

直接接続によるDNA空間およびCatalyst 9800またはEmbedded Wireless Controller(EWC)の設定とトラブルシューティング

内容

[概要](#)

[前提条件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[コントローラの設定](#)

[ルート証明書のインストール](#)

[Webインターフェイス経由の設定](#)

[CLIによる設定](#)

[ロケーション階層へのEWCのインポート](#)

[Cisco DNAスペースのロケーション階層の編成](#)

[トラブルシューティングと一般的な問題](#)

[一般的な問題](#)

[放射能追跡](#)

概要

Mobility Expressの代わりに、シスコの最新の9000シリーズのアクセスポイント(9115、9117、9120、9130)はEmbedded Wireless Controller(EWC)イメージを実行できます。EWCはCisco 9800 WLCコードに基づいており、1つのアクセスポイントが最大100台の他のAPのコントローラとして機能できます。

EWCまたはCatalyst 9800は、次の3つの方法でDNA Spacesクラウドに接続できます。

1. 直接接続
2. DNAスペースコネクタ経由
3. Cisco Connected Mobile Xperience(CMX)オンプレミスアプライアンスまたはVM経由

DNA空間との統合は、EWCのすべてのバージョンでサポートされています。この記事では、手順が同じであるため、Catalyst APと9800の両方のEWCでの直接接続のセットアップとトラブルシューティングのみを取り上げます。

重要：直接接続は、最大50台のクライアントを導入する場合にのみ推奨されます。より大きい場合は、DNAスペースコネクタを使用します。

前提条件

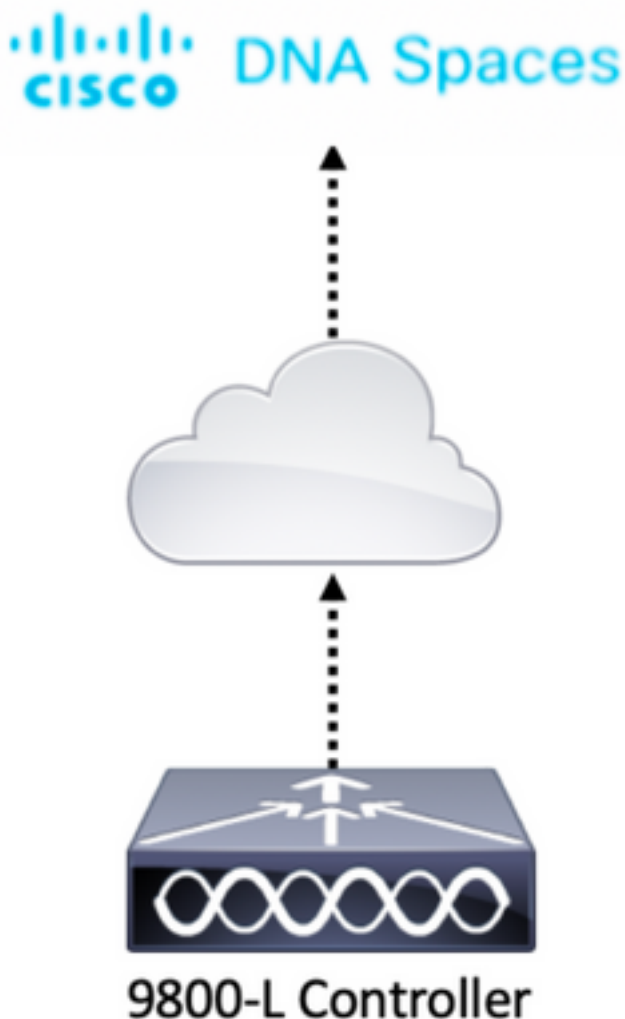
使用するコンポーネント

- 組み込みワイヤレスコントローライメージバージョン17.1.1または16.12.1を使用する Catalyst 9800-L
- 9115 AP
- DNA Spacesクラウド

この記事で概説する手順は、EWCまたは9800がすでに導入され、動作するWebインターフェイスとSSHがあることを前提としています。

設定

ネットワーク図



コントローラの設定

DNA SpacesクラウドノードとコントローラがHTTPSプロトコルを介して通信しています。このテストセットアップでは、コントローラは完全なインターネットアクセスを持つNATの背後に配置されています。

ルート証明書のインストール

コントローラを設定する前に、DigiCertルート証明書をダウンロードする必要があります。コントローラにSSH接続し、次のコマンドを実行します。

```
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.
```

