Configurazione e risoluzione dei problemi di DNA Spaces e Catalyst 9800 o Embedded Wireless Controller (EWC) con Direct Connect

Sommario

Introduzione

Al posto di Mobility Express, i più recenti Access Point Cisco serie 9000 (9115, 9117, 9120, 9130) sono in grado di eseguire l'immagine EWC (Embedded Wireless Controller). EWC è basato sul codice WLC Cisco 9800 e consente a uno dei punti di accesso di agire come controller per un massimo di 100 altri access point.

EWC o Catalyst 9800 possono essere collegati al cloud DNA Spaces in 3 modi diversi:

1. Connessione diretta
2. Tramite connettore DNA Spaces
3. Tramite dispositivo on-prem Cisco Connected Mobile Xperience (CMX) o VM

L'integrazione con DNA Spaces è supportata in ogni versione di EWC. Questo articolo riguarda la configurazione e la risoluzione dei problemi di connessione diretta solo per EWC su un Catalyst AP e per 9800, in quanto la procedura è identica.

> **Importante:** La connessione diretta è consigliata solo per le distribuzioni con un massimo di 50 client. Per quelle più grandi, utilizzare DNA Spaces Connector.

Prerequisiti

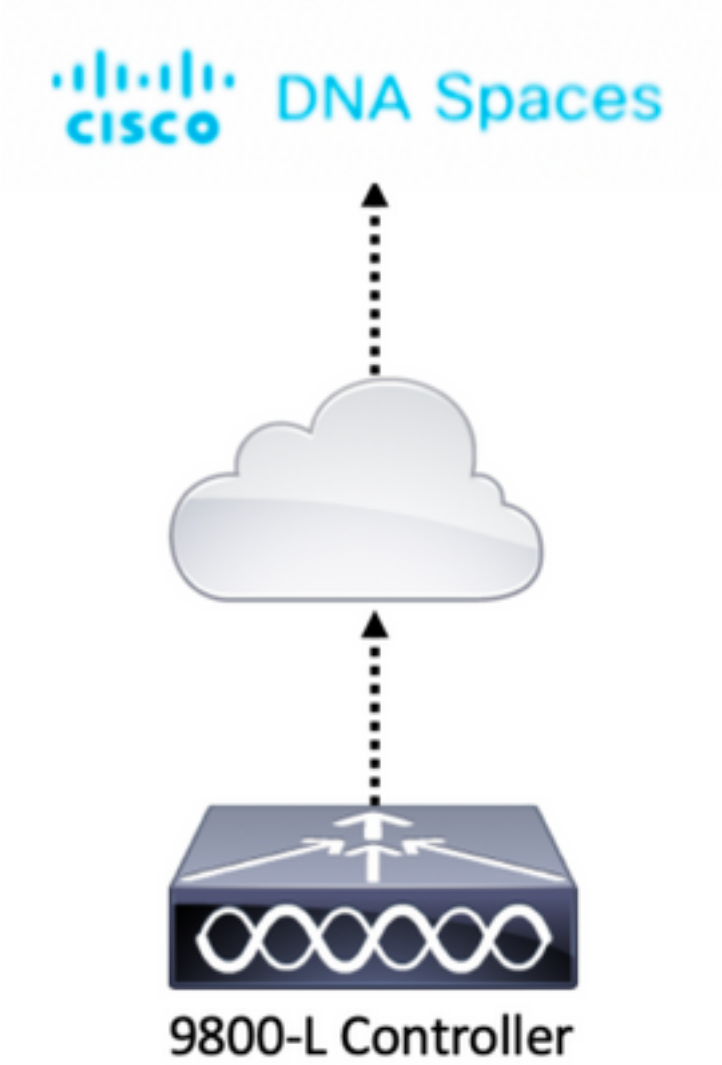
Componenti usati

- Immagine del controller wireless integrato versione 17.1.1s o Catalyst 9800-L con 16.12.1
- 9115 AP
- Cloud DNA Spaces

Per le procedure descritte in questo articolo, si presume che EWC o 9800 sia già stato implementato e che disponga di un'interfaccia Web funzionante e di SSH.

Configurazione

Esempio di rete



Configurare il controller

I nodi cloud di DNA Spaces e il controller stanno comunicando tramite il protocollo HTTPS. In questa configurazione di test, il controller è stato posizionato dietro un NAT con accesso completo a Internet.

Installa certificato radice

Prima di configurare il controller, è necessario scaricare un certificato radice DigiCert. SSH nel controller ed eseguire:

```
WLC# conf t
Enter configuration commands, one per line. End with CNTL/Z.
WLC(config)# ip name-server <DNS ip>
WLC(config)# ip domain-lookup WLC(config)# crypto pki trustpool import url
https://www.cisco.com/security/pki/trs/ios.p7b
Reading file from http://www.cisco.com/security/pki/trs/ios.p7b
Loading http://www.cisco.com/security/pki/trs/ios.p7b !!!
% PEM files import succeeded.
```

Per impostazione predefinita, i servizi EWC dispongono di DNS configurato utilizzando server DNS Cisco, ma questo passaggio sarà obbligatorio per un controller 9800.

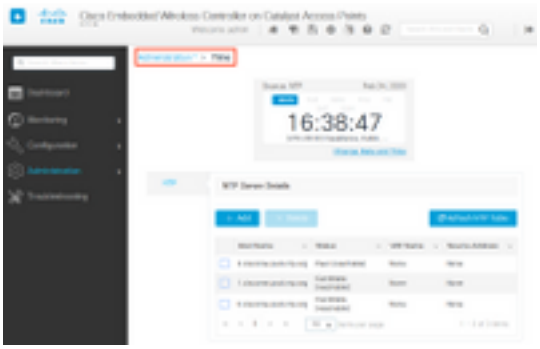
Per verificare che il certificato sia stato installato, eseguire:

```
EWC(config)#do show crypto pki trustpool | s DigiCert Global Root CA
cn=DigiCert Global Root CA
cn=DigiCert Global Root CA
```

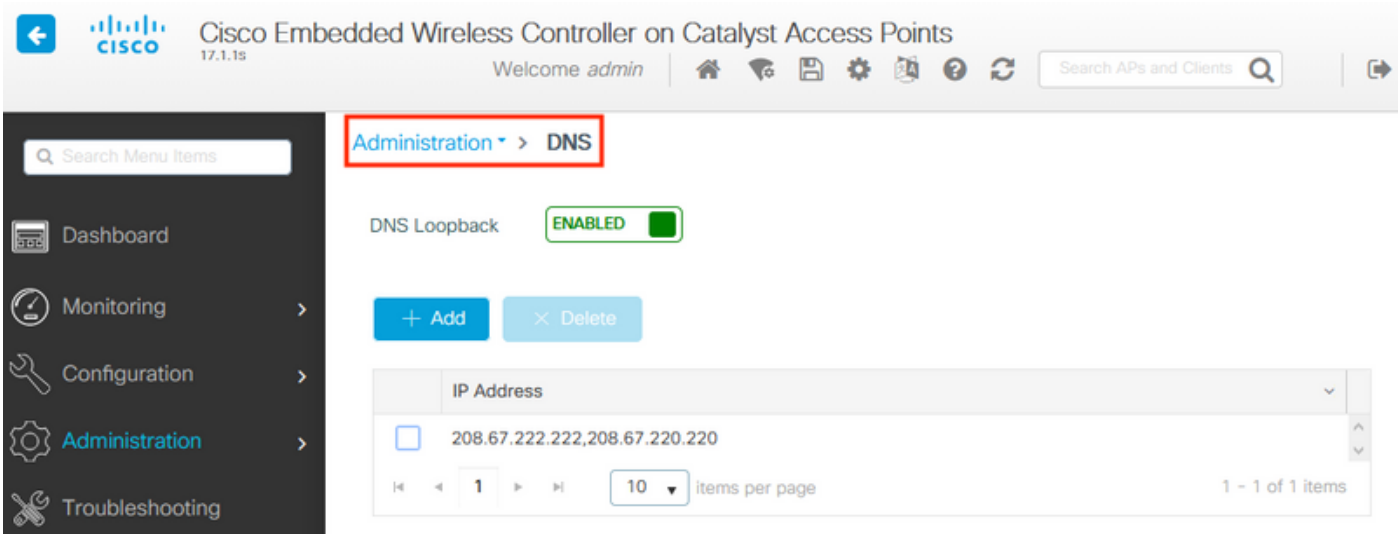
Configurazione tramite interfaccia Web

Prima che il controller possa essere connesso a DNA Spaces, è necessario configurare i server NTP e DNS e aggiungere almeno un punto di accesso.

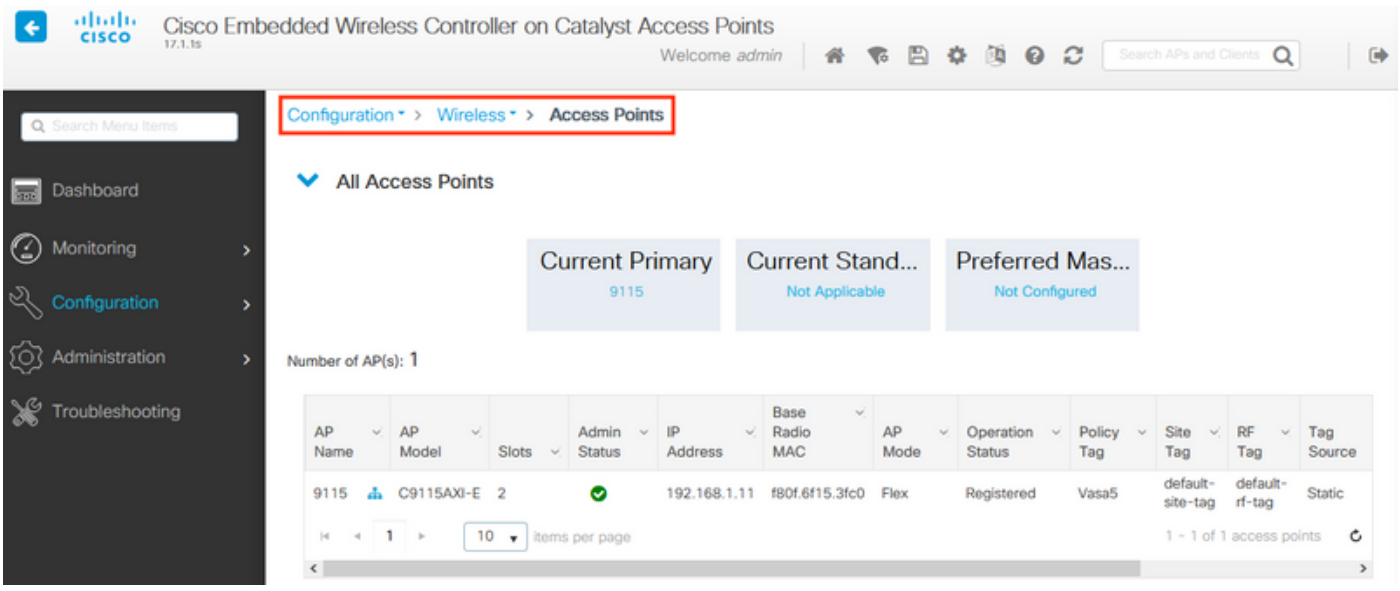
Aprire l'interfaccia Web del CAE e selezionare **Amministrazione > Tempo**. Verificare che il WLC sia sincronizzato con un server NTP. Per impostazione predefinita, EWC è preconfigurato per l'utilizzo di ciscome.pool.ntp.org server NTP. Nel caso di 9800, è possibile utilizzare lo stesso NTP o il server NTP preferito:



