Otimizar o desempenho do CMX

Contents

Introduction

Este artigo explicará como reconhecer e redistribuir a carga de um único nó CMX (Connected Mobile eXperience) para acomodar uma grande quantidade de dispositivos sendo rastreados. Problemas como esse são frequentemente observados em implantações extremamente grandes em áreas públicas ou em configurações onde o rastreamento do cliente está ativado.

Prerequisites

Requirements

Este artigo pressupõe que você tem conhecimento da configuração básica e da configuração de um CMX e se concentra apenas em dicas e truques para otimizar o desempenho em grandes implantações.

Componentes Utilizados

Todos os comandos e exemplos mostrados neste artigo foram executados na WLC 3504 executando código 8.8.125 e no CMX 10.6.1 executado no dispositivo 3375.

Sinais de um nó CMX sobrecarregado

A sobrecarga de um nó CMX pode resultar em vários problemas diferentes:

- Os serviços não podem iniciar
- Serviços que param/travam abruptamente

- Serviço de análise mostrando 0 clientes ativos
- Alarmes e alertas por e-mail dizendo que o serviço de análise ou localização está em um estado crítico
- Incapacidade de estabelecer HA entre o nó CMX primário e secundário

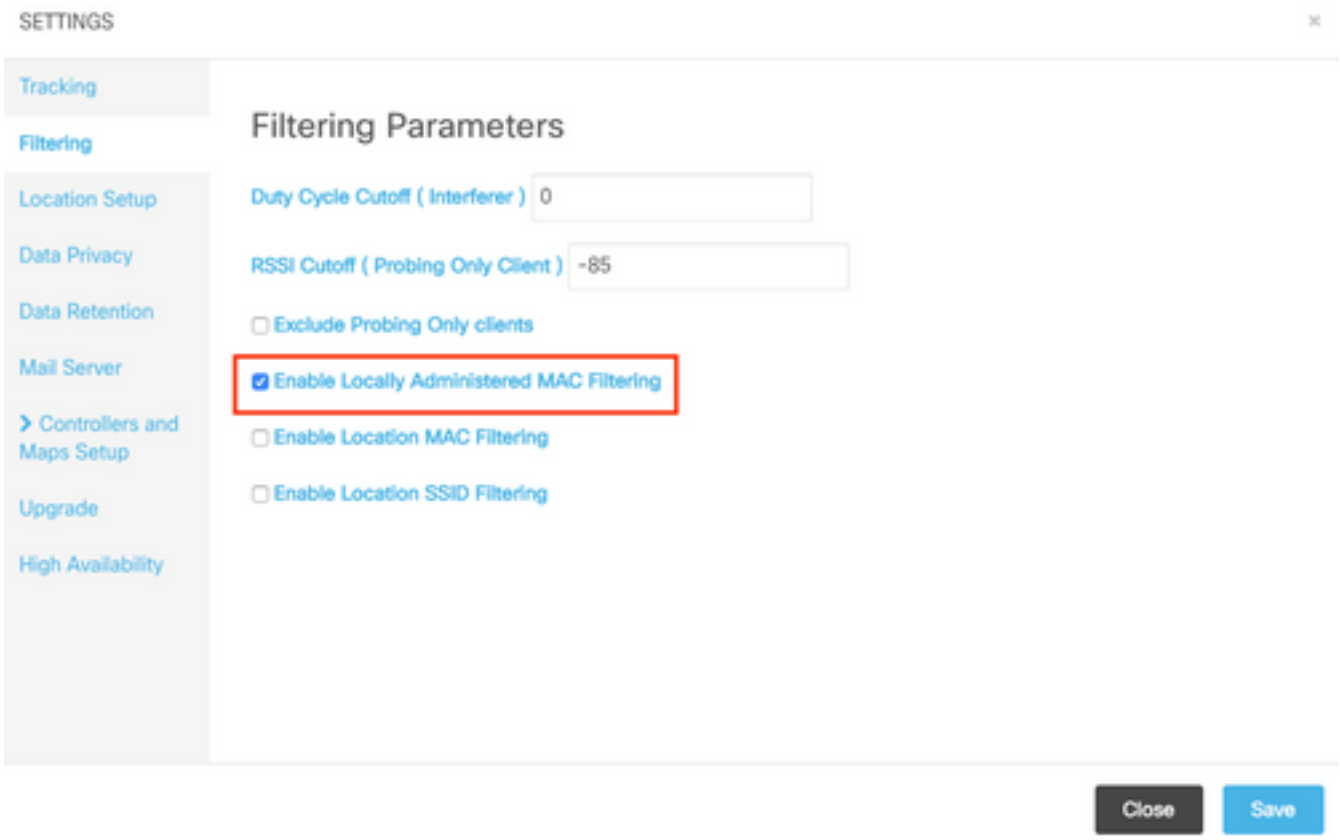
Redistribute CMX Load

Filtrando endereços MAC administrados localmente

Devido às crescentes preocupações com a privacidade, a partir do IOS 8 release em 2014, os fabricantes de smartphones começaram a implementar um recurso chamado randomização MAC, onde os dispositivos usariam um novo endereço MAC gerado aleatoriamente cada vez que enviassem uma solicitação de sondagem. Ao gerar um endereço MAC aleatório, os fabricantes podem decidir usar um endereço MAC "administrado localmente", que tem um bit especial que indica que o endereço é aleatório ou simplesmente gerar um endereço completamente aleatório que não pode ser distinguido de um endereço real. Um número muito pequeno de clientes realmente usa seu endereço MAC real ao sondar.