EWCにはデフォルトでCisco DNSサーバを使用してDNSが設定されていますが、これは9800コントローラに必要な手順です。

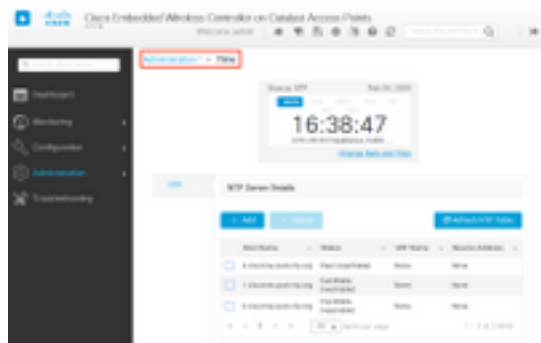
証明書がインストールされたことを確認するには、次のコマンドを実行します。

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

Webインターフェイス経由の設定

コントローラをDNA Spacesに接続するには、NTPサーバとDNSサーバを設定し、少なくとも1つのAPを接続する必要があります。

EWCのWebインターフェイスを開き、[Administration] > [Time]に移動します。WLCがNTPサーバと同期されていることを確認します。デフォルトでは、EWCはciscome.pool.ntp.org NTPサーバを使用するように事前設定されています。9800の場合は、同じNTPまたは優先するNTPサーバを使用できます。



[Administration] > [DNS] に移動し、DNSサーバが追加されたことを確認します。デフォルトでは、EWCはCisco Open DNSサーバを使用するように事前設定されています。

Cisco Embedded Wireless Controller on Catalyst Access Points
17.1.15
Welcome admin

Administration > DNS

DNS Loopback **ENABLED**

+ Add - Delete

IP Address
<input type="checkbox"/> 208.67.222.222,208.67.220.220

1 - 1 of 1 items

[Configuration] > [Wireless] > [Access Points] で、少なくとも1つのAPが加入していることを確認します。このAPは、EWCが実行されているAPと同じにすることができます。

Cisco Embedded Wireless Controller on Catalyst Access Points
17.1.15
Welcome admin

Configuration > Wireless > Access Points

All Access Points

Current Primary: 9115
Current Stand...: Not Applicable
Preferred Mas...: Not Configured

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Policy Tag	Site Tag	RF Tag	Tag Source
9115	C9115AXI-E	2	✓	192.168.1.11	f80f.6f15.3fc0	Flex	Registered	Vasa5	default-site-tag	default-rf-tag	Static

1 - 1 of 1 access points

DNA Spacesクラウドで、ホームページから[Setup] > [Wireless Networks] > [Connect WLC/Catalyst 9800 Directly] に移動します。[View Token] をクリックします。

Connect your wireless network

Connect WLC/Catalyst 9800 Directly

1. Install Span Conditions

2. Configure Tables in WLC

3. Import Controllers into Location Hierarchy

View Token

[Switch]タブをCisco Catalyst 9800に切り替えます。トークンとURLをコピーします。

Token for WLC to connect to DNA Spaces

WLC: Cisco Catalyst 9800

Follow the steps below to configure token in Cisco Catalyst 9800 Series Wireless Controller CLI

- Once you logged in,
 - type "config" command
- Execute the following steps in CLI mode
 - no nmsp cloud-services enable
 - nmsp cloud-services server url <https://vasilijeperovic.dnaspaces.eu>
 - nmsp cloud-services server token [TOKEN]

TOKEN

eyJ0eXAI0iJKV1QlLCJI
TY18krprpmRq0g

d.nmsp cloud-services enable

- Exit from config
- type "exit" command

WLC Webインターフェイスで、[Configuration] > [Services] > [Cloud Services] > [DNA Spaces] に移動します。URLと認証トークンを貼り付けます。HTTPプロキシが使用されている場合は、そのIPアドレスとポートを指定します。

Configuration > Services > Cloud Services

Network Assurance **DNA Spaces**

DNA Spaces Service Configuration

Enable Service

Service URL
Eg. https://<tdf_id>.cmxcisco.com

Authentication Token

HTTP Proxy (Hostname/IP)

Port

[Monitoring] > [Wireless] > [NMSP] で、接続が正常に確立されたことを確認します。[Service Status]に緑色の矢印が表示されます。

Monitoring > Wireless > NMSP

Cloud Services DNA Spaces Information Statistics Service Subscription Controller Settings

DNA Spaces Services Status		DNA Spaces Services Statistics	
Server	https://vasilijeperovic.dnaspaces.eu	Tx DataFrames	7
IP Address	63.33.127.190	Rx DataFrames	2
DNA Spaces Service	Enabled	Tx Heartbeat Request	4
Connectivity	https UP	Heartbeat Timeout	0
Service Status	UP	Rx Subscr Request	2
Last Request Status	HTTP/2.0 200 OK	Tx DataBytes	512
Heartbeat Status	OK	Rx DataBytes	74
		Tx Heartbeat Fail	0
		Rx Data Fail	0
		Tx Data Fail	0

