

Optimice el rendimiento de CMX

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Señales de un nodo CMX sobrecargado](#)

[Redistribuir la carga CMX](#)

[Filtrado de Direcciones MAC Administradas Localmente](#)

[Seguimiento de clientes de sondeo](#)

[Tweaking del algoritmo de detección](#)

[Aumento de los recursos de VM](#)

[Agrupación CMX \(anteriormente conocido como Agrupación AP\)](#)

[Implementaciones de nodos adicionales](#)

[Espacios de ADN: descarga del trabajo a la nube](#)

[Errores relevantes](#)

Introducción

En este artículo se explica cómo reconocer y después redistribuir la carga de un único nodo CMX (Connected Mobile eXperience) para dar cabida a una gran cantidad de dispositivos de los que se realiza un seguimiento. Problemas como este se observan a menudo en implementaciones extremadamente grandes en áreas públicas o en configuraciones donde se habilita el seguimiento de clientes de sondeo.

Prerequisites

Requirements

En este artículo se da por sentado que conoce la configuración básica de un CMX y se centra únicamente en consejos y trucos para optimizar el rendimiento en implementaciones de gran tamaño.

Componentes Utilizados

Todos los comandos y ejemplos mostrados en este artículo se realizaron en el WLC 3504 que ejecuta código 8.8.125 y CMX 10.6.1 que se ejecuta en el dispositivo 3375.

Señales de un nodo CMX sobrecargado

La sobrecarga de un nodo CMX puede resultar en varios problemas diferentes:

- Servicios que no pueden comenzar

- Servicios que se detienen o se bloquean de forma repentina
- Servicio de análisis que muestra 0 clientes activos
- Alarmas y alertas por correo electrónico que indican que el servicio de análisis o de ubicación se encuentra en un estado crítico
- Incapacidad para establecer HA entre el nodo CMX primario y secundario

Redistribuir la carga CMX

Filtrado de Direcciones MAC Administradas Localmente

Debido a la creciente preocupación por la privacidad, a partir de la versión IOS 8 de 2014, los fabricantes de smartphones han comenzado a implementar una función llamada aleatorización MAC, en la que los dispositivos utilizarían una nueva dirección MAC generada aleatoriamente cada vez que enviaran una solicitud de sonda. Al generar una dirección MAC aleatoria, los fabricantes pueden decidir utilizar una dirección MAC "administrada localmente" que tiene un bit especial que indica que la dirección es aleatoria o simplemente generar una dirección completamente aleatoria que no se puede distinguir de una dirección real. Un número muy pequeño de clientes utiliza su dirección MAC real al sondear.

CMX tiene una manera de filtrar estas direcciones MAC aleatorias falsas. En System->Settings->Filtering (Sistema->Parámetros->Filtrado), asegúrese siempre de que esté activada la opción Enable Locally Administered MAC Filter (Activar filtrado MAC administrado localmente).

Nota: Este campo se ha eliminado de la interfaz web en CMX 10.6.0 y siempre está habilitado de forma predeterminada

SETTINGS ×

- Tracking
- Filtering
- Location Setup
- Data Privacy
- Data Retention
- Mail Server
- > Controllers and Maps Setup
- Upgrade
- High Availability

Filtering Parameters

Duty Cycle Cutoff (Interferer)

RSSI Cutoff (Probing Only Client)

