

Ottimizzazione delle prestazioni CMX

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Segni di un nodo CMX sovraccarico](#)

[Ridistribuisce carico CMX](#)

[Filtraggio di indirizzi MAC amministrati localmente](#)

[Tracciamento dei client di tastatura](#)

[Modifiche all'algoritmo di rilevamento](#)

[Aumento delle risorse VM](#)

[Raggruppamento CMX \(in precedenza AP Grouping\)](#)

[Distribuzioni di nodi aggiuntivi](#)

[DNA Spaces - Offload del lavoro nel cloud](#)

[Bug rilevanti](#)

Introduzione

In questo articolo viene spiegato come riconoscere e ridistribuire il carico di un singolo nodo CMX (Connected Mobile eXperience) in modo da supportare un numero elevato di dispositivi di cui tenere traccia. Problemi di questo tipo vengono spesso riscontrati in installazioni di grandi dimensioni in aree pubbliche o in installazioni in cui è abilitata la verifica dei client.

Prerequisiti

Requisiti

In questo articolo si presume che l'utente abbia conoscenza delle impostazioni e della configurazione di base di un CMX e si concentri solo su suggerimenti e suggerimenti per ottimizzare le prestazioni in installazioni di grandi dimensioni.

Componenti usati

Tutti i comandi e gli esempi mostrati in questo articolo sono stati eseguiti su uno switch 3504 WLC con codice 8.8.125 e su CMX 10.6.1 con accessorio 3375.

Segni di un nodo CMX sovraccarico

Il sovraccarico di un nodo CMX può causare diversi problemi:

- Impossibile avviare i servizi
- Arresto o arresto improvviso dei servizi

- Servizio di analisi che visualizza 0 client attivi
- Avvisi e avvisi tramite e-mail che indicano che il servizio di analisi o di posizione è in uno stato critico
- Impossibilità di stabilire una disponibilità elevata tra il nodo CMX primario e quello secondario

