CMXパフォーマンスの最適化

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[過負荷のCMXノードの兆候](#)
[CMXロードの再配布](#)
[ローカルで管理されるMACアドレスのフィルタリング](#)
[プローブするクライアントのトラッキング](#)
[検出アルゴリズムの調整](#)
[VMリソースの増加](#)
[CMXグループ化（旧称APグループ化）](#)
[追加のノード展開](#)
[DNA空間 – 作業をクラウドにオフロード](#)
[関連するバグ](#)

概要

この記事では、トラッキングされている大量のデバイスに対応するために、単一のCMX(Connected Mobile eXperience)ノードの負荷を認識し、再配分する方法について説明します。このような問題は、パブリックエリアやクライアントのプローブ追跡が有効になっているセットアップで非常に大規模な展開が発生する場合によく見られます。

前提条件

要件

この記事では、CMXの基本的な設定と設定に関する知識を持っていることを前提とし、大規模な展開でパフォーマンスを最適化するためのヒントとテクニックのみに焦点を当てています。

使用するコンポーネント

この記事に示されているすべてのコマンドと例は、8.8.125コードを実行している3504 WLCと、3375アプライアンスを実行しているCMX 10.6.1で実行されています。

過負荷のCMXノードの兆候

CMXノードの過負荷は、いくつかの異なる問題を引き起こす可能性があります。

- サービスを開始できません
- サービスが突然停止/クラッシュする
- アクティブなクライアントが0個の分析サービス

- 分析または口ケーションサービスが重要な状態であることを示すアラームおよび電子メールアラート