Exclude Probing Only clients

Enable Locally Administered MAC Filtering

Enable Location MAC Filtering

Enable Location SSID Filtering

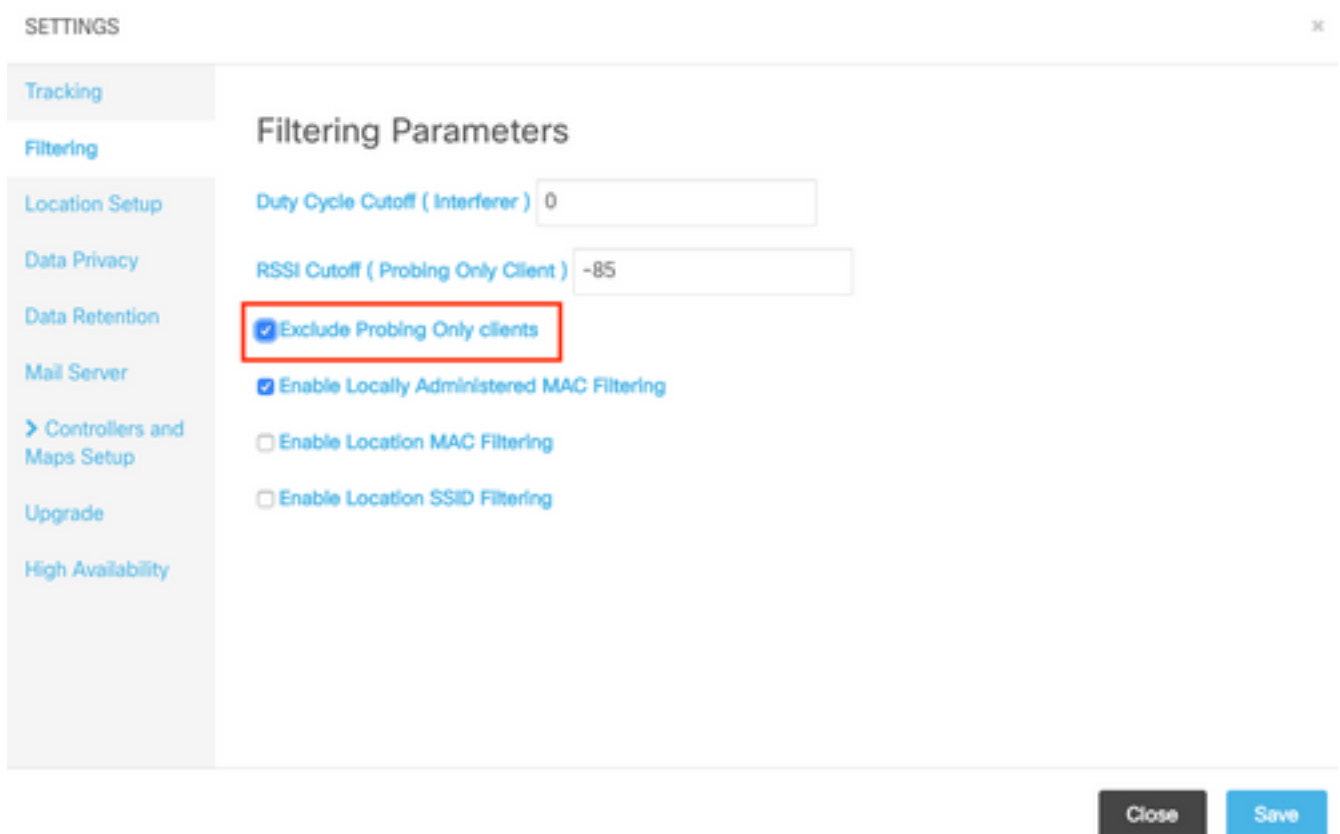
Seguimiento de clientes de sondeo

La causa principal más común de una sobrecarga de CMX con la que Cisco TAC trata es el seguimiento de los clientes que solo realizan sondeos. La activación de esta función permite el seguimiento de la ubicación de clientes no asociados. Las áreas públicas abiertas como centros comerciales y estaciones de tren con un gran número de visitantes muy a menudo superarán las limitaciones incluso de un nodo CMX de alto nivel.

En las configuraciones que realizan un seguimiento de los clientes de sondeo, las direcciones MAC generadas aleatoriamente también tienen un gran impacto en el número de clientes.

Algunos fabricantes como Apple están siguiendo un estándar y usando direcciones MAC aleatorias administradas localmente al sondear, lo que significa que **los dispositivos iPhone nunca serán detectados por CMX** al sondear y no asociarse. Los dispositivos que no siguen el estándar y que utilizan direcciones MAC aleatorias que no se administran localmente serán **registrados por CMX como un nuevo cliente cada vez que envían la solicitud de sonda** (lo que puede suceder cada par de segundos). Como resultado, el recuento de clientes de sondeo puede ser significativamente mayor/menor que el número real de dispositivos en la red.

