

Optimiser les performances CMX

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Signes d'un noeud CMX surchargé](#)

[Redistribuer la charge CMX](#)

[Filtrage des adresses MAC gérées localement](#)

[Suivi des clients de sondage](#)

[Modification de l'algorithme de détection](#)

[Augmentation des ressources de VM](#)

[Groupement CMX \(anciennement connu sous le nom de regroupement AP\)](#)

[Déploiements de noeuds supplémentaires](#)

[Espaces ADN - Déchargement du travail vers le cloud](#)

[Bogues pertinents](#)

Introduction

Cet article explique comment reconnaître et ensuite redistribuer la charge d'un noeud CMX (Connected Mobile eXperience) unique afin de prendre en charge un grand nombre d'appareils faisant l'objet d'un suivi. Des problèmes comme celui-ci sont souvent observés dans des déploiements extrêmement importants dans des zones publiques ou des configurations où le suivi des clients par sondage est activé.

Conditions préalables

Conditions requises

Cet article suppose que vous connaissez la configuration et la configuration de base d'un CMX et se concentre uniquement sur les astuces et astuces pour optimiser les performances dans les déploiements de grande envergure.

Components Used

Toutes les commandes et les exemples présentés dans cet article ont été exécutés sur le WLC 3504 exécutant le code 8.8.125 et le CMX 10.6.1 s'exécutant sur l'appliance 3375.

Signes d'un noeud CMX surchargé

La surcharge d'un noeud CMX peut entraîner plusieurs problèmes différents :

- Services ne pouvant pas démarrer

- Arrêt/panne brusque des services
- Service d'analyse montrant 0 client actif
- Alarmes et alertes par e-mail indiquant que le service d'analyse ou de localisation est dans un état critique
- Incapacité à établir la HA entre le noeud CMX principal et le noeud CMX secondaire

Redistribuer la charge CMX

Filtrage des adresses MAC gérées localement

En raison de préoccupations croissantes en matière de confidentialité, à partir de la version IOS 8 en 2014, les fabricants de smartphones ont commencé à mettre en oeuvre une fonctionnalité appelée randomisation MAC dans laquelle les périphériques utiliseraient de nouvelles adresses MAC générées aléatoirement chaque fois qu'ils envoient une requête d'analyse. Lors de la génération d'une adresse MAC aléatoire, les fabricants peuvent choisir d'utiliser une adresse MAC « administrée localement » qui a un bit spécial qui indique que l'adresse est aléatoire ou simplement générer une adresse complètement aléatoire qui ne peut pas être distinguée d'une adresse réelle. Un très petit nombre de clients utilise en fait leur adresse MAC réelle lors de l'analyse.

CMX a un moyen de filtrer ces fausses adresses MAC aléatoires. Sous System->Settings->Filtering, assurez-vous toujours que la case Activer le filtrage MAC géré localement est cochée.

Remarque : Ce champ a été supprimé de l'interface Web dans CMX 10.6.0 et est toujours activé par défaut

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 Locally Administered MAC Filtering

