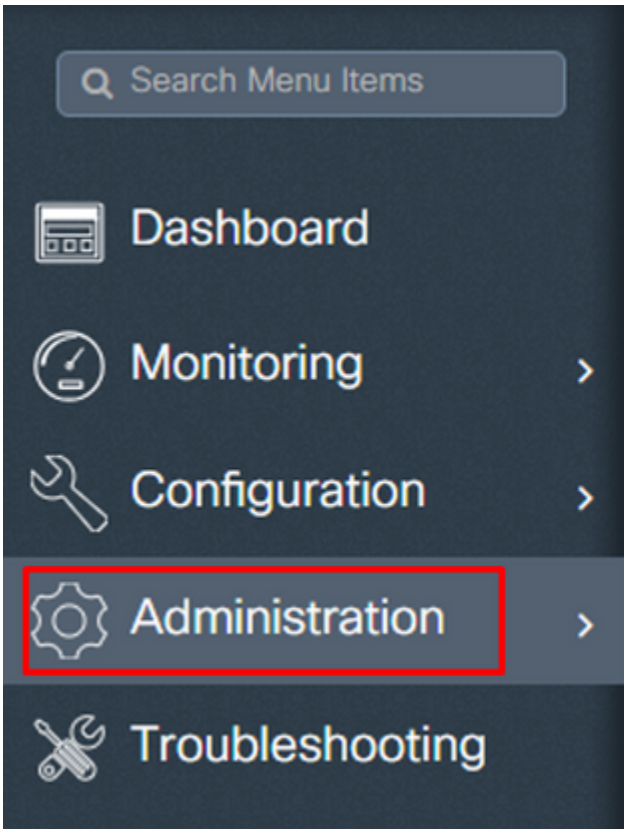
CLI:

```
# show run | inc username  
# show run | inc enable
```

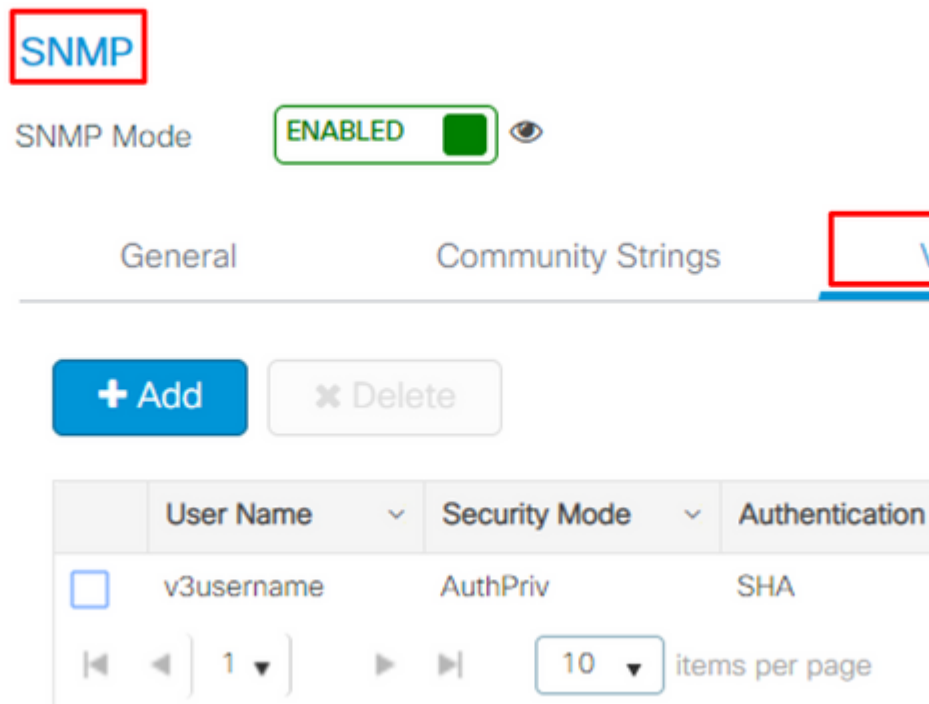
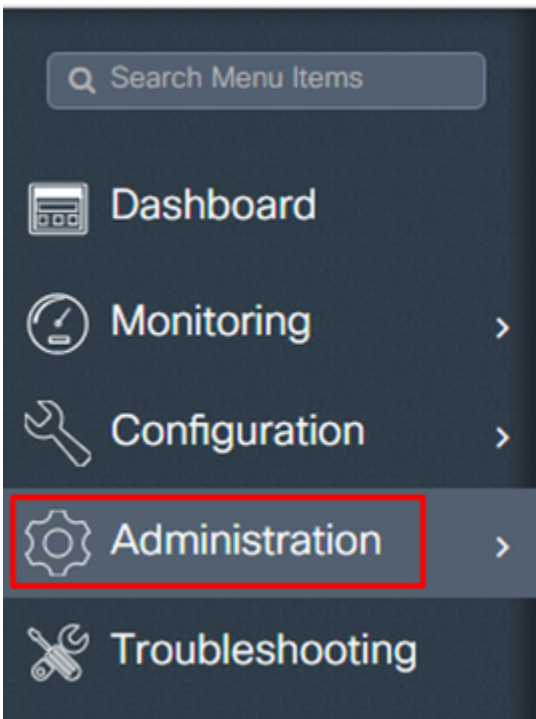
Paso 3. Obtenga las cadenas de comunidad SNMPv2 y/o el usuario SNMPv3 según corresponda.

