Verifica delle limitazioni di posizione CMX e dei requisiti hardware

Sommario

Introduzione

In questo documento vengono descritti i requisiti hardware di Connected Mobile Experience (CMX) Location, le limitazioni software e le potenziali conseguenze in caso di superamento.

Componenti usati

- Controller LAN wireless (WLC) 3504 con immagine versione 8.8.120
- CMX 10.6.1-47 installato sull'appliance fisica MSE 3375

Tutti i comandi, i requisiti e le limitazioni descritti in questo articolo sono applicabili a CMX 10.5 e versioni successive eseguito su VMware ESXi (vSphere) o su un dispositivo fisico Mobility Service Engine (MSE) 3365/3375.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Requisiti hardware per i nodi low, standard e high-end

In base alla quantità di risorse disponibili, il nodo CMX distribuito può essere di tipo low-end, standard o high-end. CMX eseguito su MSE 3365 e 3375 è un dispositivo high-end per impostazione predefinita.

La tabella 1 mostra i requisiti hardware (processore (CPU) / memoria (RAM) / disco) per tutti e tre i tipi di nodi.

Requisiti hardware	Di fascia bassa	Standard	High-end
Core CPU	8 vCPU / 4 core fisici	16 vCPU / 8 core fisici	20 vCPU / 10 core fis
Frequenza base minima CPU	2,3 GHz	2,3 GHz	2,3 GHz
RAM	24 GB	48 GB	64 GB
Storage	550 GB	550 GB	1 TB
Tipo di archiviazione	Unità a stato solido o disco rigido SAS	Unità a stato solido o disco rigido SAS	Unità a stato solido o rigido SAS

Tabella 1. Requisiti hardware CMX

Specifiche hardware di MSE 3365 e MSE 3375

Entrambi gli accessori MSE 3365 e 3375 dispongono di risorse sufficienti per l'installazione del nodo CMX high-end. Le specifiche hardware sono riportate nella Tabella 2.

Specifiche hardware	MSE 3375	MSE 3375
CPU	Intel E5-2650 v3 a 10 core a 2,4 GHz	Processore Intel Xeon Gold 51 12 core a 2,4 GHz
Storage	4 dischi rigidi SAS da 600 GB	2 SSD SATA da 960 GB
Fattore di forma	1U	1U

Tabella 2. Specifiche hardware dell'accessorio MSE

Limitazioni di CMX

La quantità di dati che la posizione CMX è in grado di gestire dipende dalle dimensioni del nodo. Le limitazioni software dei nodi Low, Standard e High-end sono riportate nella Tabella 3:

Limitazioni	Di fascia bassa	Standard	High-end
Numero massimo di punti di accesso	2,000	5,000	10,000
Numero massimo di indirizzi MAC univoci rilevati al giorno (con o senza iperposizione)	25,000	50,000	90,000
Supporto di iperlocazioni	No	No	Sì
Numero massimo di client attivi univoci (con Hyperlocation abilitato)	X	X	9,000
Numero massimo di indirizzi MAC univoci per mese (vedere nota*)	400,000	400,000	400,000
Numero massimo di zone	150	600	900
Numero massimo di elementi mappa	200	750	1000
Numero massimo di richieste API V3 di	1	10	60

posizione MAC al secondo			
Numero massimo di messaggi NMSP al secondo	750	1300	2500
Numero massimo di notifiche in direzione nord al secondo	10	50	300
Numero massimo di ricevitori di notifiche in direzione nord	5	5	5
Numero massimo di connessioni CMX Connect al secondo	10	10	10

Tabella 3. Limitazioni della posizione CMX

Nota: Quando il numero di indirizzi MAC univoci supera i 400.000 in un mese, CMX non è in grado di distinguere tra nuovi e visitatori che ritornano. Altri servizi continuano a funzionare se non vengono superate altre limitazioni.

Conseguenze dell'insufficienza delle risorse e del superamento dei limiti

Se si superano i limiti indicati nella tabella 3, si possono verificare conseguenze fatali sul nodo CMX. Prima di installare un nodo CMX, valutare le dimensioni della distribuzione e decidere le dimensioni di distribuzione adatte alle proprie esigenze.

