CMX-Standortbeschränkungen und Hardwareanforderungen

Inhalt

Einführung

In diesem Artikel werden die Hardware-Anforderungen von Cisco CMX Location, die Softwarebeschränkungen und die möglichen Folgen einer Überschreitung beschrieben. Alle in diesem Artikel beschriebenen Befehle, Anforderungen und Einschränkungen gelten für CMX 10.5 und höher, die entweder auf VMware ESXi (vSphere) oder auf einer physischen Appliance wie MSE 3365/3375 ausgeführt werden. Wenn Sie noch CMX 10.4 oder niedriger ausführen, sollten Sie ein Upgrade in Betracht ziehen.

Verwendete Komponenten

Alle in diesem Artikel beschriebenen Beispiele und Befehle wurden auf einem Cisco 3504 WLC mit 8.8.120-Image und CMX 10.6.1-47 auf der physischen MSE 3375-Appliance ausgeführt.

Hardware-Anforderungen für Knoten mit niedriger, standardmäßiger und hoher Auflösung

Je nach verfügbarer Ressourcenmenge kann der bereitgestellte CMX-Knoten entweder Low-End, Standard oder High-End sein. CMX, das auf der MSE 3365- und 3375-Appliance ausgeführt wird, ist standardmäßig High-End.

In Tabelle 1 werden die Hardwareanforderungen (CPU/RAM/Disk) für alle drei Knotentypen aufgeführt.

Hardware-Anforderungen	Low-End	Standard	High-End
CPU-Kerne	8 vCPUs/4 physische Kerne	16 vCPUs/8 physische Kerne	20 vCPUs/10 physisc Kerne
Min. CPU-Basisfrequenz	2,3 GHz	2,3 GHz	2,3 GHz
RAM	24 GB	48 GB	64 GB
Speicher	550 GB	550 GB	1 TB
Speichertyp	SSD- oder SAS-HDD	SSD- oder SAS-HDD	SSD- oder SAS-HDD

Tabelle 1: CMX-Hardwareanforderungen

Hardwarespezifikationen für MSE 3365 und MSE 3375

Sowohl die MSE 3365- als auch die MSE 3375-Appliances verfügen über genügend Ressourcen für die Bereitstellung des High-End-CMX-Knotens. Die Hardwarespezifikationen der Kunden sind in der folgenden Tabelle aufgeführt:

Hardwarespezifikationen	MSE 3375	MSE 3375
CPU	Intel E5-2650 v3 mit 10 Kernen bei 2,4 GHz	Intel Xeon 5118 mit 12 Kernen 2,4 GHz
Speicher	4 x 600-GB-SAS-HDD	2 SATA-SSD mit 960 GB
Formfaktor	1 HE	1 HE

Tabelle 2: Hardwarespezifikationen der MSE-Appliance

CMX-Einschränkungen

Die Datenmenge, die der CMX-Standort verarbeiten kann, hängt von der Knotengröße ab. Softwareeinschränkungen für Knoten mit niedrigen, standardmäßigen und hohen Bandbreiten finden Sie in der folgenden Tabelle:

Einschränkungen	Low-End	Standard	High-End
Max. APs	2.000	5.000	10.000
Maximale Anzahl von eindeutigen MAC-Adressen pro Tag (mit oder ohne Hyperlocation)	25.000	50.000	90.000
Hyperlocation-Unterstützung	Nein	Nein	Ja
Maximale Anzahl eindeutiger aktiver Clients (mit aktivierter Hyperlocation)	X	X	9.000
Maximale Anzahl eindeutiger MAC-Adressen pro Monat (siehe Hinweis unten)	400.000	400.000	400.000
Max. Zonen	150	600	900
Max. Zuordnungspunkte	200	750	1000
Max. Anzahl von API-V3-Anfragen am MAC-Standort pro Sekunde	1	10	60

Max. Anzahl von NMSP-Nachrichten pro Sekunde	750	1300	2500
Max. Northbound-Benachrichtigungen pro Sekunde	10	50	300
Maximale Anzahl an CMX Connect-Verbindungen pro Sekunde	10	10	10

Tabelle 3: CMX-Standortbeschränkungen

Hinweis: Wenn die Anzahl der eindeutigen MAC-Adressen innerhalb eines Monats 400.000 überschreitet, kann CMX nicht mehr zwischen neuen und zurückkehrenden Besuchern unterscheiden. Andere Standorte werden weiterhin funktionieren.