O CMX tem uma maneira de filtrar esses endereços MAC aleatórios falsos. Em System->Settings->Filtering (Sistema->Configurações->Filtragem), verifique sempre se a opção "Enable Locally Administered MAC Filtering" (Ativar filtragem MAC administrada localmente) está marcada.

> **Observação**: esse campo foi removido da interface da Web no CMX 10.6.0 e está sempre ativado por padrão



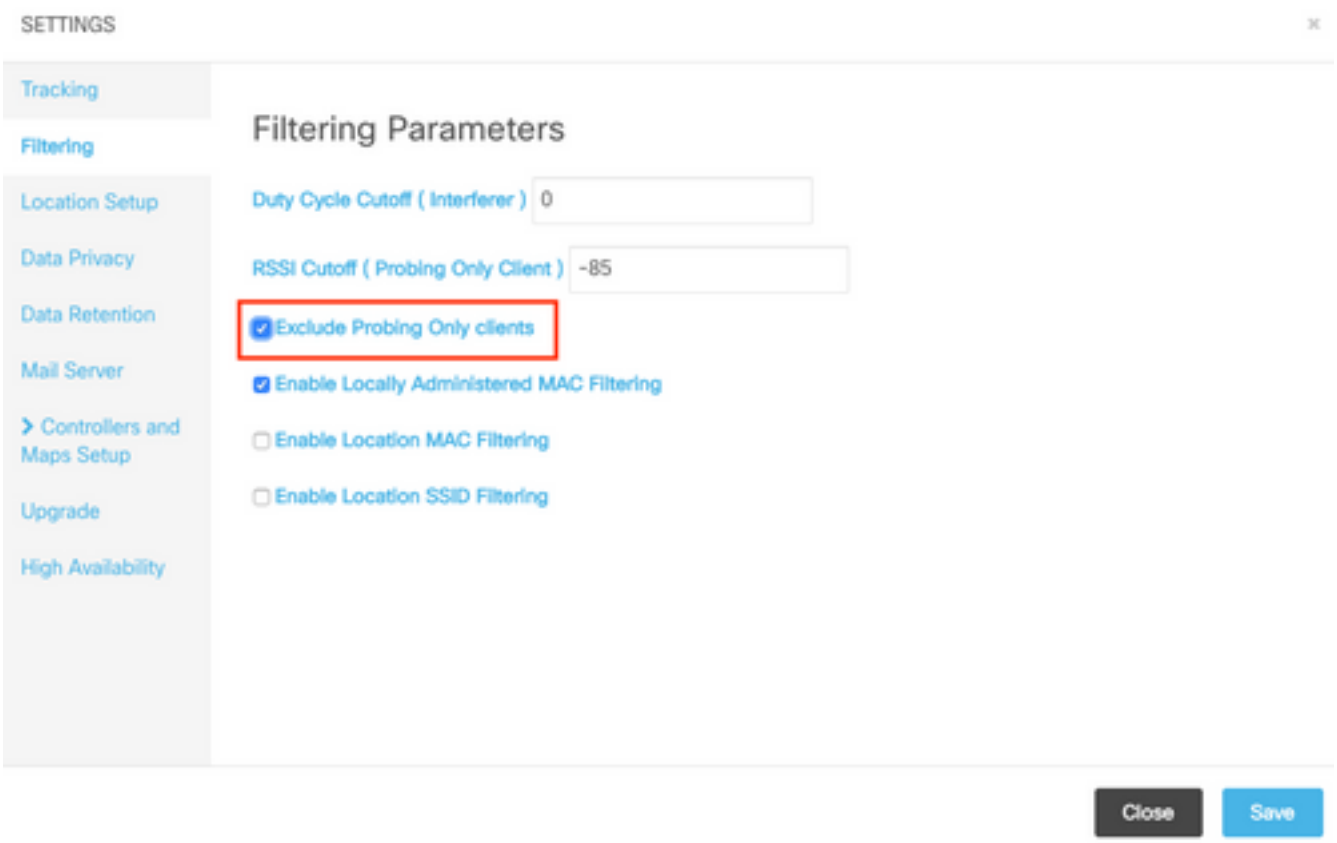
Rastreamento de clientes de sondagem

A causa principal mais comum de uma sobrecarga de CMX com a qual o Cisco TAC lida é o rastreamento de sondagem somente de clientes. Habilitar esse recurso permite o rastreamento de localização de clientes não associados. Áreas públicas abertas, como shoppings e estações de trem com um grande número de visitantes, muitas vezes excedem as limitações até mesmo de um nó CMX high-end.