Se le dimensioni dell'installazione sono semplicemente troppo grandi anche per diversi nodi CMX, prendiamo in considerazione il passaggio a DNA Spaces, la nuova piattaforma di analisi basata su cloud di Cisco disponibile per sostituire CMX. Con DNA Spaces, tutti i calcoli vengono scaricati sull'infrastruttura cloud in cui le risorse vengono allocate dinamicamente in base al carico.

Tutti i sintomi e le soluzioni proposte di seguito si basano sull'esperienza precedente del Technical Assistance Center (TAC) con installazioni che vanno da singoli nodi di fascia bassa a più nodi di fascia alta che coprono centinaia di sedi.

Per ulteriori informazioni su come gestire il sovraccarico di CMX, consultare il documento: https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/214894-optimize-cmx-performance.html

Oltre 400.000 indirizzi MAC univoci al mese

Sintomi:

- CMX si ferma per poter distinguere tra nuovi visitatori e visitatori che ritornano. Altri servizi di posizione continuano a funzionare a meno che non vengano superate altre limitazioni

Soluzioni:

- Disabilita il rilevamento dei client di prova

- Se la rete è costituita da più controller e un nodo high-end non è sufficiente, considerare la suddivisione del carico da più controller a più nodi CMX
- Se un high-end non è sufficiente per un singolo controller, considerare l'aggiornamento di WLC alla versione 8.8 o successive e l'utilizzo di una speciale funzione di raggruppamento CMX che consente a un singolo WLC di scaricare parti dei dati su più nodi CMX
- Si consideri la migrazione a DNA Spaces, un servizio di analisi basato su cloud che sostituisce CMX. Tutto il carico di lavoro viene scaricato sull'infrastruttura cloud scalabile in modo dinamico

Superamento della quantità massima di indirizzi MAC univoci giornalieri

Sintomi:

- Interfaccia Web molto lenta o interrotta
- Utilizzo elevato di CPU e memoria
- Perdita di dati di analisi
- Servizi CMX bloccati o non avviabili
- Danneggiamento dei dati potenzialmente irreversibile che richiede la reinstallazione
- Messaggi di errore all'interno di **locationserver.log** in del bundle del log di supporto tecnico con il seguente messaggio:
  `Cleaning up element counts, unique devices 347684, locally administered macs 0 as partof daily midnight job`

Soluzioni:

- Interrompere la traccia di probe dei client almeno fino a quando CMX non ritorna stabile
- Aumentare le dimensioni del nodo CMX (low-end -> standard -> high-end) o implementare nodi CMX aggiuntivi per ridistribuire il carico
- Si consideri la migrazione a DNA Spaces, un servizio di analisi basato su cloud che sostituisce CMX. Tutto il carico di lavoro viene scaricato sull'infrastruttura cloud scalabile in modo dinamico
- Se si aggiungono più controller a un unico CMX, rimuoverli tutti e tentare di aggiungerli di nuovo uno alla volta ogni giorno mentre si controlla il numero totale giornaliero di dispositivi

Numero di elementi mappa superiore

Sintomi:

- Interfaccia Web lenta, in particolare la scheda Rileva e individua
- Servizi CMX in caso di arresto anomalo
- Perdita di dati di analisi

Soluzioni:

- Aumentare le dimensioni del nodo CMX (low-end -> standard -> high-end) o installare nodi CMX aggiuntivi
- Rimuovere alcuni elementi della mappa

Numero di messaggi NMSP superato al secondo

Questo problema si verifica in genere quando una grande quantità di controller con carico elevato viene aggiunta a un singolo nodo CMX.

Sintomi:

- Interfaccia Web lenta
- Perdita di dati di analisi
- Utilizzo elevato di CPU e memoria
- Servizi CMX bloccati o non avviabili
- Messaggi di errore all'interno di **analyticsserver.log** in del bundle del log di supporto tecnico con il seguente messaggio:
  ```
  Notification queue is full  - incoming notifications are being rejected. Please increase
  more processing capacity
  ```

Soluzioni:

- Distribuzione di nodi CMX aggiuntivi per suddividere il carico
- Si consideri la migrazione a DNA Spaces, un servizio di analisi basato su cloud che sostituisce CMX. Tutto il carico di lavoro viene scaricato sull'infrastruttura cloud scalabile in modo dinamico

Numero massimo di notifiche Northbound al secondo

Questo problema si verifica in genere quando CMX è configurato per l'invio di notifiche a un numero elevato di server. CMX 10.6.3 ha introdotto un limite di 5 ricevitori di notifiche in direzione nord