Enable Location MAC Filtering

Enable Location SSID Filtering

Close Save

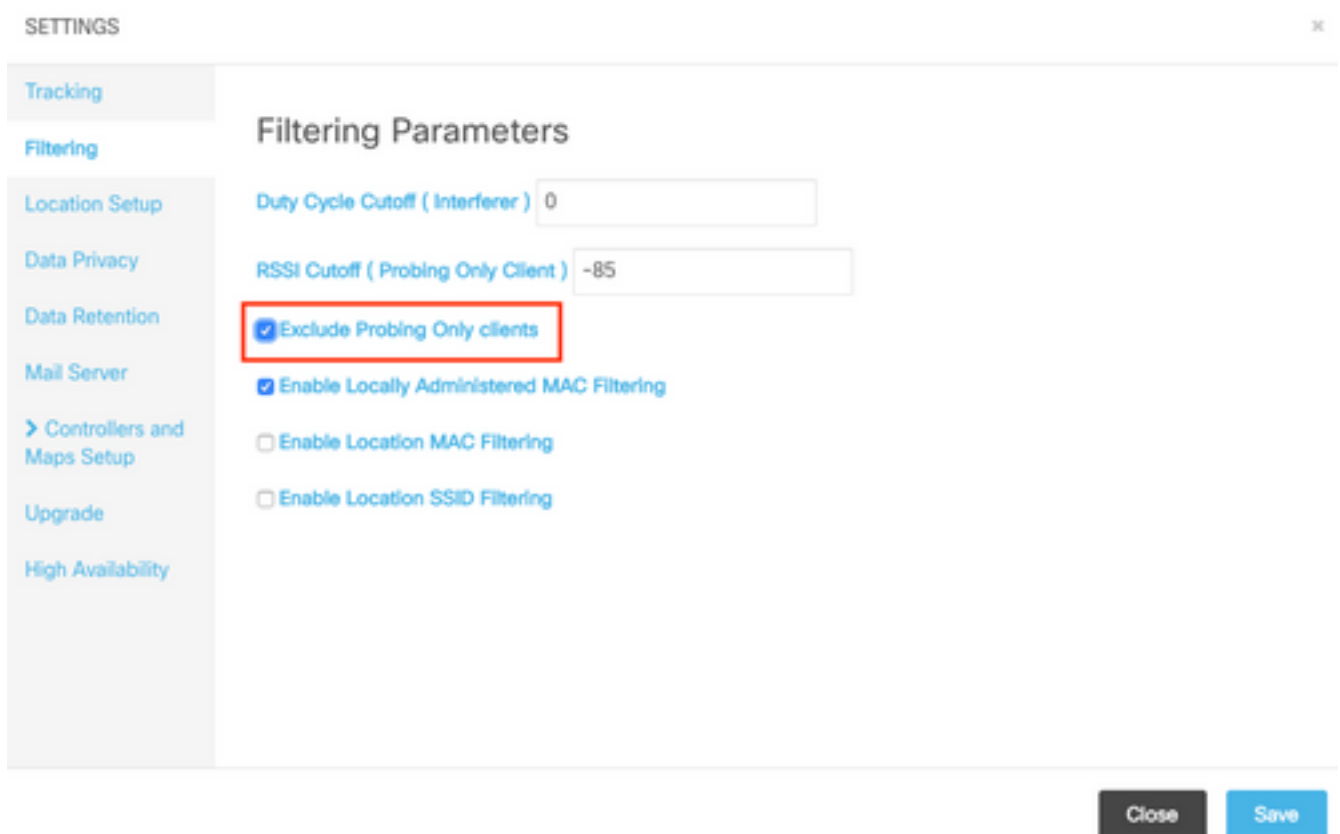
Suivi des clients de sondage

La cause principale la plus courante d'une surcharge CMX traitée par le TAC Cisco est le suivi des clients d'analyse uniquement. L'activation de cette fonctionnalité permet le suivi de l'emplacement des clients non associés. Les espaces publics ouverts, comme les centres commerciaux et les gares ferroviaires, qui accueillent un grand nombre de visiteurs, dépasseront très souvent les limites même d'un noeud CMX haut de gamme.

Dans les configurations qui suivent des clients de sondage, les adresses MAC générées aléatoirement ont également un impact très important sur le nombre de clients.

Certains fabricants comme Apple suivent une norme et utilisent des adresses MAC aléatoires administrées localement lors de l'analyse, ce qui signifie que **les appareils iPhone ne seront jamais détectés par CMX** lors de l'analyse et de l'absence d'association. Les périphériques qui ne suivent pas la norme et qui utilisent des adresses MAC aléatoires qui ne sont pas administrées localement seront **enregistrés par CMX en tant que nouveau client chaque fois qu'ils envoient la requête d'analyse** (ce qui peut se produire toutes les deux secondes). Par conséquent, le nombre de clients d'analyse peut être sensiblement plus élevé/inférieur au nombre réel de périphériques du réseau.

Le suivi des clients d'analyse peut être désactivé à partir des interfaces Web CMX sous System->Settings->Filtering en cochant l'option Exclude Probing Only clients :



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

En raison de toutes les variations mentionnées ci-dessus, le nombre de clients de sondage ne doit pas être utilisé comme compteur de pas et le TAC de Cisco recommande fortement de ne pas suivre les clients de sondage.

