# Sostituzione dei server serie X con un dispositivo Cisco Meeting Server o una macchina virtuale

## Sommario



## Introduzione

In questo documento viene descritto come sostituire in modo sicuro e affidabile i server Acano serie X con i server Cisco Meeting Server (CMS) Virtual Machine (VM), CMS1000 o CMS2000. Il supporto per i server Acano serie X è stato eliminato dalla versione 3.0 in poi.  La versione più recente del software eseguibile su una serie X è la 2.9.5, supportata solo fino al 1 marzo 2022. Non saranno quindi più disponibili versioni di manutenzione o correzioni di bug.  Ciò significa che se si dispone di un server Acano serie X, è necessario pianificare la sostituzione prima di quel momento.

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione CMS
- Aggiornamenti CMS
- Creazione e firma di certificati

### Componenti usati

Per la stesura del documento, sono stati usati server Cisco Meeting Server (VM o CMS1K o CMS2K) e Acano serie X.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Quando si sostituiscono i server serie X, è necessario conoscere le capacità di chiamata dei vari

server. Per ulteriori informazioni sul dimensionamento, consultare le guide alla distribuzione di Cisco Meeting Server nell'Appendice C (https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html).

Dimensioni serie X come riferimento:

- X1 - 25 chiamate HD (720p)
- X2 - 125 chiamate HD (720p)
- X3 - 250 chiamate HD (720p)

Il processo di configurazione del server sostitutivo è descritto nella documentazione di installazione e non è descritto di seguito. Le guide all'installazione sono disponibili qui: https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-guides-list.html.

# Sostituzione dei server serie X con un accessorio CMS o una macchina virtuale

Il metodo supportato per sostituire i server serie X consiste nell'aggiungere la nuova periferica al cluster di database in modo che ottenga una copia del database.

> **Attenzione:** Non utilizzare un backup da un server serie X per implementare la sostituzione.

Non tutti i passaggi seguenti sono necessari per completare la sostituzione. Raggruppare i nuovi server con i server precedenti in modo che ottengano una copia del database è la parte più importante.

Una volta completato il processo di migrazione, tutte le informazioni del database (regole in entrata, regole in uscita, cospazi, ID chiamata e così via) si trovano anche sui nuovi server.

> **Nota:** I dati immessi nell'interfaccia utente grafica (GUI) in **Configurazione > Generale** e **Configurazione > Active Directory** NON si trovano nel database. È necessario spostare la configurazione del protocollo LDAP (Lightweight Directory Access Protocol) dalla GUI all'API (Application Programming Interface). Se non si è ancora pronti per eseguire questa operazione, copiare tutti i dati da queste due pagine in modo che possano essere reimmessi sui nuovi server. Tenere presente che la password per il nome utente LDAP è obbligatoria anche per LDAP, in quanto non è possibile copiare tali informazioni.

Viene innanzitutto visualizzata una descrizione di alto livello del flusso di lavoro, seguita da istruzioni dettagliate. Si consiglia di seguire le istruzioni dettagliate per la procedura di sostituzione.

## Descrizione dettagliata del lavoro

Passaggio 1. Creare i file di backup dai vecchi server Acano serie X.

Passaggio 2. Scaricare il file di backup e il file logbundle.tar.gz dai vecchi server qualora siano necessarie informazioni per configurare il processore di gestione della scheda madre (MMP) del

nuovo server.

Passaggio 3. Sul vecchio server serie X, accedere a MMP e ottenere l'output di ciascun servizio/configurazione e copiare le informazioni in un file di nota.

Passaggio 4. Configurare nuovi server.

Passaggio 5. Ottenere le licenze sui nuovi server.

Passaggio 6. Copiare i certificati dai server precedenti ai nuovi server.

Passaggio 7. Abilitare i servizi MMP nei nuovi server configurati nel server precedente. (Acano serie X può utilizzare un'interfaccia di amministrazione dedicata per la gestione. È necessario gestire il nuovo server tramite l'interfaccia A-D, ma tutti i servizi sul nuovo server possono trovarsi sull'interfaccia A.)

Passaggio 8. Creare gli stessi account utente nei nuovi server utilizzati nei server precedenti.

Passaggio 9. Copiare il database nei nuovi server.

Passaggio 10. Rimuovere la serie X dal cluster di database.

Passaggio 11. Arrestare il server serie X sostituito dal nuovo server.

Passaggio 12. Modificare l'indirizzo IP sul nuovo dispositivo in modo che corrisponda all'indirizzo IP dell'interfaccia A della serie X precedente da sostituire.  Se si utilizzano più interfacce sulla serie X, è necessario utilizzarle anche sui nuovi server, in quanto ciò elimina la necessità di modificare qualsiasi record DNS.