Folgen unzureichender Ressourcen und Überschreitung der Grenzen

Überschreiten der in Tabelle 3 genannten Einschränkungen kann schwerwiegende Folgen für Ihren CMX-Knoten haben. Bevor Sie mit der Installation eines CMX-Knotens fortfahren, prüfen Sie, wie groß die Bereitstellung ist, und entscheiden Sie, welche Bereitstellungsgröße Ihren Anforderungen entspricht. Wenn die Bereitstellungsgröße selbst für mehrere CMX-Knoten einfach zu groß ist, sollten Sie in Betracht ziehen, zu DNA Spaces zu wechseln, der neuen Cloud-basierten Analyseplattform von Cisco, die CMX bald ersetzen wird. Bei DNA Spaces werden alle Berechnungen in Cloud-Infrastrukturen ausgelagert, wo Ressourcen basierend auf der Last dynamisch zugewiesen werden.

Alle Symptome und vorgeschlagenen Problemumgehungen basieren auf den bisherigen Erfahrungen des TAC mit Bereitstellungen, die von einem Low-End-Knoten bis hin zu mehreren High-End-Knoten für Hunderte von Standorten reichen.

Über 400.000 eindeutige MAC-Adressen pro Monat

Symptome:

- CMX kann nicht mehr zwischen neuen und zurückkehrenden Besuchern unterscheiden. Andere Standortdienste funktionieren weiterhin

Problemumgehungen:

- Deaktivierung der Nachverfolgung von Clients
- Wenn das Netzwerk aus mehreren Controllern besteht und ein High-End-Knoten nicht ausreicht, sollten Sie die Last von mehreren Controllern auf mehrere CMX-Knoten aufteilen.
- Wenn ein High-End für einen einzelnen Controller nicht ausreicht, sollten Sie ein Upgrade von WLC auf Version 8.8.x oder höher sowie die Aktivierung einer speziellen CMX-Gruppierungsfunktion in Erwägung ziehen, die es einem WLC ermöglicht, Daten gleichzeitig auf mehrere CMXs zu entlasten.
- Erwägen Sie die Umstellung auf DNA Space, einen Cloud-basierten Analyseservice, der CMX ersetzen wird.

Überschreiten der maximalen Anzahl an eindeutigen täglichen MAC-Adressen

Symptome:

- Sehr langsame Webschnittstelle
- Hohe CPU- und Arbeitsspeichernutzung
- Verlust von Analysedaten
- CMX-Services stürzen ab oder können nicht starten
- Potenziell nicht behebbare Datenbeschädigungen, die eine Neuinstallation erfordern
- Mögliche nicht wiederherstellbare Datenbeschädigung

Problemumgehungen:

- Deaktivieren der Nachverfolgung von Clients mindestens bis CMX wieder stabil ist
- Vergrößern Sie den CMX-Knoten (Low-End -> Standard -> High-End) oder die Bereitstellung zusätzlicher CMX-Knoten, um die Last neu zu verteilen.
- Erwägen Sie die Umstellung auf DNA Space, einen Cloud-basierten Analyseservice, der CMX ersetzen wird. Alle Workloads werden in die Cloud-Infrastruktur ausgelagert.
- Wenn einem CMX mehrere Controller hinzugefügt werden, entfernen Sie alle Controller, und versuchen Sie, sie einzeln erneut hinzuzufügen.

Anzahl der Kartenelemente überschreiten

Symptome:

- Langsame Webschnittstelle, insbesondere Registerkarte "Erkennen und Suchen"
- CMX-Services stürzen ab
- Verlust von Analysedaten

Problemumgehungen:

- Vergrößern Sie den CMX-Knoten (Low-End -> Standard -> High-End) oder Bereitstellung zusätzlicher Knoten.
- Entfernen einiger Kartenelemente

Überschreiten der Anzahl von NMSP-Nachrichten pro Sekunde

Dieser Fehler tritt in der Regel auf, wenn eine große Anzahl von Controllern einem einzelnen CMX-Knoten hinzugefügt wird.