Modification de l'algorithme de détection

En modifiant les options de filtrage sur CMX, le nombre de clients d'analyse enregistrés peut être considérablement limité. Il existe deux options principales qui ont un impact significatif sur la

détection des clients (en particulier la recherche uniquement) :

1. Décalage du cycle de service (Interfereur)
2. Couplage RSSI
3. Nombre minimum de points d'accès qui doivent entendre le client, de sorte qu'il soit enregistré

Dans les zones denses et très peuplées, on s'attend à ce qu'il y ait un grand nombre d'interfereurs. Les périphériques tels que les montres Bluetooth n'auront pas d'impact énorme sur le réseau. En augmentant la valeur du cycle de service des interfereurs plus près, par exemple, de 50, seuls les interfereurs forts qui prennent plus de 50 % du temps d'antenne seront enregistrés par CMX. Cette valeur peut être configurée à partir de l'interface Web CMX, sous System->Settings->Filtering :

Note: Pour éviter d'enregistrer une grande quantité de données d'interférence, CMX enregistre uniquement les interfereurs présents pendant un certain temps.

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

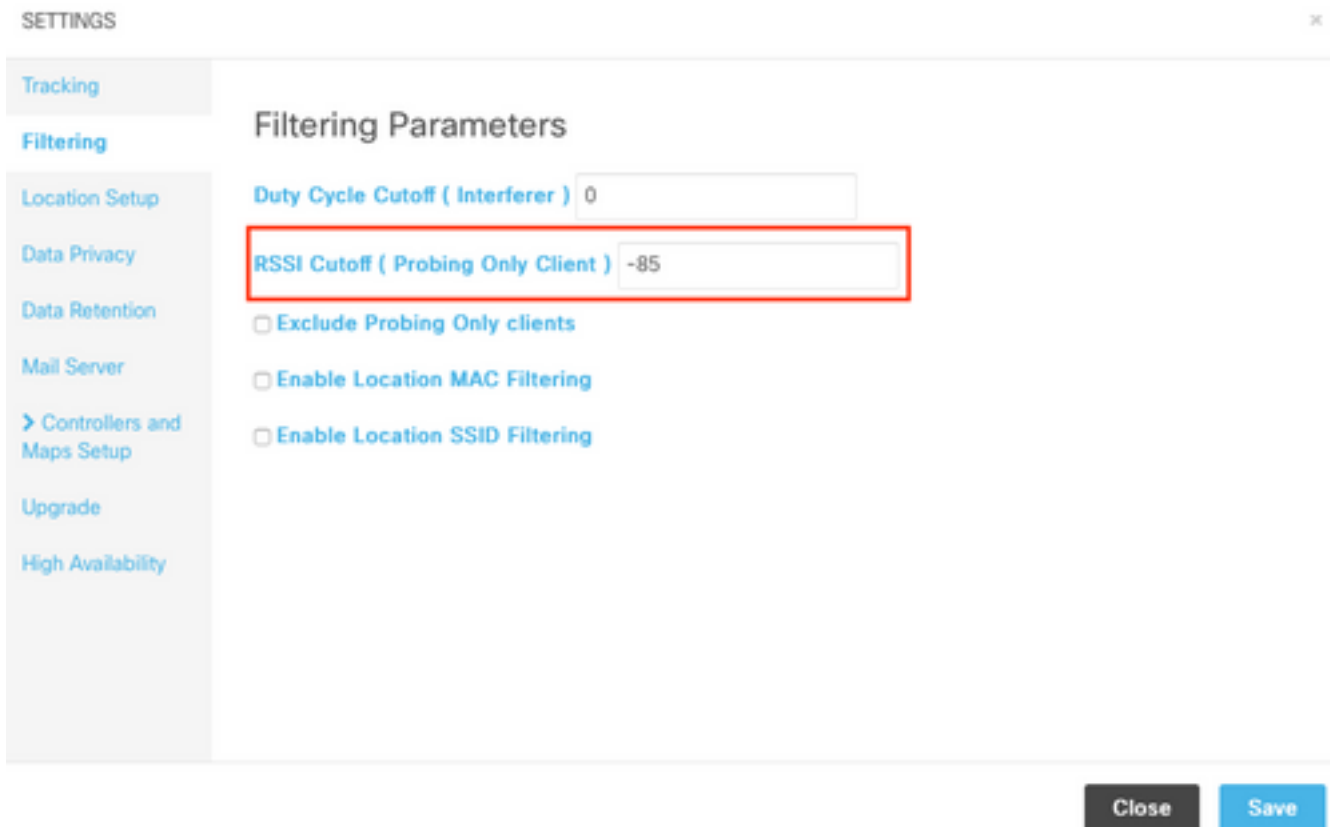
Exclude Probing Only clients

Enable Location MAC Filtering

Enable Location SSID Filtering

Close Save

La fonction de coupure RSSI permet d'éviter d'enregistrer les clients qui passent juste à côté des locaux et ne pénètrent pas réellement. Cela peut avoir un impact énorme sur les déploiements avec l'analyse du suivi des clients seulement activée et une gare routière ou une rue à proximité. Par défaut, cette valeur est définie sur -85 dBm. Avant de modifier cette valeur, il convient de mesurer le RSSI d'un client en dehors des locaux. Cette valeur peut être configurée à partir de l'interface Web CMX, sous System->Settings->Filtering :