El seguimiento de los clientes de sondeo se puede inhabilitar desde las interfaces web CMX en System->Settings->Filtering (Sistema->Parámetros->Filtrado), marcando la opción "Excluir clientes de sondeo":



Debido a todas las variaciones mencionadas, el sondeo del número de clientes no debe utilizarse como contador de clientes y Cisco TAC recomienda encarecidamente no realizar el seguimiento de los clientes de sondeo.

Tweaking del algoritmo de detección

Al ajustar las opciones de filtrado en CMX, el número de clientes de sondeo que se registran puede estar muy limitado. Hay dos opciones principales que tienen un impacto significativo en la

detección de clientes (especialmente en la detección de solo sondeo):

1. Reducción del ciclo de servicio (interferente)
2. RSSI Cutoff
3. Cantidad mínima de AP que necesitan escuchar al cliente, para que se registre

En zonas densas y muy pobladas, se espera que tenga un gran número de interferencias. Los dispositivos como los relojes Bluetooth no tendrán un gran impacto en la red. Al aumentar el valor del ciclo de trabajo de los interferencias más cerca, por ejemplo, del 50%, CMX registrará sólo los interferencias fuertes que estén tomando más del 50% del tiempo de aire. Este valor se puede configurar desde la interfaz web de CMX, en System->Settings->Filtering:

Nota: Para evitar el registro de una gran cantidad de datos de interferencias, CMX sólo registra los interferencias que están presentes durante cierto tiempo.