次の章をスキップし、「コントローラを場所階層にインポート」に移動します。

CLIによる設定

NTPが設定され、同期されていることを確認します。

```
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

```

新しいNTPサーバを追加するには、`ntp server <ntp_ip_addr>`コマンドを使用します。

DNSサーバが設定されていることを確認します。

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

```

208.67.222.222
208.67.220.220

```

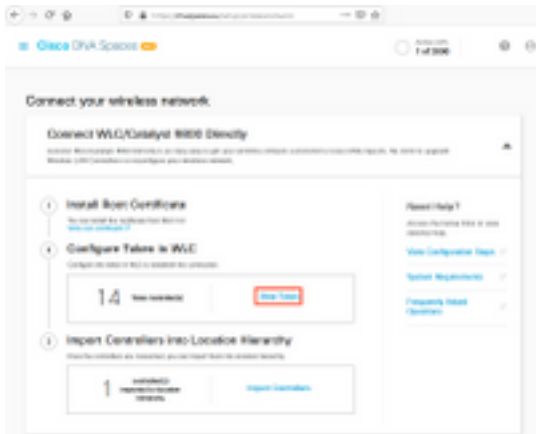
新しいDNSサーバを追加するには、`ip name-server <dns_ip>`コマンドを使用します。

APが加入したことを確認するには、次の手順を実行します。

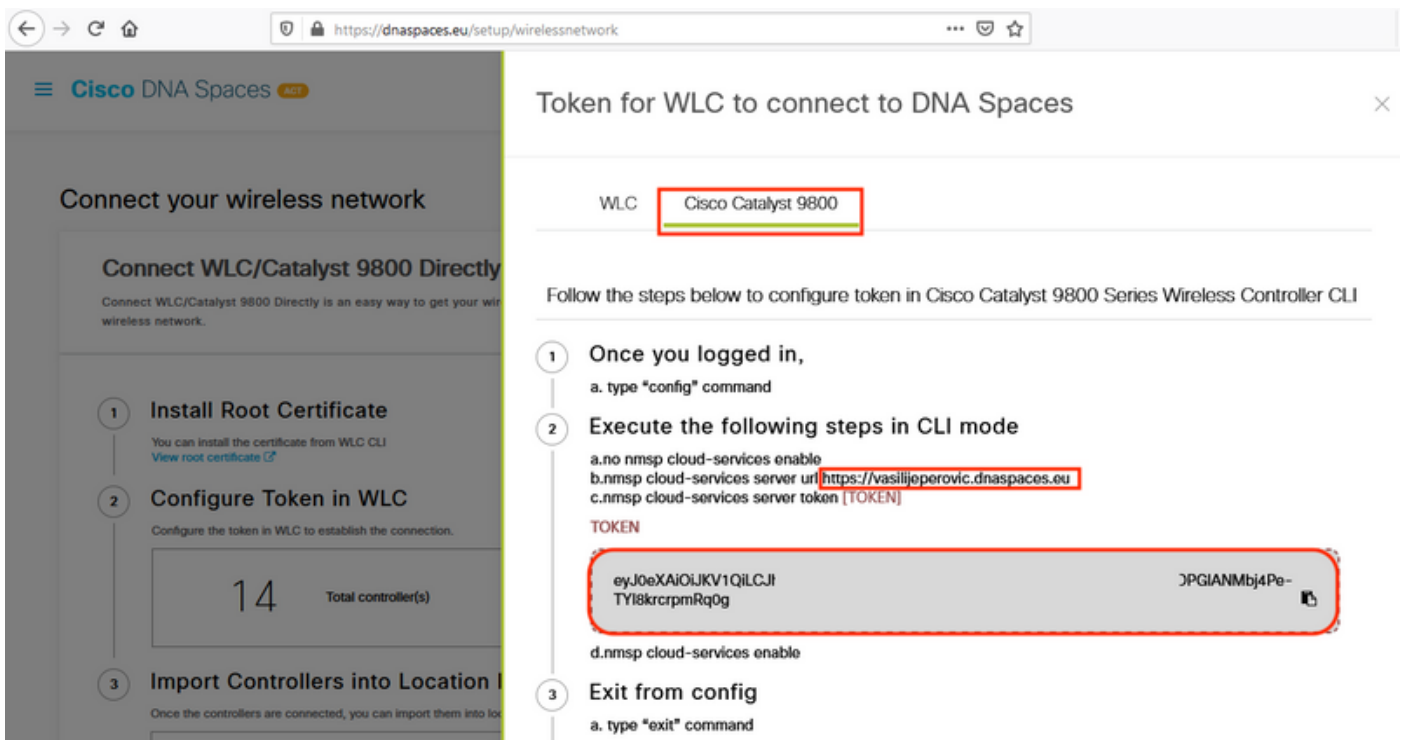
EWC#show ap status

AP Name	Status	Mode	Country
9115	Enabled	Local	BE

前述のように、DNA Spacesクラウドにアクセスし、[Setup] > [Wireless Networks] > [Connect WLC/Catalyst 9800 Directly] に移動して、[View Token] をクリックします。