Depuis CMX 10.6, la modification de la **quantité minimale d'AP requise pour entendre un client** pour qu'il soit enregistré par CMX ne peut être effectuée que par un appel API. Tout d'abord, une requête GET peut être utilisée pour afficher la configuration actuelle :

```
[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}
```

Dans cette configuration, la valeur `minapwithvalidrssi` est définie sur 1, qui est la valeur par défaut. La modification de cette valeur à 3 peut être effectuée à l'aide d'une requête POST. Une fois ces paramètres appliqués, le client sera enregistré par CMX une fois qu'il sera entendu par le troisième AP à RSSI égal ou supérieur au minimum spécifié :

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

Après avoir modifié l'une des valeurs, assurez-vous d'exécuter une requête GET pour confirmer que les paramètres ont été appliqués correctement.

Augmentation des ressources de VM

Si un nœud CMX en cours s'exécute dans une machine virtuelle et que sa taille n'est pas suffisante pour accueillir tous les clients, il est possible d'augmenter les ressources de la machine virtuelle et donc sa puissance de traitement. Il vous suffit d'allouer plus de cœurs de CPU, de mémoire et d'espace disque. Vous trouverez ici les conditions requises pour les nœuds bas de gamme, standard et haut de gamme CMX.

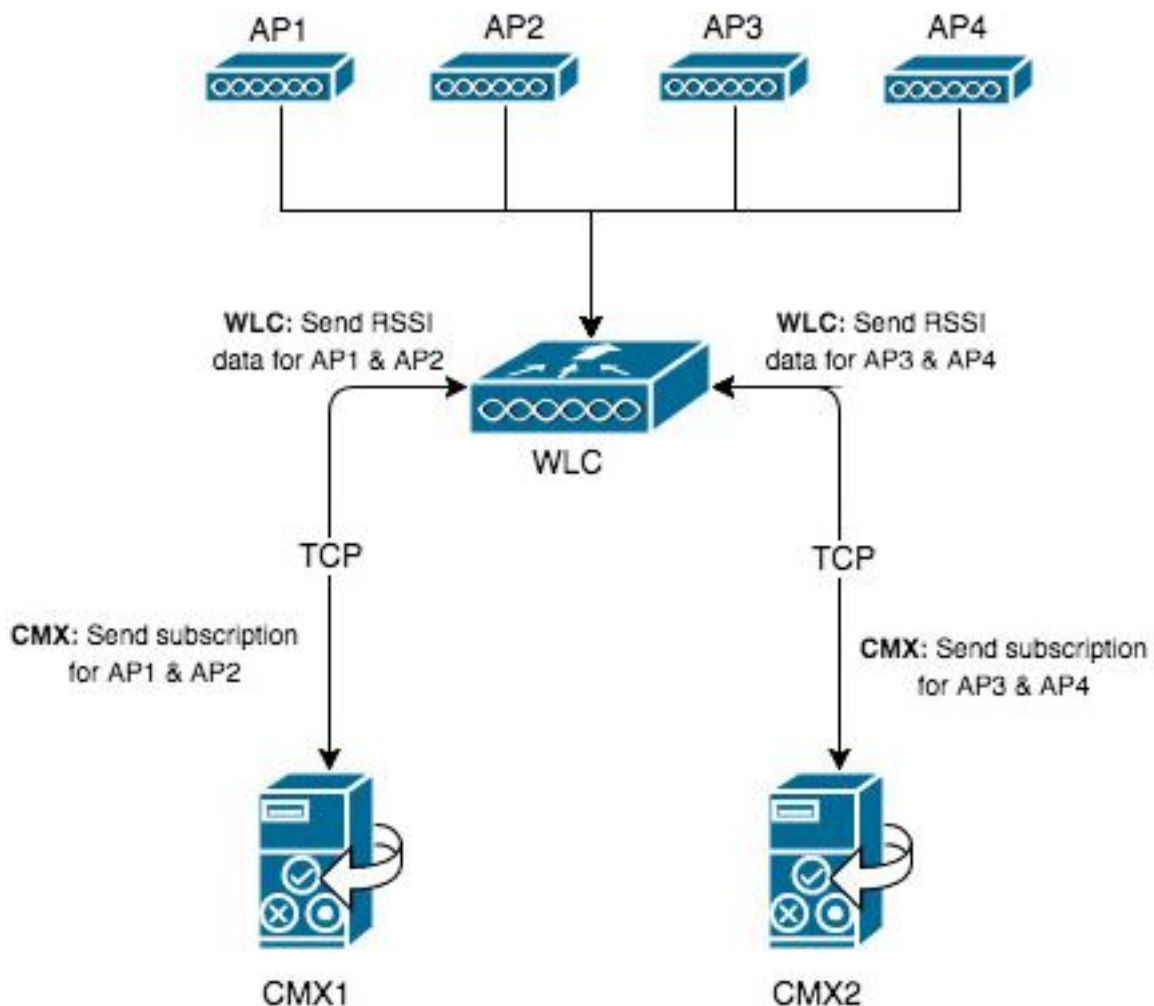
Si la configuration CMX actuelle est déjà un nœud haut de gamme, prenez en compte d'autres