SETTINGS

Tracking

Filtering

Location Setup

Data Privacy

Data Retention

Mail Server

> Controllers and Maps Setup

Upgrade

High Availability

Filtering Parameters

Duty Cycle Cutoff (Interferer) 0

RSSI Cutoff (Probing Only Client) -85

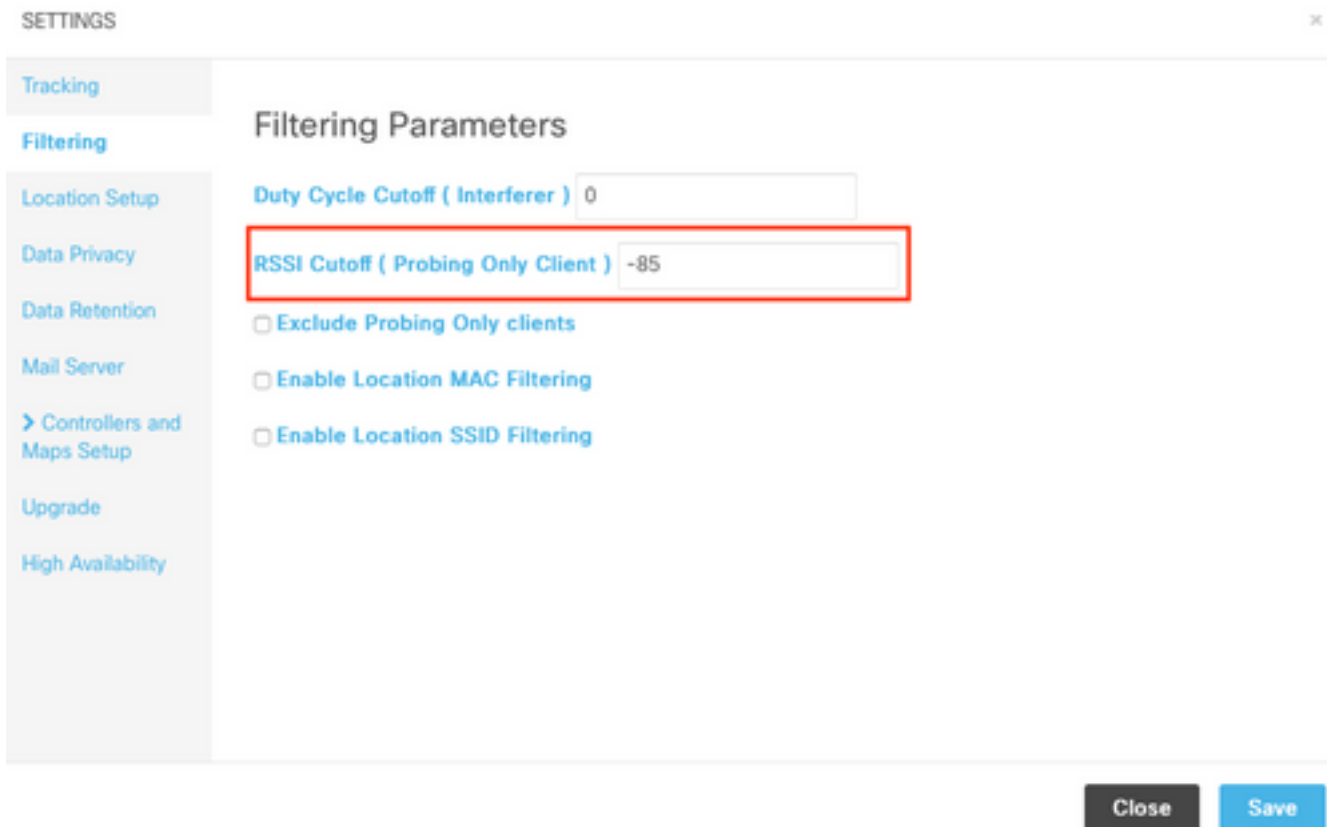
Exclude Probing Only clients

Enable Location MAC Filtering

Enable Location SSID Filtering

Close Save

La función de corte RSSI se utiliza para evitar registrar clientes que pasan por las instalaciones y no entran realmente. Esto puede tener un gran impacto en las implementaciones, ya que solo se permite realizar el seguimiento de clientes con sondeo y se habilita una estación de autobuses o una calle cercana. De forma predeterminada, este valor se establece en -85 dBm. Antes de cambiar este valor, se debe medir el RSSI de un cliente fuera de las instalaciones. Este valor se puede configurar desde la interfaz web de CMX, en System->Settings->Filtering:



A partir de CMX 10.6, cambiar la **cantidad mínima de AP requerida para escuchar a un cliente** para que sea registrado por CMX sólo puede hacerse a través de una llamada de API. En primer lugar, se puede utilizar una solicitud GET para ver la configuración actual:

```
[cmxadmin@mse3375 ~]$ curl -X get http://localhost/api/config/v1/filteringParams/1
{"name":null,"allowedMacs":[],"disallowedMacs":[],"blockedList":[],"noLocationSsids":[],"noAnalyticsSsids":[],"disallowprobingclienttracking":false,"macfilter":false,"ssidfilter":false,"probin
grssicutoff":-
85,"minapwithvalidrssi":1,"filterLocallyAdministered":true,"objectId":0,"dutyCycleCutoff":0}
```

En esta configuración, el valor `minapwithvalidrssi` se establece en 1, que es el valor predeterminado. El cambio de este valor a 3 se puede realizar mediante una solicitud POST. Una vez que se aplican estas configuraciones, el cliente será registrado por CMX una vez que sea escuchado por el tercer AP en RSSI igual o mejor que el mínimo especificado:

```
[cmxadmin@mse3375 ~]$ curl -X POST -H "Content-Type: application/json" -d
'{"minapwithvalidrssi":3}' http://localhost/api/config/v1/filteringParams/1
```

Después de cambiar cualquiera de los valores, asegúrese de realizar una solicitud GET para confirmar que la configuración se ha aplicado correctamente.

