

Gestione dei controller wireless Catalyst serie 9800 con Prime Infrastructure con SNMP V2 e V3 e NetCONF

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Porte usate](#)

[Configurazione SNMPv2 su Cat 9800 WLC](#)

[Configurazione SNMPv3 su Cat 9800 WLC](#)

[Configurazione Netconf sul Cat 9800 WLC](#)

[Configurazione \(Prime Infrastructure 3.5 e versioni successive\)](#)

[Verifica](#)

[Verifica stato telemetria](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi relativi a Prime Infrastructure](#)

[Risoluzione dei problemi su Catalyst 9800 WLC](#)

[Elimina tutta la sottoscrizione di telemetria dalla configurazione WLC](#)

[Verifica ID sottoscrizione per informazioni AP](#)

[Migrazione da PI a DNA-Center](#)

Introduzione

Questo documento descrive come integrare i controller wireless Catalyst serie 9800 (C9800 WLC) con Prime Infrastructure (3.x).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- C9800 WLC
- Prime Infrastructure (PI) versione 3.5
- Protocollo SNMP (Simple Network Management Protocol)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.



Nota: Prime Infra 3.8 supporta solo WLC 17,x 9800. I client non vengono visualizzati su Prime Infrastructure se si tenta di gestire un WLC 16.12 con Prime Infra 3.8.

Configurazione

Per configurare, gestire e monitorare i controller LAN wireless Catalyst serie 9800, Prime Infrastructure deve essere in grado di accedere a C9800 tramite CLI, SNMP e Netconf. Quando si aggiunge C9800 a Prime Infrastructure, è necessario specificare le credenziali telnet/SSH, nonché la stringa della community SNMP, la versione e così via. PI utilizza queste informazioni per verificare la raggiungibilità e per inventariare il WLC C9800. Utilizza inoltre il protocollo SNMP per eseguire il push dei modelli di configurazione e supporta trap per gli eventi dei client e dei punti di accesso. Tuttavia, per consentire a PI di raccogliere le statistiche AP e client, Netconf viene utilizzato. Netconf non è abilitato per impostazione predefinita sul WLC C9800 e deve essere configurato manualmente tramite CLI nella versione 16.10.1 (GUI disponibile nella versione 16.11.1).


Porte usate


La comunicazione tra C9800 e Prime Infrastructure utilizza porte diverse.

- Tutte le configurazioni e i modelli disponibili in Prime Infra vengono distribuiti tramite SNMP e CLI. viene utilizzata la porta UDP 161.
- I dati operativi per il WLC C9800 si ottengono tramite SNMP. Viene utilizzata la porta UDP 162.
- I dati operativi dei client e dei punti di accesso sfruttano la telemetria in streaming.

Prime Infrastructure per WLC: porta TCP 830 - Utilizzata da Prime Infra per trasferire la configurazione della telemetria ai dispositivi 9800 (usando Netconf).

WLC su Prime Infrastructure: porta TCP 20828 (per Cisco® IOS XE 16.10 e 16.11) o 20830 (per Cisco IOS XE 16.12,17.x e versioni successive).