Em configurações que estão rastreando clientes em sondagem, os endereços MAC gerados aleatoriamente também têm um impacto muito grande na contagem de clientes.

Alguns fabricantes, como a Apple, estão seguindo um padrão e usando endereços MAC aleatórios administrados localmente durante a sondagem, o que significa que **os dispositivos iPhone nunca serão detectados pelo CMX** durante a sondagem e não associados. Os dispositivos que não estão seguindo o padrão e usando endereços MAC aleatórios que não são administrados localmente serão **registrados pelo CMX como um novo cliente toda vez que enviarem a solicitação de sondagem** (o que pode acontecer a cada dois segundos). Como resultado, a contagem de clientes de sondagem pode ser significativamente maior/menor do que o número real de dispositivos na rede.

O rastreamento de clientes em sondagem pode ser desabilitado das interfaces da Web do CMX em System->Settings->Filtering marcando a opção "Exclude clientes somente sondagem":



Devido a todas as variações acima mencionadas, sondar a contagem de clientes não deve ser usado como um contador de queda de carbono e o Cisco TAC recomenda muito contra o rastreamento de clientes de sondagem.

Ajuste do algoritmo de detecção

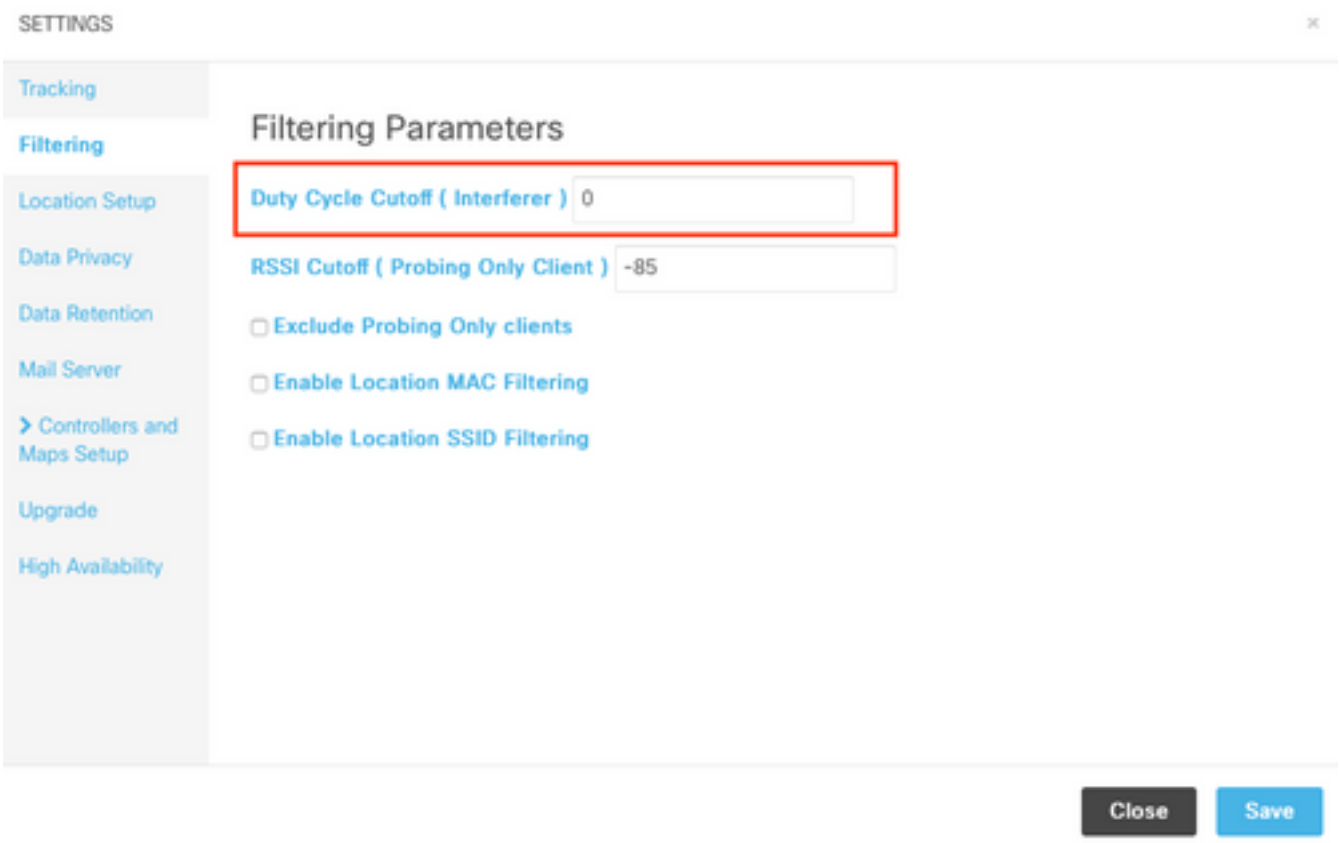
Ao ajustar as opções de filtragem no CMX, o número de clientes em sondagem que estão sendo gravados pode ser severamente limitado. Há duas opções principais que têm um impacto

significativo na detecção de clientes (especialmente somente para sondagem):