Aumento de los recursos de VM

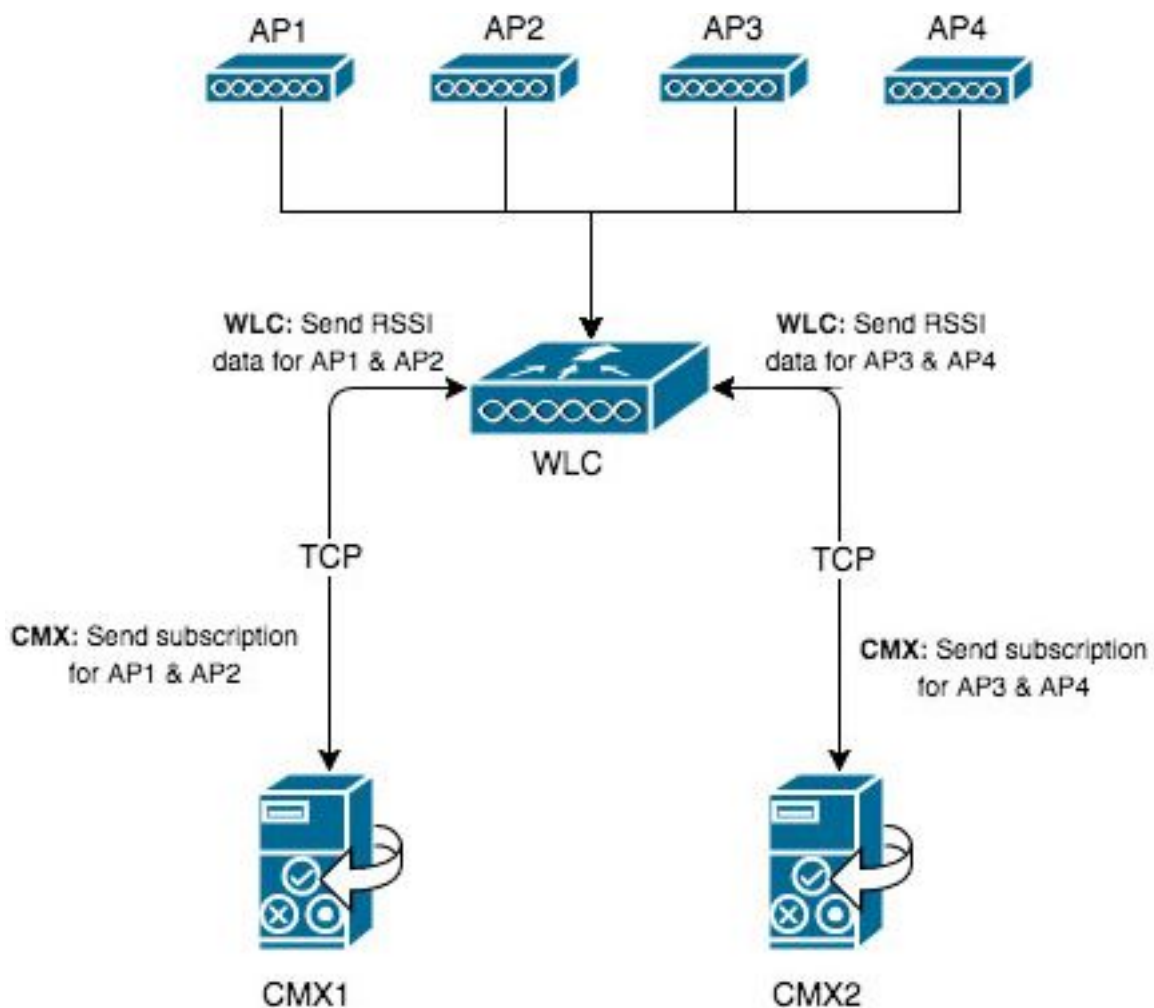
Si un nodo CMX actual se ejecuta en una VM y su tamaño no es suficiente para alojar a todos los clientes, es posible aumentar los recursos de VM y, por lo tanto, su potencia de procesamiento. Simplemente asigne más núcleos de CPU, memoria y espacio en disco. Los requisitos exactos para los nodos CMX de gama baja, estándar y alta se pueden encontrar [AQUÍ](#).

Si la configuración CMX actual ya es un nodo de gama alta, considere otras opciones mencionadas en este artículo.

Nota: Tener una instantánea activa en una VM puede tener un impacto negativo en el rendimiento y no se recomienda para entornos de producción.