Passaggio 13. Aggiungere nuovamente il server al cluster di database (solo se la distribuzione originale non era un singolo server combinato).

Passaggio 14. Regolare di conseguenza i limiti di carico sui nuovi server in API - api/v1/system/configuration/cluster.

Passaggio 15. Testare la distribuzione per verificare che funzioni ancora.

## Istruzioni dettagliate

Passaggio 1. Creare un backup utilizzando il comando MMP **backup snapshot <nome_file_specifico_server>**.

Passaggio 2. Scaricare il file di backup e un file logbundle.tar.gz (https://video.cisco.com/video/5810051601001) da ciascuno dei server serie X da sostituire.

Passaggio 3. Eseguire i comandi seguenti sui server serie X per ottenere la configurazione dei vari servizi e inserirli in un file di nota. In questo modo viene fornito un riferimento semplice su come riconfigurare i nuovi server.

**'webadmin', 'callbridge', 'webbridge', 'xmpp', 'turn', 'dns', 'elenco server ntp', 'tls sip', 'tls ldap', 'tls dtls', 'tls webadmin', 'stato cluster di database', 'elenco utenti', 'ipv4 a', 'ipv4 b', 'ipv4 c', 'ipv4 d', 'ipv4 admin', 'registratore', 'streamer', 'uploader', 'dscp', 'sipedge', 'h33 3_gateway', 'syslog', 'ldap'**

**Nota:** H323_gateway, Sip Edge e XMPP sono obsoleti in CMS 3.0.

Se si utilizza SIP Edge, è necessario disporre di un Cisco Expressway-C ed E per instradare il traffico da e verso Internet.
Se si utilizza il gateway H323, è necessario configurarlo utilizzando un server Cisco Expressway per eseguire l'interoperabilità H.323-SIP.
Se si utilizza XMPP, dopo l'aggiornamento a CMS 3.x sarà necessario apportare alcune modifiche alla configurazione. Tuttavia, se si sta per sostituire la serie X e rimanere sulla versione 2.9.x per un certo periodo di tempo e si desidera utilizzare WebRTC, registratore o streamer, è necessario riconfigurare XMPP sul nuovo server.

In questo documento è possibile leggere ulteriori informazioni sulle modifiche di cui tenere conto prima di eseguire l'aggiornamento a CMS 3.0.

Passaggio 4. Configurare i nuovi server. Assicurarsi che dispongano della stessa versione del codice dei server serie X. Assegnare ai server gli IP non utilizzati da utilizzare per il momento (**ipv4 <interfaccia> add <indirizzo>/<lunghezza prefisso> <gateway>**), ma al termine del lavoro, gli IP verranno modificati in base a quanto utilizzato sui sistemi serie X. In questo modo si evitano modifiche ai record e ai certificati DNS.  Se non si desidera riutilizzare gli IP precedenti, è necessario aggiornare il DNS e i certificati di conseguenza.

Passaggio 5. Nel nuovo server e nel protocollo MMP del vecchio server serie X, eseguire il comando **iface a** per ottenere l'indirizzo MAC delle interfacce A. Dalla serie X che sta per essere sostituita, scaricare il file cms.lic e aprire una richiesta di assistenza in TAC Licensing. Assegnare all'agente di gestione licenze l'indirizzo MAC dell'interfaccia del nuovo server e l'indirizzo MAC del server precedente e indicare che si desidera sostituire il server precedente con uno nuovo. Chiedere loro di scambiare le licenze dal vecchio MAC al nuovo MAC. Viene quindi fornito un nuovo file di licenza, che è necessario decomprimere, rinominare come cms.lic e caricare sul nuovo server.

Passaggio 6. Copiare i certificati, le chiavi e i file dell'Autorità di certificazione (CA) utilizzati nella vecchia serie X nei nuovi server che utilizzano WinSCP o qualsiasi altro programma SFTP.

Passaggio 7. Sul nuovo server, abilitare gli stessi servizi e le stesse impostazioni in MMP di quelli della vecchia serie X. Fare riferimento alle informazioni raccolte al punto 3 per assicurarsi di eseguire le stesse configurazioni di prima.

**Nota:** Se si intende eseguire l'aggiornamento a CMS 3.x subito dopo la configurazione di questi nuovi server, non è necessario configurare i componenti XMPP, Webbridge, SIP Edge o H323_gateway. Questi non vengono più utilizzati in CMS 3.x.