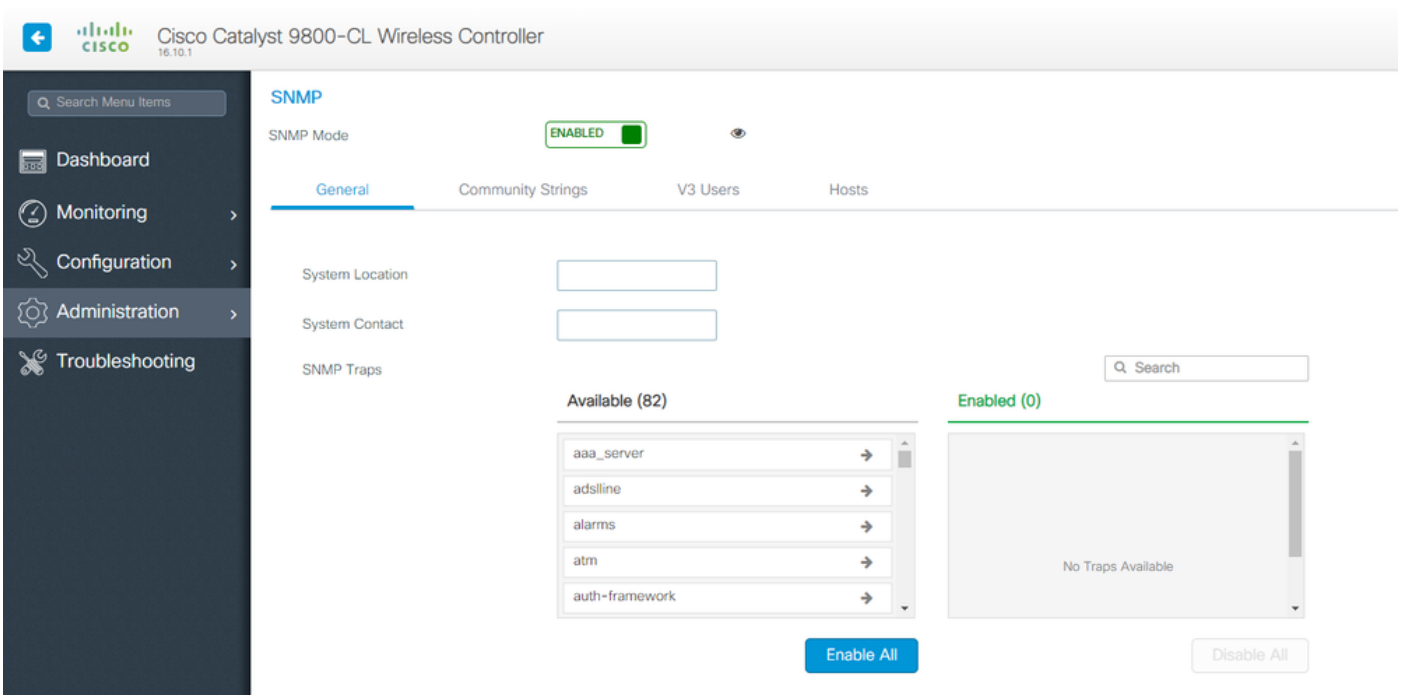
 Nota: i pacchetti keepalive vengono inviati ogni 5 secondi anche in assenza di dati di telemetria da segnalare.

 Nota: se esiste un firewall tra Prime Infrastructure e C9800, aprire queste porte per stabilire la comunicazione.

Configurazione SNMPv2 su Cat 9800 WLC

GUI:

Passaggio 1. Passa a **Administration > SNMP > Slide to Enable SNMP**.



The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller GUI. The main header shows the Cisco logo and the device name 'Cisco Catalyst 9800-CL Wireless Controller' with IP '16.10.1'. A left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration (selected), and Troubleshooting. The main content area is titled 'SNMP' and features a sub-header 'SNMP Mode' with a green 'ENABLED' toggle and an eye icon. Below this are four tabs: 'General' (selected), 'Community Strings', 'V3 Users', and 'Hosts'. The 'General' tab contains input fields for 'System Location' and 'System Contact'. The 'SNMP Traps' section is divided into two panes: 'Available (82)' and 'Enabled (0)'. The 'Available' pane lists traps such as 'aaa_server', 'adslline', 'alarms', 'atm', and 'auth-framework', each with a right-pointing arrow. The 'Enabled' pane is empty and shows 'No Traps Available'. A search bar is located above the traps. At the bottom, there are 'Enable All' and 'Disable All' buttons.

Passaggio 2. Fare clic su **Community Strings** e creare un nome di community di sola lettura e di lettura/scrittura.


The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The main page is titled 'SNMP' and has tabs for 'General', 'Community Strings', 'V3 Users', and 'Hosts'. The 'Community Strings' tab is active. A modal window titled 'Community Strings' is open, showing a form with 'Community Name*' and 'Access Mode' (set to 'Read Only') fields. There are 'Cancel' and 'Save & Apply to Device' buttons at the bottom of the modal. The background shows the 'SNMP Mode' is 'ENABLED' and a search bar at the top left.

CLI:

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

Configurazione SNMPv3 su Cat 9800 WLC

GUI:

 Nota: a partire dalla versione 17.1 di Cisco IOS XE, l'interfaccia utente Web consente solo di creare utenti v3 di sola lettura. Per creare un utente v3 in lettura/scrittura, è necessario eseguire la procedura CLI.