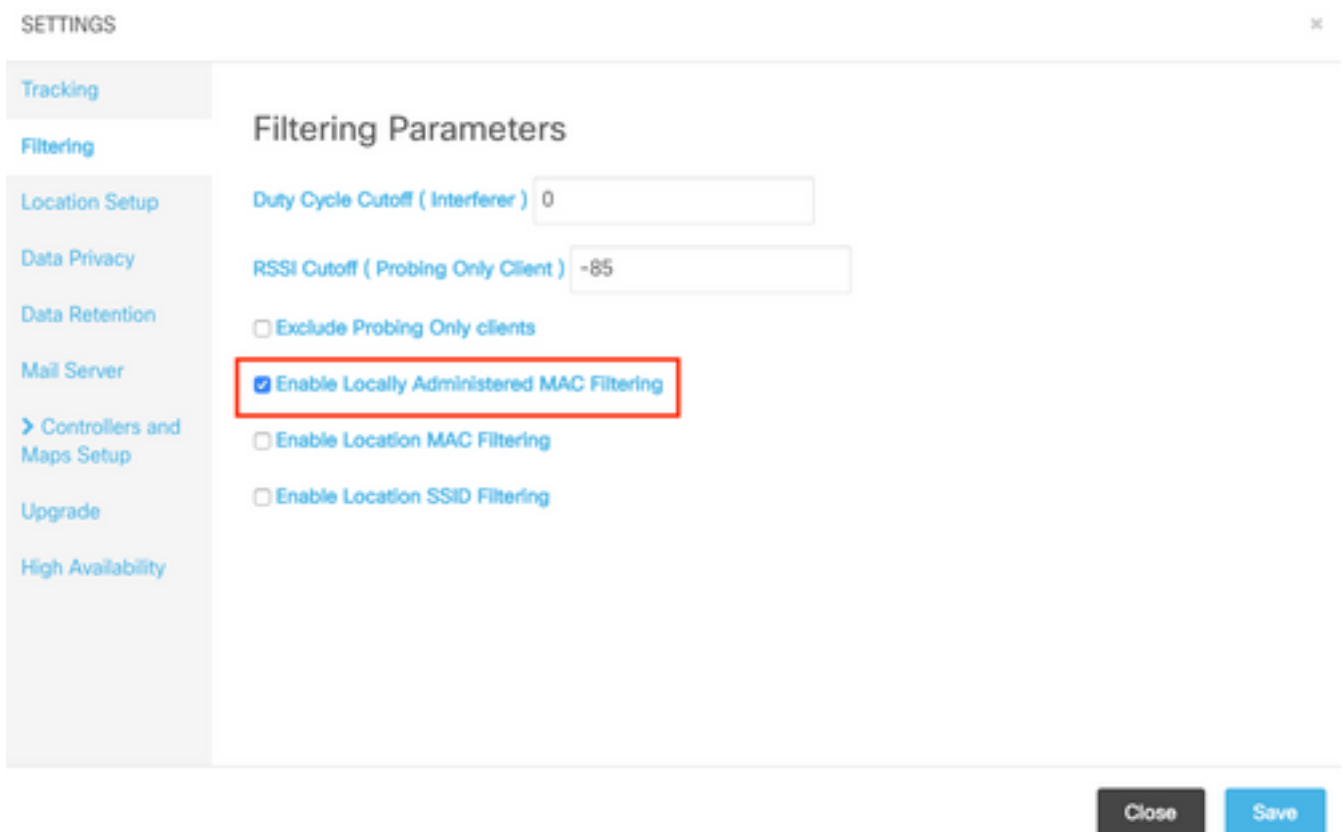
Ridistribuisce carico CMX

Filtraggio di indirizzi MAC amministrati localmente

A causa dei crescenti problemi di privacy, a partire dalla versione IOS 8 nel 2014, i produttori di smartphone hanno iniziato a implementare una funzionalità chiamata randomizzazione MAC, dove i dispositivi userebbero un nuovo indirizzo MAC generato casualmente ogni volta che inviano una richiesta di sonda. Quando si genera un indirizzo MAC casuale, i produttori possono decidere di utilizzare un indirizzo MAC "amministrato localmente" che ha un bit speciale che indica che l'indirizzo è casuale o semplicemente generare un indirizzo completamente casuale non distinguibile da uno reale. Un numero molto ridotto di client utilizza effettivamente il proprio indirizzo MAC reale durante la ricerca.

CMX consente di filtrare questi falsi indirizzi MAC casuali. In Sistema->Impostazioni->Filtraggio, assicurarsi sempre che l'opzione "Abilita filtro MAC amministrato localmente" sia selezionata.

Nota: questo campo è stato rimosso dall'interfaccia Web in CMX 10.6.0 ed è sempre abilitato per impostazione predefinita