- プライマリとセカンダリのCMXノード間でHAを確立できない

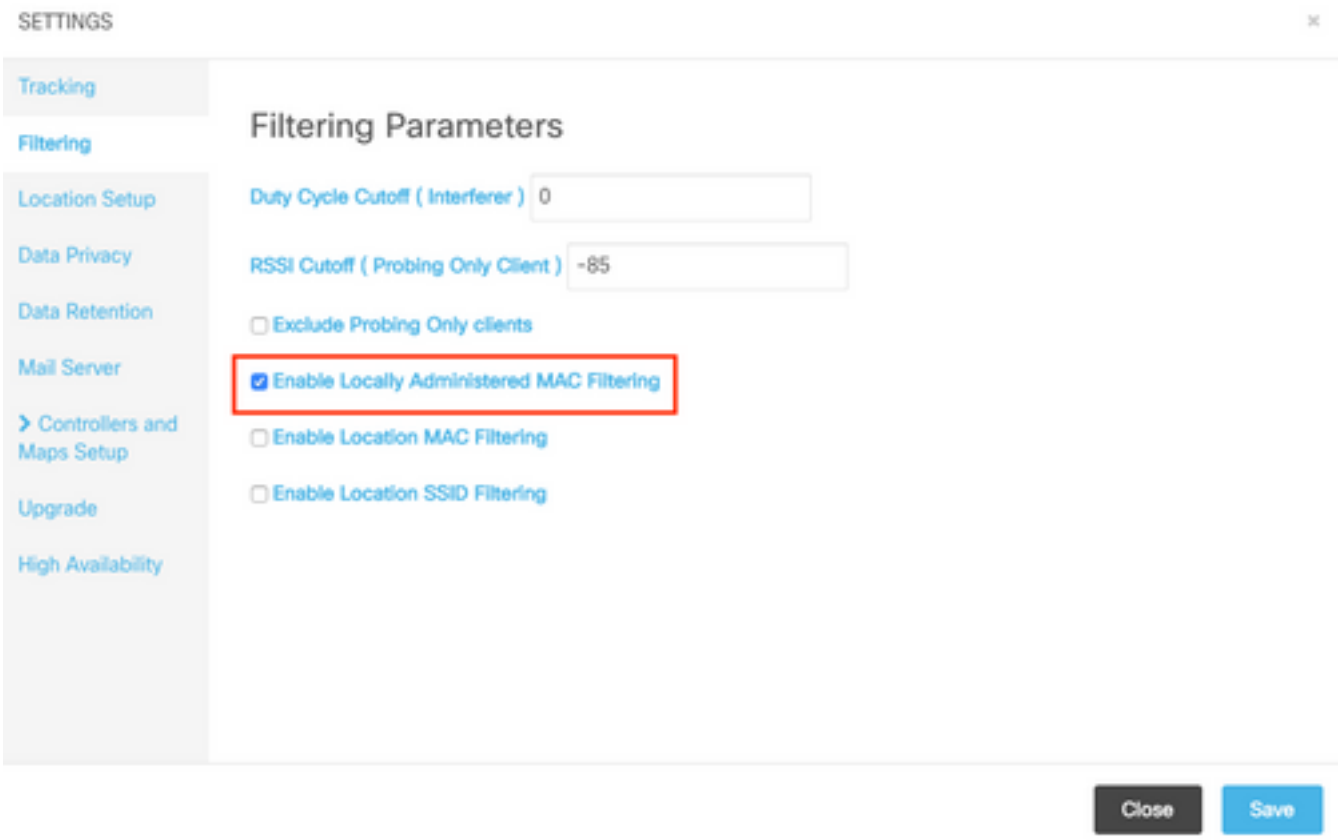
CMXロードの再配布

ローカルで管理されるMACアドレスのフィルタリング

2014年のIOS 8リリース以降のプライバシーの懸念が高まっているため、携帯電話のメーカーは、プローブ要求を送信するたびにデバイスがランダムに生成された新しいMACアドレスを使用するMACランダム化という機能を実装し始めました。ランダムなMACアドレスを生成する場合、メーカーは、アドレスがランダムであることを示す特殊なビットを持つ「ローカルに管理された」MACアドレスを使用するか、単に実際のアドレスと区別できない完全にランダムなアドレスを生成できます。非常に少数のクライアントが、プローブ時に実際のMACアドレスを使用します。

CMXには、これらの疑似ランダムMACアドレスをフィルタリングする方法があります。[System] -> [Settings] -> [Filtering]で、[Enable Locally Administrated MAC filtering]がオンになっていることを確認します。

> **注:このフィールドはCMX 10.6.0のWebインターフェイスから削除されており、常にデフォルトで有効になっています**



プローブするクライアントのトラッキング

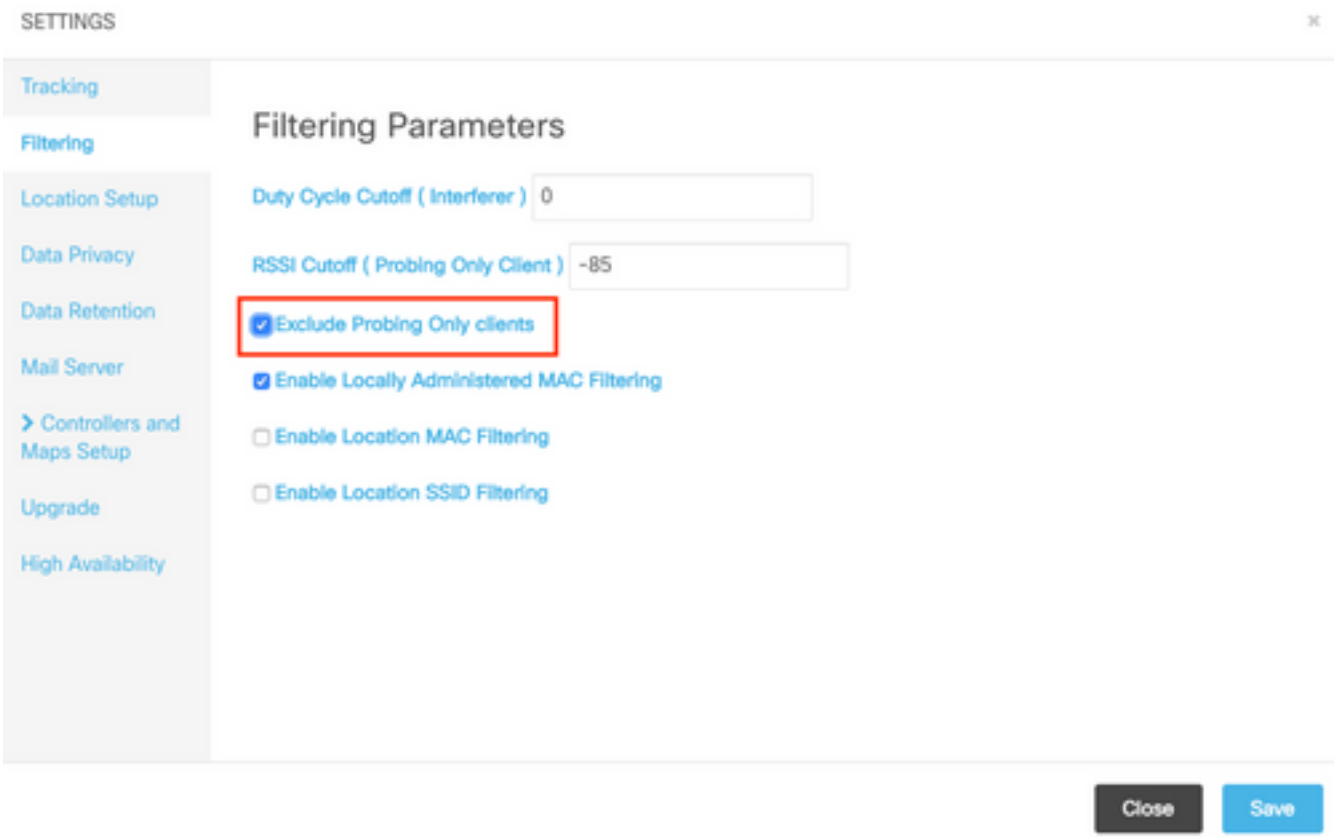
Cisco TACが処理するCMXオーバーロードの最も一般的な根本原因は、クライアントのみをプローブすることです。この機能を有効にすると、関連付けられていないクライアントの口ケーション追跡が可能になります。ショッピングモールや駅などのオープンな公共エリアは、非常に多く