CLI:

Fare clic su **V3 users** e creare un utente. Scegli **authPriv**, **SHA** e **AES protocols** e scegliere password lunghe. **MD5** e **DES/3DES** sono protocolli non sicuri e, sebbene siano ancora un'opzione del 9800, non devono essere selezionati e non sono più completamente testati.

The screenshot shows the Cisco Catalyst 9800-80 Wireless Controller GUI. The main page is titled 'SNMP' and has tabs for 'General', 'Community Strings', 'V3 Users', and 'Hosts'. The 'V3 Users' tab is active, and a configuration window is open. The window contains the following fields:

- User Name*: snmpuser
- Security Mode*: AuthPriv
- Authentication Protocol: SHA
- Authentication Password*: [Redacted]
- Privacy Protocol: AES128
- Privacy Password*: [Redacted]

Buttons at the bottom of the window include 'Cancel' and 'Save & Apply to Device'.

 Nota: la configurazione utente SNMPv3 non si riflette sulla configurazione in esecuzione. Viene visualizzata solo la configurazione del gruppo 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 |
```

```
9800#show snmp user
```

```
User name: Nico
Engine ID: 800000090300706D1535998C
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: SnmpAuthPrivGroup
```

Configurazione Netconf sul Cat 9800 WLC

Interfaccia grafica (a partire da 16,11):

Passa a **Administration > 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
```

 **Attenzione:** se su C9800 è abilitato un nuovo modello, è necessario configurare anche:
(config)#aaa authorization exec default <gruppo locale o radius/tacacs>
(config)#aaa authentication login default <gruppo locale o radius/tacacs>
Netconf su C9800 utilizza il metodo predefinito (e non può essere modificato) sia per l'accesso con autenticazione aaa che per l'esecuzione con autorizzazione aaa. Per definire un metodo diverso per le connessioni SSH, usare il comando `line vty` riga di comando. Netconf

 continua a utilizzare i metodi predefiniti.

 **Attenzione:** Prime infrastructure, quando si aggiunge un controller 9800 al proprio inventario, sovrascrive l'impostazione predefinita di accesso con autenticazione aaa e i metodi predefiniti di esecuzione delle autorizzazioni aaa configurati e li indirizza all'autenticazione locale solo se Netconf non è già abilitato sul WLC. Se Prime Infrastructure è in grado di eseguire il login con Netconf, la configurazione non viene modificata. Ciò significa che, se si stava utilizzando TACACS, si perde l'accesso dalla CLI dopo aver aggiunto lo switch 9800 a Prime. È possibile ripristinare questi comandi di configurazione in un secondo momento e impostarli in modo che puntino a TACACS, se lo si desidera.

Configurazione (Prime Infrastructure 3.5 e versioni successive)

Passaggio 1. Acquisire l'indirizzo IP di gestione wireless configurato sul WLC di Catalyst 9800.

GUI:

Passa a **Configuration > Interface: Wireless**.



The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller GUI. The top header shows the Cisco logo and the device name 'Cisco Catalyst 9800-CL Wireless Controller' with the IP address '16.10.1e'. The left sidebar contains a search bar and navigation items: 'Dashboard', 'Monitoring', 'Configuration' (highlighted with a red box), 'Administration', and 'Troubleshooting'. The main content area shows a tree view under 'Interface' with sub-items: 'Logical', 'Ethernet', 'Wireless' (highlighted with a blue bar and a red box), 'Layer2', 'VLAN', 'VTP', 'Radio Configurations', 'CleanAir', and 'High Throughput'. The right sidebar shows 'Services' with various options like 'AireOS Config Translator', 'Application Visibility', 'Cloud Services', 'Custom Application', 'IOx', 'Multicast', 'NetFlow', 'Python Sandbox', 'QoS', and 'RA Throttle Policy'.