GUI:

Para SNMPv2, vaya a **Administration > SNMP > Community Strings**.



Para SNMPv3, vaya a Administration > SNMP > V3 Users.

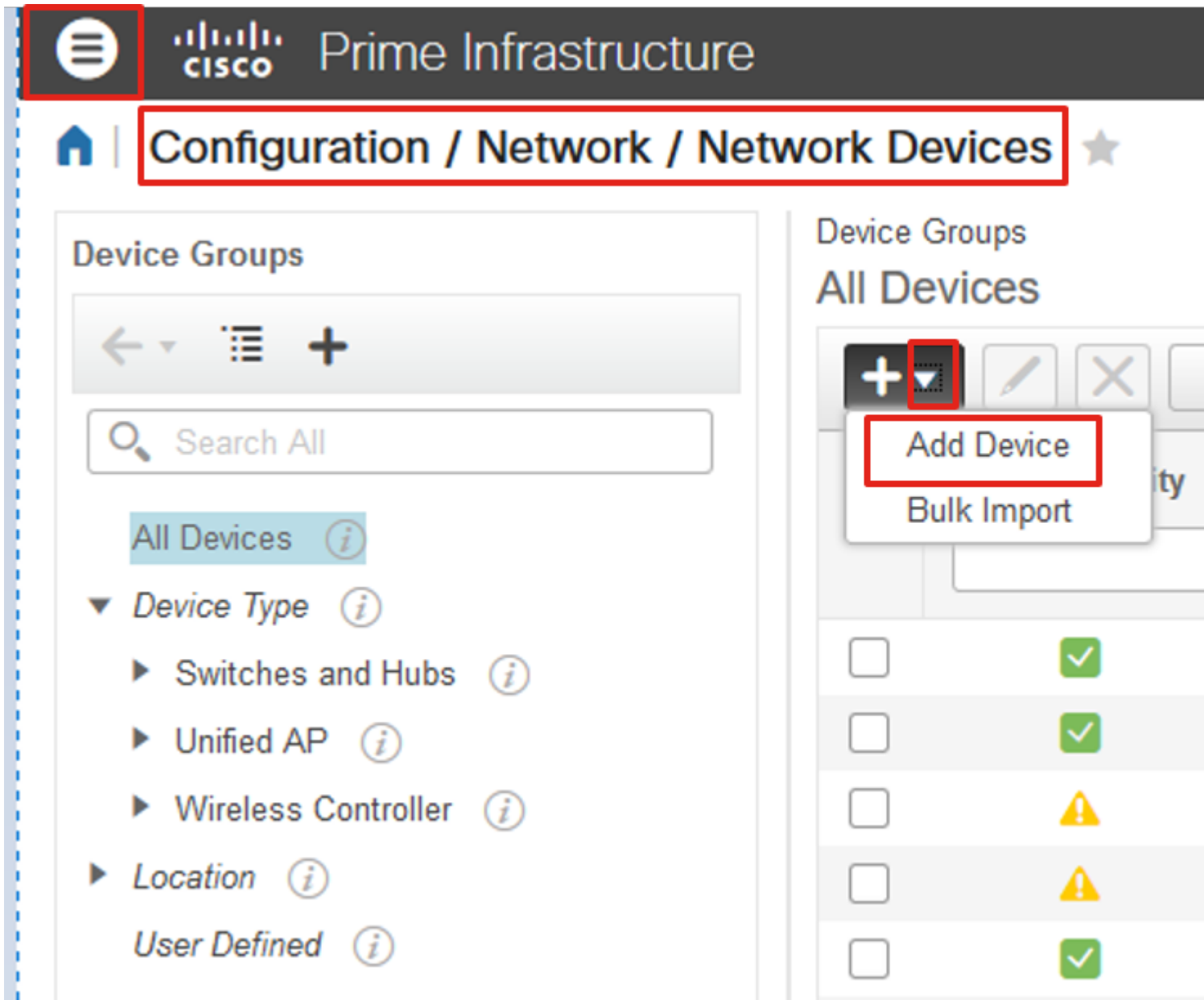


CLI:

For SNMPv2 community strings  
# show run | sec snmp

For SNMPv3 user  
# show user

Paso 4. En la GUI de Prime Infrastructure, vaya a **Configuration > Network: Network Devices**, haga clic en el menú desplegable situado junto a + y elija **Add Device**.



Paso 5. En el **Add Device** , introduzca la dirección ip de la interfaz en 9800 que se utiliza para establecer la comunicación con Prime Infrastructure.

## Add Device

**\* General**

\* SNMP

Telnet/SSH

HTTP/HTTPS

Civic Location

### \* General Parameters

IP Address

DNS Name

License Level

Credential Profile

Device Role

Add to Group

Add

Verify Cre

Paso 6. Desplácese hasta el **SNMP** y proporcionar **SNMPv2 Read-Only and Read-Write Community Strings** configurado en C9800 WLC.

## Add Device

\* General

\* SNMP ✓

Telnet/SSH

HTTP/HTTPS

Civic Location

### \* SNMP Parameters

Version

\* SNMP Retries

\* SNMP Timeout  (Secs)

\* SNMP Port

\* Read Community

\* Confirm Read Community

Write Community

Confirm Write Community

Add

Verify Credentials

Paso 7. Si utiliza SNMPv3, en la lista desplegable seleccione v3y proporcione el nombre de usuario SNMPv3. Desde Auth-Type coincide con el tipo de autenticación previamente configurado y con el Privacy Type seleccione el método de encriptación configurado en el WLC C9800.

## Add Device

\* General