の訪問者を超え、ハイエンドCMXノードの制限を超えます。

プローブするクライアントを追跡するセットアップでは、ランダムに生成されたMACアドレスもクライアント数に大きな影響を与えます。

Appleなどの一部のメーカーは標準に従い、プローブ時にローカルで管理されたランダムなMACアドレスを使用しています。つまり、iPhoneデバイスはプローブ時および関連付け解除の際にCMXによって検出されないということです。標準に従っていないデバイスで、ローカルで管理されていないランダムなMACアドレスを使用しているデバイスは、プローブ要求を送信するたびに**CMXによって新しいクライアントとして記録されます**（数秒ごとに発生する可能性があります）。 その結果、プローブ中のクライアント数は、ネットワーク内の実際のデバイス数よりも大幅に多い/低い場合があります。

プローブ中のクライアントの追跡は、[システム(System)] > [設定(Settings)] > [フィルタリング(Filtering)]で[プローブ専用クライアントの除外(Exclude Probing Only clients)]オプションをオンにして無効にできます。



上記のすべてのバリエーションのため、プローブするクライアント数はフットフォールカウンタとして使用しないでください。Cisco TACでは、プローブするクライアントのトラッキングに対して強く推奨しています。

検出アルゴリズムの調整

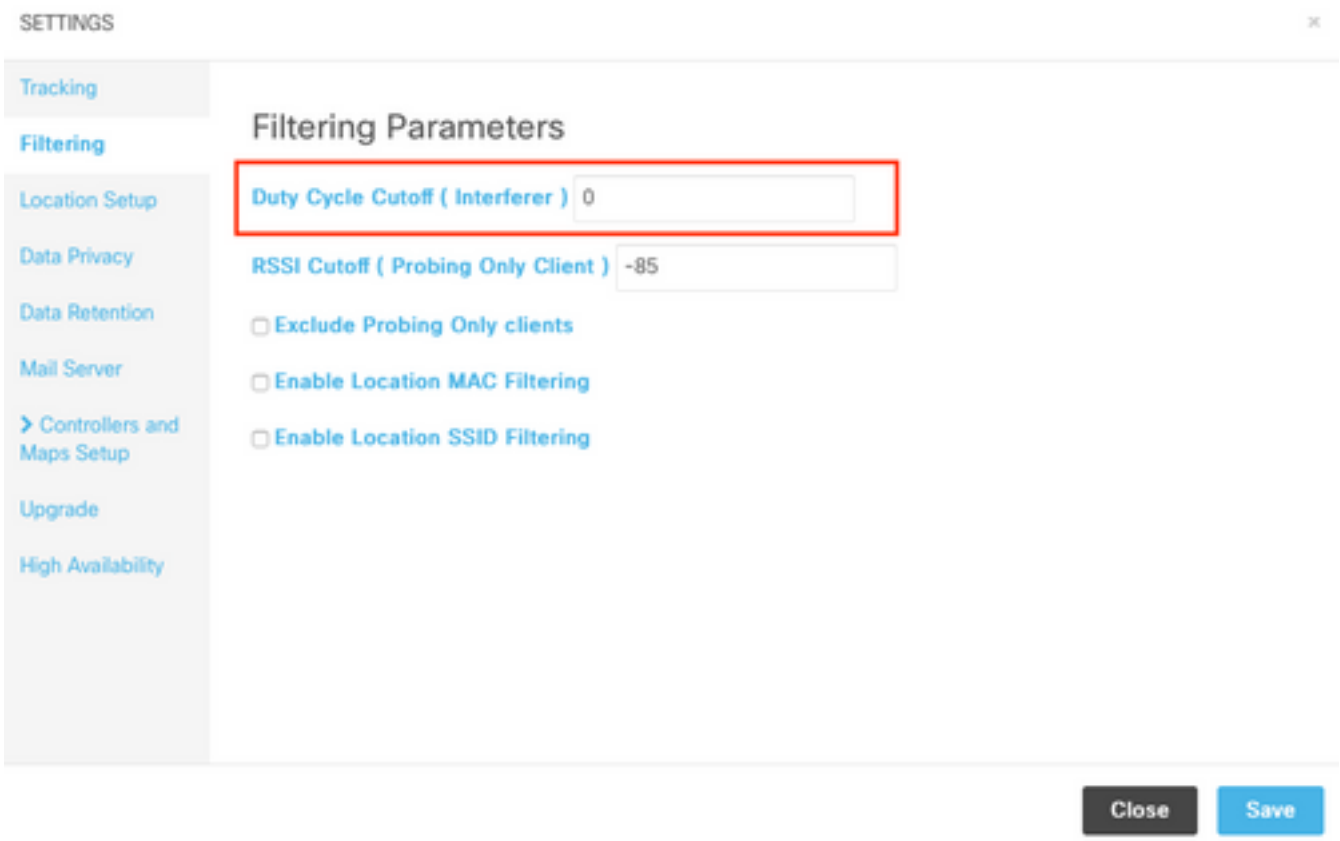
CMXのフィルタリングオプションを調整することで、記録されるプロービングクライアントの数が大幅に制限される可能性があります。クライアント検出に大きな影響を与える主なオプションは2つあります（特にプローブ専用）。