Passaggio 8. Creare gli stessi account utente presenti sui server serie X nel pannello di gestione usando il comando **user add <nomeutente> <ruolo>** (nonché la **regola utente <nome regola> <valore>** se sono state impostate delle regole). È possibile configurare altri dispositivi, quali Cisco Meeting Management (CMM), TelePresence Management Suite (TMS) o Cisco Unified Communications Manager (CUCM), per le funzionalità con questi account, in modo da poterli configurare sui nuovi server.

Passaggio 9. Caricare una copia del database nei nuovi server.

9 bis. Se la distribuzione corrente è un singolo server combinato (nessun cluster di database), è

necessario inizializzare un cluster di database in tale server. A partire dalla versione 2.7 di CMS, un cluster di database richiede certificati. Pertanto, a partire dalla versione 2.7 di CMS è stata introdotta un'Autorità di certificazione incorporata che è possibile utilizzare per firmare i certificati del database:

1. Sul singolo MP della serie X combinato, eseguire **pki selfsigned dbca CN:<Nome società>** (es. pki selfsigned dbca (CN:tplab.local)

2. Sul singolo MP della serie X combinato, creare un certificato per il server di database con **pki csr dbserver CN:xseries.example.com subjectAltName:<newcms1fqdn>**

A questo punto non è necessario disporre di record A DNS.

3. Sul singolo MMP serie X combinato, creare un certificato per il client del database con **pki csr dbclient CN:postgres**

4. Sul singolo MP della serie X combinato, utilizzare dbca (dal passaggio 1) per firmare il dbserver (dal passaggio 2) certificato **pki firma dbserver dbca**

5. Sul singolo MMP della serie X combinato, utilizzare dbca (dal passaggio 1) per firmare il dbclient (dal passaggio 3) certificato **pki firma dbclient dbca**

6. Copiare i file dbserver.crt, dbserver.key, dbclient.crt e dbclient.key in tutti i server che verranno aggiunti al database (nodi che costituiscono il cluster di database) dalla serie X ai nuovi server

7. Copiare il file dbca.crt su tutti i server della serie X

8. Sul singolo MMP serie X combinato, eseguire i **certificati cluster di database dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt** (dbca.crt come certificato CA radice)

9. Sul singolo MMP serie X combinato, eseguire il **cluster di database localnode a**

10. Sul modulo MMP della serie X combinato, eseguire il comando **database cluster initialize**

11. Eseguire lo **stato cluster** del **database** sul modulo MMP della serie X combinato. È necessario visualizzare:
Nodi: <XseriesIP> (me): Connected Primary

12. Nei nuovi server da aggiungere al cluster di database, da MP eseguire **i certificati cluster di database dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt**

13. Sui nuovi server ai quali si intende unire il computer (nel percorso condiviso con un database), da MP:

r. esegui **cluster di database localnode a**

b. esegui **database cluster join <IP nodo primario>**

A questo punto, i nuovi server dispongono di una copia del database. Eseguire **lo stato del cluster di database** in MMP sul nuovo server per assicurarsi che venga visualizzato come sincronizzato. In caso affermativo, si è terminato con il passaggio 9 e si può continuare con il passaggio 10. Tuttavia, se non sono sincronizzati, è necessario rivedere le configurazioni del cluster di database e verificare che nella rete non sia presente alcun elemento che bloccherebbe la comunicazione su

TCP 5432 tra i server.

9 ter. Se la distribuzione corrente è già un cluster di database, si desidera sostituire i server serie X uno alla volta. Nella serie X, eseguire in **stato cluster di database** MMP per verificare se il server è collegato al cluster di database o connesso. Se l'indirizzo IP del server è incluso nell'elenco dei cluster di database, viene aggiunto. In caso contrario, e l'ultimo comando visualizzato è 'database cluster connect', il nodo è connesso.

Se si desidera aggiungere nuovamente il nuovo nodo con lo stesso ruolo (unito o connesso), prendere nota del ruolo del server serie X. Se la serie X è il database primario, riavviare il server in modo che diventi una replica.

1. Nella serie X che sta per essere sostituita, annotare i certificati utilizzati per chiave server/certificato, chiave client/certificato e certificato CA

2. Sulla serie X che sta per essere sostituita, eseguire **database cluster remove**

Passaggio 10. Se si sostituisce un **singolo server serie X combinato**, continuare con il passaggio 10. Se si tratta di un cluster, andare al passaggio 11.