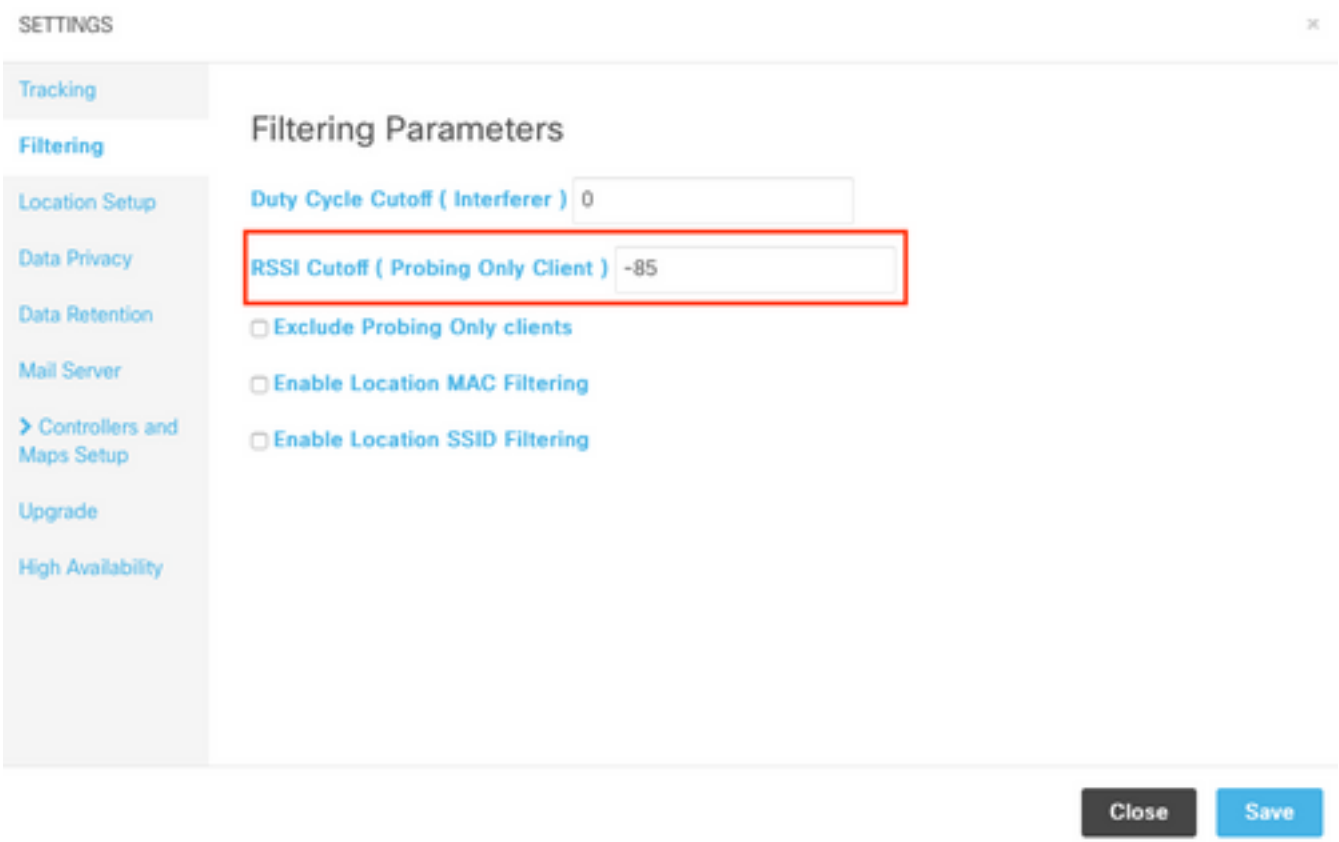
1. Corte do ciclo de funcionamento (interferente)
2. Corte RSSI
3. Quantidade mínima de APs que precisam ouvir o cliente, para que ele seja gravado

Em áreas densas e altamente povoadas, espera-se que tenha um grande número de interferências. Dispositivos como relógios Bluetooth não terão um impacto enorme na rede. Aumentando o valor do ciclo de interferência mais próximo, por exemplo, de 50, apenas os interferentes fortes que estão tomando mais de 50% do tempo de ar serão registrados pelo CMX. Esse valor pode ser configurado na interface da Web do CMX, em System->Settings->Filtering:

> **Note**: Para evitar gravar uma grande quantidade de dados de interferência, o CMX está registrando apenas as interferências presentes por um determinado período de tempo.