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

Tracciamento dei client di tastatura

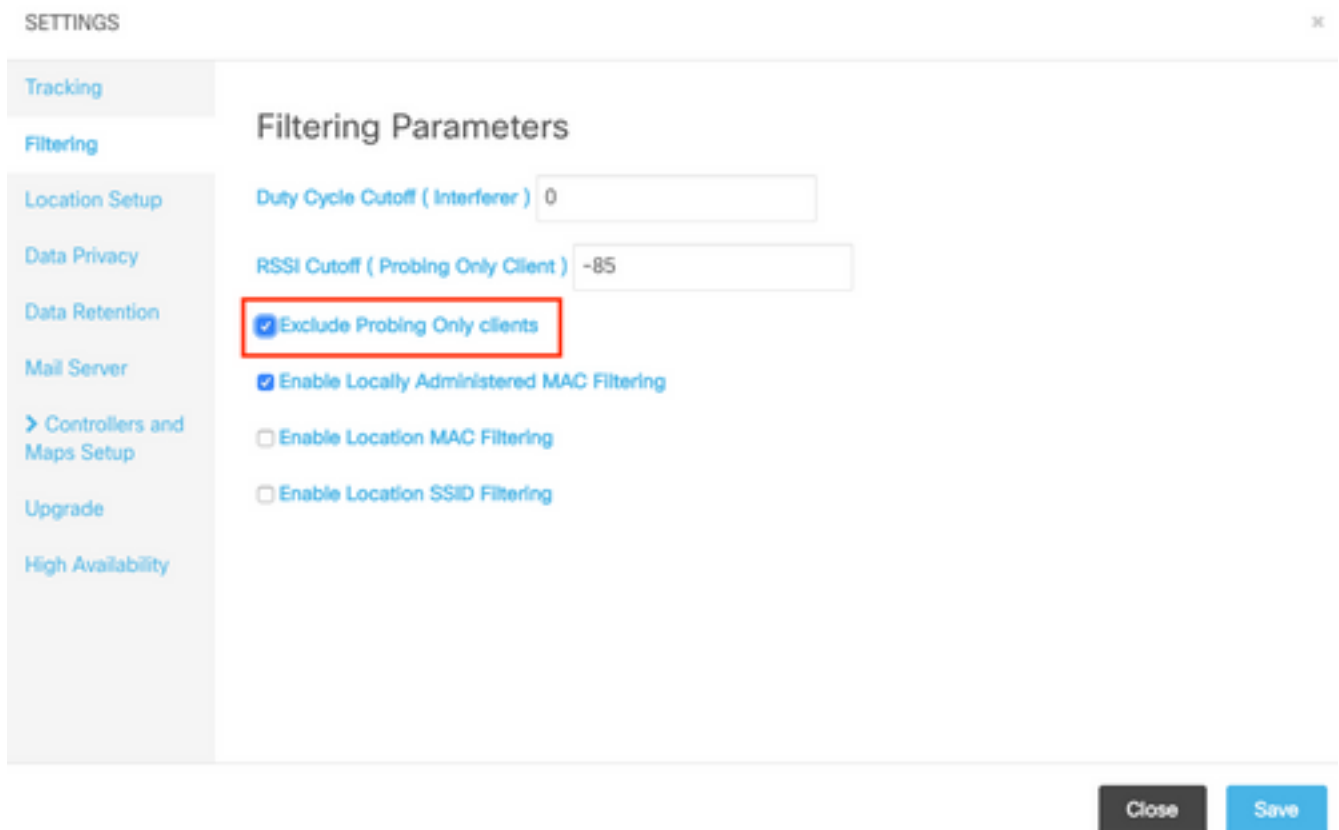
La causa principale più comune di un sovraccarico CMX di cui si occupa Cisco TAC è il

rilevamento dei client di prova. L'attivazione di questa funzionalità consente di tenere traccia della posizione dei client non associati. Aree pubbliche aperte come centri commerciali e stazioni ferroviarie con un numero enorme di visitatori molto spesso superano le limitazioni anche di un nodo CMX high-end.

Nelle configurazioni che tengono traccia dei client in prova, gli indirizzi MAC generati in modo casuale hanno anche un impatto molto forte sul numero dei client.

Alcuni produttori, come Apple, stanno seguendo uno standard e utilizzano indirizzi MAC casuali amministrati localmente durante il probe, il che significa che **i dispositivi iPhone non saranno mai rilevati da CMX** quando si esegue il probe e non associati. I dispositivi che non seguono lo standard e utilizzano indirizzi MAC casuali che non sono amministrati localmente verranno **registrati da CMX come nuovo client ogni volta che inviano la richiesta di verifica** (che può avvenire ogni due secondi). Di conseguenza, il numero di client che eseguono il probe può essere significativamente superiore/inferiore al numero effettivo di dispositivi nella rete.

La registrazione dei client di prova può essere disabilitata dalle interfacce Web CMX in Sistema->Impostazioni->Filtraggio selezionando l'opzione "Escludi client di prova":



A causa di tutte le variazioni sopra menzionate, il conteggio dei client di prova non deve essere utilizzato come contatore di caduta e Cisco TAC sconsiglia vivamente di tracciare i client di prova.