[Switch]タブをCisco Catalyst 9800に切り替えます。トークンとURLをコピーします。



Token for WLC to connect to DNA Spaces

WLC: Cisco Catalyst 9800

Follow the steps below to configure token in Cisco Catalyst 9800 Series Wireless Controller CLI

- 1 Once you logged in,
 - a. type "config" command
- 2 Execute the following steps in CLI mode
 - a. no nmsp cloud-services enable
 - b. nmsp cloud-services server url <https://vasilijeperovic.dnaspaces.eu>
 - c. nmsp cloud-services server token [TOKEN]

TOKEN

eyJ0eXAiOiJKV1QiLCJl... JPGIANMbj4Pe-

 - d. nmsp cloud-services enable
- 3 Exit from config
 - a. type "exit" command

次のコマンドを実行します。

```
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
```

DNA Spacesクラウドとの接続が正常に確立されたことを確認するには、次のコマンドを実行します。


```
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
```

ロケーション階層へのEWCのインポート

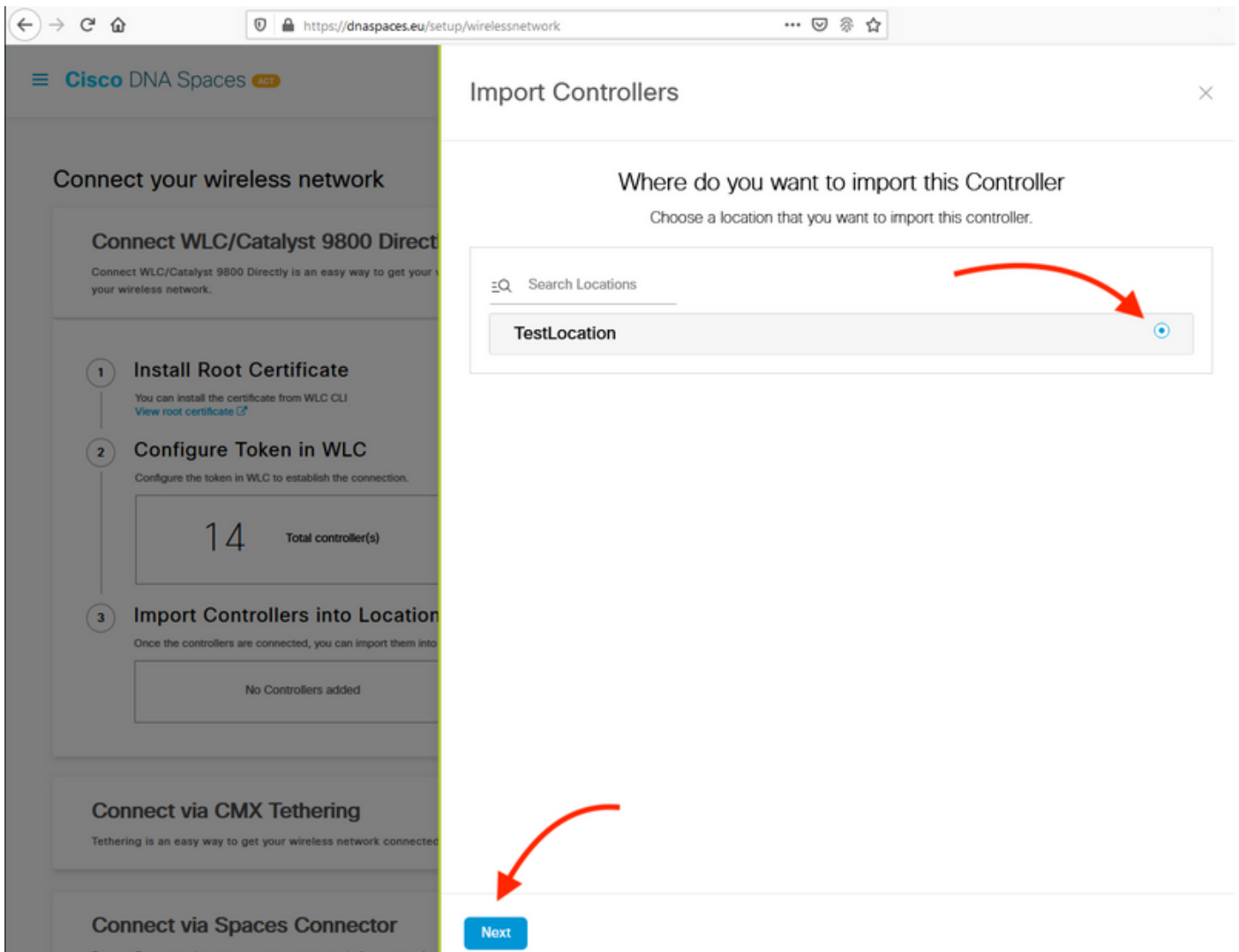
ステップ1：残りの設定はDNA空間で行います。[Setup] > [Wireless Networks] > [Connect WLC/Catalyst 9800 Directly] で、[Import Controllers] をクリックします。