\* SNMP ✓

Telnet/SSH

HTTP/HTTPS

Civic Location

### \* SNMP Parameters

Version

\* SNMP Retries

\* SNMP Timeout

\* SNMP Port

\* Username

Mode

Auth. Type

Auth. Password

Privacy Type

Privacy Password

Add

Verify Credentials

Paso 8. Desplácese hasta **Telnet/SSH** ficha de Add Device, proporcione el nombre de usuario y la contraseña de Privilege 15 junto con Enable Password (Activar contraseña). Haga clic en **Verify Credentials** para garantizar que las credenciales de CLI y SNMP funcionan correctamente. Haga clic en **Add**.

## Add Device

\* General

\* SNMP ✓

**Telnet/SSH ✓**

HTTP/HTTPS

Civic Location



### Telnet/SSH Parameters

Protocol

\* CLI Port

\* Timeout

Username

Password

Confirm Password

Enable Password

Confirm Enable Password

\* Note: Not providing Telnet/SSH credentials may result in partial collection of i

**Add**

**Verify Credential**

## Verificación

### Verificar estado de telemetría

Paso 1. Verifique que Netconf esté habilitado en C9800.

```
#show run | inc netconf  
netconf-yang
```

Si no está presente, ingrese la sección 'NETCONF configuration on the Cat 9800 WLC'.

Paso 2. Verifique la conexión de telemetría a Prime desde el C9800.

```
#show telemetry internal connection  
Telemetry connection
```

```
Address Port Transport State Profile
```

-----  
x.x.x.x 20828 cntp-tcp Active

---

**Nota:** x.x.x.x es la dirección IP de Prime Infrastructure y el estado debe ser Active. Si el estado no es Activo, consulte la sección Resolución de problemas.