options mentionnées dans cet article.

Note: Le fait qu'un snapshot soit actif sur une machine virtuelle peut avoir un impact négatif sur les performances et n'est pas recommandé pour les environnements de production.

Groupement CMX (anciennement appelé regroupement AP)

Le regroupement CMX est une fonctionnalité disponible sur CMX 10.5 ou version ultérieure et les WLC AireOS exécutant les versions 8.7 ou ultérieures. Puisque la version 8.7 ne recevra plus de mises à jour à l'avenir, il est recommandé d'utiliser la version 8.8 ou ultérieure. Cette fonctionnalité permet à un contrôleur unique de distribuer la charge à plusieurs noeuds CMX en sélectionnant des groupes d'AP et en assignant un groupe à un noeud CMX spécifique. Ces groupes d'AP ne sont pas liés à la fonctionnalité de groupe d'AP sur le WLC.



Les cartes sur CMX1 ne comportent que AP1 et AP2 placés. CMX1 communiquera avec WLC au sujet des 2 points d'accès qui se trouvent sur la carte. Une fois la fonctionnalité de regroupement CMX activée, toutes les informations enregistrées par AP1 et AP2 (y compris les clients associés et les analyseurs uniquement, les interféreurs, les balises BLE, les balises RFID..) seront envoyées uniquement à CMX1.

Un contrôleur unique peut avoir jusqu'à 4 connexions NMSP établies à l'époque, ce qui signifie qu'il peut y ajouter jusqu'à 4 noeuds CMX. Avec 4 noeuds haut de gamme, cela permettrait théoriquement d'enregistrer jusqu'à 360 000 (4 x 90 000) adresses MAC client uniques par jour.

Il est possible d'augmenter la quantité de serveurs CMX auxquels un WLC peut se connecter à

l'aide de la commande de test suivante

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

Important : le contrôleur exécutant un code inférieur à 8.7 ou supérieur à 8.7 sans la fonctionnalité de regroupement CMX activée ne doit jamais être ajouté à plusieurs WLC. Cela peut entraîner l'enregistrement de données inexactes, en particulier dans les configurations HyperLocation.

Sur chaque noeud CMX auquel ce contrôleur sera ajouté, il est nécessaire d'activer la fonctionnalité et de redémarrer les services :

1. Activez la fonction à l'aide de la commande :

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

Le remplacement du mot true par false désactive la fonctionnalité.