A questo punto, il nuovo server dispone di una copia del database. È possibile verificare questa condizione con un login all'interfaccia Web del nuovo server e controllare la configurazione di utenti e spazi. Dopo la conferma, rimuovere il nuovo server dal cluster di database e modificare gli indirizzi IP:

1. Sul nuovo server, eseguire '**database cluster remove**'.

2. Arrestare il server serie X.

3. Sostituire gli indirizzi IP del nuovo server con quelli utilizzati nel server serie X.

4. Riavviare il nuovo server.

5. Se si utilizza la versione CMS 2.9.x, provare il nuovo server per verificare che tutte le configurazioni funzionino correttamente.

6. Accedere alla pagina web admin del nuovo server e osservare gli spazi e gli utenti. È necessario visualizzare tutti gli spazi e gli utenti precedentemente presenti nel server quando si è eseguito il join al database, mentre ne è stata eseguita una copia.

Passaggio 11. Se si sostituisce un server serie X che fa parte di un cluster, è possibile eseguire la procedura seguente:

1. Chiudere il server serie X di cui si intende disattivare il sistema.

2. Sostituire gli indirizzi IP sul nuovo server con quelli utilizzati in precedenza sull'interfaccia del nodo locale del database del server serie X (in genere a).

3. Copiare la chiave/il certificato del server, la chiave/il certificato del client e il certificato della CA sul nuovo server con un programma SFTP.

4. Sul nuovo server, eseguire il comando: '**database cluster localnode a**'

5 bis. Se il nuovo nodo deve essere aggiunto al cluster di database, eseguire il comando '**database cluster certs <server.key> <server.crt> <client.key> <client.crt> <ca.crt>**'

5 ter. Se il nuovo nodo deve essere connesso (non nel percorso condiviso con un database) al cluster di database, eseguire il comando '**database cluster certs <client.key> <client.crt> <ca.crt>**'.

6 bis. Se è necessario unire il nuovo nodo (posizionato insieme a un database), eseguire il comando: '**join del cluster di database <IP nodo primario>**'

6 ter. Se è necessario connettere il nuovo nodo (non nel percorso condiviso con un database) eseguire il comando:'**database cluster connect <indirizzo IP nodo primario>**'

**Ripetere i passaggi 9b e 11 per ogni serie X di cui è necessario smantellare la macchina.**

Passaggio 12. A questo punto, i nuovi server CMS disporranno di una copia del database o, se connessi, sapranno come raggiungere i nodi del database e avranno gli stessi indirizzi IP di prima.

Passaggio 13. Il bilanciamento del carico è abilitato nella distribuzione?

Se si utilizza il bilanciamento del carico delle chiamate CMS con CallBridgeGroups sull'API impostata con Loadbalancing=True, è necessario modificare il limite di carico in modo che corrisponda ai limiti consigliati dei nuovi server nell'ambiente. Andare su **api/v1/system/configuration/cluster** e aggiornare il limite di caricamento di conseguenza:

| Sistema | Limite di carico consigliato |
|---|---|
| CMS1000 M5v2 | 120000 |
| CMS100 M4 o M5v1 | 96000 |
| CMS2000 M5v2 | 875000 |
| CMS2000 | 700000 |
| VM (numero vCPU x 1250) | esempio: 70 vCPU x 1250 = 87500 |

Passaggio 14. Se si dispone di un cluster XMPP prima di questa operazione e si intende rimanere in CMS 2.9.x per un determinato periodo di tempo, è necessario ricreare il cluster XMPP.

| Comandi MMP | Esempi |
|---|---|
| **Configurazione su tutti i nodi XMPP** | **Configurazione su tutti i nodi XMPP** |
| 1. reimpostazione xmpp | 1. reimpostazione xmpp |
| 2. xmpp domain <nome dominio> | 2. dominio xmpp example.com |
| 3. ascolto xmpp <elenco interfacce> | 3. ascolto xmpp |
| 4. xmpp certs <keyfile> <file di certificato> <cert-bundle> | 4. xmpp certs xmppcluster.key xmppcluster.cer root.cer |
| 5. trust cluster xmpp <certificato xmpp> | 5. trust cluster xmpp xmppcluster.cer ***** Nota 1** |
| **Configurazione del primo nodo** | **Configurazione del primo nodo** |
| 6. abilitazione xmpp | abilitazione xmpp |
| 7. xmpp callbridge add <nome callbridge> | 7. xmpp callbridge add cb1 |
| 8. xmpp callbridge add <nome callbridge> | 8. xmpp callbridge add cb2 |
| 9. xmpp callbridge add <nome callbridge> | 9. xmpp callbridge add cb3 |
| 10. xmpp callbridge add <nome callbridge> | 10. xmpp callbridge add cb4 ***** Nota 2** |
| 11. elenco callbridge xmpp | 11. elenco callbridge xmpp <— copia questo ou in blocco note |
| 12. xmpp disabilitato | 12. xmpp disabilitato |
| 13. abilitazione cluster xmpp | 13. abilitazione cluster xmpp |
| 14. inizializzazione cluster xmpp | 14. inizializzazione cluster xmpp |