Modifiche all'algoritmo di rilevamento

Modificando le opzioni di filtraggio su CMX, il numero di client di prova registrati può essere severamente limitato. Esistono due opzioni principali che hanno un impatto significativo sul rilevamento dei client (in particolare il rilevamento dei client solo tramite probe):

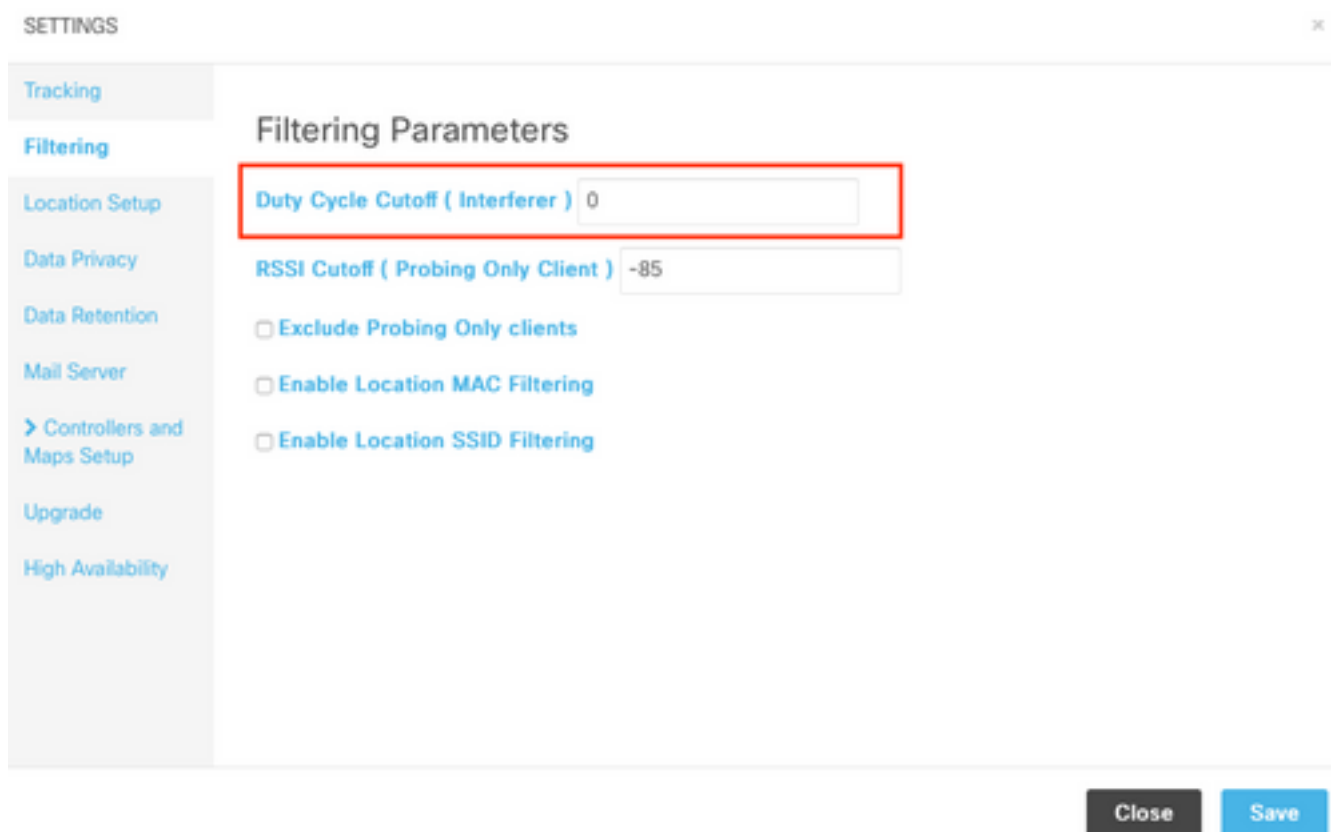
1. Interruzione del ciclo di servizio (interferente)

2. Limite RSSI

3. Numero minimo di punti di accesso che devono ascoltare il client, in modo che venga registrato

In una zona densamente popolata, si prevede di avere un gran numero di interferenti. Dispositivi come gli orologi Bluetooth non avranno un impatto enorme sulla rete. Aumentando il valore del ciclo di servizio delle interferenze in modo che si avvicinino, ad esempio, a 50, CMX registrerà solo le interferenze forti che assorbono oltre il 50% del tempo di trasmissione. Questo valore può essere configurato dall'interfaccia Web CMX, in Sistema->Impostazioni->Filtro:

Nota: Per evitare la registrazione di un'enorme quantità di dati interferenti, CMX registra solo gli interferenti presenti per un certo periodo di tempo.