2. Redémarrer l'agent CMX :

```
cmxctl restart agent
```

3. Redémarrez l'équilibreur de charge NMSP :

```
cmxctl nmsplb stop
```

```
cmxctl nmsplb start
```

4. Pour vérifier si la fonctionnalité a été correctement activée, exécutez :

```
[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 |
+-----+
```

Sous Monitor > Cloud Services > CMX, il doit être visible quel noeud CMX a la fonctionnalité de

regroupement activée. « Aucun » indique que la fonction de regroupement est désactivée, tandis que « voir Groupes » qu'elle est activée.

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		

En ouvrant la page « voir le groupe », il est possible d'accéder à la liste des points d'accès auxquels ce noeud CMX est abonné.

CMX Server Ip : 10.48.71.41

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

CMX Server IP : 10.48.71.41

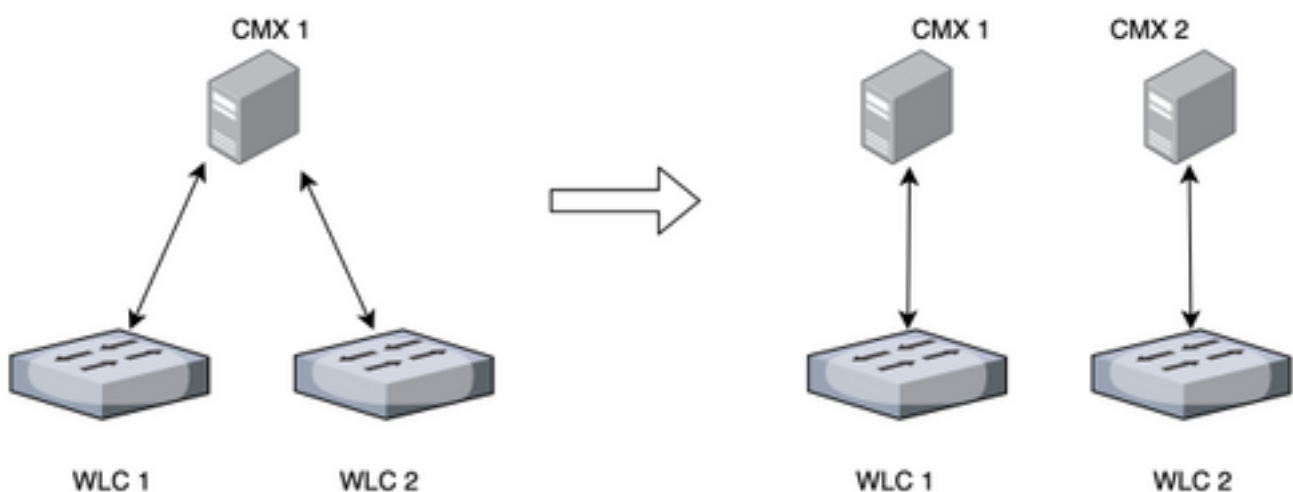
CMX Group Name : CMX_10.48.71.41

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

Sur le total de 4 points d'accès associés à ce contrôleur, seuls 3 sont placés sur la carte CMX. WLC apprend cela à partir de CMX et envoie uniquement les informations détectées par eux au noeud CMX situé sur 10.48.71.41.

Déploiements de noeuds supplémentaires

Si le réseau est constitué de plusieurs contrôleurs sans fil, il est possible de déployer des noeuds CMX supplémentaires et de créer un mappage 1-1 entre plusieurs WLC et CMX. Il n'y a pas de conditions particulières quand il s'agit de version WLC. Veillez à ne pas avoir un seul WLC ajouté simultanément à plusieurs noeuds CMX.



La nouvelle plate-forme cloud DNA Spaces de Cisco vise à déplacer le suivi des clients vers le cloud. Les ressources sont automatiquement allouées en fonction de la charge actuelle. Il est possible de connecter votre réseau sans fil au cloud de plusieurs manières :

1. Connexion directe du WLC au cloud
2. Connecteur d'espace ADN (petite machine virtuelle qui agit comme un proxy, les contrôleurs ne sont pas exposés au cloud)
3. Utilisation de CMX comme passerelle pour le cloud (cette option est nécessaire pour les déploiements HyperLocation)

Bogues pertinents

- [CSCvq25953](#) - L'activation du filtrage SSID de l'emplacement désactive l'exclusion des adresses MAC gérées localement et inversement