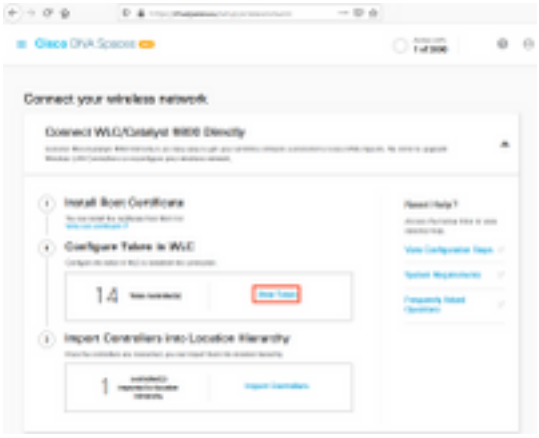
Passare a **Amministrazione > DNS** e verificare che il server DNS sia stato aggiunto. Per impostazione predefinita, EWC è preconfigurato per utilizzare i server DNS Cisco Open:



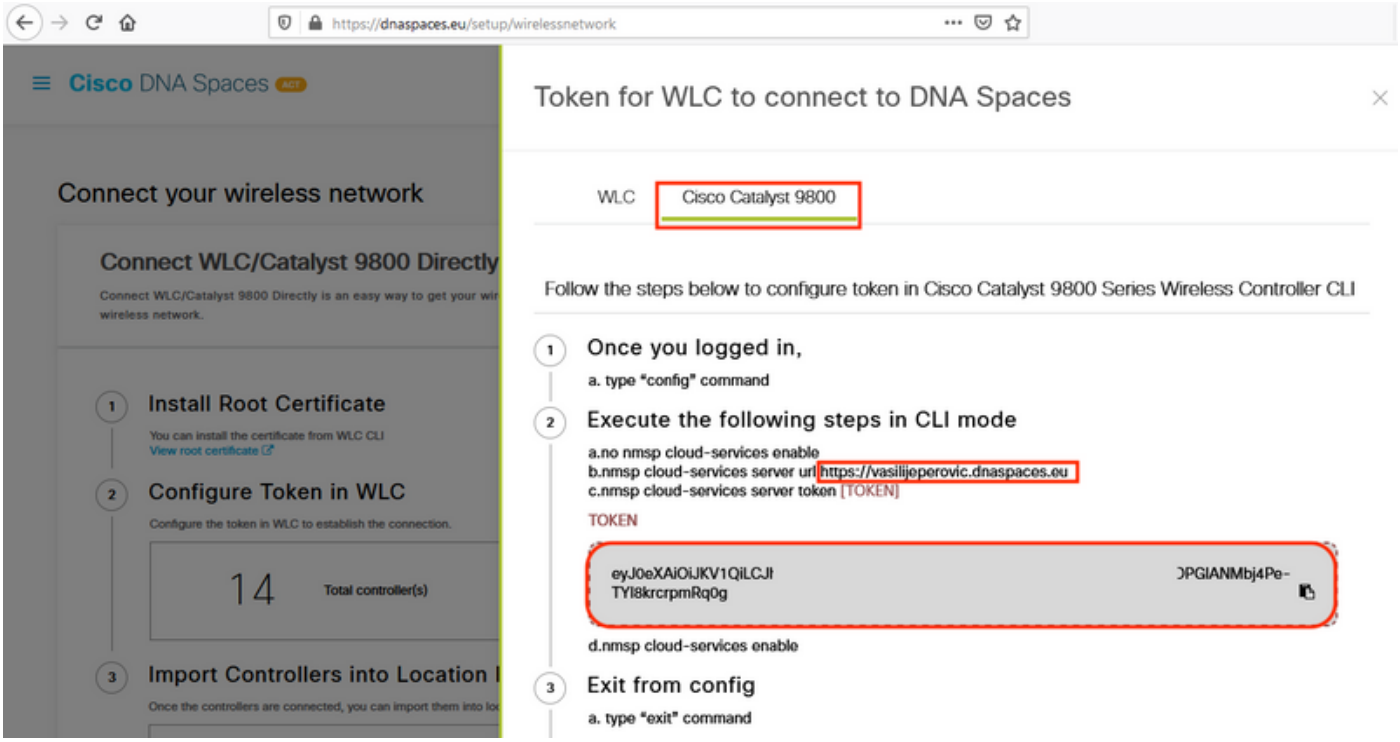
In **Configurazione > Wireless > Access Point** verificare che almeno un access point sia stato aggiunto. Questo punto di accesso può essere lo stesso sul quale è in esecuzione il CAE:



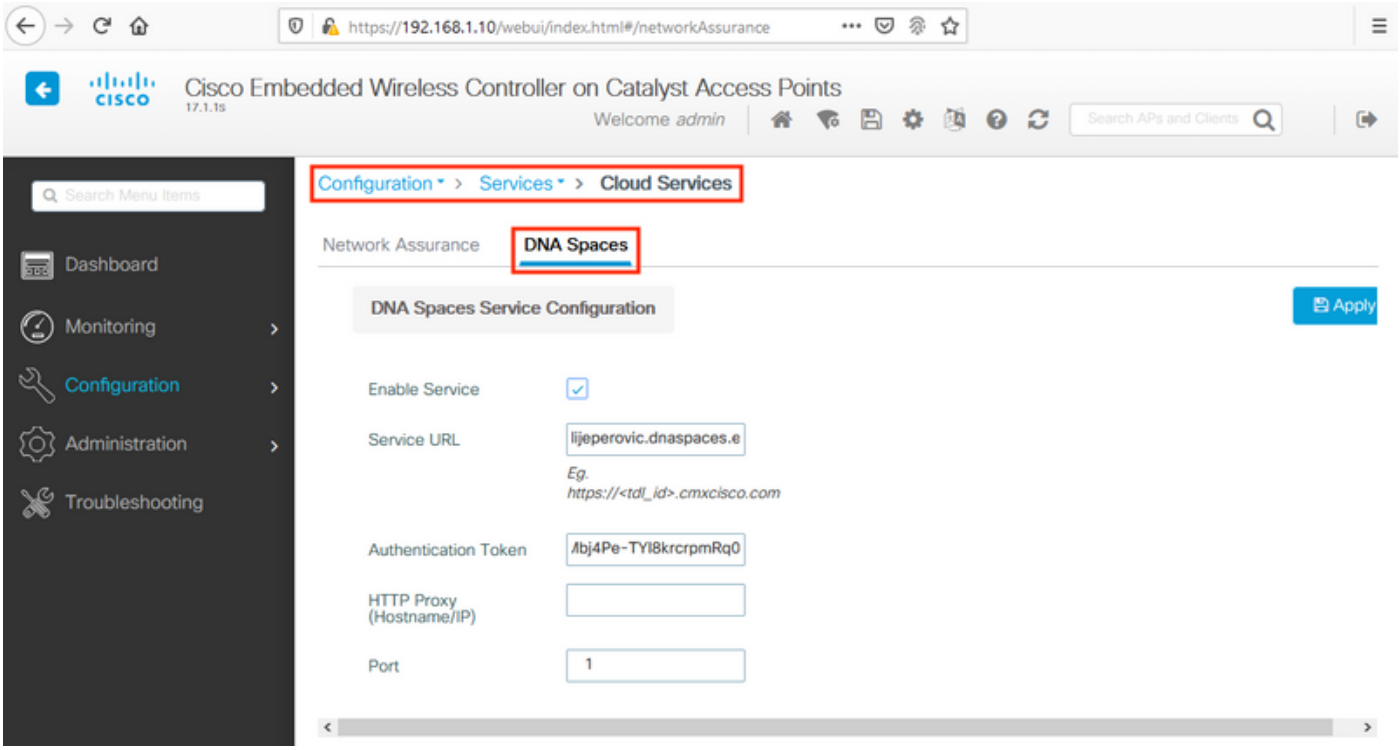
Sul cloud DNA Spaces, passare dalla home page a **Setup > Wireless Networks > Connect WLC/Catalyst 9800 Direct**. Fare clic su **View Token**:



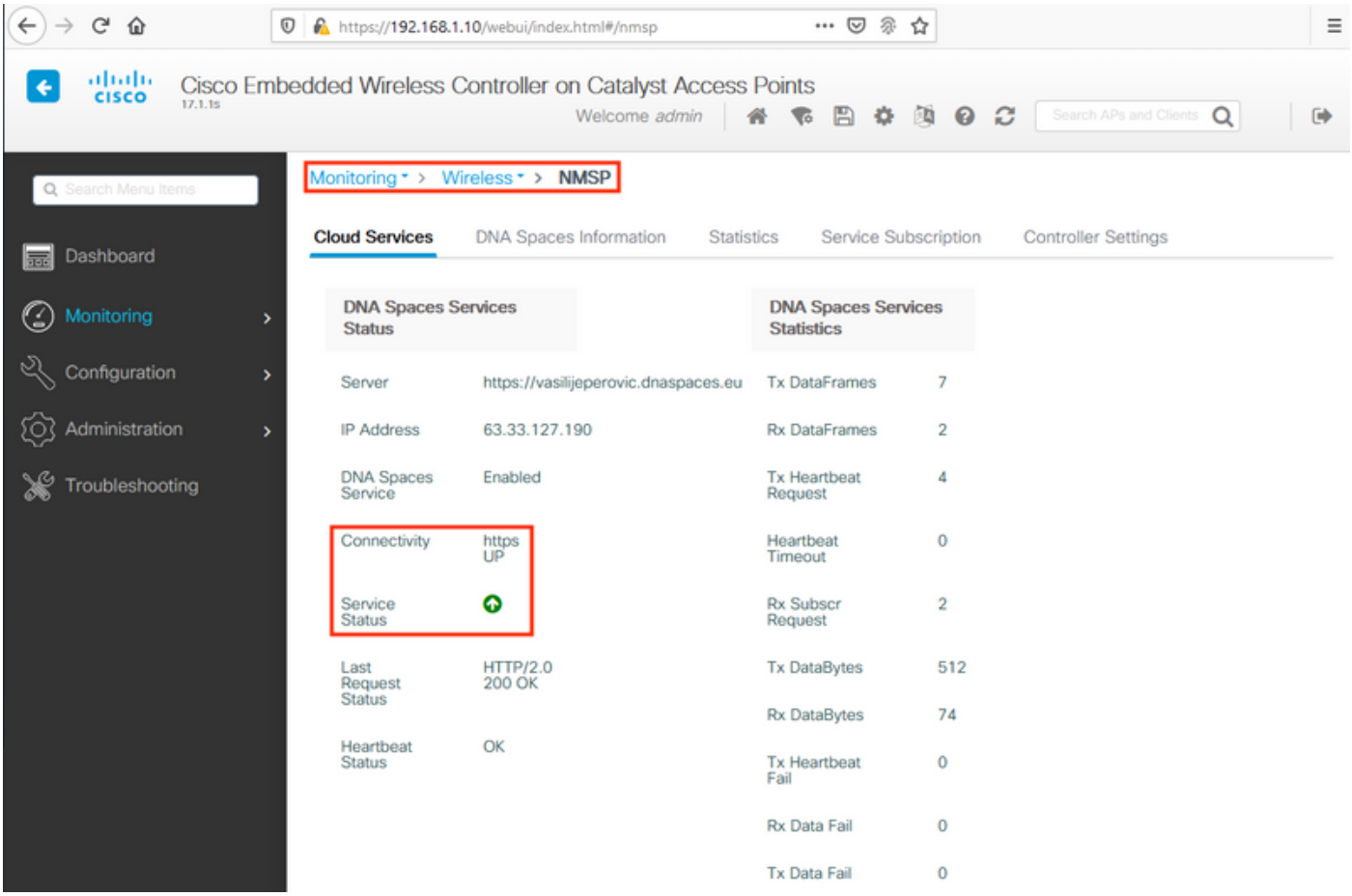
Spostare la scheda su **Cisco Catalyst 9800**. Copiare il token e l'URL:



Nell'interfaccia Web WLC, selezionare **Configuration > Services > Cloud Services > DNA Spaces**. Incolla URL e token di autenticazione. Se viene utilizzato il proxy HTTP, specificarne l'indirizzo IP e la porta.



Verificare che la connessione sia stata stabilita correttamente in **Monitoraggio > Wireless > NMSP**. Freccia verde relativa allo stato del servizio:



Ignorare il capitolo successivo e passare alla sezione "**Importa controller nella gerarchia di posizione**".

Configurazione tramite CLI

Verificare che NTP sia configurato e sincronizzato:

```
EWC#show ntp associations

  address      ref clock    st   when   poll reach  delay  offset   disp
*~45.87.76.3  193.79.237.142638   1024   377 10.919  -4.315  1.072
+~194.78.244.172  172.16.200.253   2646   1024   377 15.947  -2.967  1.084
+~91.121.216.238  193.190.230.66   2856   1024   377  8.863  -3.910  1.036
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

È possibile aggiungere nuovi server NTP utilizzando il comando ntp server <ntp_ip_addr>.

Verificare che i server DNS siano stati configurati:

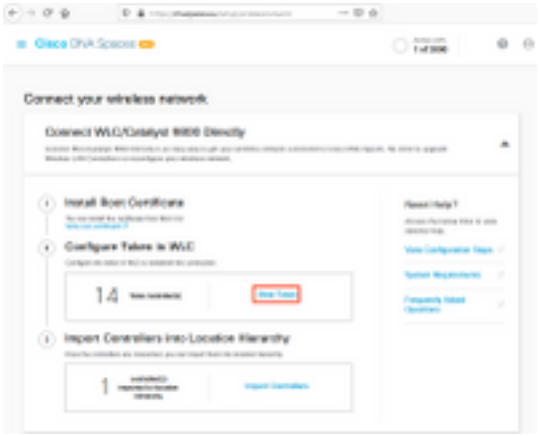
```
EWC#show ip name-servers
208.67.222.222
208.67.220.220
```

Èpossibile aggiungere nuovi server DNS utilizzando il comando ip name-server <dns_ip>.

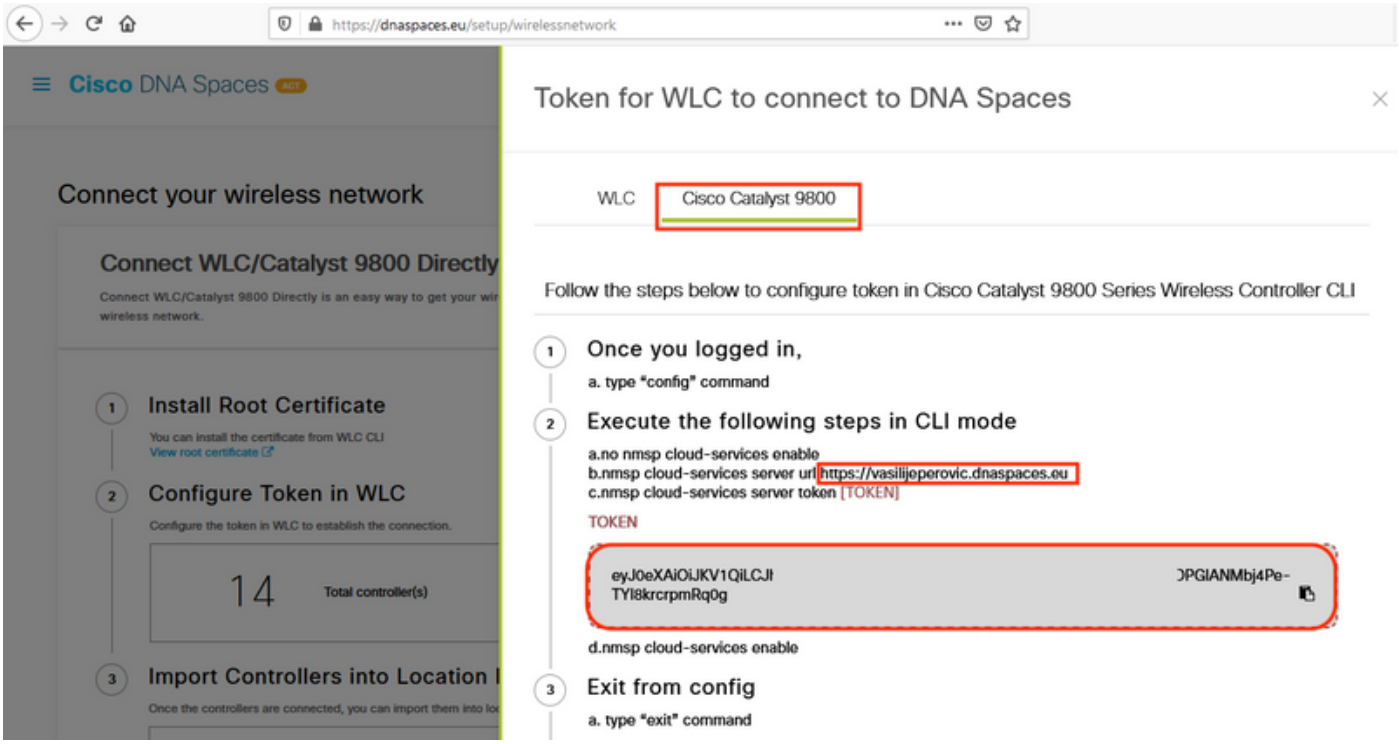
Per confermare che l'access point è stato aggiunto:

```
EWC#show ap status
AP Name     Status      Mode     Country
-------------------------------------
9115        Enabled     Local    BE
```

Come accennato in precedenza, accedere a DNA Spaces cloud, selezionare **Setup > Wireless Networks > Connect WLC/Catalyst 9800 Direct** (Configurazione > Reti wireless > **Connetti direttamente a WLC/Catalyst 9800)** e fare clic su **View Token**:



Spostare la scheda su **Cisco Catalyst 9800**. Copiare il token e l'URL:



Eseguire i comandi seguenti:

```
CL-9800-01(config)#no nmsp cloud-services enable
CL-9800-01(config)#nmsp cloud-services server url [URL]
CL-9800-01(config)#nmsp cloud-services server token [TOKEN]
CL-9800-01(config)#nmsp cloud-services enable
CL-9800-01(config)#exit
```

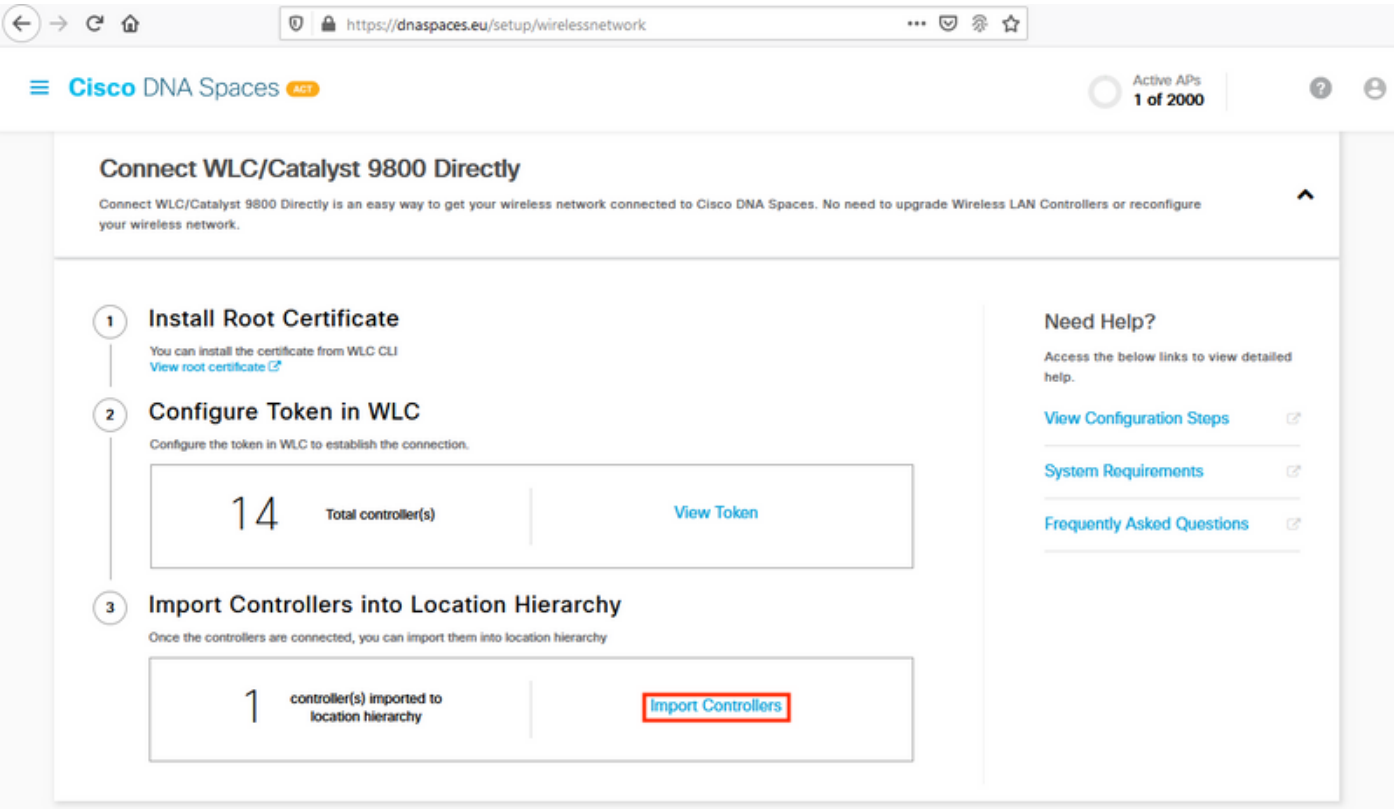
Per verificare che la connessione con il cloud DNA Spaces sia stata stabilita correttamente,

eseguire:

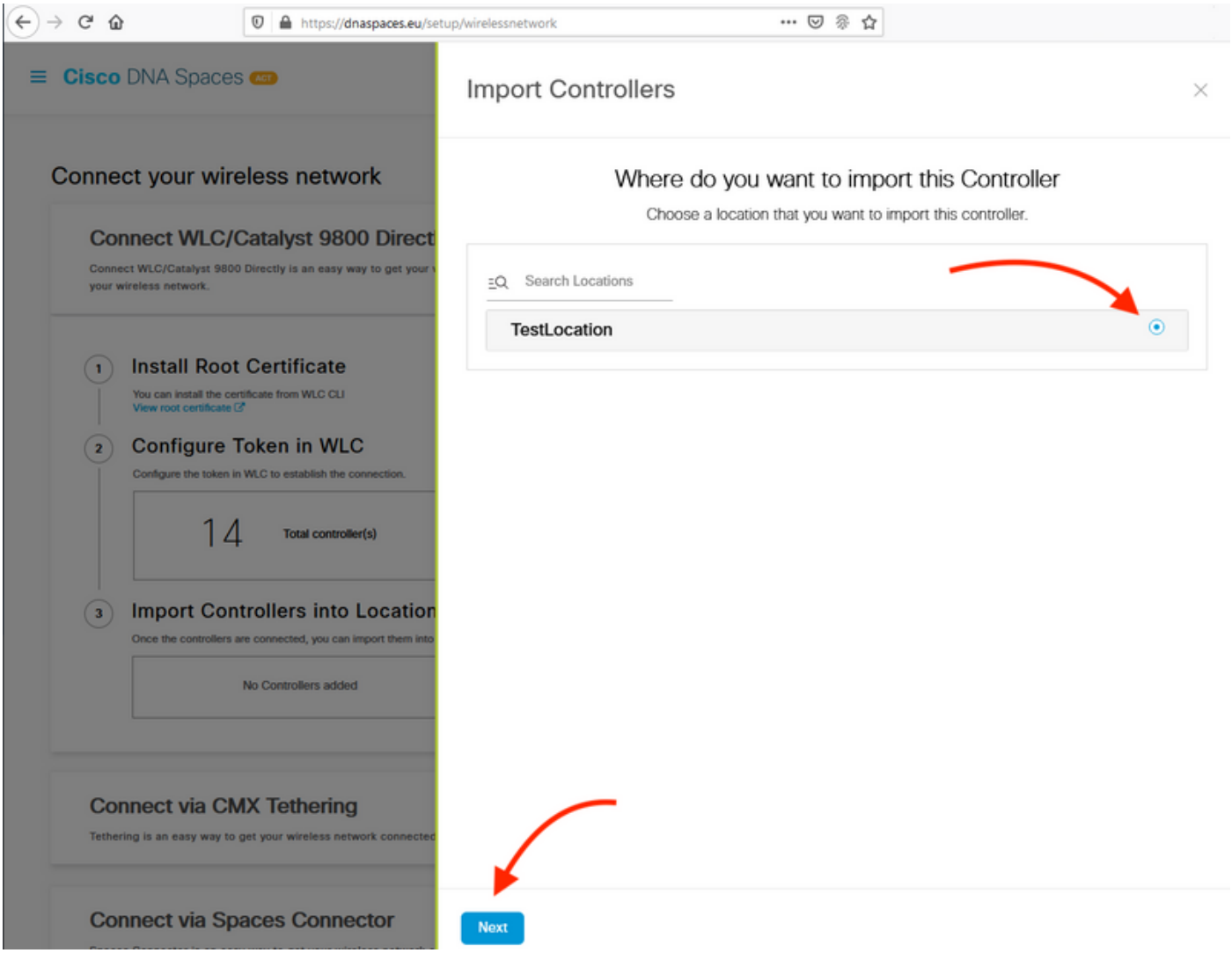
```
CL-9800-01#show nmsp cloud-services summary
CMX Cloud-Services Status
------------------------------------------------
Server : https://vasilijeperovic.dnaspaces.eu
CMX Service : Enabled
Connectivity : https: UP
Service Status : Active
Last IP Address : 63.33.127.190
Last Request Status : HTTP/2.0 200 OK
Heartbeat Status : OK
```

Importa EWC nella gerarchia ubicazioni

Passaggio 1. Il resto della configurazione verrà eseguito in DNA Spaces. In **Setup > Wireless Networks > Connect WLC/Catalyst 9800 Direct** (Configurazione **> Reti wireless > Connetti direttamente WLC/Catalyst 9800)**, fare clic su **Import Controller (Importa controller)**.



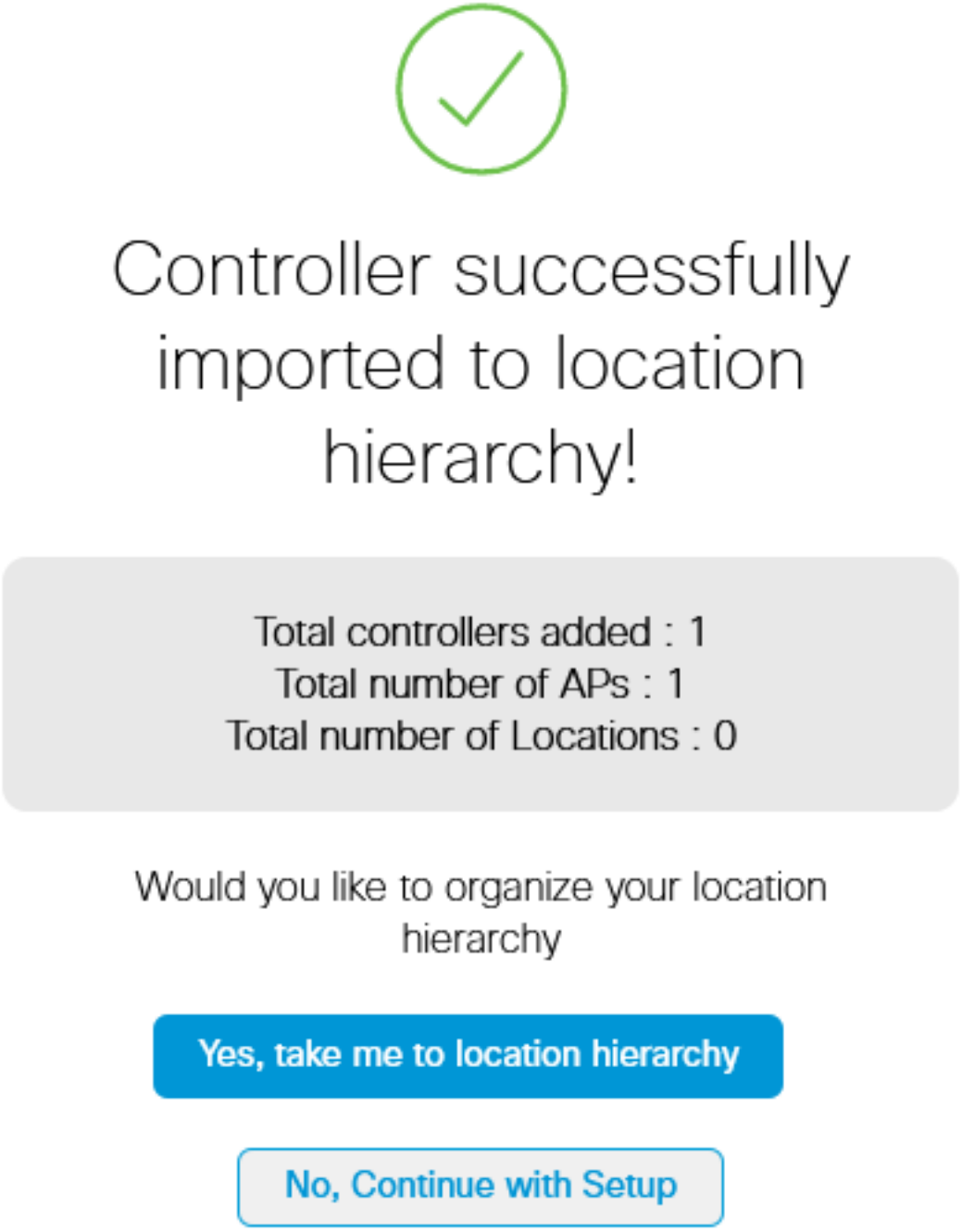
Passaggio 2. Selezionare il pulsante di opzione accanto al nome dell'account e fare clic su Avanti. Se sono già stati aggiunti dei Percorsi, questi verranno visualizzati nell'elenco seguente:



Passaggio 3. Individuare l'indirizzo IP del controller, selezionare la casella corrispondente e premere **Avanti**:

Passaggio 4. Poiché non sono state aggiunte altre sedi, fare clic su Fine:

Passaggio 5. Viene visualizzato un messaggio che indica che il WLC è stato importato correttamente nella gerarchia di posizione:



Ora che il WLC è stato collegato correttamente al cloud, puoi iniziare a usare tutte le altre funzionalità di DNA Spaces.

> **Nota:** Il traffico NMSP utilizza sempre l'interfaccia di gestione wireless per comunicare con DNA Spaces o CMX. Questa condizione non può essere modificata nella configurazione del controller 9800. Il numero di interfaccia non è rilevante, a prescindere dall'interfaccia assegnata come interfaccia di gestione wireless sul controller 9800.

Organizzazione della gerarchia di posizioni in Cisco DNA Spaces

Se si desidera creare una nuova gerarchia di posizioni o se non sono state aggiunte posizioni nel passaggio 4 della sezione **Importare il controller 9800 in Cisco DNA Spaces, è** possibile configurarle manualmente.

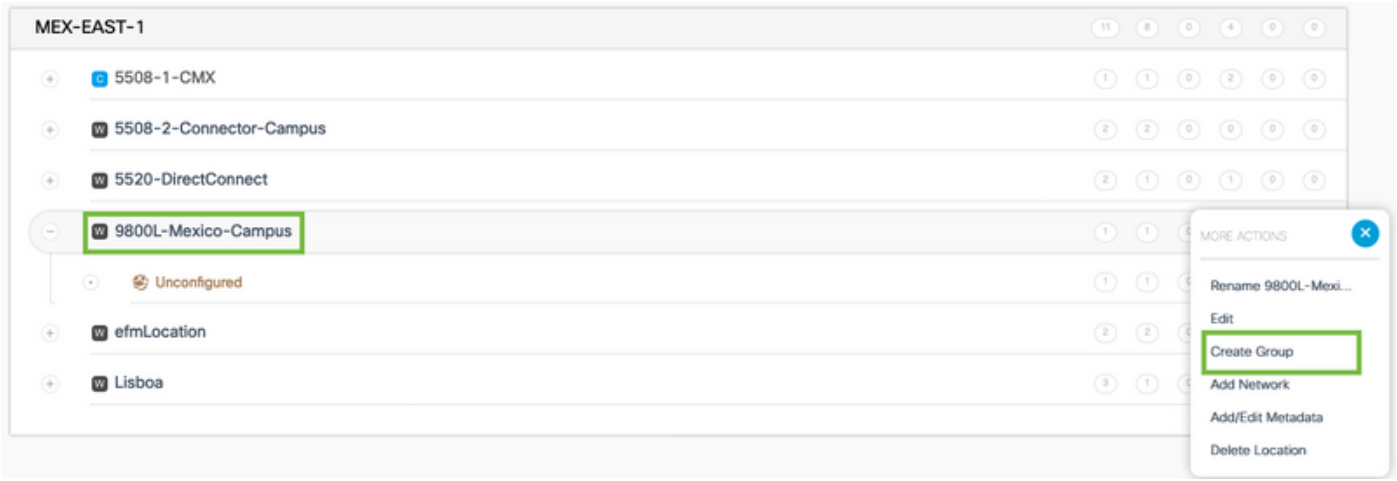