Symptome:

- Langsame Weboberfläche
- Verlust von Analysedaten
- Hohe CPU- und Arbeitsspeichernutzung
- CMX-Services stürzen ab oder können nicht starten
- Fehlermeldungen innerhalb von analyticsserver.log im technischen Support-Protokollpaket mit folgenden Worten:
  ```
  Notification queue is full  - incoming notifications are being rejected. Please increase
  more processing capacity
  ```

Problemumgehungen:

- Bereitstellung zusätzlicher CMX-Knoten zur Lastverteilung
- Erwägen Sie die Migration zu einem neuen DNA-Space, einem Cloud-basierten Analyseservice, der CMX ersetzen wird. Alle Workloads werden in die Cloud-Infrastruktur ausgelagert.

Überschreiten der Anzahl von Northbound-Benachrichtigungen pro Sekunde

Symptome:

- Benachrichtigung wird verworfen, was zu ungenauen/unvollständigen Daten auf dem Rechner führt, an den die Benachrichtigungen gesendet werden

Problemumgehungen:

- Entfernen Sie einige der konfigurierten Benachrichtigungen.
- Vergrößern Sie den CMX-Knoten (Low-End -> Standard -> High-End) oder Bereitstellung zusätzlicher Knoten.

Analyse der MAC-Randomisierung und Nachverfolgung von Testclients

MAC-Randomisierung

Bevor Wireless-Geräte eine Verbindung zum Wireless-Netzwerk herstellen, müssen sie zunächst eine Anfrage senden. Das Gerät kann entweder nach einer bestimmten SSID suchen, mit der es zuvor verbunden war, oder eine "allgemeine" Anfrage senden, die auch Wildcard genannt wird. Jedes Wireless-Gerät, das auf Anfragen hört, kann eine eingehende Anfrage "hören", die Anwesenheit eines Geräts feststellen und, falls möglich, den Gerätestandort mit einer Genauigkeit von bis zu mehreren Metern aufzeichnen.

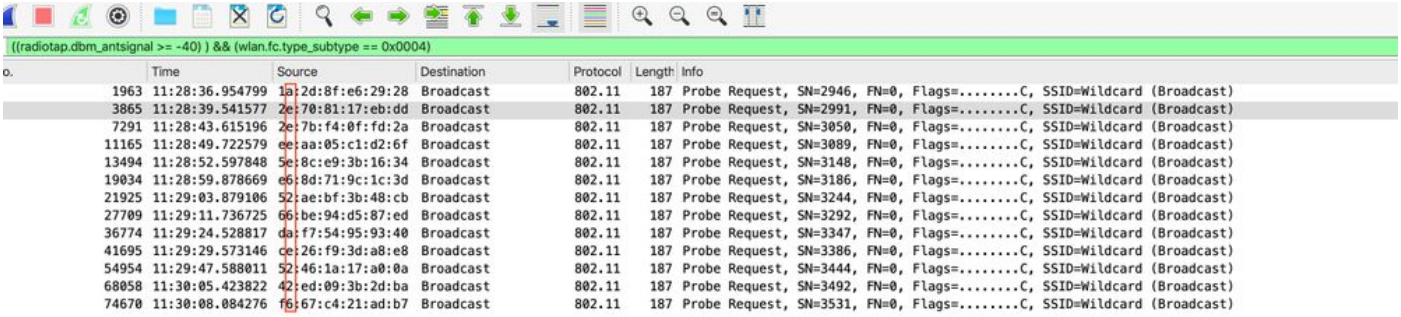
Aufgrund wachsender Datenschutzbedenken, beginnend mit der IOS 8-Version im Jahr 2014, haben Smartphone-Hersteller damit begonnen, eine Funktion namens MAC-Randomisierung zu implementieren, bei der Geräte bei jedem Senden einer Anfrage eine neue zufällig generierte MAC-Adresse verwenden. Beim Generieren einer zufälligen MAC-Adresse, die zum Senden von Anfragen verwendet wird, können Hersteller universelle oder lokal verwaltete MAC-Adressen verwenden.

Lokal verwaltete MAC-Adressen weisen den am wenigsten signifikanten Teil des ersten Oktetts der Adresse auf 1. Dieses Bit fungiert als Flag, das ankündigt, dass die MAC-Adresse tatsächlich eine zufällig generierte Adresse ist. Es gibt vier mögliche Formate von lokal verwalteten MAC-Adressen (x kann ein beliebiger Hexadezimalwert sein).