Agrupación CMX (anteriormente conocido como Agrupación AP)

CMX Group es una función disponible en CMX 10.5 o posterior y AireOS WLCs que ejecutan las versiones 8.7 o posteriores. Dado que el tren de versión 8.7 no recibirá actualizaciones en el futuro, se recomienda utilizar la versión 8.8 o posterior. Esta función permite que un único controlador distribuya la carga a varios nodos CMX seleccionando grupos de AP y asignando un grupo a un nodo CMX específico. Estos grupos de APs no están relacionados con la función del grupo AP en el WLC.



Los mapas en CMX1 sólo tienen AP1 y AP2 colocados. CMX1 se comunicará con el WLC acerca de los 2 AP que se encuentran en el mapa. Una vez habilitada la función de agrupación de CMX, toda la información registrada por AP1 y AP2 (incluidos los clientes asociados y de sondeo solamente, las interferencias, las balizas BLE, las etiquetas RFID..) se enviará solamente al CMX1.

Un único controlador puede tener hasta 4 conexiones NMSP establecidas en ese momento, lo que significa que se pueden agregar hasta 4 nodos CMX a él. En teoría, con 4 nodos de alto nivel, esto permitiría registrar hasta 360 000 (4 x 90 000) direcciones mac de cliente únicas por día.

Es posible aumentar la cantidad de servidores CMX a los que un WLC puede conectarse con el siguiente comando de prueba

```
(Cisco Controller) >test cloud-server cmx max-tls-connections
test cloud-server cmx max-tls-connections <2-6>
```

Importante: el controlador que ejecuta un código inferior a 8.7 o superior a 8.7 sin la función de agrupamiento CMX habilitada nunca debe ser agregado a varios WLC. Esto puede hacer que se registren datos inexactos, especialmente en las configuraciones HyperLocation.

En cada nodo CMX al que se agregará este controlador, es necesario habilitar la función y reiniciar los servicios:

1. Habilite la función mediante el comando:

```
cmxctl config featureflags nmsplb.cmxgrouping true
```

Reemplazar la palabra true por false inhabilita la función.

2. Reiniciar agente CMX:

```
cmxctl restart agent
```

3. Reinicie el equilibrador de carga NMSP:

```
cmxctl nmsplb stop
```

```
cmxctl nmsplb start
```

4. Para comprobar si la función se ha activado correctamente, ejecute:

```
[cmxadmin@cmx3375 ~]$ cmxctl config featureflags
+-----+-----+
| location.compactlocationhistory      | false |
+-----+-----+
| configuration.oi.host                 | true  |
+-----+-----+
| configuration.apimport                | false |
+-----+-----+
| location.ssidfilterpersistblockedmacs | false |
+-----+-----+
| location.rogueapclienthistory        | false |
+-----+-----+
| nmsplb.cmxgrouping                   | true |
+-----+-----+
| monit                                 | true  |
+-----+-----+
| container.influxdbreporter           | true  |
+-----+-----+
| nmsplb.autolearnssids                 | true  |
+-----+-----+
| configuration.highendbypass           | false |
+-----+-----+
| apiserver.enabled                     | true  |
+-----+-----+
| location.computelocthroughassociatedap | false |
+-----+-----+
| analytics.queueetime                  | false |
+-----+-----+
```

En Monitor > Cloud Services > CMX debe estar visible qué nodo CMX tiene activada la función de agrupación. "Ninguno" indica que la función de agrupación está desactivada, mientras que "consulte Grupos" que está activada.

CISCO | MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Monitor

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Clients
- Sleeping Clients
- Multicast
- Applications
- Lync
- Local Profiling
- Cloud Services
 - CMX**
 - Telemetry
 - Network Assurance
 - Webhook

CMX Server

CMX Server IP	Services	Sub-Services	AP Monitor Service Configuration	Group Subscriptions
10.48.71.41	RSSI	Mobile Station Tags Rogues		see Groups
10.48.39.25	Info	Mobile Station Rogues		None
	RSSI	Mobile Station Tags		
	Info	Mobile Station		
	Statistics	Mobile Station		

Al abrir la página "ver grupo", es posible acceder a la lista de AP a los que está suscrito este nodo CMX.