1. デューティサイクル遮断（干渉源）
2. RSSIカットオフ

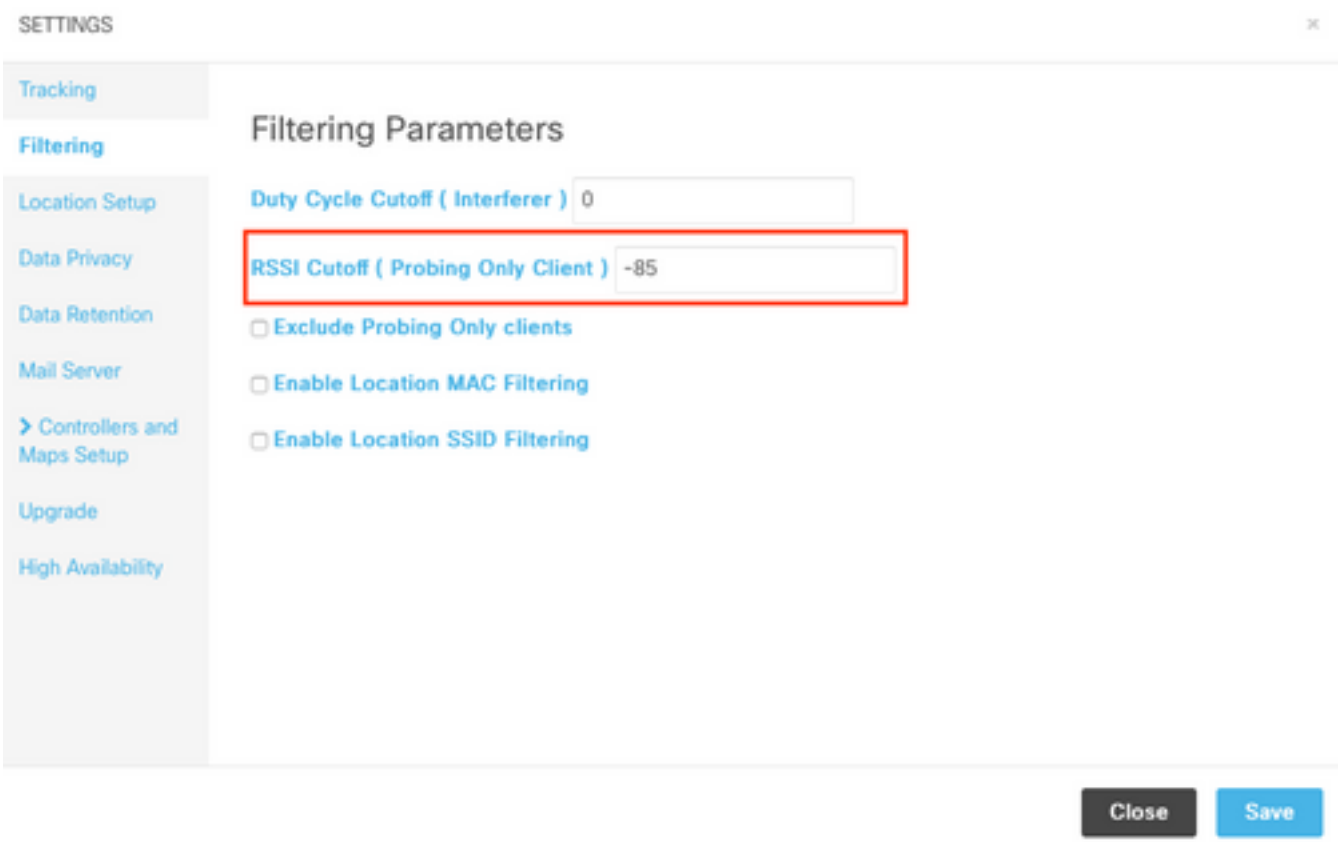
3. クライアントを受信する必要があるAPの最小量。したがって、クライアントは記録されます