---

En 17.9, debe utilizar un comando ligeramente diferente:

```
9800-17-9-2#show telemetry connection all  
Telemetry connections
```

Index	Peer Address	Port	VRF	Source Address	State	State Description
0	10.48.39.25	25103	0	10.48.39.228	Active	Connection up

```
9800-17-9-2#
```

Paso 3. En Prime Infrastructure, vaya a **Inventory > Network Devices > Device Type: Wireless Controller**.

Device Groups / Device Type / [Wireless Controller](#)  
Cisco Catalyst 9800 Series Wireless Controllers

Reachability	Admin State	IP ...	Device Type	AP Discove...	Telemetry ...	Software Ver...	Inventory C
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco Catalyst 9800-80 ...	Completed	Success	16.10.1	12-MAR-19

Paso 4. Para ver los detalles de la conexión de telemetría a Prime Infrastructure, ejecute lo siguiente:

```
#show telemetry internal protocol cntp-tcp manager x.x.x.x 20828
```

```
Telemetry protocol manager stats:
```

```
Con str           : x.x.x.x:20828::  
Sockfd           : 79  
Protocol         : cntp-tcp  
State            : CNDP_STATE_CONNECTED  
Table id        : 0  
Wait Mask       :  
Connection Retries : 0  
Send Retries     : 0  
Pending events   : 0  
Source ip       : <9800_IP_ADD>  
Bytes Sent      : 1540271694  
Msgs Sent       : 1296530  
Msgs Received   : 0
```



Paso 5. Verifique el estado de suscripción de telemetría de C9800 y el hecho de que se muestre como 'Válido'.

```
#show telemetry ietf subscription configured
Telemetry subscription brief
```

```
ID Type State Filter type
-----
68060586 Configured Valid transform-na
98468759 Configured Valid tdl-uri
520450489 Configured Valid transform-na
551293206 Configured Valid transform-na
657148953 Configured Valid transform-na
824003685 Configured Valid transform-na
996216912 Configured Valid transform-na
1072751042 Configured Valid tdl-uri
1183166899 Configured Valid transform-na
1516559804 Configured Valid transform-na
1944559252 Configured Valid transform-na
2006694178 Configured Valid transform-na
```

Paso 6: Las estadísticas de suscripción se pueden ver por ID de suscripción o para todas las suscripciones que utilicen:

```
#show telemetry internal subscription { all | id } stats
Telemetry subscription stats:
```

Subscription ID	Connection Info	Msgs Sent	Msgs Drop	Records Sent
865925973	x.x.x.x:20828::	2	0	2
634673555	x.x.x.x:20828::	0	0	0
538584704	x.x.x.x:20828::	0	0	0
1649750869	x.x.x.x:20828::	1	0	2
750608483	x.x.x.x:20828::	10	0	10
129958638	x.x.x.x:20828::	10	0	10
1050262948	x.x.x.x:20828::	1369	0	1369
209286788	x.x.x.x:20828::	15	0	15
1040991478	x.x.x.x:20828::	0	0	0
1775678906	x.x.x.x:20828::	2888	0	2889
1613608097	x.x.x.x:20828::	6	0	6
1202853917	x.x.x.x:20828::	99	0	99
1331436193	x.x.x.x:20828::	743	0	743
1988797793	x.x.x.x:20828::	0	0	0
1885346452	x.x.x.x:20828::	0	0	0
163905892	x.x.x.x:20828::	1668	0	1668
1252125139	x.x.x.x:20828::	13764	0	13764
2078345366	x.x.x.x:20828::	13764	0	13764
239168021	x.x.x.x:20828::	1668	0	1668
373185515	x.x.x.x:20828::	9012	0	9012
635732050	x.x.x.x:20828::	7284	0	7284
1275999538	x.x.x.x:20828::	1236	0	1236
825464779	x.x.x.x:20828::	1225711	0	1225780
169050560	x.x.x.x:20828::	0	0	0

229901535	x.x.x.x:20828::	372	0	372
592451065	x.x.x.x:20828::	8	0	8
2130768585	x.x.x.x:20828::	0	0	0