O recurso **de corte RSSI** é usado para evitar gravar clientes que estão apenas passando pelas instalações e não entrando na realidade. Isso pode ter um impacto enorme nas implantações com a sondagem de apenas rastreamento de cliente habilitado e uma estação de ônibus ou uma rua próxima. Por padrão, esse valor é definido como -85 dBm. Antes de alterar esse valor, deve ser medida a RSSI de um cliente fora das instalações. Esse valor pode ser configurado na interface da Web do CMX, em System->Settings->Filtering:



A partir do CMX 10.6, a alteração da **quantidade mínima de AP necessária para ouvir um cliente** para que ele seja gravado pelo CMX só pode ser feita através de uma chamada de API. Primeiro, uma solicitação GET pode ser usada para ver a configuração atual:

```
[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}
```

Nesta configuração, o valor minapwithvalidrssi é definido como 1, que é o valor padrão. A alteração desse valor para 3 pode ser feita usando uma solicitação POST. Depois que essas configurações forem aplicadas, o cliente será gravado pelo CMX quando for ouvido pelo terceiro AP no RSSI igual ou melhor que o mínimo especificado:

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

Depois de alterar qualquer um dos valores, certifique-se de executar uma solicitação GET para confirmar se as configurações foram aplicadas com êxito.

Aumento dos recursos de VM

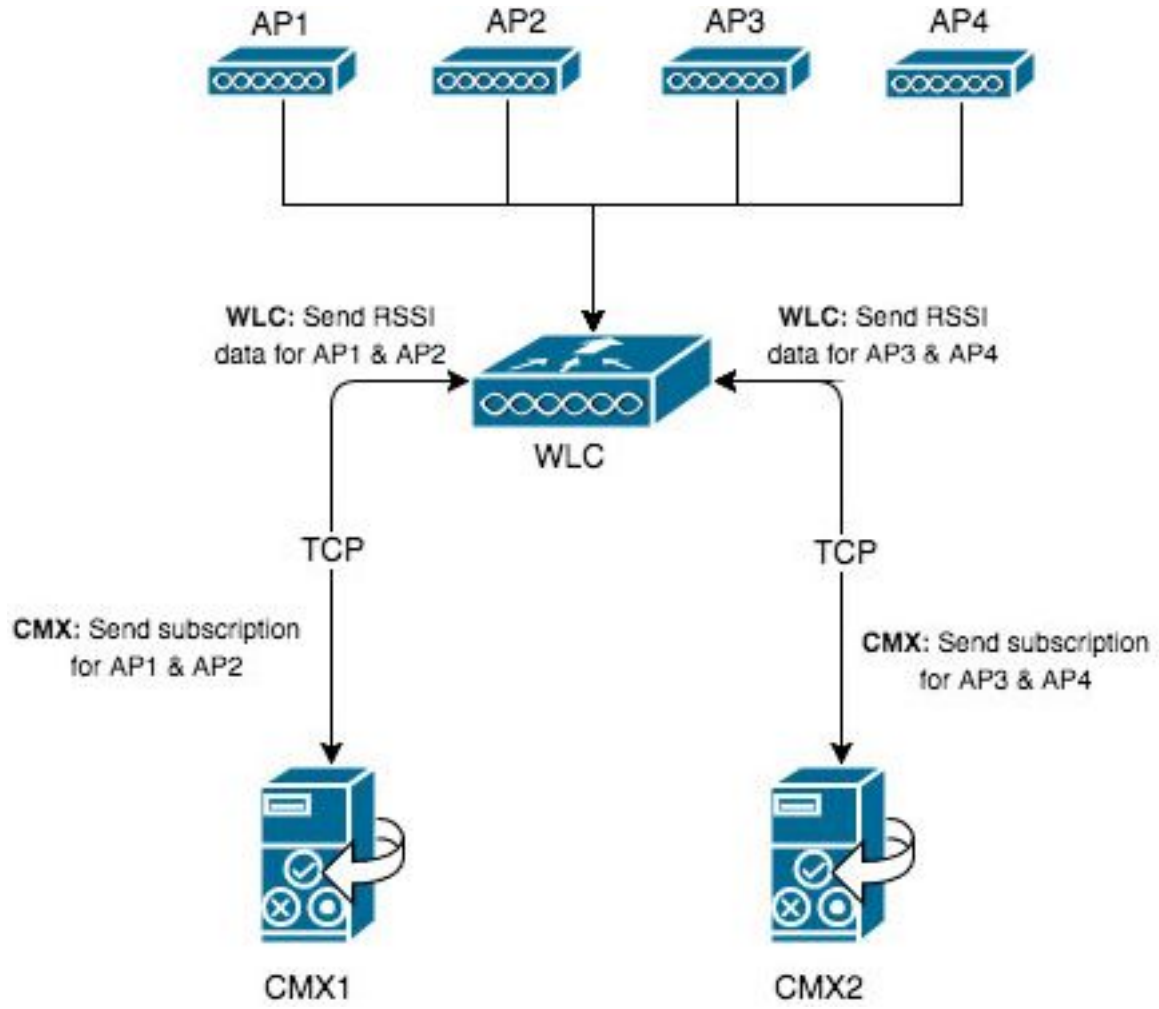
Se um nó CMX atual estiver sendo executado em uma VM e seu tamanho não for suficiente para acomodar todos os clientes, é possível aumentar os recursos da VM e, portanto, sua potência de processamento. Basta alocar mais núcleos de CPU, memória e espaço em disco. Os requisitos exatos para os nós Baixo, Padrão e High-End do CMX podem ser encontrados AQUI.