人口密度が高いエリアでは、多数の干渉源が存在することが予想されます。Bluetoothウォッチなどのデバイスは、ネットワークに大きな影響を与えません。たとえば50に近い範囲で干渉源デューティサイクルの値を増やすと、CMXによって記録されるのは電波時間の50 %を超える強力な干渉源だけです。この値は、CMX Webインターフェイスの[System] -> [Settings] -> [Filtering:

注：大量の干渉源データの記録を回避するため、CMXは一定時間の間に存在する干渉源のみを記録します。



RSSIカットオフ機能は、宅内を通過するクライアントが実際に入らないように記録を回避するために使用されます。これは、クライアント追跡のみを有効にし、バスの駅や近くの通りを調査することで、導入に大きな影響を与える可能性があります。デフォルトでは、この値は–85 dBmに設定されています。この値を変更する前に、宅外のクライアントのRSSIを測定する必要があります。この値は、CMX Webインターフェイスの[System] -> [Settings] -> [Filtering:



CMX 10.6の時点で、CMXで記録されるクライアントの受信に必要なAPの最小量を変更するは、API呼び出しによってのみ行うことができます。まず、GET要求を使用して現在の設定を確認できます。

```
[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}
```

この設定では、値minapwithvalidrssiは1に設定されています。これはデフォルト値です。この値を3に変更するには、POST要求を使用します。これらの設定が適用されると、クライアントは、CMXによって記録されます。これは、RSSIで3番目のAPから受信された時点で、指定された最小値と同じかそれ以上の値になります。

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

いずれかの値を変更したら、GET要求を実行して、設定が正常に適用されたことを確認します。

VMリソースの増加

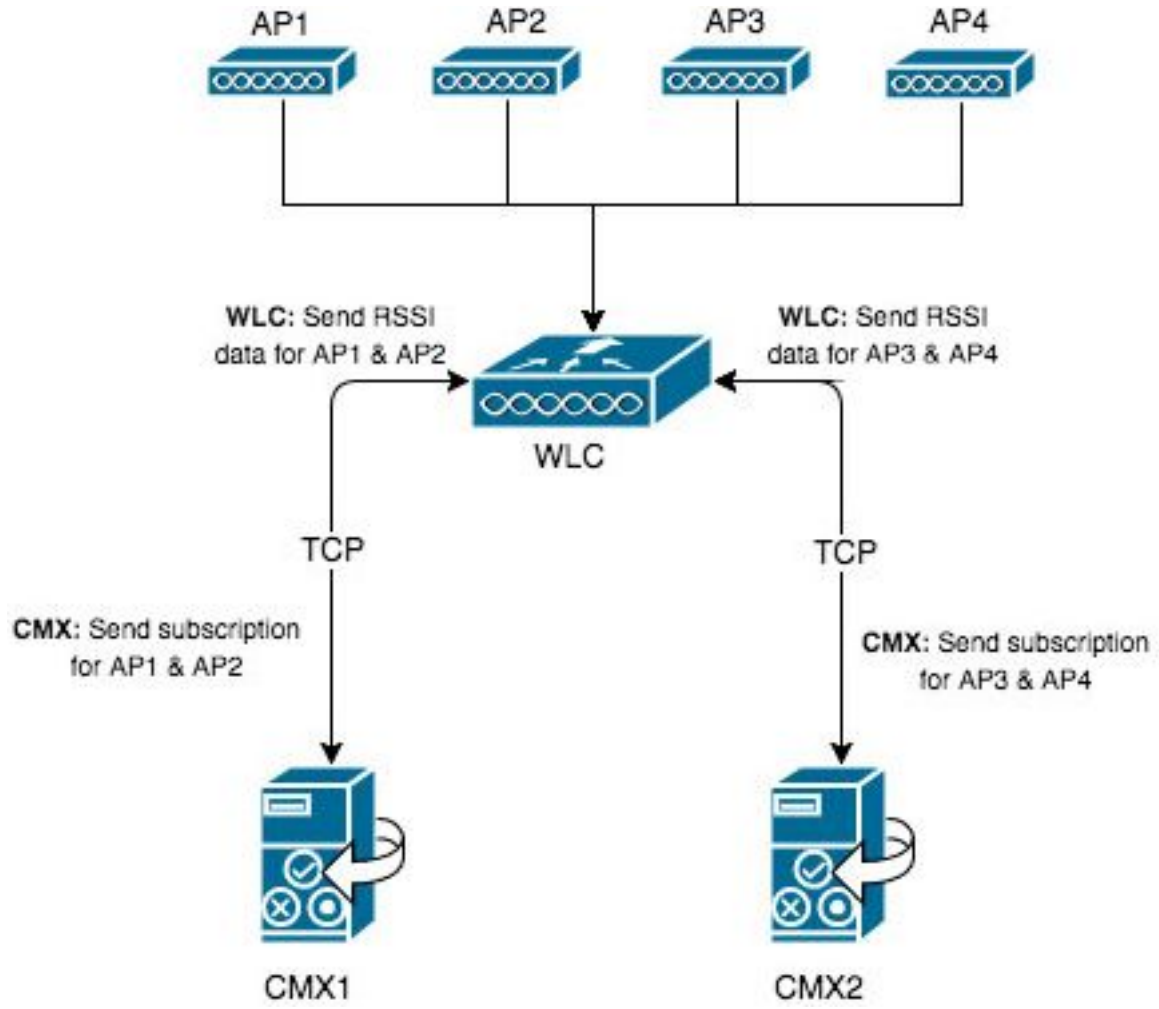
現在のCMXノードがVMで実行されていて、そのサイズがすべてのクライアントに対応するには十分でない場合、VMリソースを増やすことができるため、処理能力を高めることができます。CPUコア、メモリ、およびディスク領域を単純に割り当てます。CMXローエンド、スタンダード、ハイエンドノードの正確な要件はこちらをご覧ください。