15. abilitazione xmpp
16. stato cluster xmpp

Configurazione del secondo e del terzo nodo

17. abilitazione xmpp
18. xmpp callbridge add-secret <nome callbridge>
19. inserire il segreto di callbridge:
20. xmpp callbridge add-secret <nome callbridge>
21. Inserire il segreto di callbridge:
2. xmpp callbridge add-secret <nome callbridge>
23. Inserire il segreto di callbridge:
24. xmpp callbridge add-secret <nome callbridge>
25. Inserire il segreto di callbridge:
26. xmpp disabilitato
27. abilitazione cluster xmpp
28. abilitazione xmpp
29. join cluster xmpp <cluster>

Configurare le impostazioni XMPP in Amministrazione Web

Su ogni server con il servizio CallBridge

30. Immettere il nome univoco dei bridge di chiamate configurato in precedenza
31. Inserire il dominio
32. Inserire il segreto del Blocco note
3. Controllare la pagina di stato di webadmin per l'autenticazione

15. abilitazione xmpp
16. stato cluster xmpp

Configurazione del secondo e del terzo nodo

17. abilitazione xmpp
18. xmpp callbridge add-secret cb1
19. Inserire il segreto di callbridge: <copia segre
per cb1 da blocco note>
20. xmpp callbridge add-secret cb2
21. Inserire il segreto di callbridge: <copia segre
per cb2 da blocco note>
22. xmpp callbridge add-secret cb3
23: Immettere il segreto callbridge: <copia segre
per cb3 da blocco note>
24. xmpp callbridge add-secret cb4 *** Nota 3
25. Inserire il segreto di callbridge: <copia segre
per cb4 da blocco note>
26. xmpp disabilitato
27. abilitazione cluster xmpp
28. abilitazione xmpp
29. xmpp cluster join <indirizzo IP o FQDN del n
1>

Configurare le impostazioni XMPP in Amministrazione Web

Su ogni server con il servizio CallBridge

30. Immettere cb1 su callbridge1, ecc.
31. Immettere il dominio: example.com
32. Immettere il segreto dal blocco note per il callbridge corrispondente
3. Controllare la pagina di stato di webadmin pe
l'autenticazione

**Nota 1:** L'attendibilità del cluster xmpp nell'esempio è il certificato XMPP perché contiene tutti gli FQDN del server XMPP nell'attributo SAN (Subject Alternative Name) oppure è un certificato con caratteri jolly. Se ogni server XMPP dispone di un proprio certificato, è necessario combinarli e aggiungerli come attendibilità cluster xmpp.

**Nota 2:** xmpp callbridge add cb4. Questo passaggio è stato aggiunto come esempio in cui è possibile avere più bridge di chiamate rispetto ai server xmpp. Questo passaggio non è necessario, ma è stato aggiunto come esempio.

**Nota 3:** xmpp callbridge ad-secret cb4. È stato aggiunto questo passo per accompagnare la nota 2. Se si dispone di 4 bridge di chiamate, è necessario aggiungerli tutti e quattro a tutti i nodi nel cluster xmpp.

Se si continua a utilizzare la versione CMS 2.9.x, è possibile iniziare subito i test e la convalida per verificare che i nuovi server funzionino come previsto.

# Verifica

Dopo la migrazione ai nuovi server, verificare che tutti gli utenti e gli spazi siano visibili e che le

chiamate SIP continuino a funzionare.  Se si continua a utilizzare la versione CMS 2.9.x, verificare che XMPP funzioni ancora (gli utenti WebRTC possono comunque accedere/accedere, il registratore può connettersi, ecc.).  Verificare che i server in comunicazione con CMS siano ancora funzionanti (Cisco Meeting Manager (CMM), Cisco Unified Communications Manager (CUCM), TelePresence Management Suite (TMS), Expressway).  È inoltre consigliabile eseguire 'syslog follow' nel pannello di gestione per verificare la presenza di errori che è necessario correggere.

## Risoluzione dei problemi

In caso di problemi, è possibile ripristinare i server serie X oppure contattare Cisco TAC per assistenza.