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

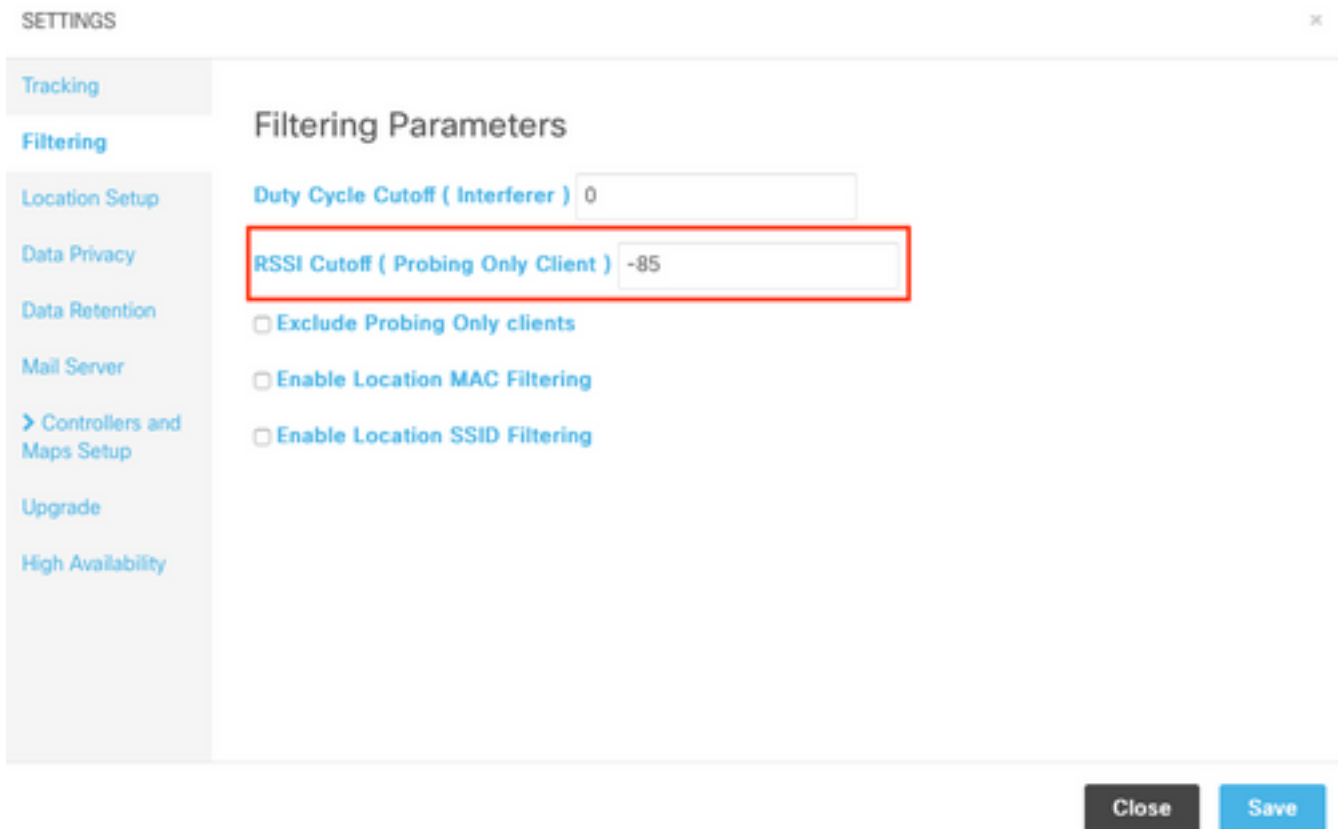
Exclude Probing Only clients

Enable Location MAC Filtering

Enable Location SSID Filtering

Close Save

La funzione **RSSI cutoff** viene utilizzata per evitare di registrare i clienti che stanno solo passando per la sede e non effettivamente entrando. Questo può avere un enorme impatto sulle installazioni, con il rilevamento dei soli client abilitato e una stazione degli autobus o una strada vicina. Per impostazione predefinita, questo valore è impostato su -85 dBm. Prima di modificare questo valore, si deve misurare l'RSSI di un cliente al di fuori dei locali. Questo valore può essere configurato dall'interfaccia Web CMX, in Sistema->Impostazioni->Filtro:



A partire dalla versione CMX 10.6, la modifica **della quantità minima di punti di accesso richiesta per l'ascolto di un client** per la registrazione da parte di CMX può essere effettuata solo attraverso una chiamata API. È innanzitutto possibile utilizzare una richiesta GET per visualizzare la configurazione corrente:

```
[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}
```

In questa impostazione, il valore `minapwithvalidrssi` è impostato su 1, che è il valore predefinito. È possibile modificare questo valore in 3 utilizzando una richiesta POST. Una volta applicate queste impostazioni, il client verrà registrato da CMX dopo essere stato ascoltato dal terzo punto di accesso in RSSI uguale o superiore al minimo specificato:

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

Dopo aver modificato uno dei valori, accertarsi di eseguire una richiesta GET per verificare che le impostazioni siano state applicate correttamente.

Aumento delle risorse VM

Se un nodo CMX corrente è in esecuzione in una VM e le sue dimensioni non sono sufficienti per tutti i client, è possibile aumentare le risorse della VM e quindi la potenza di elaborazione. È sufficiente allocare più core CPU, memoria e spazio su disco. I requisiti esatti per i nodi CMX di fascia bassa, standard e alta sono disponibili [QUI](#).

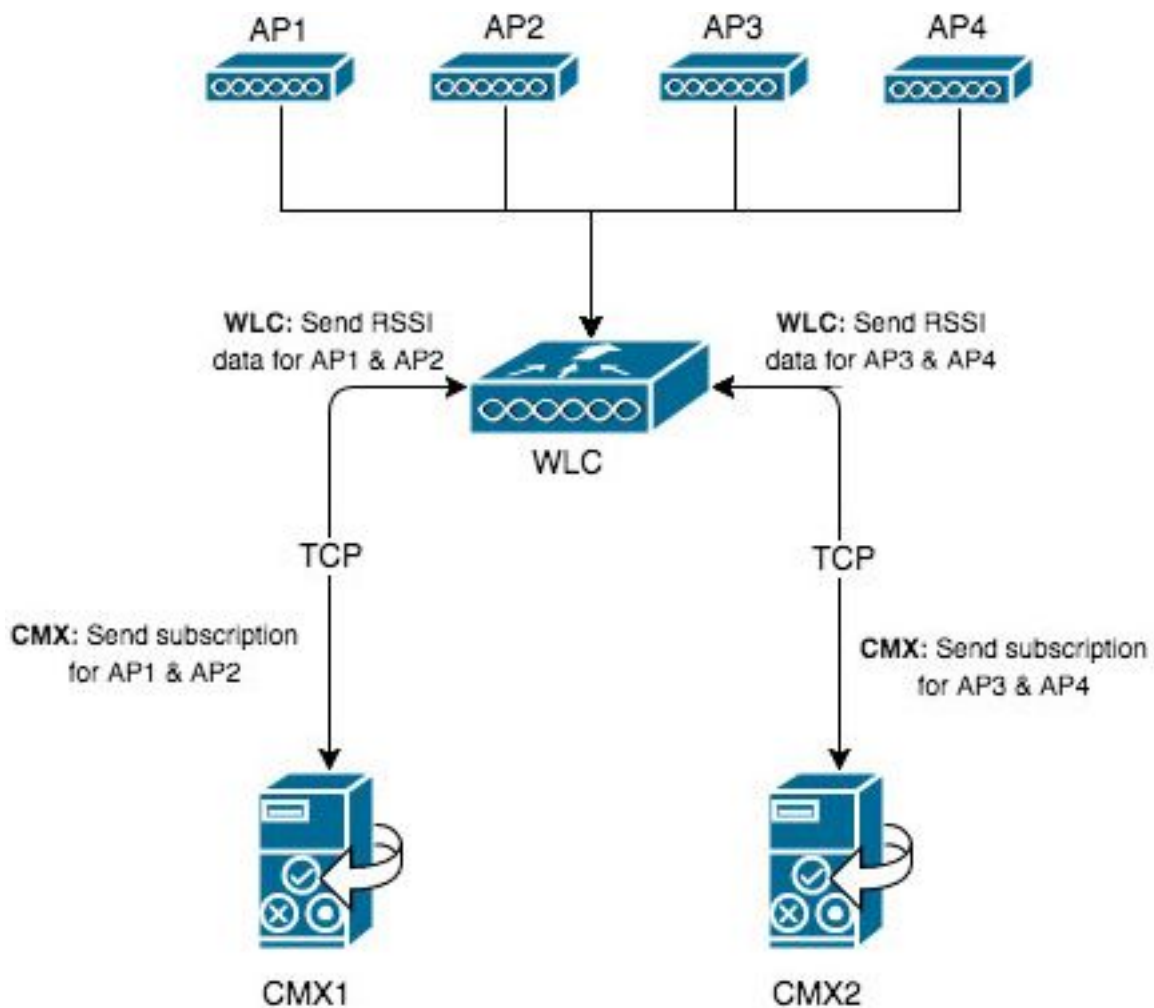
Se l'impostazione CMX corrente è già un nodo di fascia alta, prendere in considerazione altre

