

Implementazione del riutilizzo del certificato Multi-SAN Tomcat per CallManager

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Riutilizza certificato Tomcat per CallManager](#)

[Verifica](#)

Introduzione

In questo documento viene descritto un processo dettagliato su come riutilizzare il certificato Multi-SAN Tomcat per CallManager su CUCM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager (CUCM)
- Certificati CUCM
- ITL (Identity Trust List)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM release 15 SU1

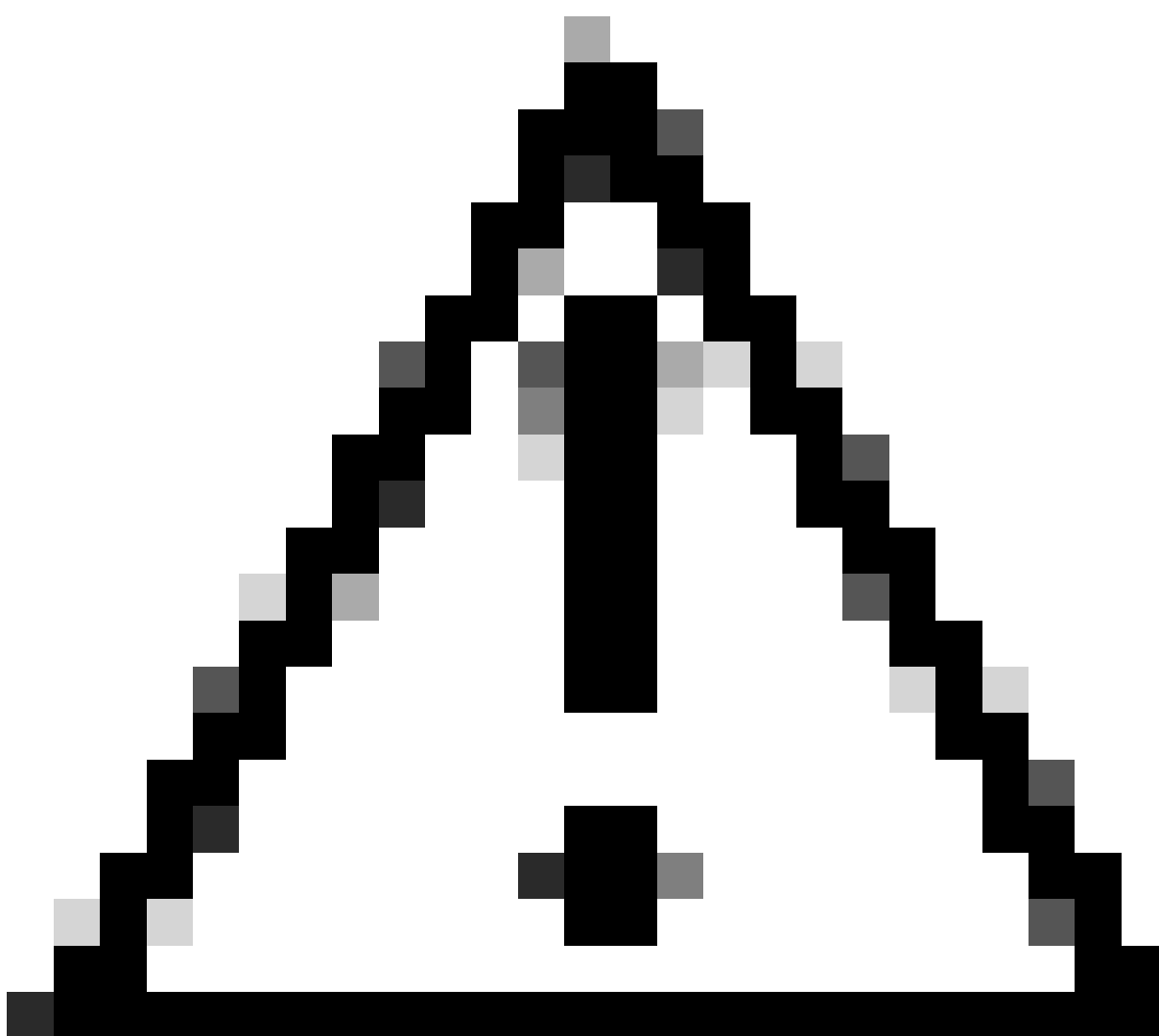
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Premesse