The screenshot displays the Cisco DNA Spaces web interface for connecting WLC/Catalyst 9800 controllers. The main heading is "Connect WLC/Catalyst 9800 Directly". Below the heading, there are three numbered steps:

- 1 Install Root Certificate**: You can install the certificate from WLC CLI. [View root certificate](#)
- 2 Configure Token in WLC**: Configure the token in WLC to establish the connection. A box shows "14 Total controller(s)" and a [View Token](#) button.
- 3 Import Controllers into Location Hierarchy**: Once the controllers are connected, you can import them into location hierarchy. A box shows "1 controller(s) imported to location hierarchy" and a red-bordered [Import Controllers](#) button.

On the right side, there is a "Need Help?" section with links to "View Configuration Steps", "System Requirements", and "Frequently Asked Questions". The top navigation bar includes "Cisco DNA Spaces" and "Active APs 1 of 2000".

ステップ2：アカウント名の横にあるオプションボタンをオンにし、[Next (次へ)]をクリックします。追加したロケーションがある場合は、次のリストに表示されます。



ステップ3 : コントローラのIPアドレスを検索し、その横のチェックボックスをオンにして、[Next]を押します。



ステップ4 : 他のロケーションが追加されていないため、[Finish]をクリックします。



ステップ5:[Location Hierarchy]にWLCが正常にインポートされたことを示すプロンプトがポップアップ表示されます。



Controller successfully
imported to location
hierarchy!

Total controllers added : 1
Total number of APs : 1
Total number of Locations : 0

Would you like to organize your location
hierarchy

Yes, take me to location hierarchy

No, Continue with Setup

WLCがクラウドに正常に接続されたため、他のすべてのDNA Spaces機能の使用を開始できます。

注：NMSPトラフィックは常に、DNA空間またはCMXとの通信にワイヤレス管理インターフェイスを使用します。これは、9800コントローラ設定では変更できません。インターフェイス番号は関係なく、9800コントローラ上でワイヤレス管理インターフェイスとして割り当てられたインターフェイスが使用されます。

Cisco DNAスペースのロケーション階層の編成

新しいロケーション階層が必要な場合、または「9800コントローラをCisco DNAスペースにインポートする」セクションのステップ4でロケーションが追加されていない場合は、手動で設定できます。

ロケーション階層は、分析情報に使用され、それに基づいてキャプティブポータルルールが設定されるため、DNA空間の最も重要な機能の1つです。ロケーション階層がより詳細に表示されるほど、キャプティブポータルルールやDNA空間から取得できる情報に対してより細かい制御が行われます。

DNA Spacesのロケーション階層機能は、Cisco Prime InfrastructureまたはCisco CMXの従来の階層と同じように機能しますが、名前は大きく異なります。コントローラがロケーション階層にインポートされる場合、従来の階層からのキャンパスと同じものになります。コントローラの下に、**建物**と同等のグループを作成することができます。次に、グループの下で床に相当するネットワークを設定できます。最後に、ネットワークの下で、従来のロケーション階層で使用されていたレベルと同じレベルに維持されたゾーンを作成できます。合計すると、これが等価になります。

表1従来の階層レベルとDNA空間レベルの等価。

DNA空間階層	従来の階層
コントローラ (ワイヤレスネットワーク)	キャンパス
Group	建物
Network	フロア
Zone	Zone

ステップ1：グループを設定します。グループは、ビジネスに応じて、位置情報、ブランド、またはその他の種類のグループに基づいて、複数の場所またはゾーンを編成します。[Location Hierarchy]に移動し、**既存のワイヤレスコントローラ上でマウスを移動し、[Create Group]をクリックします。**