La gerarchia delle posizioni è una delle caratteristiche più importanti degli spazi DNA in quanto viene utilizzata per le informazioni di analisi e, in base ad essa, vengono configurate le regole dei portali vincolati. Più la gerarchia delle posizioni è granulare, maggiore è il controllo che si ha sulle regole del portale captive e sulle informazioni che possono essere recuperate da DNA Spaces.

La funzione di gerarchia della posizione in DNA Spaces funziona allo stesso modo della gerarchia tradizionale di Cisco Prime Infrastructure o Cisco CMX, ma la denominazione è abbastanza diversa. Quando il controller viene importato nella gerarchia di posizioni, rappresenta l'equivalente del **campus** dalla gerarchia tradizionale; sotto il controllo, possono essere creati **gruppi** equivalenti agli **edifici**; quindi, sotto i gruppi, **le reti** possono essere configurate che sono l'equivalente dei **piani**, infine, sotto le reti, si possono creare zone che rimangono nello stesso livello a cui erano abituati nella tradizionale gerarchia di posizione. Per riassumere, questa è l'equivalenza:

Tabella 1. Equivalenza tra i livelli gerarchici tradizionali con i livelli degli spazi DNA.

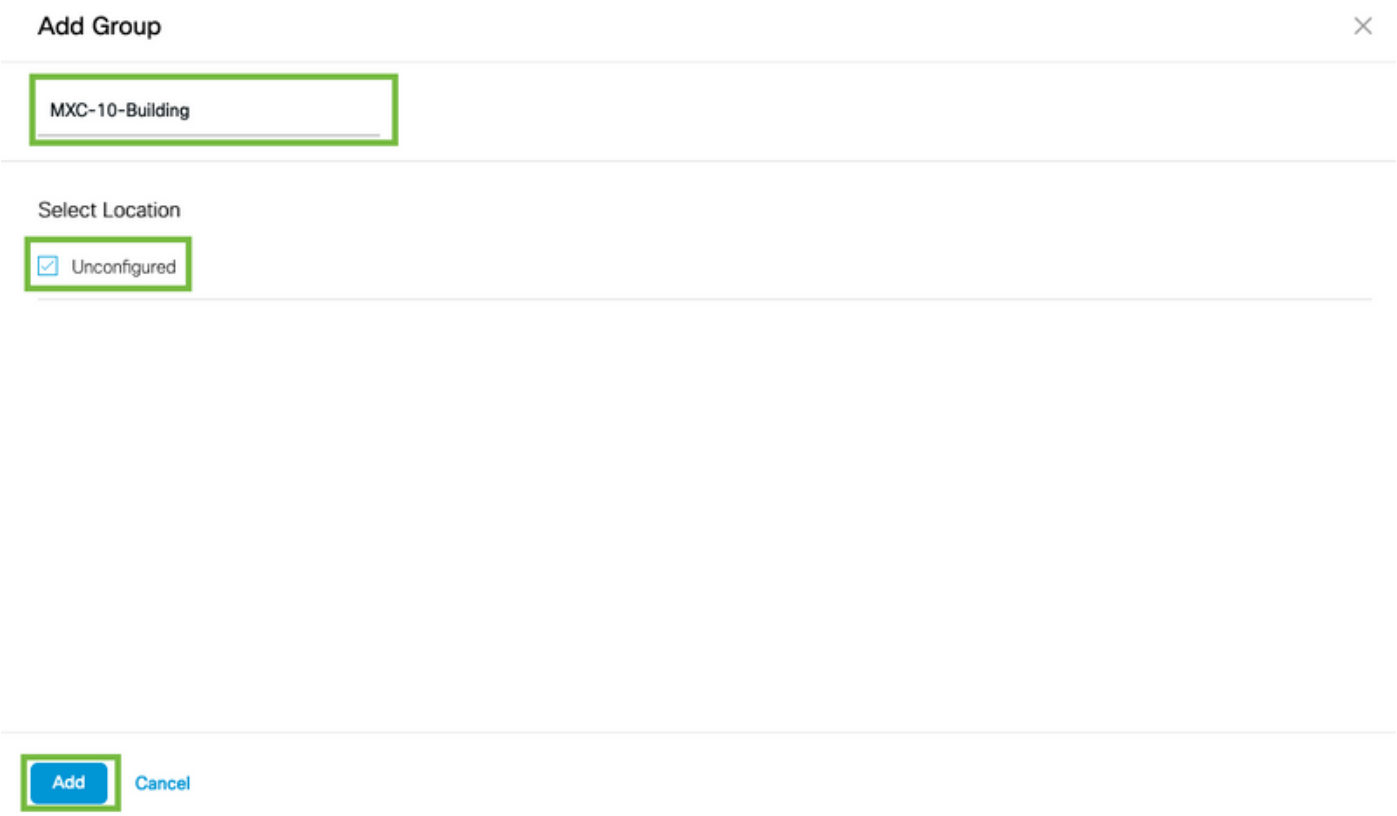
Gerarchia spazi DNA	Gerarchia tradizionale
Controller (rete wireless)	Campus
Group	Edificio
Rete	Piano
Zona	Zona

Passaggio 1. Configurare un gruppo. I gruppi organizzano più ubicazioni o zone in base alla geolocalizzazione, al marchio o a qualsiasi altro tipo di raggruppamento, a seconda dell'azienda. Passare a **Gerarchia posizione,** passare il mouse sul controller wireless esistente e fare clic su **Crea gruppo**.

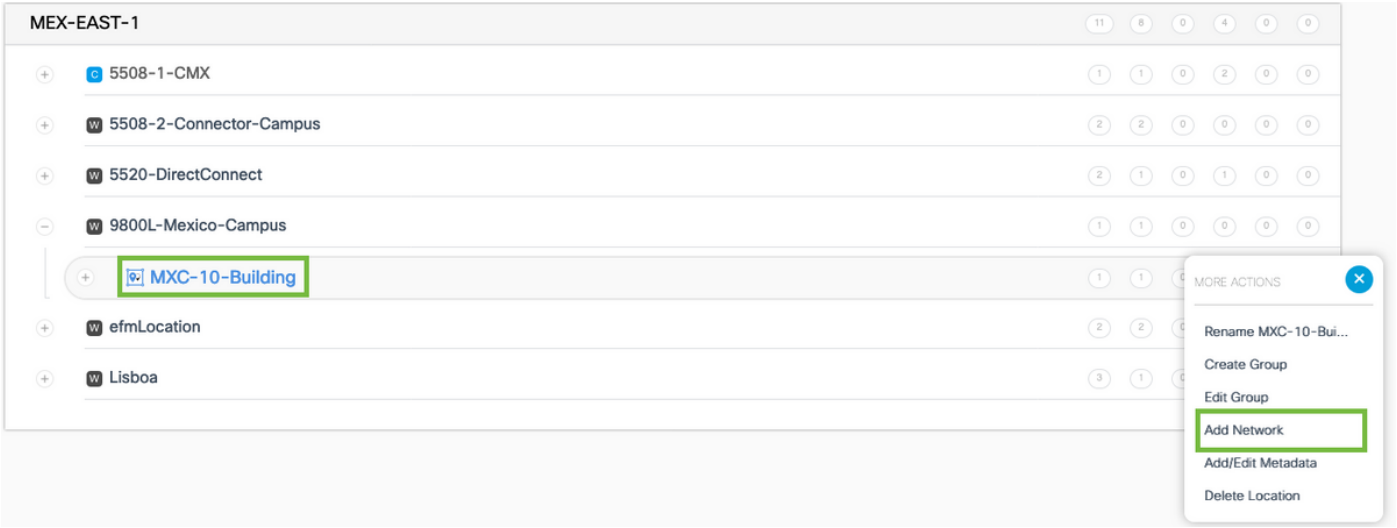


Per modificare il nome del livello di posizione, passare il mouse sulla rete e fare clic su **"Rinomina".**

Passaggio 2. Immettere il nome del gruppo e selezionare la posizione **Non configurato** in quanto include tutti gli access point importati con il controller. Tali access point verranno mappati alle reti e alle zone in base alle esigenze. Fare clic su **Add.**

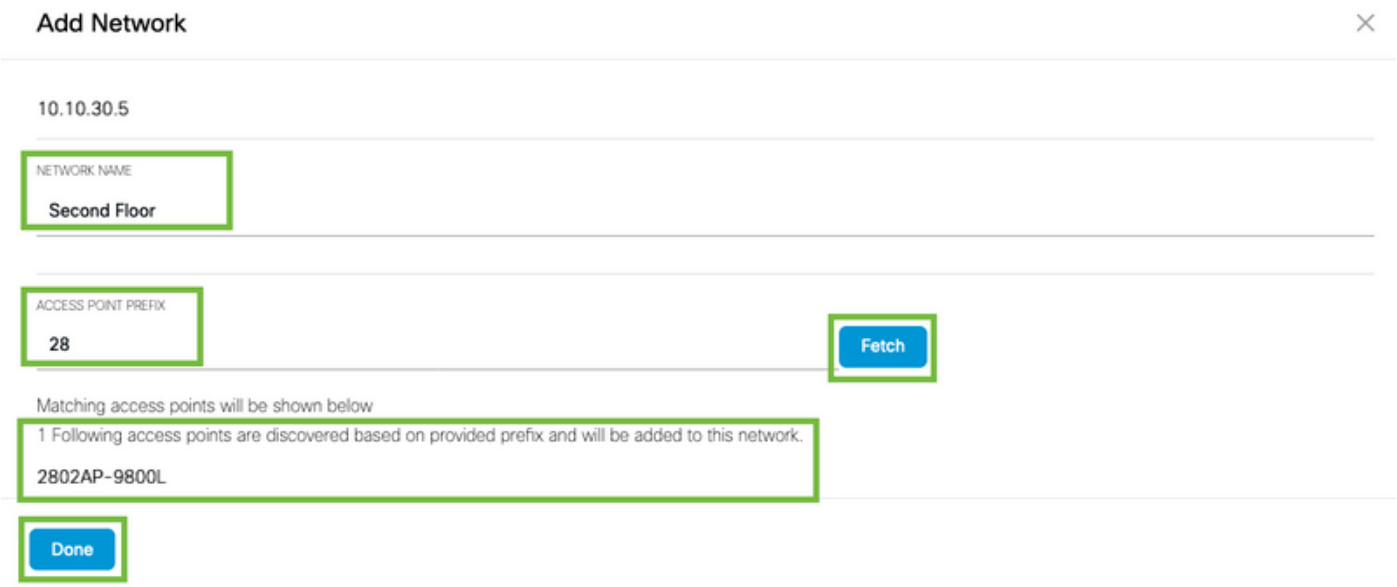


Passaggio 3. Creare una rete. In Cisco DNA Spaces una rete o una posizione sono definiti come tutti i punti di accesso all'interno di un edificio fisico consolidato come posizione. Posizionare il puntatore del mouse sul gruppo e fare clic su **Aggiungi rete.**

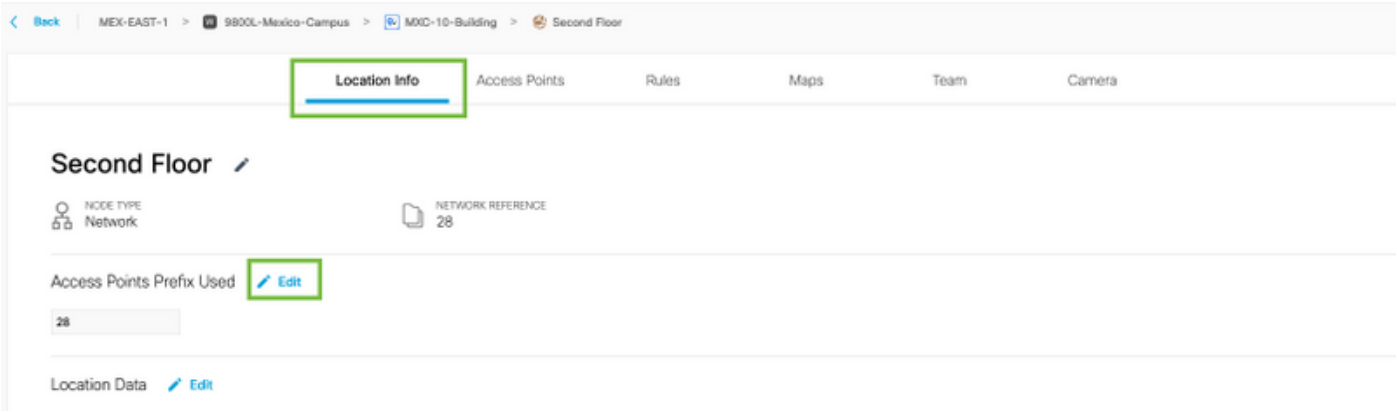


Nota: Questo è il nodo più importante nella gerarchia di posizioni, poiché da qui vengono generati informazioni aziendali e calcoli di analisi delle posizioni.

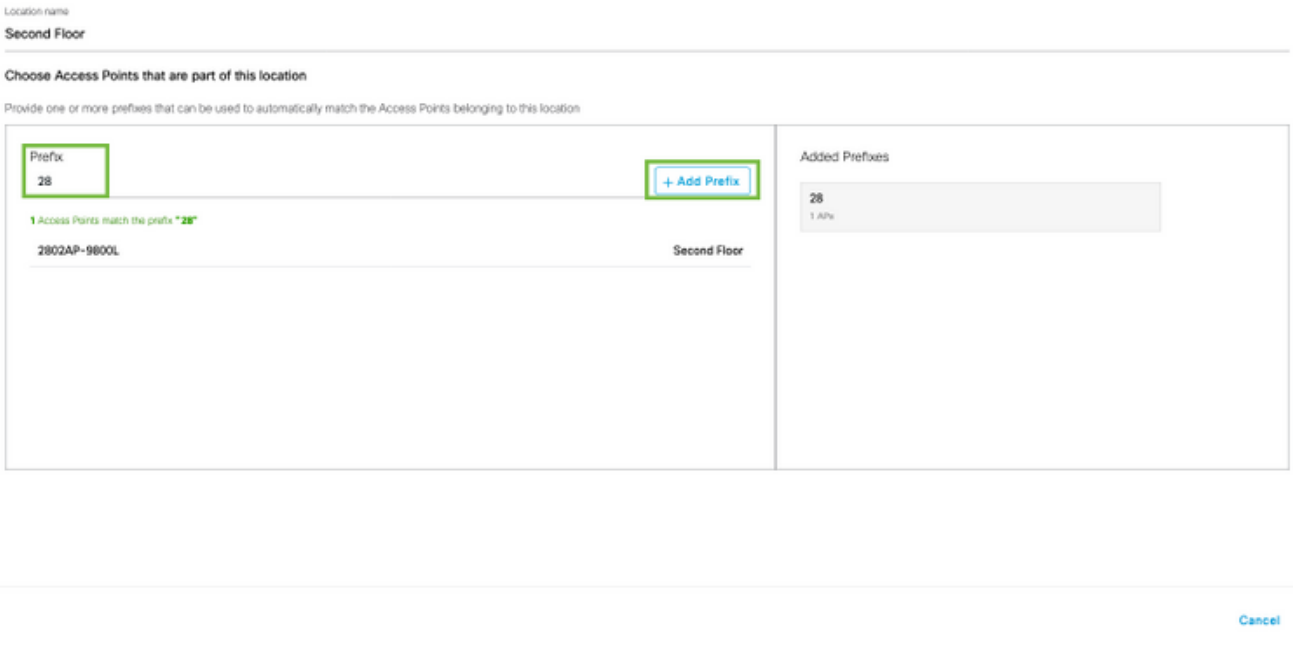
