Optimierung der CMX-Leistung

Inhalt

Einführung

In diesem Artikel wird erläutert, wie die Last eines einzelnen CMX-Knotens (Connected Mobile eXperience) erkannt und dann neu verteilt wird, um eine große Anzahl von verfolgten Geräten zu unterstützen. Probleme wie diese werden häufig in extrem großen Bereitstellungen in öffentlichen Bereichen oder in Einrichtungen beobachtet, in denen die Überprüfung der Client-Verfolgung aktiviert ist.

Voraussetzungen

Anforderungen

In diesem Artikel wird davon ausgegangen, dass Sie mit der grundlegenden Einrichtung und Konfiguration eines CMX vertraut sind und sich nur auf Tipps und Tricks zur Optimierung der Leistung in umfangreichen Bereitstellungen konzentrieren.

Verwendete Komponenten

Alle Befehle und Beispiele in diesem Artikel wurden auf 3504 WLC ausgeführt, auf dem 8.8.125-Code ausgeführt wird, und auf CMX 10.6.1, das auf der 3375-Appliance ausgeführt wird.

Zeichen eines überladenen CMX-Knotens

Die Überlastung eines CMX-Knotens kann zu mehreren Problemen führen:

- Services können nicht starten

- Services werden abrupt beendet/abgestürzt
- Analyseservice zeigt 0 aktive Clients an
- Alarme und E-Mail-Warnmeldungen weisen darauf hin, dass Analysen oder Standortdienste einen kritischen Zustand aufweisen
- Es ist nicht möglich, HA zwischen dem primären und sekundären CMX-Knoten einzurichten.