opzioni menzionate in questo articolo.

Nota: Una copia istantanea attiva su una VM può avere un impatto negativo sulle prestazioni e non è consigliata per gli ambienti di produzione.

Raggruppamento CMX (in precedenza AP Grouping)

Il raggruppamento CMX è una funzione disponibile su CMX versione 10.5 o successive e sui WLC AireOS con versione 8.7 o successive. Poiché il treno della release 8.7 non riceverà aggiornamenti in futuro, si consiglia di utilizzare la release 8.8 o successive. Questa funzione consente a un singolo controller di distribuire il carico a più nodi CMX selezionando gruppi di AP e assegnando un gruppo a un nodo CMX specifico. Questi gruppi di access point non sono correlati alla funzionalità Gruppo AP nel WLC.



Le mappe su CMX1 hanno solo AP1 e AP2. CMX1 comunicherà con il WLC riguardo ai 2 AP che si trovano sulla mappa. Una volta attivata la funzione di raggruppamento CMX, tutte le informazioni registrate da AP1 e AP2 (compresi i client associati e solo probe, gli interferenti, i beacon BLE, i tag RFID...) verranno inviate solo a CMX1.

Un singolo controller può avere fino a 4 connessioni NMSP stabilite contemporaneamente, il che significa che è possibile aggiungere fino a 4 nodi CMX. Con 4 nodi high-end, in teoria sarebbe possibile registrare fino a 360.000 (4x90.000) indirizzi MAC client univoci al giorno.

È possibile aumentare la quantità di server CMX a cui un WLC può connettersi con il seguente comando di test

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

Importante: un controller con codice inferiore a 8,7 o superiore a 8,7 senza la funzionalità CMX Grouping abilitata non deve mai essere aggiunto a più WLC. Ciò può causare la registrazione di dati non accurati, in particolare nelle impostazioni di HyperLocation.

In ogni nodo CMX a cui verrà aggiunto questo controller, è necessario attivare la funzionalità e riavviare i servizi:

1. Abilitare la funzionalità utilizzando il comando:

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

Sostituendo la parola true con false, la funzione viene disattivata.

2. Riavviare l'agente CMX:

```
cmxctl restart agent
```

3. Riavviare il servizio di bilanciamento del carico NMSPLB:

```
cmxctl nmsplb stop
cmxctl nmsplb start
```

4. Per verificare se la funzionalità è stata attivata correttamente, eseguire:

```
[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.queueuptime                 | false |
+-----+-----+
```

In Monitor > Servizi cloud > CMX dovrebbe essere visibile il nodo CMX con funzionalità di raggruppamento abilitata. "Nessuno" indica che la funzione di raggruppamento è disattivata, mentre "Vedere Gruppi" indica che è attivata.