Passaggio 4. Inserire il nome della rete e il prefisso del punto di accesso, quindi fare clic su **Fetch.** DNA Spaces recupera tutti gli access point associati al controller con il prefisso specificato e consente di aggiungere gli access point al pavimento. È possibile immettere un solo prefisso.



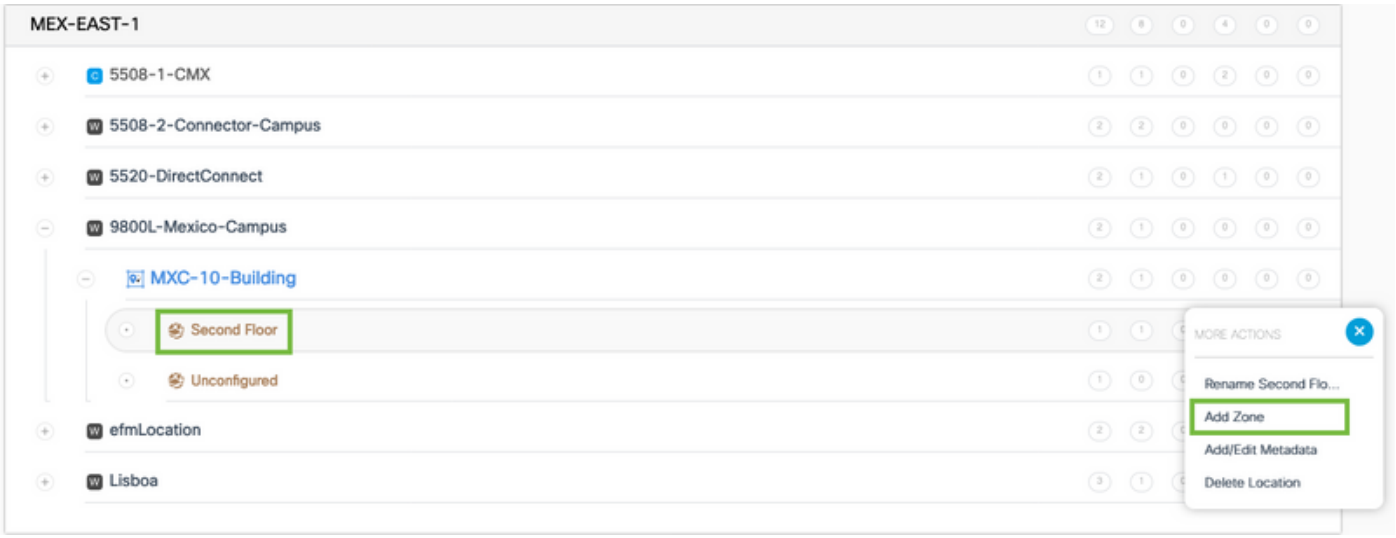
Passaggio 5. Se nella rete sono necessari più prefissi. Fare clic sul nome della rete, nella scheda **Informazioni posizione** fare clic sul pulsante **Modifica** accanto a **Prefisso Access Point utilizzato.**



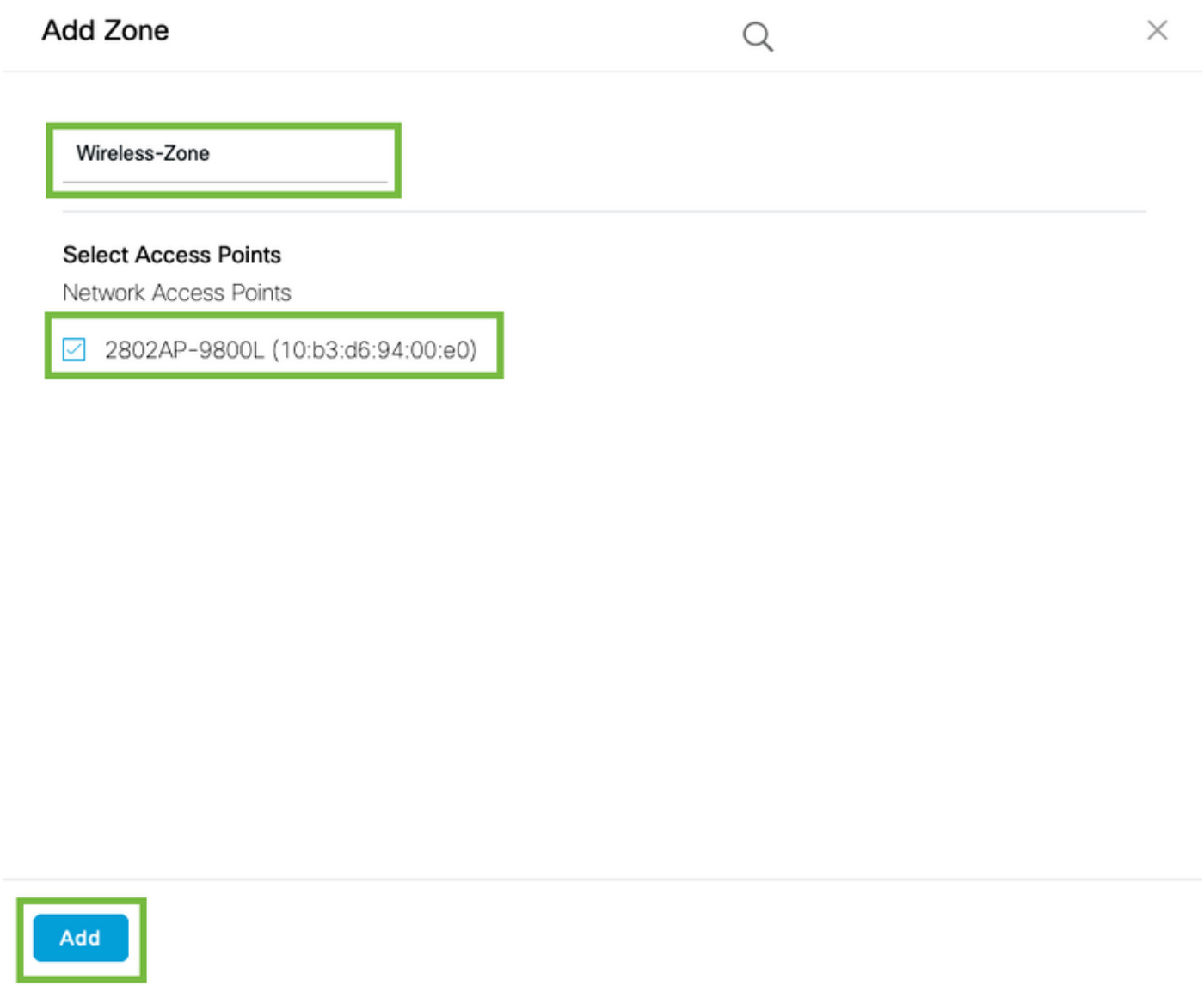
Immettete il nome del prefisso, fate clic su **+Aggiungi prefisso (Add Prefix)** e **Salva (Save).** Ripetere l'operazione per tutti i prefissi, in base alle esigenze, per mappare gli access point alla rete e consentire di associare gli access point alle zone in un secondo momento.



Passaggio 6. Creare una zona. Una zona è una raccolta di punti di accesso all'interno di una sezione di un edificio/una posizione. Può essere definito in base ai reparti di un edificio fisico o di un'organizzazione. Posizionare il puntatore del mouse sulla rete e selezionare **Add Zone.**



Passaggio 7. Configurare il **nome** della **zona** e selezionare i punti di accesso per la zona, quindi fare clic su **Aggiungi:**

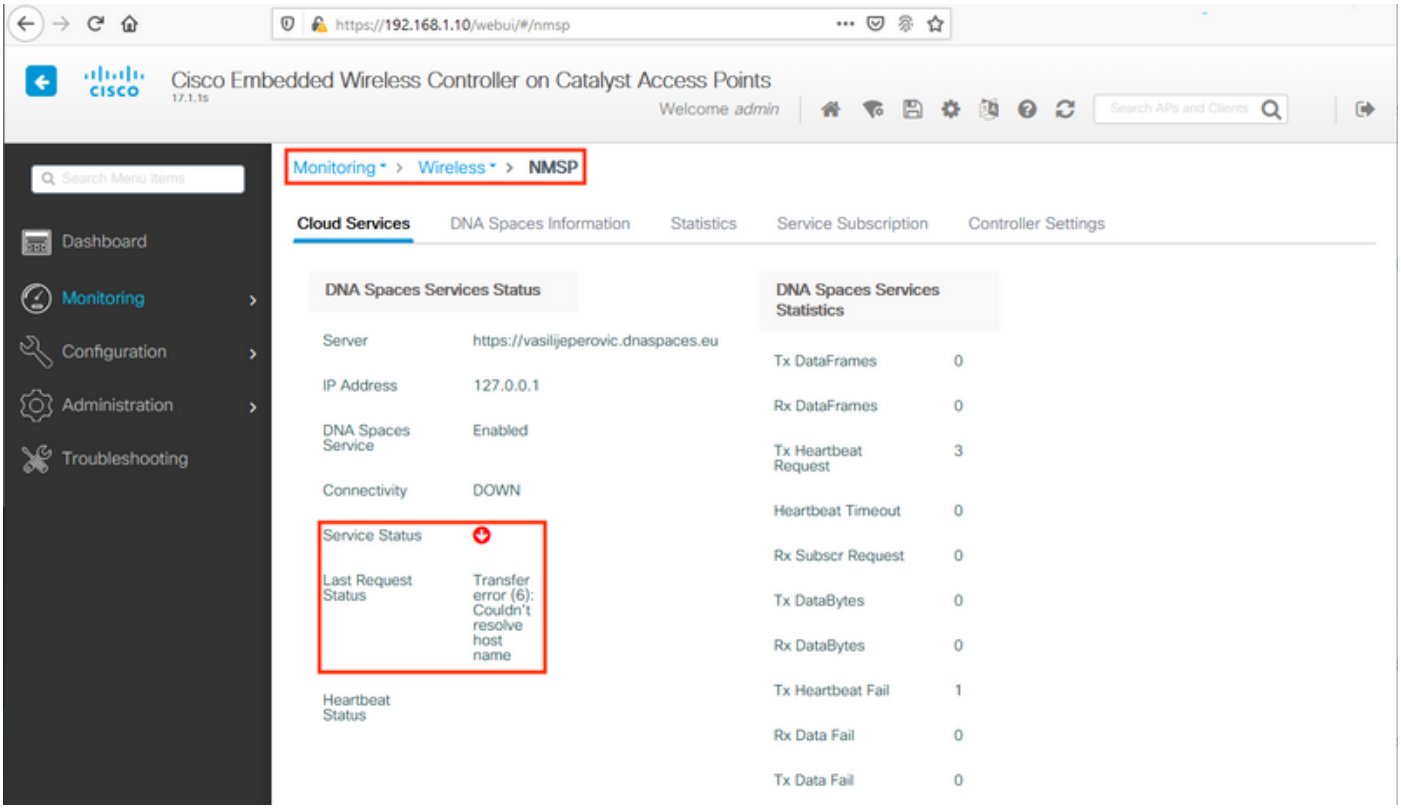


Risoluzione dei problemi e problemi comuni

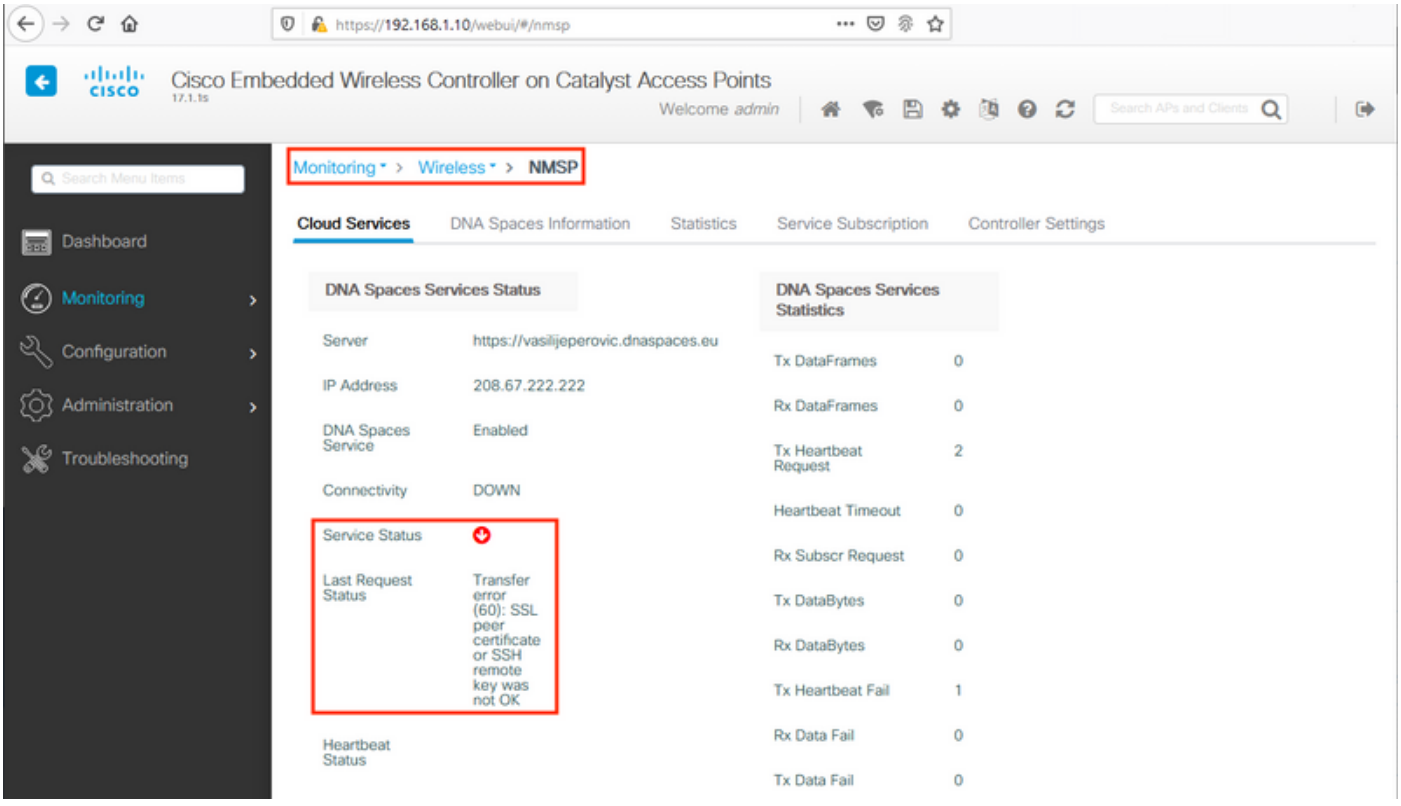
Problemi comuni

La pagina dell'interfaccia Web in **Monitoraggio > Wireless > NMSP** (o in esecuzione del comando show nmsp cloud-services summary) visualizza in genere informazioni sufficienti sull'errore di connessione. Di seguito sono riportati alcuni errori comuni:

1. Quando il DNS non è configurato, viene visualizzato il messaggio di errore "*Errore di trasferimento (6): Can't Resolve Host Name*" (*Impossibile risolvere il nome host*) viene visualizzato:



La mancata installazione del certificato o la mancata configurazione del protocollo NTP genera il messaggio di errore seguente: "*Errore di trasferimento (60): Il certificato peer SSL o la chiave remota SSH non è corretta*":



Traccia radioattiva

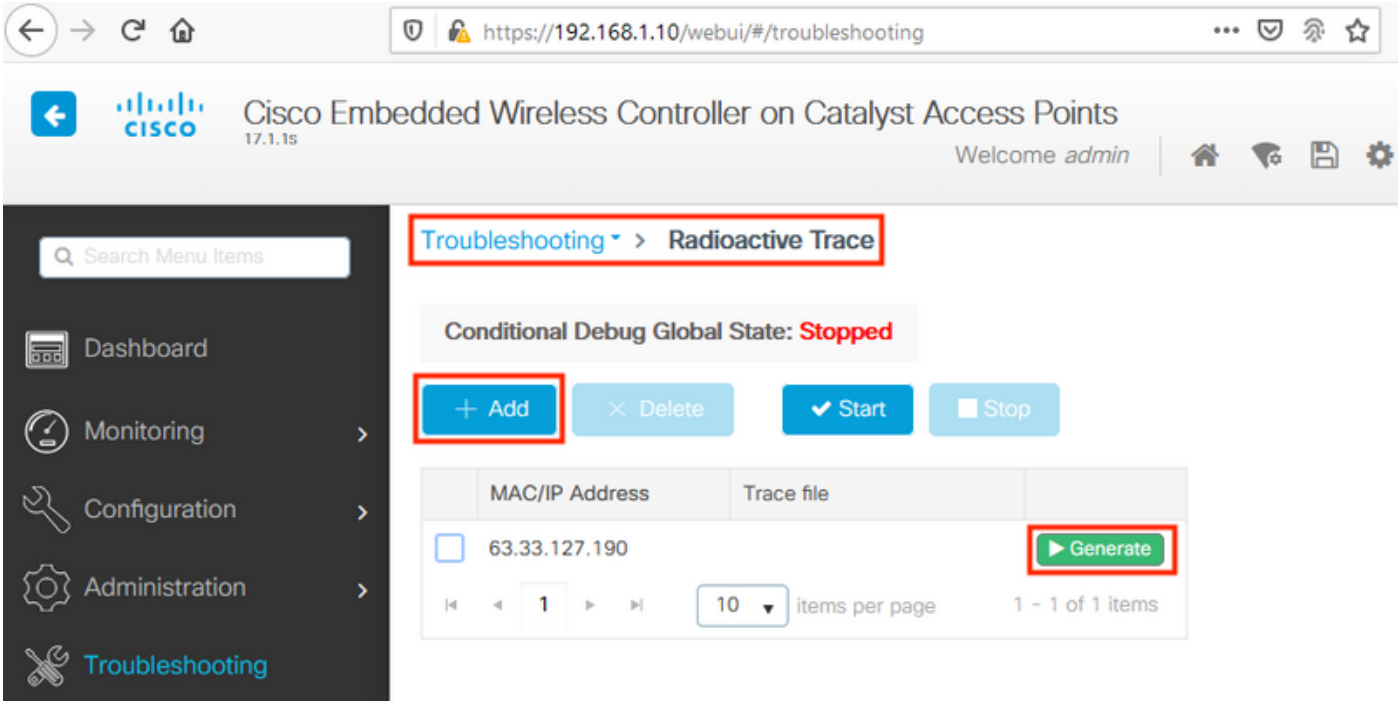
EWC, come tutti gli altri controller 9800, supporta le tracce radioattive sempre attive. Per raccoglierli e capire perché la connessione non viene stabilita, è necessario sapere a quale indirizzo IP di Spazi DNA il CAE si sta rivolgendo. Questa condizione può essere rilevata in

Monitor > Wireless > NMSP o tramite la CLI:

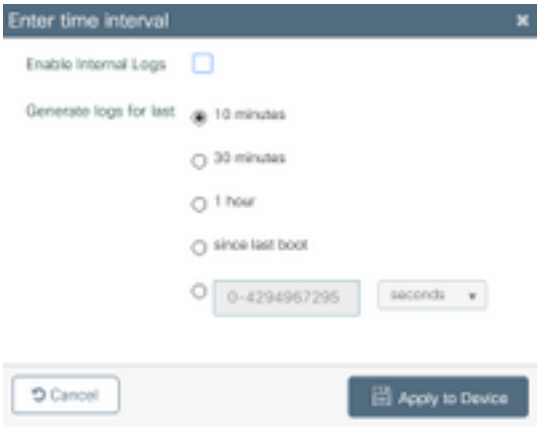
```
EWC#show nmsp status
NMSP Status
-----------