Sintomi:

- Le notifiche non vengono elaborate e i dati sul server che le riceve risultano inesatti o incompleti

Soluzioni:

- Rimuovere alcuni dei ricevitori di notifica configurati
- Aumento delle dimensioni del nodo CMX (low-end -> standard -> high-end) o installazione di nodi aggiuntivi

Randomizzazione e tracking MAC dei client di prova

Randomizzazione MAC

Prima dell'associazione alla rete wireless, i dispositivi wireless devono inviare una richiesta di verifica. Il dispositivo può eseguire il probe di un SSID specifico a cui è stato associato in precedenza oppure inviare una richiesta di probe "generale", nota anche come carattere jolly.

Qualsiasi dispositivo wireless in ascolto di richieste di sonda può "ascoltare" una sonda, annotare la presenza del dispositivo e, se possibile, registrare la posizione dei dispositivi con una precisione fino a diversi metri.

A causa dell'aumento dei problemi di privacy, con il rilascio di Cisco IOS 8 nel 2014, i produttori di

smartphone hanno iniziato a implementare una funzione chiamata randomizzazione MAC dove i dispositivi userebbero un nuovo indirizzo MAC generato casualmente ogni volta che inviano una richiesta di sonda.

Quando generano un indirizzo mac casuale che viene utilizzato per inviare le richieste di richieste di richieste, i produttori possono utilizzare indirizzi mac amministrati universalmente o localmente.

Gli indirizzi MAC amministrati localmente hanno il secondo bit meno significativo del primo ottetto dell'indirizzo impostato su 1. Questo bit funge da flag che annuncia che l'indirizzo MAC è in realtà un indirizzo generato casualmente.

Esistono quattro possibili formati di indirizzi MAC amministrati localmente (x può essere qualsiasi valore esadecimale)

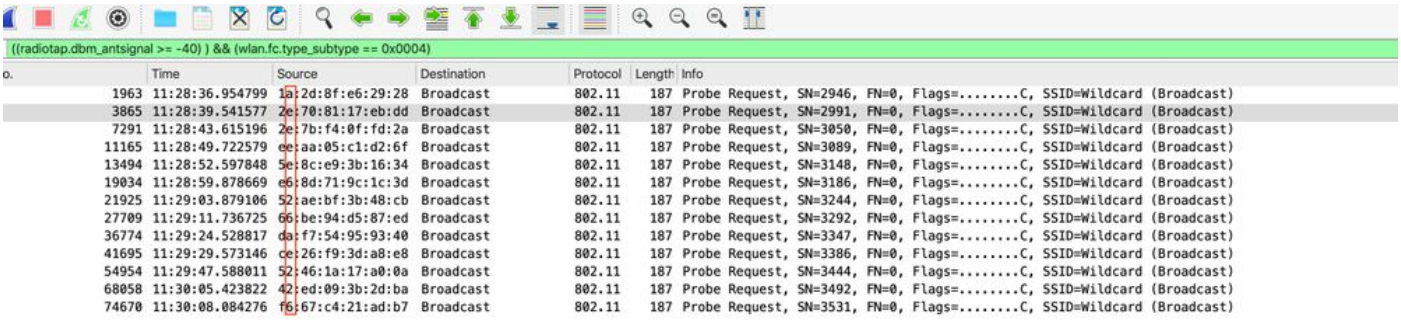
- x2-xx-xx-xx-xx-xx
- x6-xx-xx-xx-xx-xx
- xA-xx-xx-xx-xx-xx
- xE-xx-xx-xx-xx-xx

Tutti gli altri indirizzi MAC sono considerati amministrati universalmente. I primi 3 ottetti di indirizzi MAC amministrati universalmente sono chiamati identificatori univoci dell'organizzazione (OUI, Organizationally Unique Identifier) e sono specifici del produttore.

Ogni produttore ha assegnato un certo numero di OUI univoci.

Nelle riprese over-the-air di un iPhone con IOS 12.3, che invia richieste di sonda, vediamo che le richieste di sonda vengono inviate ogni pochi secondi se lo schermo del dispositivo è acceso, e ogni due minuti se lo schermo del dispositivo è spento.