ロケーションレベルの名前を変更するには、ネットワーク上でマウスを移動し、[名前の変更]をクリックします。

ステップ2：グループ名を入力し、[Unconfigured location]を選択します。コントローラでインポートされたすべてのAPが含まれます。これらのAPは、必要に応じてネットワークとゾーンにマッピングされます。[Add] をクリックします。

Add Group

Select Location

 Unconfigured

ステップ3：ネットワークを作成します。Cisco DNA Spacesでは、物理的な建物内のすべてのアクセスポイントがLocationとして統合され、ネットワークまたは場所が定義されています。グループ上でマウスを移動し、[ネットワークの追加]をクリックします。

MEX-EAST-1		11	8	0	4	0	0
+	5508-1-CMX	1	1	0	2	0	0
+	5508-2-Connector-Campus	2	2	0	0	0	0
+	5520-DirectConnect	2	1	0	1	0	0
-	9800L-Mexico-Campus	1	1	0	0	0	0
+	MXC-10-Building	1	1	0	0	0	0
+	efmLocation	2	2	0	0	0	0
+	Lisboa	3	1	0	0	0	0

MORE ACTIONS

- Rename MXC-10-Bui...
- Create Group
- Edit Group
- Add Network**
- Add/Edit Metadata
- Delete Location

注：これは、ビジネスのインサイトとロケーション分析の計算がここから生成されるため、ロケーション階層で最も重要なノードです。

ステップ4：ネットワーク名とアクセスポイントのプレフィックスを入力し、[Fetch]をクリックします。DNAスペースは、そのプレフィックスを持つコントローラに関連付けられたすべてのAPを取得し、APをフロアに追加できるようにします。プレフィックスは1つだけ入力できます。

Add Network ✕

10.10.30.5

NETWORK NAME
Second Floor

ACCESS POINT PREFIX
28 **Fetch**

Matching access points will be shown below

1 Following access points are discovered based on provided prefix and will be added to this network.

2802AP-9800L

Done

ステップ5：ネットワークでより多くのプレフィックスが必要な場合。ネットワーク名をクリックし、[場所情報]タブで、[Access Points Prefix Used]の横の[編集]ボタンをクリックします。

[Back](#) | MEX-EAST-1 > 9800L-Mexico-Campus > **MXC-10-Building** > **Second Floor**

Location Info | Access Points | Rules | Maps | Team | Camera

Second Floor ✎

○ NODE TYPE Network 📄 NETWORK REFERENCE 28

Access Points Prefix Used **Edit**

28

Location Data **Edit**

プレフィックス名を入力し、[+プレフィックスの追加]をクリックして、[保存]をクリックします。必要に応じてすべてのプレフィックスについて繰り返し、APをネットワークにマッピングし、後でAPをゾーンに関連付けることができます。

Location name
Second Floor

Choose Access Points that are part of this location

Provide one or more prefixes that can be used to automatically match the Access Points belonging to this location

Prefix	Added Prefixes
28	28 1 APs

1 Access Points match the prefix "28"

2802AP-9800L Second Floor

+ Add Prefix

Cancel Save

ステップ6：ゾーンを作成します。ゾーンは、建物またはロケーションのセクション内のアクセスポイントの集合です。物理的な建物または組織の部門に基づいて定義できます。ネットワーク上でマウスを移動し、[Add Zone]を選択します。

MEX-EAST-1

+	5508-1-CMX	12	0	0	4	0	0
+	5508-2-Connector-Campus	1	1	0	2	0	0
+	5520-DirectConnect	2	2	0	0	0	0
-	9800L-Mexico-Campus	2	1	0	1	0	0
-	MXC-10-Building	2	1	0	0	0	0
-	Second Floor	1	1	0	0	0	0
-	Unconfigured	1	0	0	0	0	0
+	efmLocation	2	2	0	0	0	0
+	Lisboa	3	1	0	0	0	0

MORE ACTIONS

- Rename Second Flo...
- Add Zone
- Add/Edit Metadata
- Delete Location

ステップ7:[Zone Name]を設定し、ゾーンのAPを選択して、[Add]をクリックします。



Wireless-Zone

Select Access Points

Network Access Points

2802AP-9800L (10:b3:d6:94:00:e0)

Add

トラブルシューティングと一般的な問題

一般的な問題

[Monitoring] > [Wireless] > [NMSP] (または `show nmsp cloud-services summary` コマンドを実行) の下のWebインターフェイスページには、通常、接続障害に関する十分な情報が表示されます。次のスクリーンショットには、いくつかの一般的な間違いが示されています。

1. DNSが設定されていない場合、エラーメッセージ「*Transfer error (6): Could not resolve host name*」というメッセージが表示されます。

The screenshot shows the Cisco Embedded Wireless Controller web interface. The breadcrumb navigation is **Monitoring > Wireless > NMSP**. The page displays the following information:

DNA Spaces Services Status		DNA Spaces Services Statistics	
Server	https://vasilijeperovic.dnaspaces.eu	Tx DataFrames	0
IP Address	127.0.0.1	Rx DataFrames	0
DNA Spaces Service	Enabled	Tx Heartbeat Request	3
Connectivity	DOWN	Heartbeat Timeout	0
Service Status	Transfer error (6): Couldn't resolve host name	Rx Subscr Request	0
Last Request Status		Tx DataBytes	0
		Rx DataBytes	0
Heartbeat Status		Tx Heartbeat Fail	1
		Rx Data Fail	0
		Tx Data Fail	0

証明書がインストールされていない、またはNTPが両方とも設定されていない場合、次のエラーメッセージが表示されます。「転送エラー(60):SSLピア証明書またはSSHリモートキーが正しくありませんでした」:

The screenshot shows the Cisco Embedded Wireless Controller web interface. The breadcrumb navigation is **Monitoring > Wireless > NMSP**. The page displays the following information:

DNA Spaces Services Status		DNA Spaces Services Statistics	
Server	https://vasilijeperovic.dnaspaces.eu	Tx DataFrames	0
IP Address	208.67.222.222	Rx DataFrames	0
DNA Spaces Service	Enabled	Tx Heartbeat Request	2
Connectivity	DOWN	Heartbeat Timeout	0
Service Status	Transfer error (60): SSL peer certificate or SSH remote key was not OK	Rx Subscr Request	0
Last Request Status		Tx DataBytes	0
		Rx DataBytes	0
Heartbeat Status		Tx Heartbeat Fail	1
		Rx Data Fail	0
		Tx Data Fail	0

放射能追跡

EWCは、他のすべての9800コントローラと同様に、常時接続のRadioactive Tracesをサポートしています。これらを収集し、接続が確立されない理由を確認するには、EWCが到達しているDNA空間のIPアドレスを知る必要があります。これは、[Monitor] > [Wireless] > [NMSP] の下また

はCLIから確認できます。

```
EWC#show nmsp status
```

```
NMSP Status
```

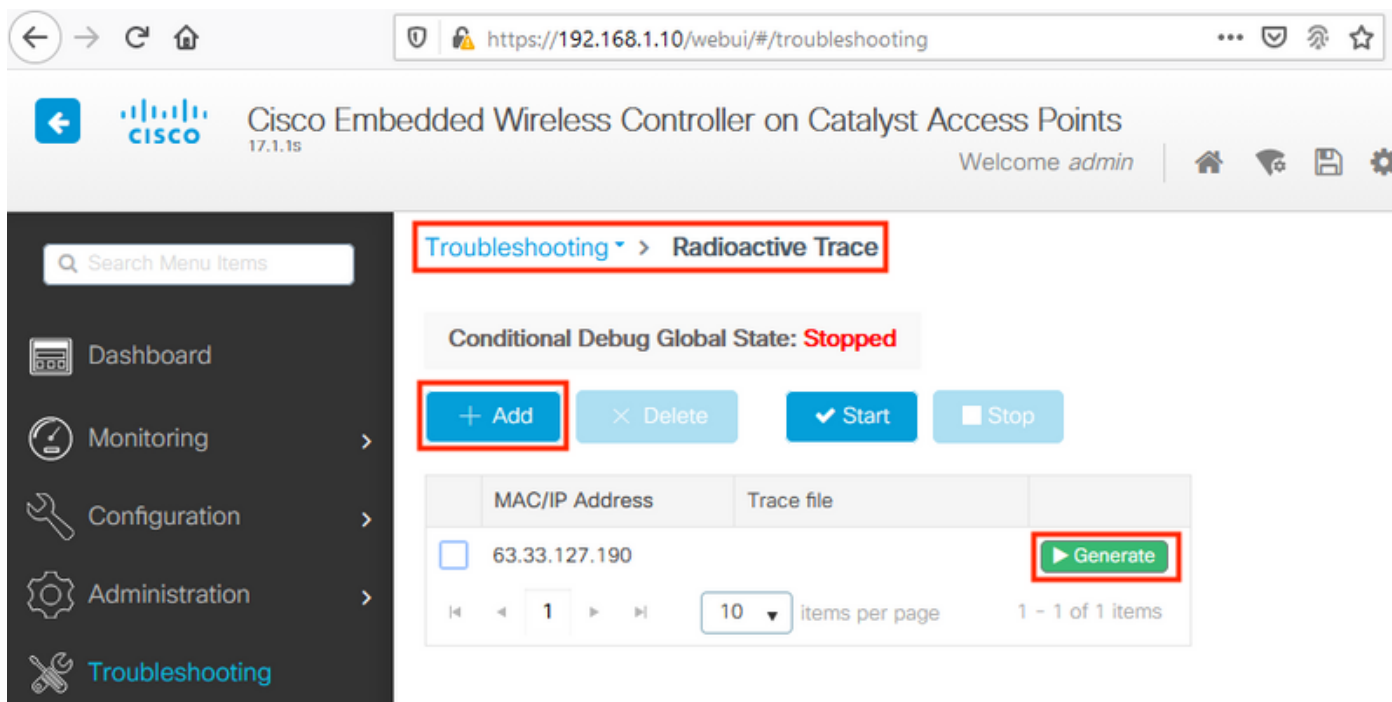
```
-----
```

```
CMX IP Address      ActiveTx Echo Resp  Rx Echo Req  Tx Data Rx Data Transport
```