CMX IP Address      ActiveTx Echo Resp  Rx Echo Req   Tx Data Rx Data Transport
------------------------------------------------------------------------------------------------
--
63.33.127.190       Active0             0             38      2       HTTPS
```

Il CAE in questa configurazione di test si sta collegando alla versione 63.33.127.190. Copiare questo indirizzo IP e selezionare **Risoluzione dei problemi > Traccia radioattiva**. Fare clic su Aggiungi, incollare l'indirizzo IP e fare clic su Genera:



Selezionare **Genera log** per gli ultimi 10 minuti e fare clic su Applica. L'attivazione dei registri interni può generare grandi quantità di dati difficili da analizzare:



Nota: una configurazione errata di DNS, NTP e mancanza di certificato non genererà tracce radioattive

Esempio di traccia radioattiva in un caso in cui il firewall blocca il protocollo HTTPS:

```
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (note): CMX [63.33.127.190]:[32]:
closing
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Called 'is_ready'
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (info): CMX [63.33.127.190]:[32]:
Processing connection event NMSP_APP_LBS_DOWN(201)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (info): Started or incremented
transaction (TID: -1, ref count: 1, started: 0, abort: 0)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-enc] [11100]: (debug): Decoding control message
structure
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-enc] [11100]: (debug): Control structure was
successfully decoded from message
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (debug): Retrieving CMX entry: 32
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (ERR): CMX entry 32 not found
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (debug): CMX Pool processing NMSP
message (id: event NMSP_APP_LBS_DOWN(201), length: 48, client: 0, CMX id: 32)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (info): Ending transaction (TID: -1,
ref count: 1, started: 0, abort: 0)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (info): Ended transaction (TID: -1,
ref count: 0, started: 0, abort: 0)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-client] [11100]: (debug): NMSP IPC sent message
to NMSPd NMSP message (id: event NMSP_APP_LBS_DOWN(201), length: 48, client: 0, CMX id: 32)
successfully
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (info): CMX [63.33.127.190]:[32]:
successfully broadcasted IPC event NMSP_APP_LBS_DOWN(201)
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (note): CMX [63.33.127.190]:[32]:
down
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-main] [11100]: (debug): NMSP timer 0xab774af4:
close
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Decrease reference count
for https_con object: Now it's 1
```

Esempio di traccia radioattiva per una connessione riuscita al cloud:

```
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (note): Server did not reply to
V2 method. Falling back to V1.
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Cloud authentication 2
step failed, trying legacy mode
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (note): Set connection status
from HTTP_CON_AUTH_PROGRESS_2STEP to HTTP_CON_AUTH_IDLE
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): tenant ID:
vasilijeperovic
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): hostname is:
data.dnaspaces.eu
2020/02/24 18:53:20.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (note): Starting authentication
V1 using Heartbeat URL https://data.dnaspaces.eu/api/config/v1/nmspconfig and Data URL
https://data.dnaspaces.eu/networkdata
2020/02/24 18:53:20.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (note): Set connection status
from HTTP_CON_AUTH_IDLE to HTTP_CON_AUTH_PROGRESS_1STEP
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): tenant ID:
vasilijeperovic
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): hostname is:
data.dnaspaces.eu
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Authenticator V1 get
heartbeat host: https://data.dnaspaces.eu/api/config/v1/nmspconfig
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Authenticator V1 get
access token: eyJ0eX[information omitted]rpmRq0g
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-db] [11100]: (debug): DNSs used for cloud
services: 208.67.222.222,208.67.220.220
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): Using nameservers:
```

208.67.222.222,208.67.220.220
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): **IP resolution preference is set to IPv4**
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-https] [11100]: (debug): **Not using proxy for cloud services**
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): Found bundle for host data.dnaspaces.eu: 0xab764f98 [can multiplex]
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): Re-using existing connection! (#0) with host data.dnaspaces.eu
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): **Connected to data.dnaspaces.eu** (63.33.127.190) **port 443** (#0)
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): Using Stream ID: 3 (easy handle 0xab761440)
2020/02/24 18:53:21.636 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): POST /api/config/v1/nmspconfig/192.168.1.10?recordType=nmsp_hrbt_init&jwttoken=eeyJ0eX[information omitted]70%3A69%3A5a%3A74%3A8e%3A58 HTTP/2
Host: data.dnaspaces.eu
Accept: */*
Accept-Encoding: gzip

2020/02/24 18:53:21.665 {nmspd_R0-0}{1}: [nmsp-dump-https] [11100]: (debug): **We are completely uploaded and fine**
HTTP/2 200

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).