È possibile notare che il bit amministrato localmente è impostato su 1. Con il rilascio di IOS 14 e Android 10, l'indirizzo mac randomizzato viene utilizzato anche quando il dispositivo si associa alla rete. I dispositivi utilizzano in genere un unico indirizzo MAC amministrato localmente e casuale per SSID.


((radiotap.dbm_antsignal >= -40)) && (wlan.fc.type_subtype == 0x0004)

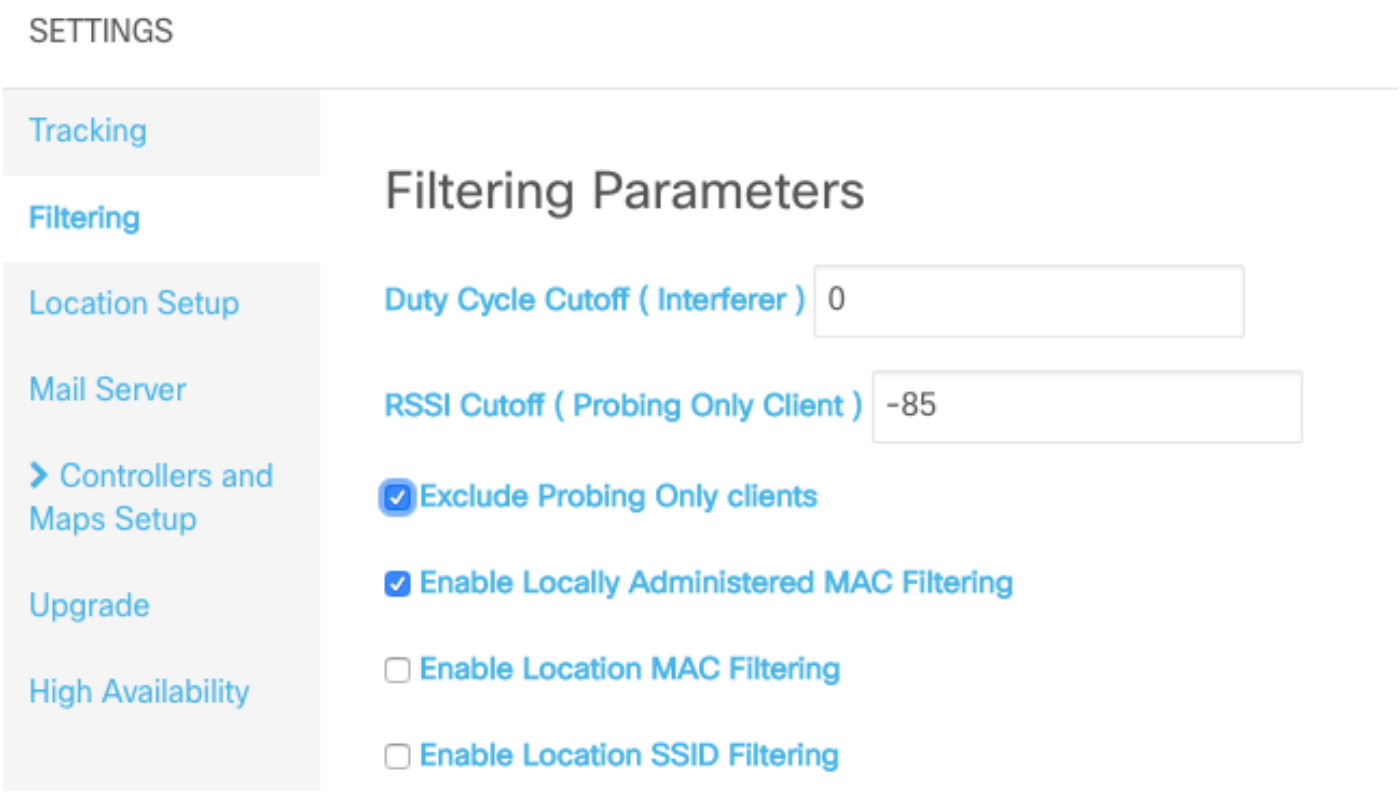
o.	Time	Source	Destination	Protocol	Length	Info
1963	11:28:36.954799	1a:2d:8f:e6:29:28	Broadcast	802.11	187	Probe Request, SN=2946, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
3865	11:28:39.541577	2e:70:81:17:eb:dd	Broadcast	802.11	187	Probe Request, SN=2991, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
7291	11:28:43.615196	2e:7b:f4:0f:fd:2a	Broadcast	802.11	187	Probe Request, SN=3050, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
11165	11:28:49.722579	ee:aa:05:c1:d2:6f	Broadcast	802.11	187	Probe Request, SN=3089, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
13494	11:28:52.597848	5e:8c:e9:3b:16:34	Broadcast	802.11	187	Probe Request, SN=3148, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
19034	11:28:59.878669	e6:8d:71:9c:1c:3d	Broadcast	802.11	187	Probe Request, SN=3186, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
21925	11:29:03.879106	52:ae:bf:3b:48:cb	Broadcast	802.11	187	Probe Request, SN=3244, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
27709	11:29:11.736725	66:be:94:d5:87:ed	Broadcast	802.11	187	Probe Request, SN=3292, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
36774	11:29:24.528817	da:f7:54:95:93:40	Broadcast	802.11	187	Probe Request, SN=3347, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
41695	11:29:29.573146	ce:26:f9:3d:a8:e8	Broadcast	802.11	187	Probe Request, SN=3386, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
54954	11:29:47.588011	52:46:1a:17:a0:0a	Broadcast	802.11	187	Probe Request, SN=3444, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
68058	11:30:05.423822	42:ed:09:3b:2d:ba	Broadcast	802.11	187	Probe Request, SN=3492, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
74670	11:30:08.084276	f6:67:c4:21:ad:b7	Broadcast	802.11	187	Probe Request, SN=3531, FN=0, Flags=........C, SSID=Wildcard (Broadcast)