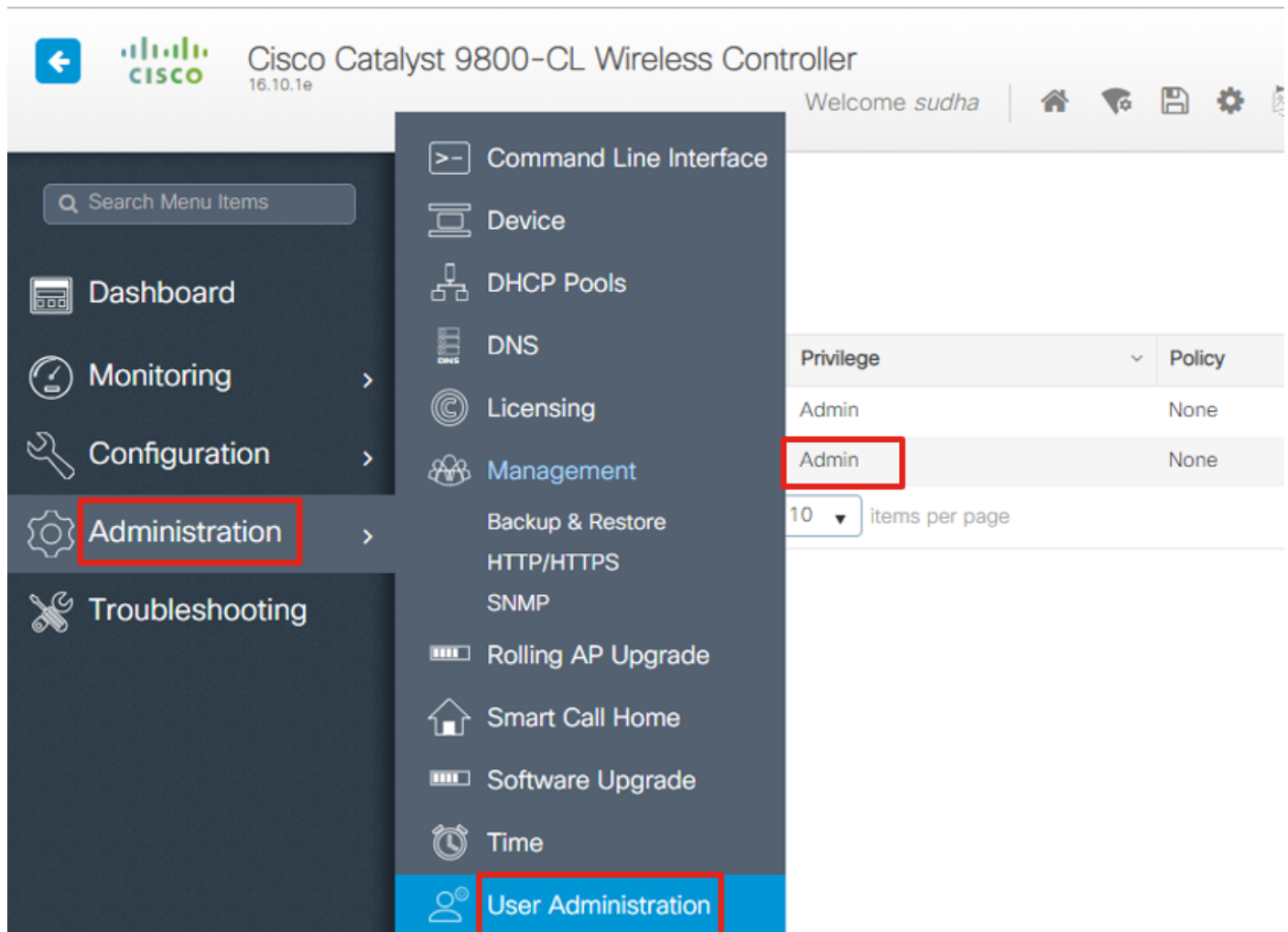
CLI:

```
# show wireless interface summary
```

Passaggio 2. Acquisire le credenziali utente con privilegi 15 e abilitare la password.

GUI:

Passa a **Administration > User Administration**.



CLI:

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

Passaggio 3. Ottenere le stringhe della community SNMPv2 e/o l'utente SNMPv3, a seconda dei casi.

GUI:

Per SNMPv2, passare a **Administration > SNMP > Community Strings**.