Se a configuração atual do CMX já for um nó high-end, considere outras opções mencionadas neste artigo.

Note: Ter um snapshot ativo em uma VM pode ter um impacto negativo no desempenho e não é recomendado para ambientes de produção.

Agrupamento CMX (anteriormente conhecido como Agrupamento AP)

O Agrupamento CMX é um recurso disponível no CMX 10.5 ou posterior e WLCs AireOS executando as versões 8.7 ou posterior. Como a versão 8.7 do treinamento não receberá atualizações no futuro, é recomendável usar a versão 8.8 ou posterior. Esse recurso permite que um único controlador distribua a carga para vários nós CMX selecionando grupos de APs e atribuindo um grupo a um nó CMX específico. Esses grupos de APs não estão relacionados ao recurso Grupo AP na WLC.



Os mapas no CMX1 têm apenas AP1 e AP2 colocados. O CMX1 se comunicará com o WLC sobre os 2 APs encontrados no mapa. Quando o recurso de agrupamento CMX estiver ativado, todas as informações registradas pelo AP1 e AP2 (incluindo somente clientes associados e sondagens, interferentes, beacons BLE, tags de RFID..) serão enviadas somente para o CMX1.

Um único controlador pode ter até 4 conexões NMSP estabelecidas no momento, o que significa que até 4 nós CMX podem ser adicionados a ele. Com 4 nós high-end, isso permitiria teoricamente até 360.000 (4x90.000) endereços mac de cliente únicos a serem gravados por dia.

Épossível aumentar a quantidade de servidores CMX aos quais uma WLC pode se conectar com o seguinte comando de teste

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

Importante: o controlador que executa um código inferior a 8.7 ou superior a 8.7 sem recurso de Agrupamento CMX habilitado nunca deve ser adicionado a várias WLCs. Isso pode fazer com que dados imprecisos sejam gravados, especialmente em configurações do HyperLocation.

Em cada nó CMX ao qual esse controlador será adicionado, é necessário habilitar o recurso e reiniciar os serviços:

1. Ative o recurso usando o comando:

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

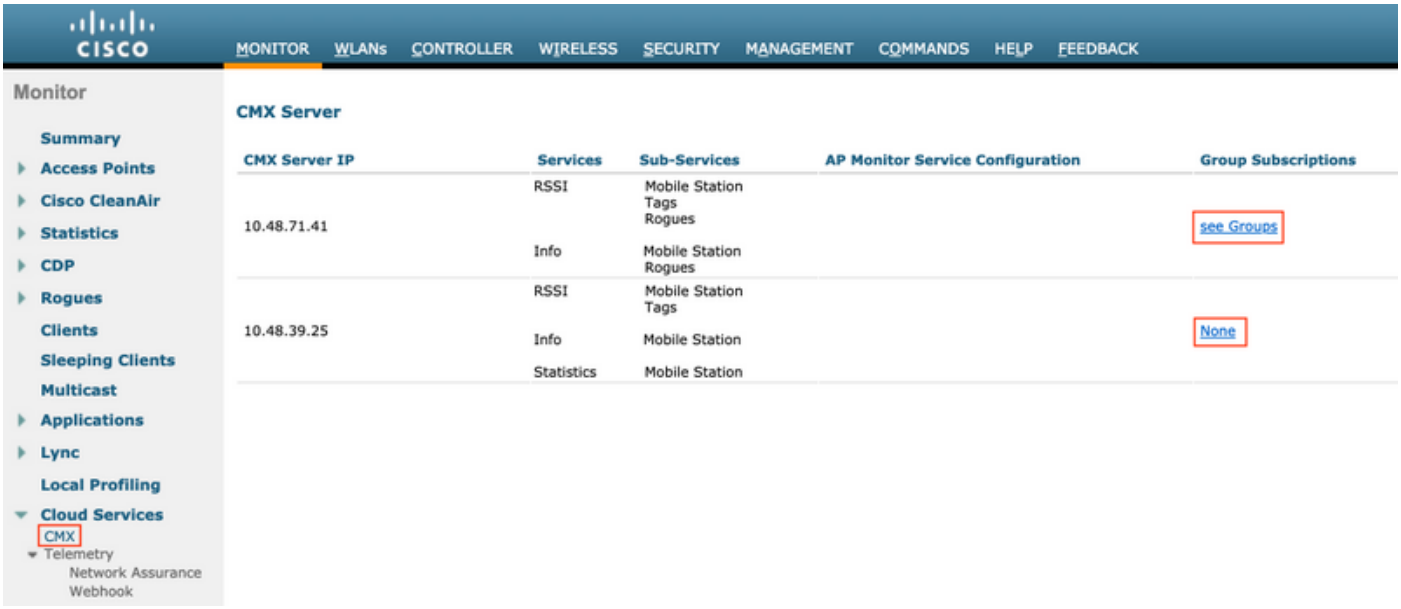
   Substituir a palavra true por false desabilita o recurso.
2. Reiniciar agente do CMX:

   ```
   cmxctl restart agent
   ```

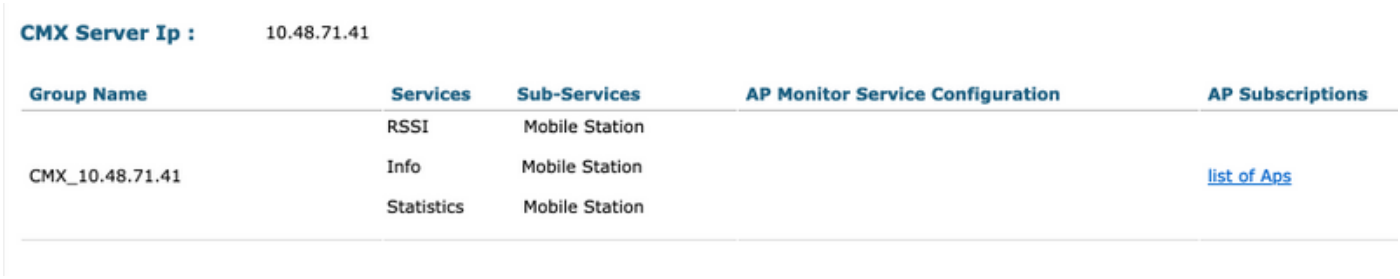
3. Reinicie o balanceador de carga NMSP:
   ```
   cmxctl nmsplb stop
   cmxctl nmsplb start
   ```
4. Para verificar se o recurso foi habilitado com êxito, execute:

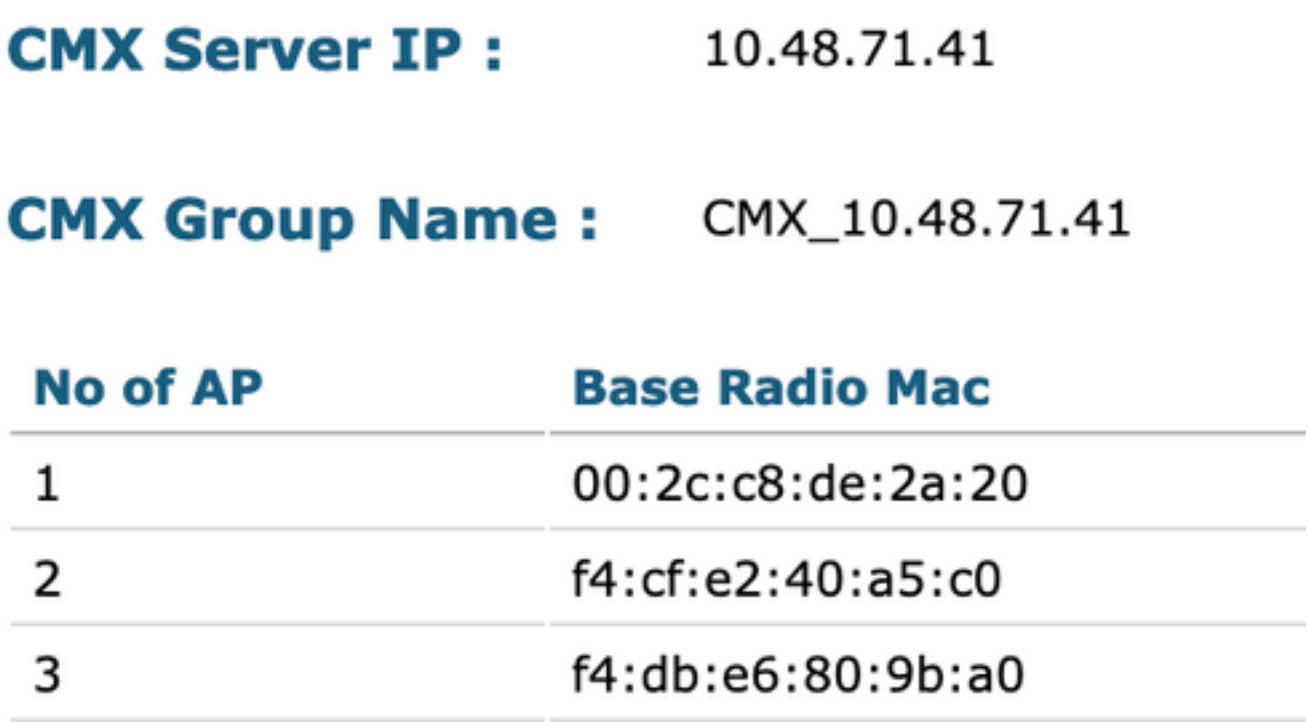
   ```
   [cmxadmin@cmx3375 ~]$ cmxctl config featureflags
   +----------------------------------------+-------+
   | location.compactlocationhistory        | false |
   +----------------------------------------+-------+
   | configuration.oi.host                  | true  |
   +----------------------------------------+-------+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

Em Monitor > Cloud Services > CMX, deve ser visível qual nó CMX tem o recurso de agrupamento ativado. "Nenhum" indica que o recurso de agrupamento está desabilitado, enquanto "consulte Grupos" indica que ele está habilitado.



Ao abrir a página "ver grupo", é possível acessar a lista de APs aos quais esse nó CMX está inscrito.



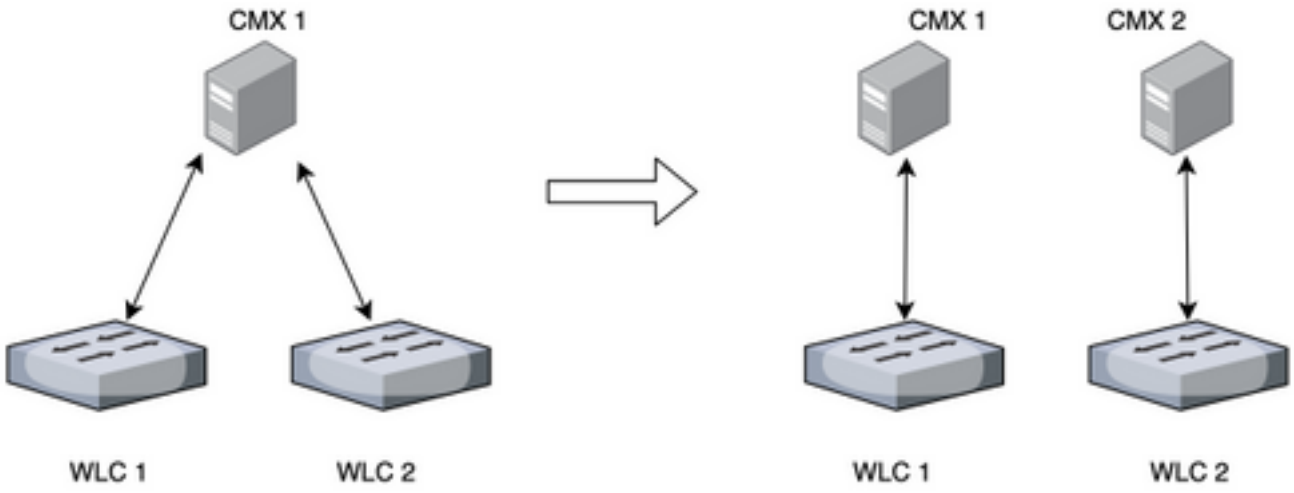


Dos 4 APs associados a esse controlador, apenas 3 são colocados no mapa CMX. A WLC

aprende isso do CMX e envia apenas as informações detectadas por eles ao nó do CMX localizado em 10.48.71.41.

Implantações adicionais de nó

Se a rede consiste em vários controladores sem fio, é possível implantar nós CMX adicionais e criar um mapeamento 1-1 entre várias WLCs e CMXs. Não há requisitos especiais quando se trata de uma versão de WLC. Certifique-se de não ter uma única WLC adicionada a vários nós CMX ao mesmo tempo.



Espaços do DNA - Descarregamento do trabalho para a nuvem

O novo Cisco Cloud Platform DNA Spaces tem como objetivo mover o rastreamento do cliente para a nuvem. Os recursos são alocados automaticamente com base na carga atual. É possível conectar sua rede sem fio à nuvem de várias maneiras:

1. Conectando diretamente a WLC à nuvem
2. Conector do DNA Spaces (uma pequena VM que atua como proxy, os controladores não são expostos à nuvem)
3. Usar o CMX como gateway para a nuvem (essa opção é necessária para implantações de HyperLocation)

Bugs relevantes

- CSCvq25953 - Habilitar a filtragem de SSID de local desabilita a exclusão de MACs administrados localmente e vice-versa