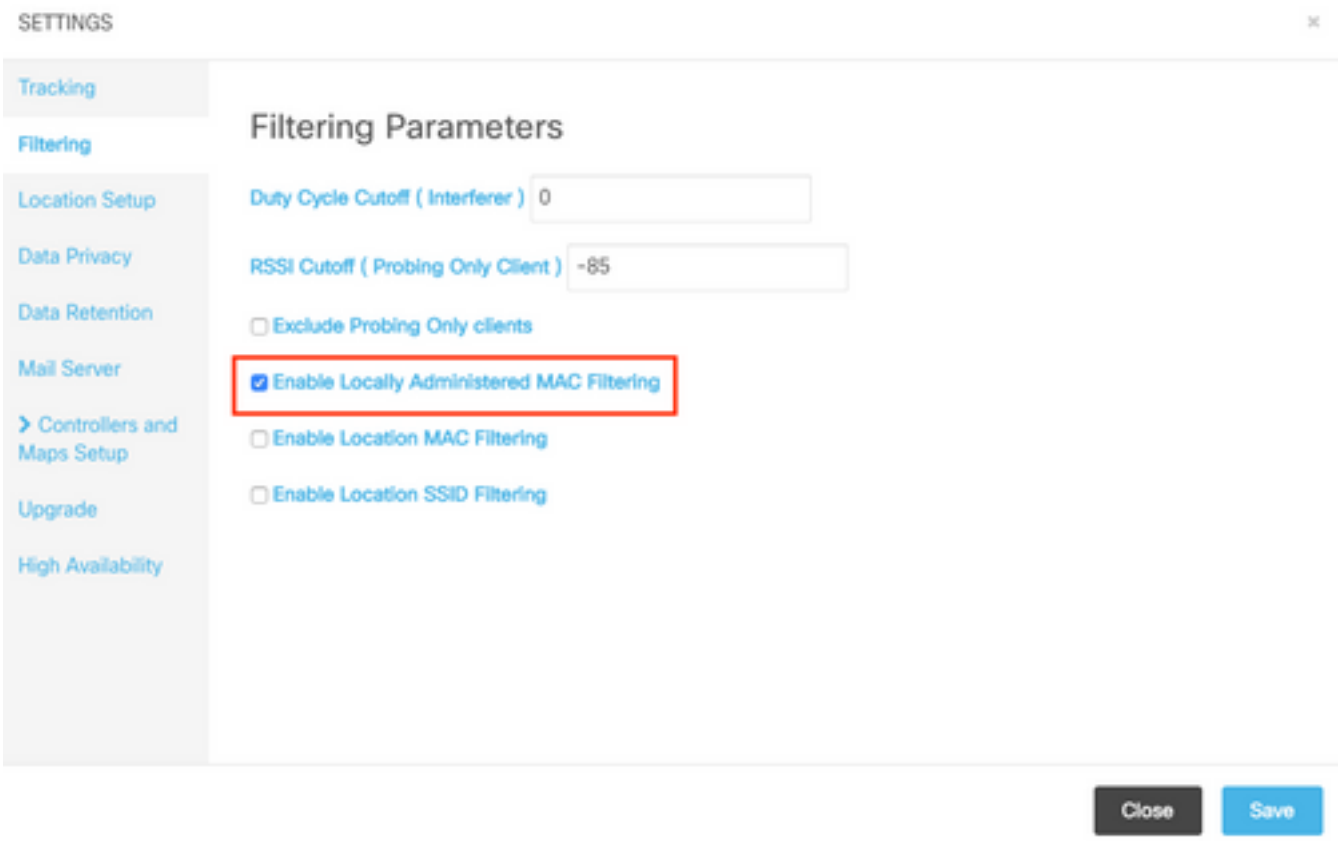
Neuverteilung der CMX-Last

Filtern lokal verwalteter MAC-Adressen

Aufgrund wachsender Datenschutzbedenken, beginnend mit der IOS 8-Version im Jahr 2014, haben Smartphone-Hersteller damit begonnen, eine Funktion namens MAC-Randomisierung zu implementieren, bei der Geräte bei jedem Senden einer Anfrage eine neue zufällig generierte MAC-Adresse verwenden. Beim Generieren einer zufälligen MAC-Adresse können Hersteller entscheiden, entweder eine "lokal verwaltete" MAC-Adresse zu verwenden, die ein spezielles Bit aufweist, das anzeigt, dass die Adresse zufällig ist, oder einfach eine vollständig zufällige Adresse zu generieren, die nicht von einer echten Adresse unterscheidbar ist. Nur sehr wenige Clients verwenden bei der Suche ihre tatsächliche MAC-Adresse.

CMX kann diese gefälschten zufälligen MAC-Adressen filtern. Stellen Sie unter System->Einstellungen->Filterung immer sicher, dass "Lokal verwaltete MAC-Filterung aktivieren" aktiviert ist.

> **Hinweis**: Dieses Feld wurde in CMX 10.6.0 von der Webschnittstelle entfernt und ist immer standardmäßig aktiviert.