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		

Aperto la pagina "vedi Gruppo", è possibile accedere all'elenco degli AP a cui questo nodo CMX è sottoscritto.

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

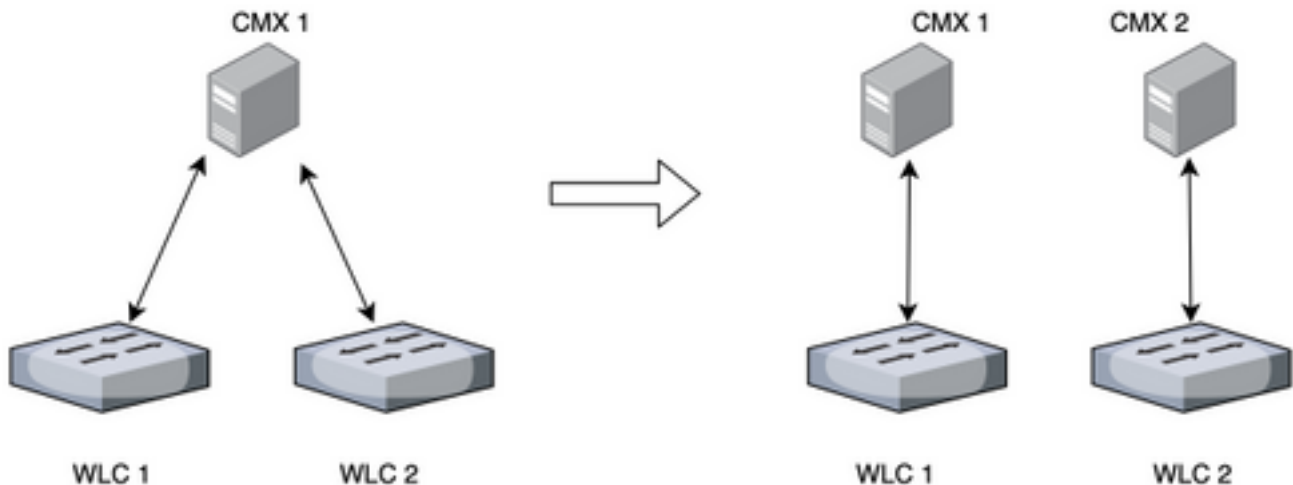
No of AP	Base Radio Mac
1	00:2c:c8:de:2a:20
2	f4:cf:e2:40:a5:c0
3	f4:db:e6:80:9b:a0

Dei 4 punti di accesso associati a questo controller, solo 3 vengono posizionati sulla mappa CMX.

WLC apprende questo da CMX e invia le informazioni rilevate solo al nodo CMX situato in 10.48.71.41.

Distribuzioni di nodi aggiuntivi

Se la rete è costituita da più controller wireless, è possibile installare nodi CMX aggiuntivi e creare un mapping 1-1 tra più WLC e CMX. Non sono previsti requisiti speciali per la versione WLC. Accertarsi di non aggiungere un singolo WLC a più nodi CMX contemporaneamente.



DNA Spaces - Offload del lavoro nel cloud

La nuova piattaforma cloud di Cisco, DNA Spaces, mira a spostare il monitoraggio dei client nel cloud. Le risorse vengono allocate automaticamente in base al carico corrente. È possibile connettere la rete wireless al cloud in diversi modi:

1. Connessione diretta del WLC al cloud
2. DNA Spaces Connector (una piccola VM che funge da proxy, i controller non sono esposti al cloud)
3. Utilizzo di CMX come gateway per il cloud (questa opzione è necessaria per le distribuzioni HyperLocation)

Bug rilevanti

- [CSCvq25953](#) - L'attivazione del filtro SSID percorso disabilita l'esclusione degli MAC amministrati localmente e viceversa