- x2-xx-xx-xx-xx-xx
- x6-xx-xx-xx-xx-xx
- xA-xx-xx-xx-xx-xx-xx
- xE-xx-xx-xx-xx-xx

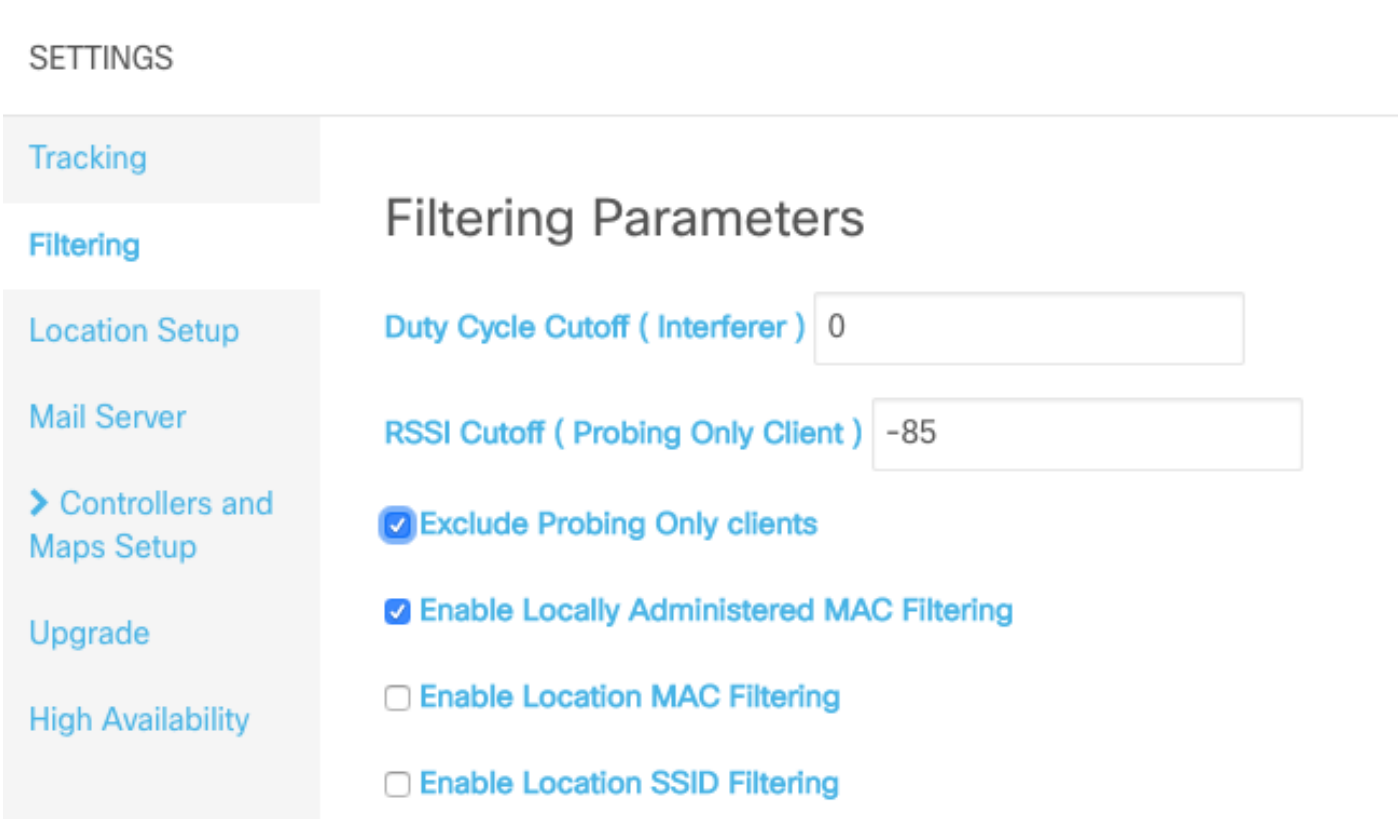
Alle anderen MAC-Adressen werden als universell verwaltet angesehen. Die ersten drei Oktette universell verwalteter MAC-Adressen werden als Organizational Unique Identifier (OUI) bezeichnet und sind herstellerspezifisch. Jeder Hersteller hat mehrere eindeutige OUIs zugewiesen.