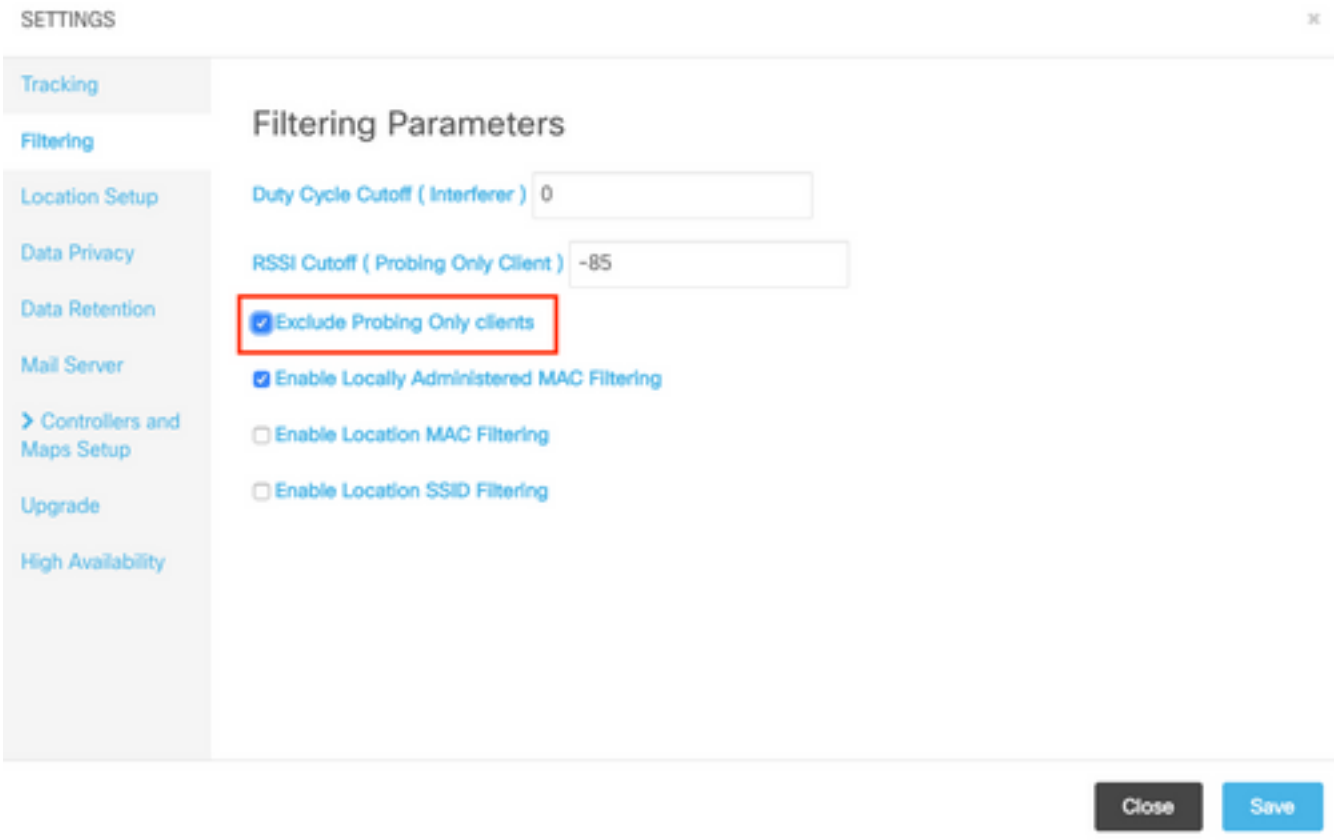
Nachverfolgung von Testing-Clients

Die häufigste Ursache für eine CMX-Überlastung, mit der sich das Cisco TAC befasst, ist die Nachverfolgung von nur Clients. Die Aktivierung dieser Funktion ermöglicht die Standortverfolgung nicht verbundener Clients. Offene öffentliche Bereiche wie Einkaufszentren und Bahnhöfe mit einer hohen Besucherzahl werden die Grenzen selbst eines High-End-CMX-Knotens oft überschreiten.

In Setups, die die Suche nach Clients verfolgen, haben zufällig generierte MAC-Adressen ebenfalls einen sehr großen Einfluss auf die Client-Anzahl.

Einige Hersteller wie Apple befolgen einen Standard und verwenden lokal verwaltete zufällige MAC-Adressen, wenn sie nachfragen. Das bedeutet, dass **iPhone-Geräte von CMX nie erkannt werden,** wenn sie nachfragen und nicht zugeordnet werden. Geräte, die nicht dem Standard entsprechen und willkürliche MAC-Adressen verwenden, die nicht lokal verwaltet werden, werden **von CMX als neuer Client bei jedem Senden der Anfrage aufgezeichnet** (was alle paar Sekunden erfolgen kann). Daher kann die Anzahl der untersuchenden Clients deutlich höher/niedriger sein als die tatsächliche Anzahl der Geräte im Netzwerk.

Die Nachverfolgung von Clients kann über CMX-Webschnittstellen unter System->Settings->Filtering deaktiviert werden, indem die Option "Exclude Probing Only Clients" aktiviert wird:



Aufgrund der oben genannten Variationen sollte die Anzahl der Testkunden nicht als Fußfallzähler verwendet werden, und das Cisco TAC empfiehlt nachdrücklich, die Nachverfolgung von Clients zu unterbinden.