現在のCMXセットアップがすでにハイエンドノードである場合は、この記事で説明する他のオプションを検討してください。

注：VM上でスナップショットをアクティブにすると、パフォーマンスに悪影響を及ぼす可能性があるため、実稼働環境では推奨されません。

CMXグループ化（旧称APグループ化）

CMXグループ化は、リリース8.7以降を実行するCMX 10.5以降およびAireOS WLCで使用できる機能です。8.7リリーストレインは今後アップデートを受信しないため、8.8以降のリリースを使用することを推奨します。この機能により、単一のコントローラは、APのグループを選択し、特定のCMXノードにグループを割り当てることで、複数のCMXノードに負荷を分散できます。これらのAPグループは、WLCのAPグループ機能とは関係ありません。



CMX1のマップには、AP1とAP2だけが配置されます。CMX1は、マップ上にある2つのAPについてWLCと通信します。CMXグループ化機能を有効にすると、AP1とAP2によって記録されたすべての情報（関連付けおよびプローブ専用クライアント、干渉源、BLEビーコン、RFIDタグなど）がCMX1にのみ送信されます。

1つのコントローラに同時に最大4つのNMSP接続を確立できます。つまり、最大4つのCMXノードを追加できます。4つのハイエンドノードを使用すると、理論上、1日あたり最大360,000(4x90,000)の一意のクライアントMACアドレスを記録できます。

次のtestコマンドを使用すると、WLCが接続できるCMXサーバの数を増やすことができます

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

重要:CMXグループ化機能が有効になっていない場合、8.7より低いコードまたは8.7より高いコードを実行しているコントローラは、複数のWLCに追加しないでください。これにより、特にHyperLocationの設定で、不正確なデータが記録される可能性があります。

このコントローラが追加されるすべてのCMXノードで、機能を有効にしてサービスを再起動するために必要な操作は次のとおりです。

1. 次のコマンドを使用して、機能を有効にします。

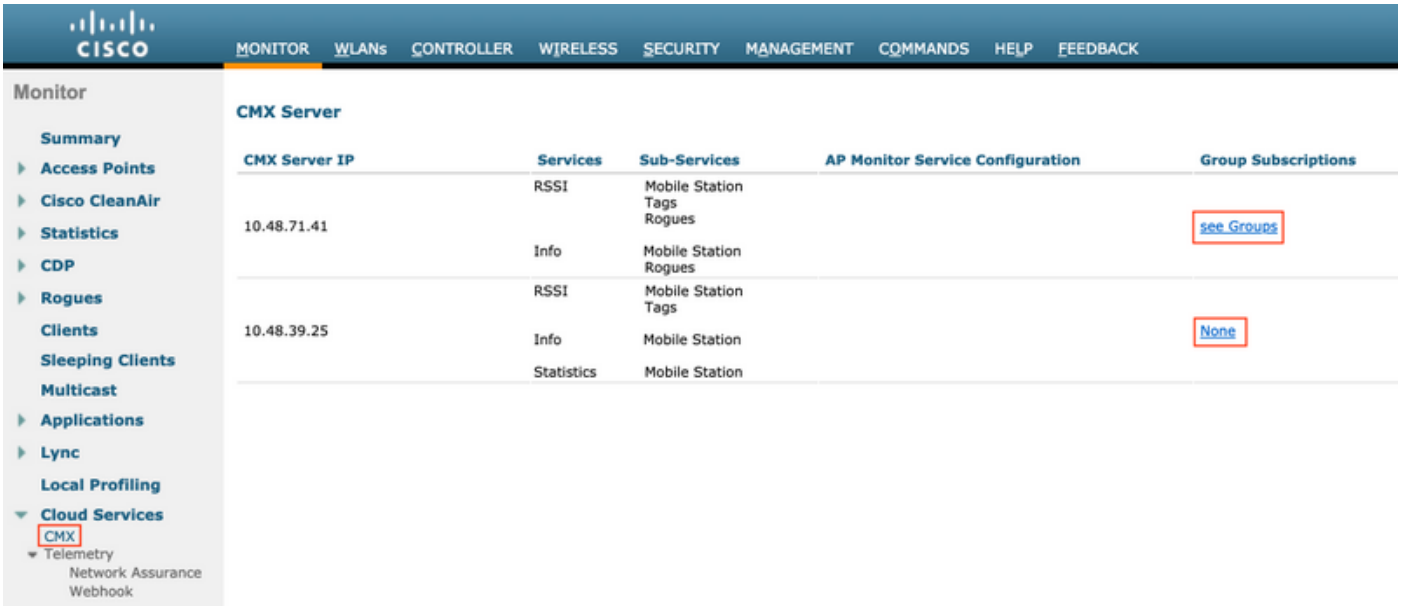
   ```
   cmxctl config featureflags nmsplb.cmxgrouping true
   ```
   trueをfalseに置き換えると機能が無効になります。
2. CMXエージェントを再起動します。