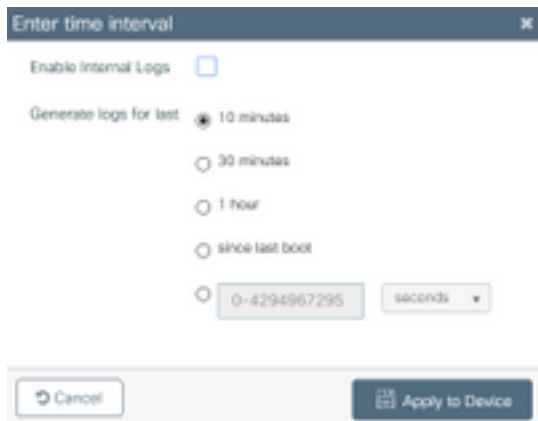
```
-----
```

```
63.33.127.190      Active0              0             38           2           HTTPS
```

このテストセットアップのEWCは63.33.127.190に接続しています。このIPアドレスをコピーし、[トラブルシューティング] > [Radioactive Trace] に移動します。[Add]をクリックし、IPアドレスを貼り付けて[Generate]をクリックします。



[Generate logs for the last 10 minutes]を選択し、[Apply]をクリックします。内部ログを有効にすると、分析が困難な大量のデータが生成される可能性があります。



注: DNS、NTPの設定が誤っており、証明書が不足していても、Radioactive Tracesは生成されません

ファイアウォールがHTTPSをブロックしている場合のRadioactive Traceの例：

```
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmstp-main] [11100]: (note): CMX [63.33.127.190]:[32]: closing
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmstp-https] [11100]: (debug): Called 'is_ready'
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmstp-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}: [nmstp-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}: [nmstp-enc] [11100]: (debug): Decoding control message structure
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmstp-enc] [11100]: (debug): Control structure was successfully decoded from message
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmstp-db] [11100]: (debug): Retrieving CMX entry: 32
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmstp-db] [11100]: (ERR): CMX entry 32 not found
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmstp-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}: [nmstp-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}: [nmstp-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}: [nmstp-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}: [nmstp-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}: [nmstp-main] [11100]: (note): CMX [63.33.127.190]:[32]: down
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmstp-main] [11100]: (debug): NMSP timer 0xab774af4: close
2020/02/24 18:40:30.774 {nmspd_R0-0}{1}: [nmstp-https] [11100]: (debug): Decrease reference count for https_con object: Now it's 1
```

クラウドとの接続に成功したRadioactive Traceの例：

```
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmstp-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}: [nmstp-https] [11100]: (debug): Cloud authentication 2 step failed, trying legacy mode
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmstp-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}: [nmstp-https] [11100]: (debug): tenant ID: vasilijeperovic
2020/02/24 18:53:20.634 {nmspd_R0-0}{1}: [nmstp-https] [11100]: (debug): hostname is: data.dnaspaces.eu
2020/02/24 18:53:20.635 {nmspd_R0-0}{1}: [nmstp-https] [11100]: (note): Starting authentication V1 using Heartbeat URL https://data.dnaspaces.eu/api/config/v1/nmstpconfig and Data URL https://data.dnaspaces.eu/networkdata
2020/02/24 18:53:20.635 {nmspd_R0-0}{1}: [nmstp-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}: [nmstp-https] [11100]: (debug): tenant ID: vasilijeperovic
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmstp-https] [11100]: (debug): hostname is: data.dnaspaces.eu
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmstp-https] [11100]: (debug): Authenticator V1 get heartbeat host: https://data.dnaspaces.eu/api/config/v1/nmstpconfig
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmstp-https] [11100]: (debug): Authenticator V1 get access token: eyJ0eX[information omitted]rpmRq0g
2020/02/24 18:53:21.635 {nmspd_R0-0}{1}: [nmstp-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}: [nmstp-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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。