Einige Hersteller wie Apple verwenden lokal verwaltete MAC-Adressen für ihre Untersuchungen. Nachfolgend finden Sie den Screenshot der Over-the-Air-Paketerfassung von iPhones, auf denen IOS 12.3 gesendet wird. Testanfragen werden alle paar Sekunden gesendet, wenn der Bildschirm des Geräts eingeschaltet ist, und alle paar Minuten, wenn der Bildschirm des Geräts deaktiviert ist. Wir können sehen, dass lokal verwaltetes Bit auf 1 festgelegt ist. Die MAC-Randomisierung findet nur statt, wenn das iPhone keiner SSID zugeordnet ist. Wenn sie zugeordnet wird, wird sie weniger häufig nachforschen und auch die MAC-Adresse verwenden, mit der sie verknüpft ist, um zu sondieren.



CMX und Nachverfolgung von Clients

CMX kann die Suche nach Wireless-Clients verfolgen. Diese Option ist standardmäßig aktiviert. Um Clients auszuschließen, die lokal verwaltete MAC-Adressen verwenden, muss die Option unter System->Settings->Filtering->Enable Locally Administered MAC Filtering aktiviert sein. Dieses Feld ist in CMX 10.5.x vorhanden, wurde jedoch aus der Webschnittstelle 10.6.x entfernt und ist standardmäßig aktiviert.



Einige Hersteller entscheiden sich, beim Testen keine lokal verwalteten Adressen zu verwenden. CMX kann nicht zwischen zufälligen, nicht lokal verwalteten MAC-Adressen und tatsächlichen MAC-Adressen des Geräts unterscheiden.

Das bedeutet, dass ein solches Client-Gerät jedes Mal als neuer Client aufgezeichnet werden

kann, wenn es eine neue Anfrage sendet. In einem Zeitraum von 1 Minute wird ein durchschnittliches Smartphone etwa das 8-fache der Testergebnisse ermitteln. In CMX wird dieses Gerät als 8 verschiedene Clients aufgezeichnet. Dadurch werden die CMX-Analysen vollständig verzerrt und manchmal fast unbrauchbare Analysedaten erzeugt.

Bei der Verbindung mit dem Wireless-Netzwerk verwenden die Geräte ihre tatsächliche MAC-Adresse. Die Anzahl der zugeordneten Clients ist immer niedriger als die Anzahl der Testkunden, aber die Daten werden fast 100 % genau sein. Zusätzliche Tests des Cisco TAC zeigen, dass Windows 10-Computer mit aktivierter "MAC Randomization"-Funktion auch lokal verwaltete MAC-Adressen verwenden, wenn sie eine Verbindung zum Netzwerk herstellen. Dies bedeutet, dass sie niemals von CMX aufgezeichnet werden, auch nicht, wenn sie mit dem Netzwerk verbunden sind.

Aus allen oben genannten Gründen sollte die Nachverfolgung von Kunden nicht dazu verwendet werden, die Anzahl der Besucher zu zählen. Sie kann jedoch verwendet werden, um die täglichen Trends zu verfolgen (z. B. wenn Mittwoch häufiger als Dienstag ist), aber auch diese Daten können aufgrund extrem hoher Abweichungen ungenau sein. Das Cisco TAC befasst sich häufig mit Problemen bei größeren Bereitstellungen (Flughäfen, Einkaufszentren, offene öffentliche Bereiche), bei denen die Nachverfolgung von Clients eine extrem große Anzahl eindeutiger MAC-Adressen pro Tag mit sich bringt, die selbst High-End-CMX-Knoten nicht bewältigen können (über 90.000 pro Tag). Durch die Nachverfolgung nur verbundener Clients werden diese Nummern verringert, die gesammelten Analysedaten werden jedoch genau erfasst.

Das Cisco TAC empfiehlt nachdrücklich, die Nachverfolgung von Clients zu deaktivieren.

Relevante Bugs

- CSCvq25953 - Durch die Aktivierung der Standort-SSID-Filterung wird der Ausschluss lokal verwalteter MACs und umgekehrt deaktiviert.
- CSCvo43574 - Cmxos vergewissern sich, dass der Befehl bezüglich der Mindestvoraussetzungen für die Festplatte falsch ist.