   ```
   cmxctl restart agent
   ```

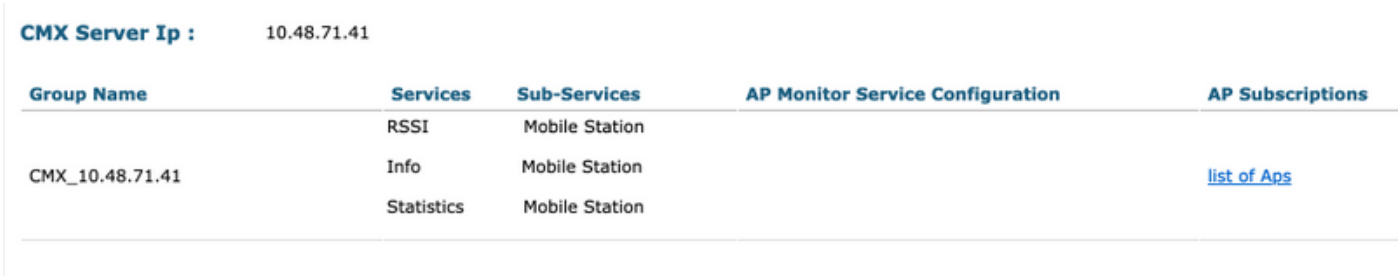
3. NMSPロードバランサを再起動します。
   ```
   cmxctl nmsplb stop
   cmxctl nmsplb start
   ```
4. 機能が正常に有効になっているかどうかを確認するには、次のコマンドを実行します。

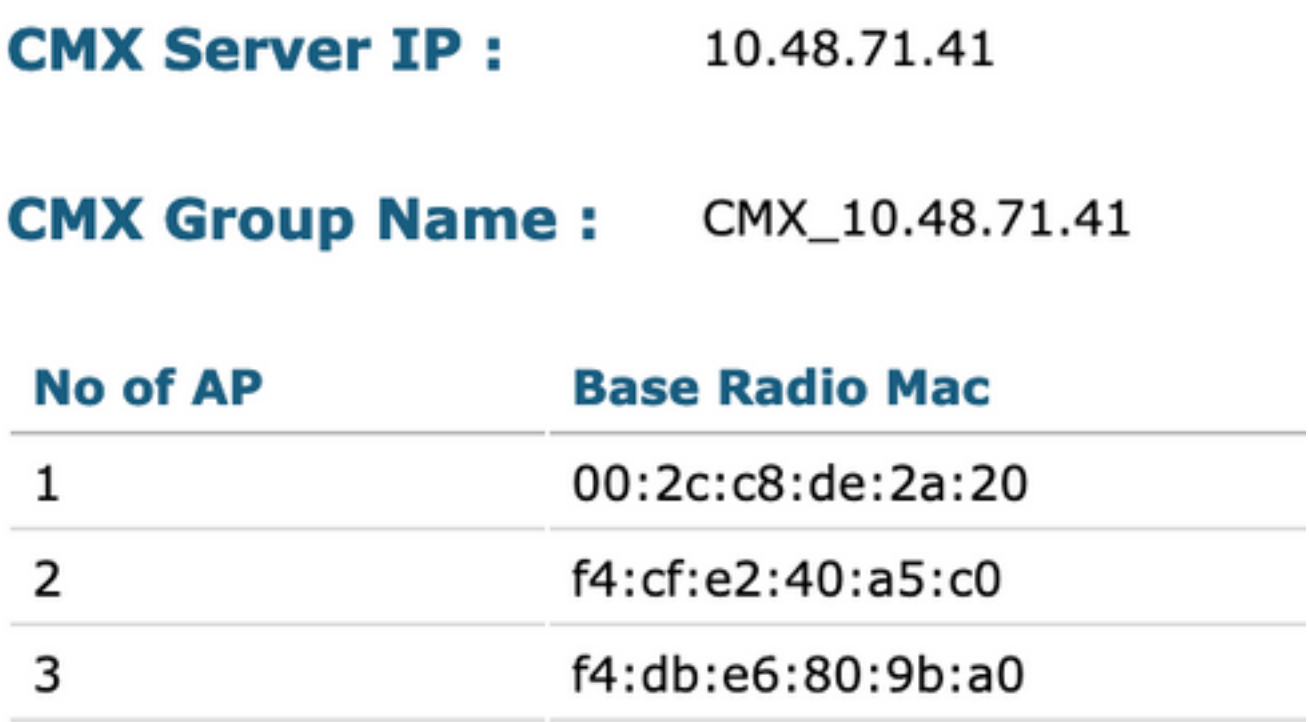
   ```
   [cmxadmin@cmx3375 ~]$ cmxctl config featureflags
   +----------------------------------------+-------+
   | location.compactlocationhistory        | false |
   +----------------------------------------+-------+
   | configuration.oi.host                  | true  |
   +----------------------------------------+-------+
   | 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 |
   +----------------------------------------+-------+
   ```