Le versioni precedenti di CUCM utilizzavano certificati diversi per ogni servizio per il cluster completo, con un conseguente aumento del numero di certificati e dei costi. Ciò include Cisco Tomcat e Cisco CallManager, servizi critici in esecuzione su CUCM che dispongono anche dei rispettivi certificati di identità.

A partire dalla versione 14 di CUCM, è stata aggiunta una nuova funzionalità per riutilizzare il certificato Multi-SAN Tomcat per il servizio CallManager.

Il vantaggio di questa funzionalità è che è possibile ottenere un certificato dalla CA e utilizzarlo in diverse applicazioni. Ciò assicura l'ottimizzazione dei costi e una riduzione della gestione e riduce le dimensioni del file ITL, riducendo in tal modo il sovraccarico.



Attenzione: prima di procedere con la configurazione del riutilizzo, verificare che il certificato Tomcat sia un certificato SAN multiserver. Il certificato Multi-SAN Tomcat può essere autofirmato o firmato dalla CA.

Riutilizza certificato Tomcat per CallManager



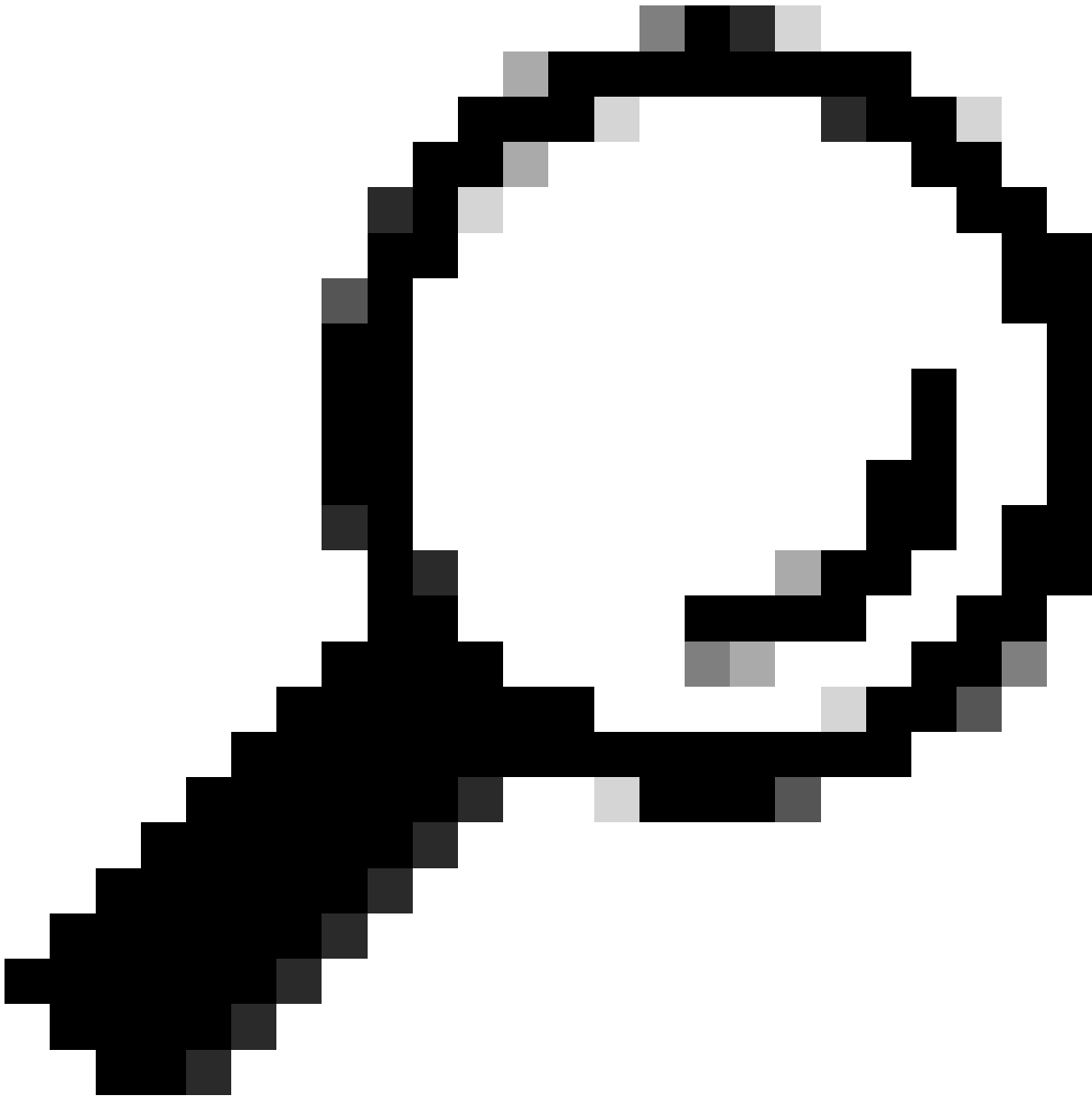
Avviso: verificare di aver identificato se il cluster è in modalità mista o non protetta prima di procedere.