## Troubleshoot

### Resolución de problemas en Prime Infrastructure

- Lo primero que se debe comprobar en la infraestructura Prime es la dirección IP y las interfaces. Prime Infrastructure no admite el modo de doble hogar y no escucha la telemetría de su segundo puerto.
- La dirección IP del WLC que usted agrega en Prime Infrastructure debe ser la dirección IP utilizada como la 'interfaz de administración inalámbrica'. La dirección IP de Prime Infrastructure debe ser accesible desde la interfaz de gestión inalámbrica del controlador.
- Si utiliza el puerto de servicio (gig0/0 en los dispositivos) para la detección, el WLC y los AP se muestran en el estado administrado en el inventario pero la telemetría para el WLC y los puntos de acceso asociados no funciona.
- Si ve que el estado de la telemetría es un 'éxito' en Prime Infrastructure pero el conteo de AP es 0, podría ser que Prime Infrastructure puede alcanzar el WLC en el puerto 830 pero el controlador no puede alcanzar de nuevo la Prime Infrastructure en el puerto 20830.

Para cualquier problema de SNMP o de configuración del dispositivo, recopile estos registros de Prime Infrastructure:

```
cd /opt/CSC0lumos/logs/
```

```
[root@prime-tdl logs]# ncs-0-0.log
```

```
Tdl.logs
```

Para problemas de telemetría/coral, lo primero es comprobar el estado del coral:

```
shell
```

```
cd /opt/CSC0lumos/coralinstances/coral2/coral/bin
```

```
./coral version 1
```

```
./coral status 1
```

```
./coral stats 1
```

Si todo está bien, recopile estos registros de la carpeta prime coral logs.

---

**Nota:** Dependiendo de la versión de Prime Infrastructure y de la cantidad de versión de Cisco IOS XE que admita, puede haber varias instancias de Coral en Prime Infrastructure. Consulte las notas de la versión para obtener más información, como:

[https://www.cisco.com/c/en/us/td/docs/net\\_mgmt/prime/infrastructure/3-7/release/notes/bk\\_Cisco\\_Prime\\_Infrastructure\\_3\\_7\\_0\\_Release\\_Notes.html](https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/release/notes/bk_Cisco_Prime_Infrastructure_3_7_0_Release_Notes.html)

---

Paso 1.

```
cd /opt/CSColumos/coral/bin/
[root@prime-tdl bin]# ./coral attach 1
Attached to Coral instance 1 [pid=8511]
Coral-1#cd /tmp/rp/trace/
Coral-1#ls
Collect the 'Prime_TDL_collector_R0-*' logs
```

```
Coral-1# cd /tmp/rp/trace/
Coral-1# btdecode P* > coralbtlog.txt
Coral-1# cat coralbtlog.txt
```

Estos registros también se pueden encontrar en este directorio:

- \* Los archivos de seguimiento descodificados están disponibles en la ruta de acceso `/opt/CSColumos/coralinstances/coral2/coral/run/1/storage/harddisk`
- \* `ade# cd /opt/CSColumos/coralinstances/coral2/coral/run/1/storage/harddisk`
- \* `ade# cp coraltrace.txt /localdisk/defaultRepo`

Paso 2. Para habilitar Coral en modo de depuración, el nivel de depuración debe establecerse en `debug.conf` archivo.

Desde el interior del recipiente:

```
echo "rp:0:0:tdlcold:-e BINOS_BTRACE_LEVEL=DEBUG;" > /harddisk/debug.conf
```

O en Prime 3.8, el servicio de Coral se puede reiniciar fuera del contenedor mediante:

```
"sudo /opt/CSC0lumos/coralinstances/coral2/coral/bin/coral restart 1"
```

Si el reinicio no ayuda, se pueden utilizar para limpiar la instancia de coral y comenzar sin problemas:

```
sudo /opt/CSC0lumos/coralinstances/coral2/coral/bin/coral stop 1
```

```
sudo /opt/CSC0lumos/coralinstances/coral2/coral/bin/coral purge 1
```

```
sudo /opt/CSC0lumos/coralinstances/coral2/coral/bin/coral start 1
```

Reinicie Coral, esto es obligatorio. Puede dejar la instancia de coral si escribe 'Exit' y, a continuación:

```
./coral/bin/coral restart 1
```

---

**Nota:** En Prime 3.8, el servicio Coral se puede reiniciar fuera del contenedor mediante 'sudo /opt/CSC0lumos/coralinstance/coral2/coral/bin/coral restart 1'

---

Si necesita descodificar los archivos de registro de Coral, puede descodificarlos dentro del contenedor de Coral con:

```
btdecode Prime_TDL_collector_*.bin
```