[Monitor] > [Cloud Services] > [CMX]で、グループ化機能が有効になっているCMXノードが表示されます。[なし]はグループ化機能が無効で、[グループを表示]は有効であることを示します。



「グループを表示」ページを開くと、このCMXノードがサブスクライブしているAPのリストにアクセスできます。



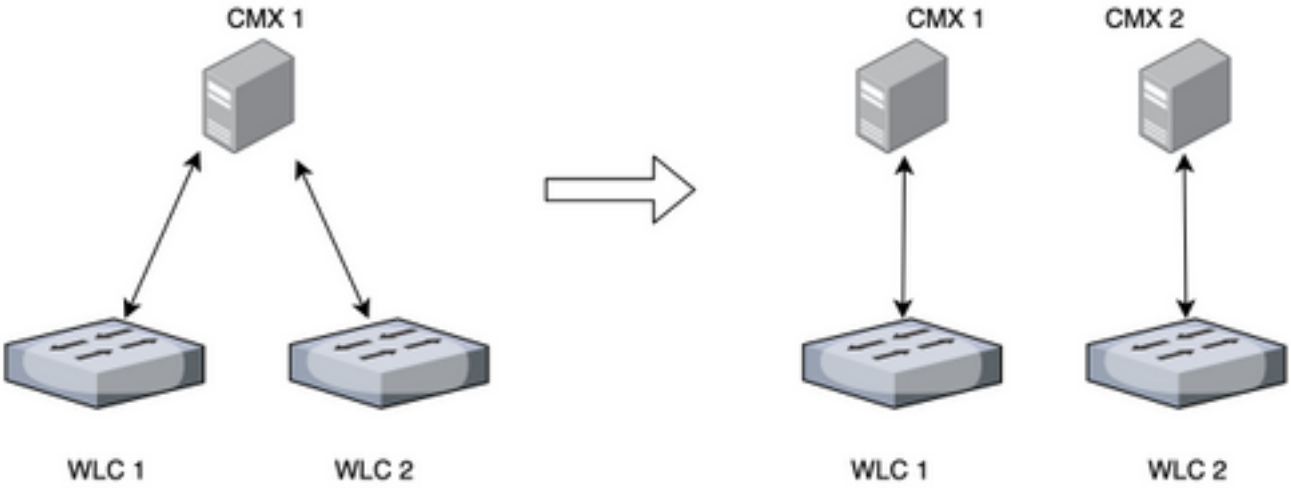


このコントローラに関連付けられている合計4つのAPのうち、CMXマップには3つだけが配置さ

れます。WLCはCMXからこれを学習し、検出された情報のみを10.48.71.41にあるCMXノードに送信します。

追加のノード展開

ネットワークが複数のワイヤレスコントローラで構成されている場合は、追加のCMXノードを導入し、複数のWLCとCMXの間に1 ~ 1のマッピングを作成できます。WLCバージョンの場合は、特別な要件はありません。1つのWLCを複数のCMXノードに同時に追加しないようにします。



DNA空間 – 作業をクラウドにオフロード

シスコの新しいクラウドプラットフォームDNA Spacesは、クライアントの追跡をクラウドに移行することを目的としています。リソースは、現在の負荷に基づいて自動的に割り当てられます。ワイヤレスネットワークをクラウドに接続するには、次の方法があります。

1. WLCをクラウドに直接接続
2. DNA Spaces Connector（プロキシとして機能する小さなVM、コントローラがクラウドに公開されない）
3. クラウドのゲートウェイとしてCMXを使用（このオプションはHyperLocationの導入に必要）

関連するバグ

- CSCvq25953 – ロケーションSSIDフィルタリングを有効にすると、ローカルで管理されるMACの除外が無効になり、その逆も無効になります