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >**
- Troubleshooting

SNMP

SNMP Mode **ENABLED**

General **Community Strings** V3 Users

+ Add

	Community Name	Access Mode
<input type="checkbox"/>	snmp-v2-community	Read Only

10 items per page

Per SNMPv3, passare a **Administration > SNMP > V3 Users**.

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >**
- Troubleshooting

SNMP

SNMP Mode **ENABLED**

General Community Strings **V3 Users** Hosts

+ Add

	User Name	Security Mode	Authentication Protocol	Privacy Protocol
<input type="checkbox"/>	v3username	AuthPriv	SHA	AES128

10 items per page 1 - 1 of 1 items

CLI:

For SNMPv2 community strings
 # show run | sec snmp

For SNMPv3 user
 # show user

Passaggio 4. Dalla GUI di Prime Infrastructure, passare a **Configuration > Network: Network Devices**, fare clic sull'elenco a discesa + e scegliere **Add Device**.

The screenshot shows the Cisco Prime Infrastructure web interface. At the top, the navigation bar includes the Cisco logo and the text "Prime Infrastructure". Below this, the breadcrumb path "Configuration / Network / Network Devices" is highlighted with a red box. On the left side, there is a "Device Groups" sidebar with a search bar and a tree view containing "All Devices", "Device Type" (with sub-items: Switches and Hubs, Unified AP, Wireless Controller), "Location", and "User Defined". The main content area is titled "Device Groups All Devices" and features a table with columns for checkboxes, status icons, and "Admin Status". A dropdown menu is open over the "+" icon, showing "Add Device" and "Bulk Import" options, with "Add Device" highlighted by a red box. The table below shows five rows of device entries, each with a checkbox, a status icon (green checkmark or yellow warning triangle), and the text "Managed".

Passaggio 5. Nella scheda **Add Device** a comparsa, immettere l'indirizzo ip dell'interfaccia su 9800 utilizzato per stabilire la comunicazione 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 Credentials

Cancel

Passaggio 6. Passare alla SNMP e fornire SNMPv2 Read-Only and Read-Write Community Strings configurata su 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

Passaggio 7. Se si utilizza SNMPv3, dall'elenco a discesa scegliere v3e fornire il nome utente SNMPv3. Da Auth-Type corrisponde al tipo di autenticazione configurato in precedenza e da Privacy Type scegliere il metodo di crittografia configurato su C9800 WLC.

Add Device



* General

* SNMP

Telnet/SSH

HTTP/HTTPS

Civic Location

* SNMP Parameters

Version

* SNMP Retries

* SNMP Timeout (Secs)

* SNMP Port

* Username

Mode

Auth. Type

Auth. Password

Privacy Type

Privacy Password

Add

Verify Credentials

Cancel

Passaggio 8. Passa a **Telnet/SSH** scheda di **Add Device**, fornire il nome utente e la password con privilegi 15 insieme all'opzione **Abilita password**. Fare clic su **Verify Credentials** per garantire il corretto funzionamento delle credenziali CLI e SNMP. Quindi fai clic su **Add**.

Add Device



* General

* SNMP ✓

Telnet/SSH ✓

HTTP/HTTPS

Civic Location

Telnet/SSH Parameters

Protocol

* CLI Port

* Timeout (Secs)

Username

Password

Confirm Password

Enable Password ?

Confirm Enable Password

* Note: Not providing Telnet/SSH credentials may result in partial collection of inventory data.

Verifica

Verifica stato telemetria

Passaggio 1. Verificare che Netconf sia abilitato su C9800.

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


Se non è presente, immettere la sezione 'NETCONF configuration on the Cat 9800 WLC'.

Passaggio 2. Verificare la connessione telemetrica a Prime dal 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 è l'indirizzo IP di Prime Infrastructure e lo stato deve essere Active. Se lo stato non è Attivo, consultare la sezione Risoluzione dei problemi.