CMX E Tracciamento Dei Client Di Controllo

CMX consente di tenere traccia dei client che eseguono solo probe. Questa opzione è attivata per default.

Per escludere i client che utilizzano indirizzi MAC amministrati localmente, selezionare l'opzione "Abilita filtro MAC amministrato localmente" in **Sistema > Impostazioni > Filtro**.

Questo campo è presente in CMX 10.5.x, ma è stato rimosso dall'interfaccia Web 10.6.x ed è stato abilitato per impostazione predefinita.



Alcuni produttori decidono di non utilizzare gli indirizzi amministrati localmente quando eseguono le richieste. CMX non consente di distinguere tra indirizzi MAC casuali non amministrati localmente e indirizzi MAC reali del dispositivo. Ciò significa che un dispositivo client di questo tipo può essere registrato come nuovo client ogni volta che invia una nuova richiesta di probe. Mentre è in uso, in un periodo di 1 minuto uno smartphone medio sonda un paio di volte. Su CMX, tale dispositivo viene registrato ogni volta come più client diversi. In questo modo l'analisi CMX viene completamente alterata e talvolta i dati analitici risultano quasi inutilizzabili.

Quando vengono associati allo stesso SSID, i dispositivi utilizzano sempre un unico indirizzo MAC che non cambia mai (questo indirizzo può essere reale o amministrato localmente tramite MAC casuale). La quantità di client associati è sempre inferiore o uguale alla quantità di client che inviano solo richieste.

La traccia dei client che solo probe non dovrebbe essere utilizzata come contatore visitatori. Può tuttavia essere utilizzato per tenere traccia delle tendenze giornaliere (ad esempio, se mercoledì è più occupato di martedì), ma anche tali dati possono essere imprecisi a causa di variazioni estremamente elevate.

Cisco TAC spesso si occupa di problemi relativi a implementazioni di maggiori dimensioni (aeroporti, centri commerciali, aree pubbliche aperte), in cui la traccia dei client su cui si basano le richieste introduce un numero estremamente elevato di indirizzi MAC univoci al giorno, che anche i nodi CMX di fascia alta non sono in grado di gestire (oltre 90.000 al giorno).

Se si tiene traccia solo dei client associati, si riduce il numero totale di client registrati, ma i dati di analisi raccolti diventano accurati.

Cisco TAC consiglia di abilitare l'opzione "Escludi solo client di prova".

Bug rilevanti

- Cisco bug ID CSCvq25953 - L'abilitazione del filtro SSID percorso disabilita l'esclusione degli MAC amministrati localmente e viceversa
- ID bug Cisco CSCvo43574 - CMX esclude gli indirizzi MAC associati amministrati localmente
- ID bug Cisco CSCvs85182 - Il comando Cmxos verify non è corretto per i requisiti minimi del disco rigido