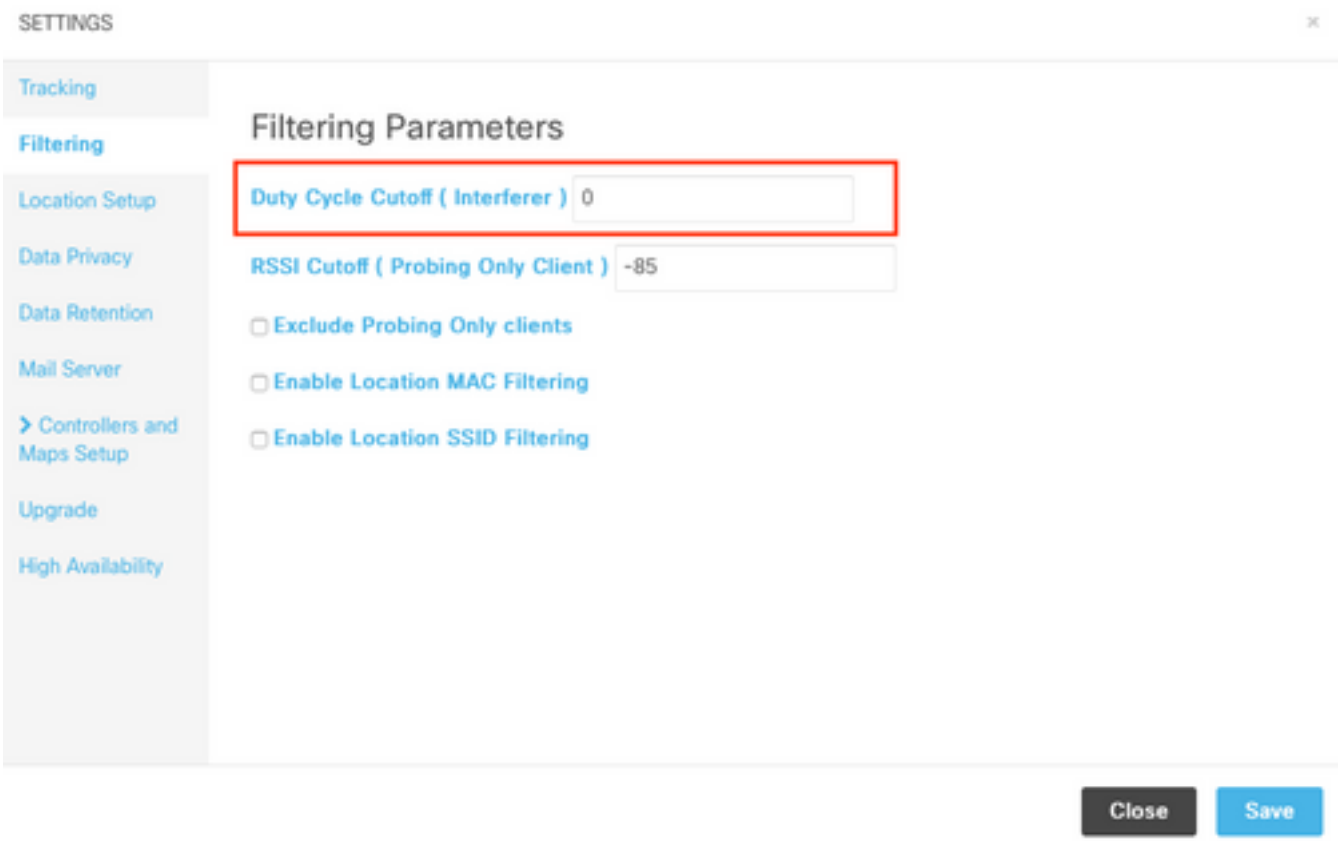
Erkennung Algorithmus - Tweaking

Durch die Anpassung der Filteroptionen für CMX kann die Anzahl der aufgenommenen Testclients stark beschränkt werden. Es gibt zwei Hauptoptionen, die sich erheblich auf die Client-Erkennung auswirken (insbesondere auf die Überprüfung):

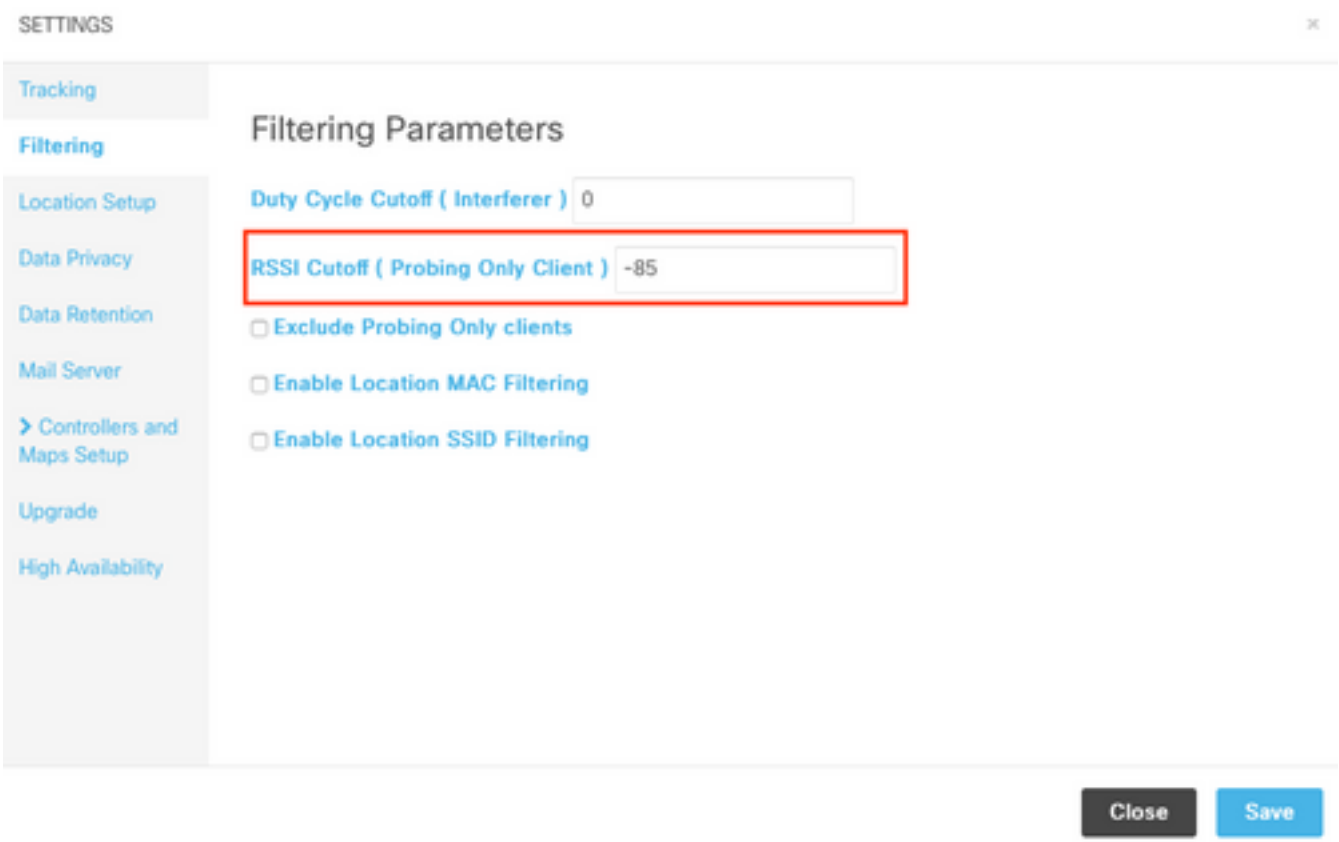
1. Duty Cycle Cutoff (Interferer)
2. RSSI-Abschaltung
3. Mindestanzahl von APs, die den Client hören müssen, damit er aufgezeichnet wird