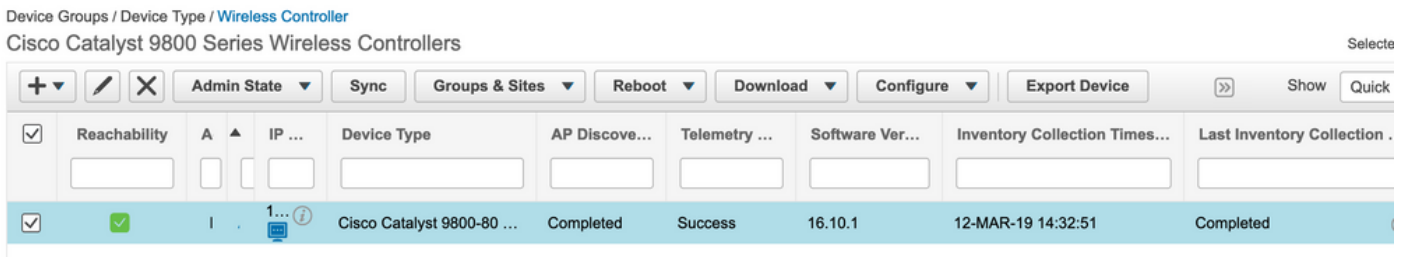
Nella versione 17.9, è necessario utilizzare un comando leggermente diverso:

```
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#
```

Passaggio 3. In Prime Infrastructure, passare a **Inventory > Network Devices > Device Type: Wireless Controller**.



Passaggio 4. Per visualizzare i dettagli della connessione telemetrica a Prime Infrastructure, eseguire quanto segue:

```
#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
```

Passaggio 5. Verificare lo stato della sottoscrizione alla telemetria da C9800 e il fatto che venga visualizzato come 'Valido'.

```
#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
```

Passaggio 6: è possibile visualizzare le statistiche della sottoscrizione per ID sottoscrizione o per tutte le sottoscrizioni che utilizzano:

```
#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

Risoluzione dei problemi

Risoluzione dei problemi relativi a Prime Infrastructure

- Il primo controllo sull'infrastruttura Prime è sull'indirizzo IP e sulle interfacce. Prime Infrastructure non supporta la configurazione dual-home e non è in grado di ascoltare la telemetria sulla seconda porta.
- L'indirizzo IP del WLC aggiunto in Prime Infrastructure deve essere l'indirizzo IP usato come 'interfaccia di gestione wireless'. L'indirizzo IP dell'infrastruttura Prime deve essere raggiungibile dall'interfaccia di gestione wireless sul lato controller.
- Se si utilizza la porta di servizio (gig0/0 sugli accessori) per il rilevamento, i WLC e gli AP vengono visualizzati nello stato Gestito in Inventario, ma la telemetria per i WLC e i punti di accesso associati non funziona.
- Se lo stato della telemetria è un "successo" su Prime Infrastructure ma il numero AP è 0, è possibile che Prime Infrastructure possa raggiungere il WLC sulla porta 830 ma il controller non possa raggiungere nuovamente Prime Infrastructure sulla porta 20830.

Per qualsiasi problema di SNMP o di configurazione dei dispositivi, raccogliere questi registri da Prime Infrastructure:

```
cd /opt/CSC01umos/logs/
```

```
[root@prime-td1 logs]# ncs-0-0.1log
```

```
Td1.1logs
```

Per i problemi di telemetria/corallo, la prima cosa è controllare lo stato del corallo:

```
shell
```


```
cd /opt/CSC01umos/coralinstances/cora12/cora1/bin
```

```
./coral version 1
```

```
./coral status 1
```

```
./coral stats 1
```

Se tutto va bene, raccogliete questi log dalla cartella dei log del corallo primario.

 Nota: a seconda della versione di Prime Infrastructure e della quantità di versioni di Cisco IOS XE supportate, possono esistere diverse istanze di Coral su Prime Infrastructure. Consultare le note sulle release per ulteriori dettagli, ad esempio: 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

Passaggio 1.