---

**Nota:** Después de habilitar el nivel de depuración de Coral, es obligatorio reiniciar Coral.

---

## Resolución de problemas en Catalyst 9800 WLC

Para monitorear la configuración enviada por Prime Infra al WLC C9800, puede ejecutar un applet EEM.

```
#config terminal
#event manager applet catchall
#event cli pattern ".*" sync no skip no
#action 1 syslog msg "$_cli_msg"
```

## Eliminar toda la suscripción de telemetría de la configuración del WLC

Puede haber ocasiones en que usted desea desconfigurar todas las suscripciones de telemetría configuradas

en el WLC. Esto se puede hacer simplemente con estos comandos:

```
WLC#term shell
WLC#function removeall() {
for id in `sh run | grep telemetry | cut -f4 -d' '`
do
conf t
no telemetry ietf subscription $id
exit
done
}
WLC#removeall
```

Para activar seguimientos:

```
# debug netconf-yang level debug
```

Para verificar:

```
WLC#show platform software trace level mdt-pubd chassis active R0 | inc Debug
pubd                                     Debug
WLC#show platform software trace level ndbman chassis active R0 | inc Debug
ndbmand                                  Debug
```

Para ver los resultados de seguimiento:

```
show platform software trace message mdt-pubd chassis active R0
show platform software trace message ndbman chassis active R0
```

## Comprobar ID de suscripción para información de AP

Haga clic en **DB Query**. Vaya a [tohttps://<Prime IP>/webacs/ncsDiag.do](https://<Prime IP>/webacs/ncsDiag.do).

Elegir \*desde `ewlcSubscription` donde `OWNINGENTITYID` como `'%Controller_IP'` y

```
CLASSNAME='UnifiedApp'.
```

Desde el WLC:

Verifique que el ID de suscripción esté enviando información y que no haya caídas en los contadores cntp.

```
show tel int sub all stats  
show telemetry internal protocol cntp-tcp connector counters drop  
show telemetry internal protocol cntp-tcp connector counters queue  
show telemetry internal protocol cntp-tcp connector counters rate  
show telemetry internal protocol cntp-tcp connector counters sub-rate  
show telemetry internal protocol cntp-tcp connector counters reset
```

---

**Nota:** El WLC 9800 soporta 100 suscripciones de telemetría antes de 17.6 y hasta 128 suscripciones después de 17.6 (como la reciente versión del centro DNA puede utilizar más de 100 suscripciones).

---

## Migración de PI a DNA-Center

El C9800 no se puede gestionar simultáneamente mediante PI y DNA Center de forma de lectura y escritura (por ejemplo, si DNAC solo garantiza la seguridad y utiliza Prime Infra para enviar las plantillas, está bien). Por lo tanto, si existe un plan para migrar a DNAC como solución de gestión de red, el C9800 debe eliminarse de Prime Infrastructure antes de agregarlo a DNA Center. Cuando se elimina/elimina C9800 de PI 3.5, toda la configuración que se enviaba a C9800 en el momento del inventario por PI no se deshace y es necesario eliminarla manualmente del sistema. Específicamente, los canales de suscripción establecidos para que el WLC C9800 publique datos de telemetría de transmisión no se eliminan.

Para identificar esta configuración específica:

```
#show run | sec telemetry
```

Para quitar esta configuración, ejecute el **no** forma del comando:

```
(config) # no telemetry ietf subscription <Subscription-Id>  
Repeat this CLI to remove each of the subscription identifiers.
```

```
(config) # no telemetry transform <Transform-Name>  
Repeat this CLI to remove each of the transform names
```

---

**Nota:** Si gestiona el controlador 9800 con DNAC y Prime Infrastructure, el cumplimiento de las normas de inventario de DNAC fallará debido a la gestión de Prime.

---

En las versiones recientes, tanto Prime Infrastructure como DNAC utilizarán demasiadas suscripciones de telemetría para el WLC para que ambos servidores administren el 9800 simultáneamente. Por lo tanto, no puede gestionar el 9800 con DNAC y Prime Infrastructure, y dispone de telemetría y estadísticas en funcionamiento. Por lo tanto, la migración de PI a DNAC debe realizarse lo más rápido posible, ya que DNAC no puede tener datos de telemetría del 9800 mientras Prime Infrastructure esté gestionando el controlador 9800.

## 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).