In dicht besiedelten Gebieten ist mit einer hohen Anzahl von Störquellen zu rechnen. Geräte wie Bluetooth-Uhren haben keine großen Auswirkungen auf das Netzwerk. Durch die Erhöhung des Werts des Störungskreislaufs beispielsweise näher an 50 werden von CMX nur starke Störungsquellen erfasst, die mehr als 50 % der Luftzeit einnehmen. Dieser Wert kann über die CMX-Webschnittstelle unter System->Settings->Filtering (System->Einstellungen->Filterung) konfiguriert werden:

> **Hinweis**: Um zu verhindern, dass große Mengen an Störungsdaten aufgezeichnet werden, zeichnet CMX nur die Störungsquellen auf, die für einen bestimmten Zeitraum vorhanden sind.



RSSI-Sperrfunktion dient dazu, Clients aufzuzeichnen, die nur am Standort vorbeilaufen und nicht tatsächlich eintreffen. Dies kann enorme Auswirkungen auf Bereitstellungen haben, bei denen nur die Client-Verfolgung aktiviert ist und eine Busstation oder eine Straße in der Nähe. Dieser Wert ist standardmäßig auf -85 dBm festgelegt. Bevor dieser Wert geändert wird, sollte die RSSI eines Clients außerhalb des Firmengeländes gemessen werden. Dieser Wert kann über die CMX-Webschnittstelle unter System->Settings->Filtering (System->Einstellungen->Filterung) konfiguriert werden:



Ab CMX 10.6 kann die Änderung der **Mindestanzahl von Access Points, die erforderlich ist, um einen Client** für die Aufzeichnung durch CMX **abzurufen**, nur über einen API-Aufruf erfolgen. Zunächst kann eine GET-Anforderung verwendet werden, um die aktuelle Konfiguration anzuzeigen:

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

In dieser Konfiguration ist der Wert minapWithvalidrssi auf 1 festgelegt, d. h. den Standardwert. Die Änderung dieses Werts in 3 kann mithilfe einer POST-Anfrage erfolgen. Sobald diese Einstellungen angewendet wurden, wird der Client von CMX aufgezeichnet, sobald er vom dritten Access Point bei RSSI gleich oder besser als der mindestens angegebene Access Point gehört wird:

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

Nachdem Sie einen der Werte geändert haben, stellen Sie sicher, dass Sie eine GET-Anforderung durchführen, um zu bestätigen, dass die Einstellungen erfolgreich angewendet wurden.