```
cd /opt/CSC01umos/coral/bin/

[root@prime-td1 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
```

Questi registri sono disponibili anche in questa directory:

* I file di traccia decodificati sono disponibili nel percorso `/opt/CSC01umos/coralinstances/coral2/coral/run/1/storage/harddisk`

- * `ade# cd /opt/CSC01umos/coralinstances/coral2/coral/run/1/storage/harddisk`
- * `ade# cp coraltrace.txt /localdisk/defaultRepo`

Passaggio 2. Per abilitare Coral in modalità debug, è necessario impostare il livello di debug in `debug.conf` file.

Dall'interno del contenitore:

```
echo "rp:0:0:td1co1d:-e BINOS_BTRACE_LEVEL=DEBUG;" > /harddisk/debug.conf
```

Oppure, su Prime 3.8, il servizio Coral può essere riavviato all'esterno del container utilizzando:

```
"sudo /opt/CSC01umos/coralinstances/coral2/coral/bin/coral restart 1"
```

Se il riavvio non aiuta questi possono essere usati per pulire l'istanza del corallo e avviarlo senza problemi:

```
sudo /opt/CSC01umos/coralinstances/coral2/coral/bin/coral stop 1
```

```
sudo /opt/CSC01umos/coralinstances/coral2/coral/bin/coral purge 1
```

```
sudo /opt/CSC01umos/coralinstances/coral2/coral/bin/coral start 1
```

Riavviare Coral, questo è obbligatorio. Se si digita 'Esci' è possibile uscire dall'istanza di corallo:

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



Nota: su Prime 3.8, il servizio Coral può essere riavviato all'esterno del contenitore utilizzando 'sudo /opt/CSC01umos/coralinstance/coral2/coral/bin/coral restart 1'

Se è necessario decodificare i file di registro Coral, è possibile decodificarli all'interno del contenitore Coral con:

```
btdecode Prime_TDL_collector_*.bin
```



Nota: dopo aver abilitato il livello di debug di Coral, è necessario riavviare Coral.

Risoluzione dei problemi su Catalyst 9800 WLC

Per monitorare la configurazione trasferita da Prime Infra al WLC C9800, è possibile eseguire un'applet EEM.

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

Elimina tutta la sottoscrizione di telemetria dalla configurazione WLC

In alcuni casi può essere necessario annullare la configurazione di tutte le sottoscrizioni di telemetria configurate sul WLC. A tale scopo, è possibile usare semplicemente i seguenti comandi:

```
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
```

Per abilitare le tracce:

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

Per verificare:

```
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
```

Per visualizzare gli output di traccia:

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

```
show platform software trace message ndbman chassis active R0
```

Verifica ID sottoscrizione per informazioni AP

Fare clic su [DB Query](#). Accedere a <https://<Prime IP>/webacs/ncsDiag.do>.

Scegli *da `ewlcSubscription` dove `OWNINGENTITYID` è simile a `'%Controller_IP'` e `CLASSNAME='UnifiedAp'`.

Da WLC:

Verificare che l'ID sottoscrizione stia inviando informazioni e che non vi siano rilasci nei contatori `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: il 9800 WLC supporta 100 abbonamenti di telemetria prima della 17.6 e fino a 128 abbonamenti dopo la 17.6 (dato che la recente release di DNA center può utilizzare più di 100 abbonamenti).

Migrazione da PI a DNA-Center

C9800 non può essere gestito contemporaneamente da PI e DNA Center. Se si prevede di passare a DNAC come soluzione di gestione di rete, è necessario rimuovere C9800 da Prime Infrastructure prima di aggiungerlo a DNA Center. Quando C9800 viene rimosso/eliminato da PI 3.5, non viene eseguito il rollback di tutta la configurazione che è stata trasferita a C9800 al momento dell'inventario da PI e che deve essere eliminata manualmente dal sistema. In particolare, i canali di abbonamento stabiliti per C9800 WLC per pubblicare i dati di telemetria in streaming non vengono rimossi.


Per identificare questa configurazione specifica:

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

Per rimuovere questa configurazione, eseguire **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: se si gestisce il controller 9800 con DNAC e Prime Infrastructure, la conformità dell'inventario DNAC si interrompe in modo imprevisto a causa di Prime Management.

Nelle versioni più recenti, sia Prime Infrastructure che DNAC possono utilizzare troppi abbonamenti di telemetria per il WLC per entrambi i server per gestire contemporaneamente il 9800. Non è quindi possibile gestire la 9800 con DNAC e Prime Infrastructure e utilizzare la telemetria e le statistiche. La migrazione da PI a DNAC deve quindi avvenire il più rapidamente possibile perché DNAC non può avere dati di telemetria dal 9800 finché Prime Infrastructure gestisce il controller 9800.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).