CMX Server Ip : 10.48.71.41

Group Name	Services	Sub-Services	AP Monitor Service Configuration	AP Subscriptions
	RSSI	Mobile Station		
CMX_10.48.71.41	Info	Mobile Station		list of Aps
	Statistics	Mobile Station		

CMX Server IP : 10.48.71.41

CMX Group Name : CMX_10.48.71.41

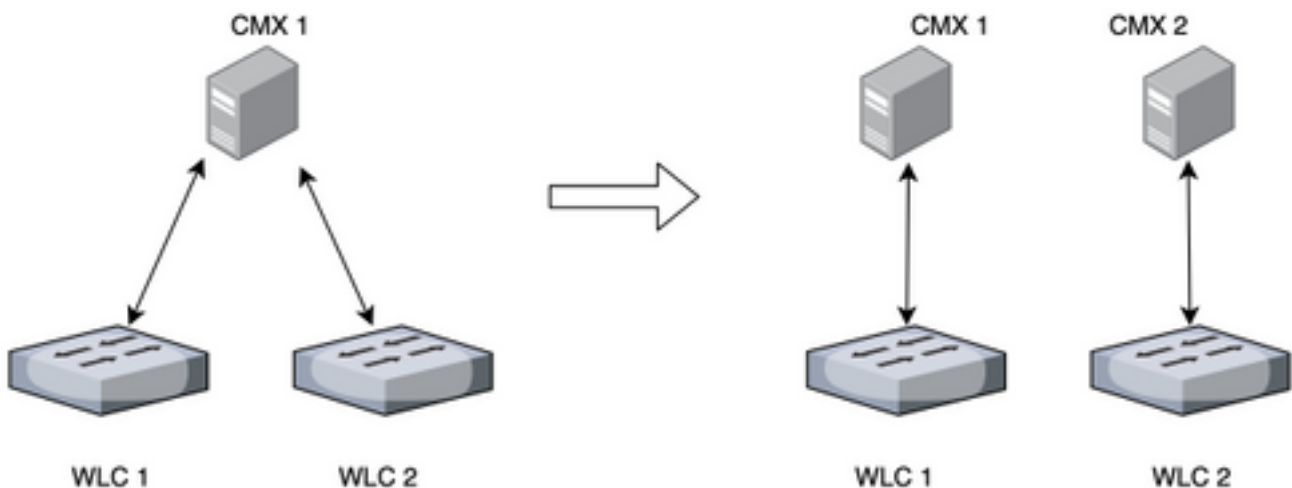
No of AP	Base Radio Mac
1	00:2c:c8:de:2a:20
2	f4:cf:e2:40:a5:c0
3	f4:db:e6:80:9b:a0

De los 4 AP totales asociados a este controlador, sólo 3 se colocan en el mapa CMX. El WLC

aprende esto de CMX y sólo envía la información detectada por ellos al nodo CMX ubicado en 10.48.71.41.

Implementaciones de nodos adicionales

Si la red consta de varios controladores inalámbricos, es posible implementar nodos CMX adicionales y crear un mapping 1-1 entre varios WLC y CMX. No hay requerimientos especiales cuando se trata de la versión del WLC. Asegúrese de no tener un solo WLC agregado a varios nodos CMX al mismo tiempo.



Espacios de ADN: descarga del trabajo a la nube

La nueva plataforma en la nube de Cisco DNA Spaces pretende trasladar el seguimiento del cliente a la nube. Los recursos se asignan automáticamente en función de la carga actual. Es posible conectar la red inalámbrica a la nube de varias formas:

1. Conexión directa del WLC a la nube
2. Conector DNA Spaces (una pequeña VM que actúa como proxy, los controladores no están expuestos a la nube)
3. Uso de CMX como gateway para la nube (esta opción es necesaria para implementaciones de HyperLocation)

Errores relevantes

- [CSCvq25953](#) - Habilitación del Filtrado SSID de Ubicación inhabilita la exclusión de MAC administradas localmente y viceversa