Aufstocken der VM-Ressourcen

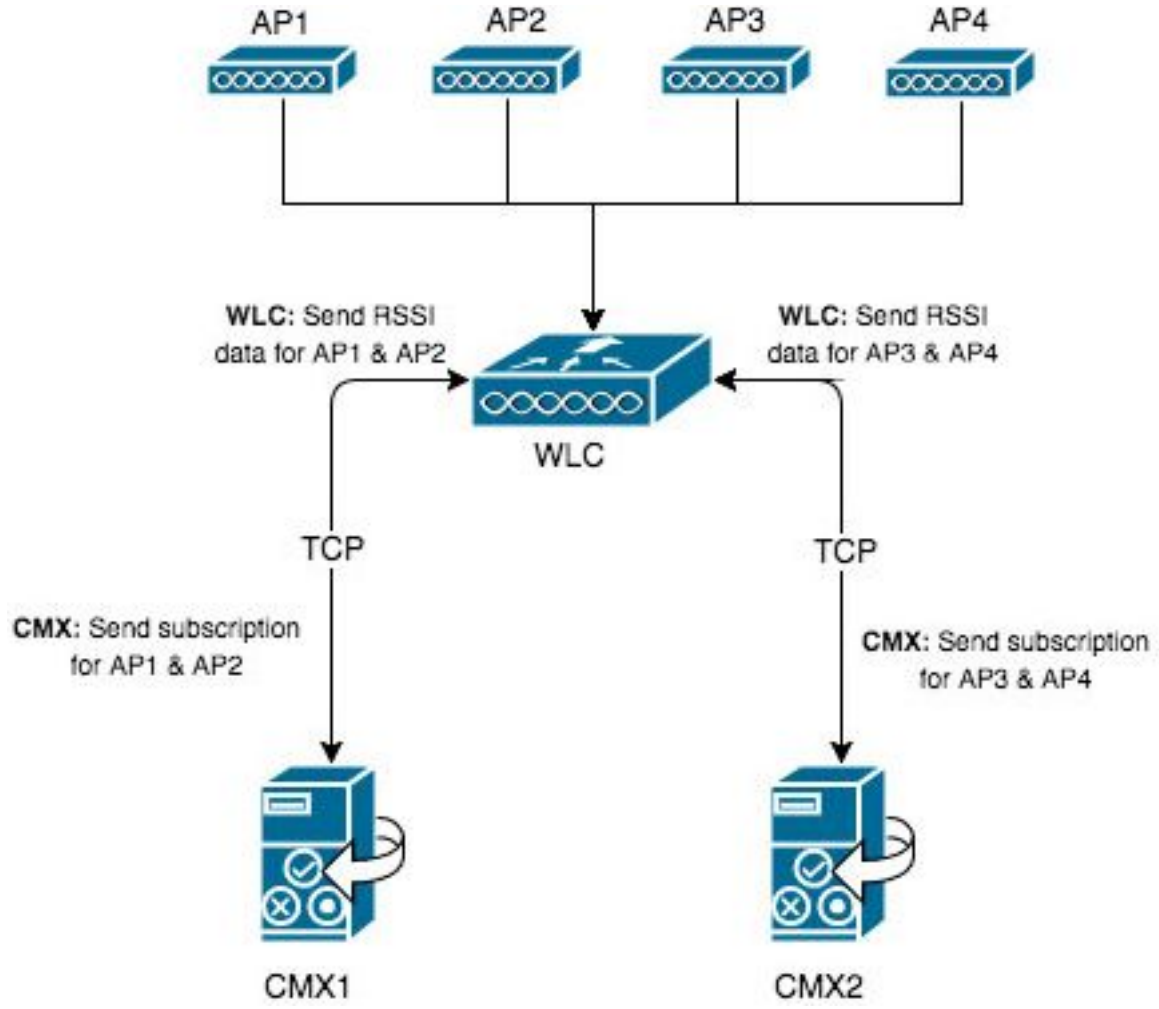
Wenn ein aktueller CMX-Knoten in einer VM ausgeführt wird und seine Größe nicht für alle Clients ausreicht, können die VM-Ressourcen und damit die Verarbeitungsleistung erhöht werden. Sie können einfach mehr CPU-Kerne, Arbeitsspeicher und Festplattenspeicher zuweisen. Die genauen Anforderungen für CMX-Knoten (Low-End, Standard und High-End) finden Sie HIER.

Wenn die aktuelle CMX-Konfiguration bereits ein High-End-Knoten ist, sollten Sie andere in diesem Artikel erwähnte Optionen in Betracht ziehen.

> **Hinweis**: Ein Snapshot, der auf einer VM aktiv ist, kann negative Auswirkungen auf die Performance haben und wird nicht für Produktionsumgebungen empfohlen.

CMX-Gruppierung (ehemals AP-Gruppierung)

CMX Grouping ist eine Funktion, die in CMX 10.5 oder höher und in AireOS WLCs mit Version 8.7 oder höher verfügbar ist. Da der Release Train 8.7 in Zukunft keine Updates mehr erhält, wird empfohlen, Version 8.8 oder höher zu verwenden. Mit dieser Funktion kann ein einzelner Controller die Last auf mehrere CMX-Knoten verteilen, indem er Gruppen von APs auswählt und einer Gruppe einen bestimmten CMX-Knoten zuweist. Diese Gruppen von APs sind nicht mit der Funktion "AP Group" (AP-Gruppe) im WLC verknüpft.



Auf CMX1-Karten sind nur AP1 und AP2 platziert. CMX1 kommuniziert mit WLC über die beiden APs, die in der Karte enthalten sind. Sobald die CMX-Gruppierungsfunktion aktiviert ist, werden alle vom AP1 und AP2 aufgezeichneten Informationen (einschließlich zugehöriger und ausschließlicher Clients, Störquellen, BLE-Beacons, RFID-Tags usw.) nur an den CMX1 gesendet.

An einem Controller können zu diesem Zeitpunkt bis zu 4 NMSP-Verbindungen eingerichtet werden, sodass dem Controller bis zu 4 CMX-Knoten hinzugefügt werden können. Bei 4 High-End-Knoten können theoretisch bis zu 360.000 (4 x 90.000) eindeutige Client-MAC-Adressen pro Tag aufgezeichnet werden.

Es ist möglich, die Anzahl der CMX-Server, mit denen ein WLC eine Verbindung herstellen kann, mit dem folgenden Testbefehl zu erhöhen

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

Wichtig: Controller, die einen Code von weniger als 8.7 oder höher als 8.7 ausführen, ohne dass die CMX-Gruppierungsfunktion aktiviert ist, sollten niemals mehreren WLCs hinzugefügt werden. Dies kann dazu führen, dass ungenaue Daten aufgezeichnet werden, insbesondere in HyperLocation-Setups.

Für jeden CMX-Knoten, dem dieser Controller hinzugefügt wird, ist es erforderlich, die Funktion zu aktivieren und die Dienste neu zu starten:

1. Aktivieren Sie die Funktion mit dem Befehl:

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

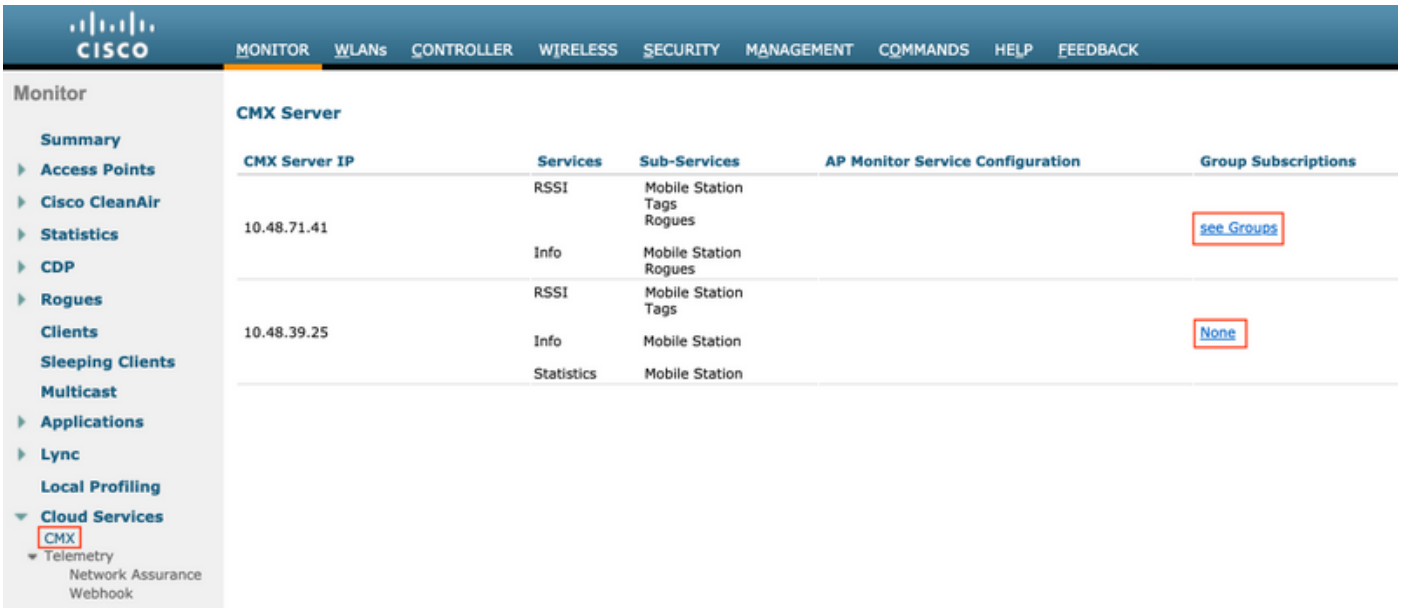
   Wenn Sie das Wort true durch false ersetzen, wird die Funktion deaktiviert.
2. CMX-Agent neu starten:

   ```
   cmxctl restart agent
   ```

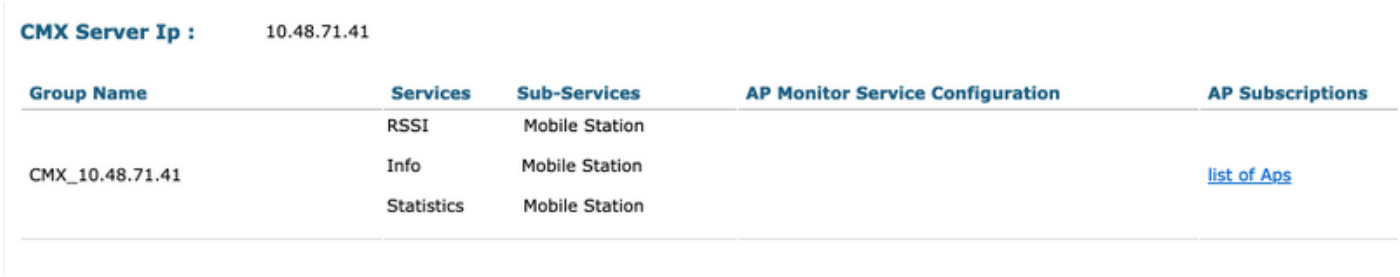
3. Starten Sie den NMSP Load Balancer neu:
   ```
   cmxctl nmsplb stop
   cmxctl nmsplb start
   ```
4. Führen Sie folgende Schritte aus, um zu überprüfen, ob die Funktion erfolgreich aktiviert wurde:

   ```
   [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.queuetime                    | false |
   +----------------------------------------+-------+
   ```

Unter Monitor > Cloud Services > CMX sollte angezeigt werden, für welchen CMX-Knoten die Gruppierungsfunktion aktiviert ist. "Keine" bedeutet, dass die Gruppierungsfunktion deaktiviert ist, während "siehe Gruppen", dass sie aktiviert ist.



Wenn Sie die Seite "siehe Gruppe" öffnen, können Sie auf die Liste der APs zugreifen, für die dieser CMX-Knoten abonniert ist.



CMX Server IP : 10.48.71.41

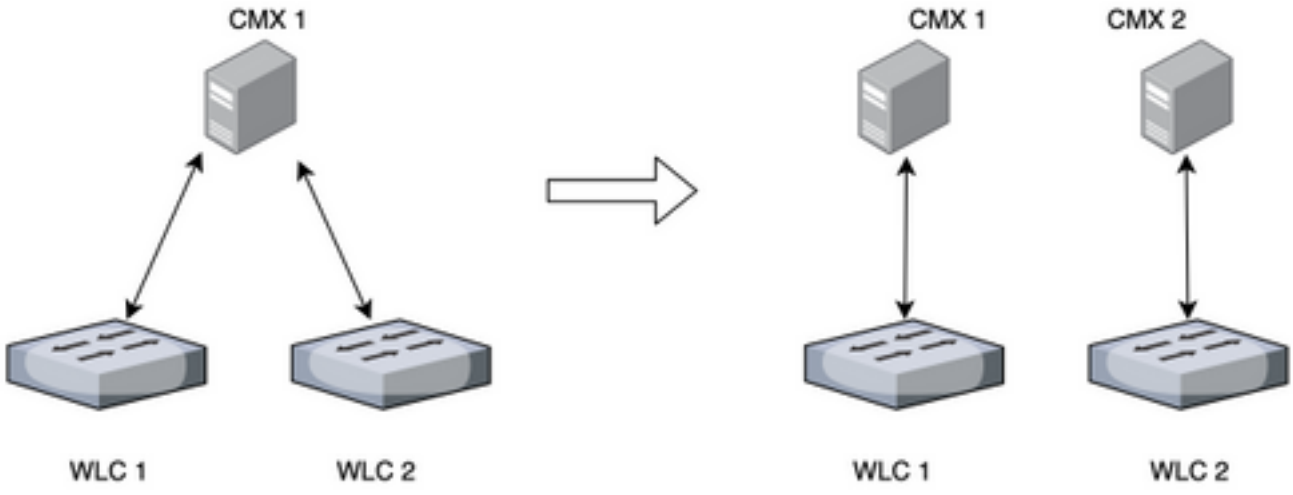
CMX Group Name : CMX_10.48.71.41

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

Von den insgesamt 4 APs, die diesem Controller zugeordnet sind, werden nur drei in der CMX-Zuordnung platziert. WLC ruft dies von CMX ab und sendet nur von diesen erkannte Informationen an den CMX-Knoten in 10.48.71.41.

Zusätzliche Node-Bereitstellungen

Wenn das Netzwerk aus mehreren Wireless-Controllern besteht, können zusätzliche CMX-Knoten bereitgestellt und eine 1-1-Zuordnung zwischen mehreren WLCs und CMXs erstellt werden. Für die WLC-Version bestehen keine speziellen Anforderungen. Achten Sie darauf, dass nicht ein einziger WLC gleichzeitig mehreren CMX-Knoten hinzugefügt wird.



DNA-Bereiche - Auslagerung der Arbeitsumgebung in die Cloud

Die neue Cisco Cloud-Plattform DNA Spaces zielt darauf ab, die Client-Verfolgung in die Cloud zu verlagern. Die Ressourcen werden auf Basis der aktuellen Last automatisch zugewiesen. Es gibt mehrere Möglichkeiten, Ihr Wireless-Netzwerk mit der Cloud zu verbinden:

1. Direkte Verbindung des WLC mit der Cloud
2. DNA Spaces Connector (ein kleines virtuelles System, das als Proxy fungiert, Controller sind der Cloud nicht ausgesetzt)
3. Verwendung von CMX als Gateway für die Cloud (diese Option ist für HyperLocation-Bereitstellungen erforderlich)

Relevante Bugs

- CSCvq25953 - Durch die Aktivierung der Standort-SSID-Filterung wird der Ausschluss lokal verwalteter MACs und umgekehrt deaktiviert.