Passaggio 1. Passare a Cisco Unified CM Administration > System > Enterprise Parameters (Amministrazione Cisco Unified CM > Sistema > Parametri aziendali):

Controllare la sezione Parametri di protezione e verificare se la modalità di protezione del cluster è impostata su 0 o 1. Se il valore è 0, il cluster è in modalità non protetta. Se il valore è 1, il cluster è in modalità mista ed è necessario aggiornare il file CTL prima del riavvio dei servizi.

Passaggio 2. Passare all'editore CUCM, quindi a Cisco Unified OS Administration > Security > Certificate Management (Amministrazione del sistema operativo unificato Cisco > Sicurezza > Gestione certificati).

Passaggio 3. Caricare la catena di certificati Multi-SAN Tomcat CA nell'archivio attendibile di



Suggerimento: se si utilizza un certificato SAN multiserver autofirmato per Tomcat, è possibile ignorare questo passaggio.

Prima di riutilizzare i certificati, assicurarsi di caricare manualmente la catena di certificati CA (che ha firmato il certificato di identità tomcat) nell'archivio attendibilità di CallManager.



Riavviare questi servizi quando si carica la catena di certificati Tomcat nell'attendibilità di CallManager.

- CallManager: servizio HAProxy Cisco
- CallManager-ECDSA: servizio Cisco CallManager e servizio Cisco HAProxy



Passaggio 4. Fare clic su Riutilizza certificato. Viene visualizzata la pagina Usa certificati Tomcat

per altri servizi.

Use Tomcat Certificate For Other Services

 Finish  Close

Status

 Tomcat-ECDSA Certificate is Not Multi-Server Certificate
 Tomcat Certificate is Multi-Server Certificate

Source

Choose Tomcat Type*

Replace Certificate for the following purpose

CallManager
 CallManager-ECDSA

Passaggio 5. Dall'elenco a discesa Tipo Tomcat, scegliere Tomcat o Tomcat-ECDSA.

Passaggio 6. Dal riquadro Sostituisci certificato per lo scopo seguente selezionare la casella di controllo CallManager o CallManager-ECDSA in base al certificato selezionato nel passaggio precedente.



Nota: se si sceglie Tomcat come tipo di certificato, CallManager viene abilitato come sostituzione. Se si sceglie tomcat-ECDSA come tipo di certificato, CallManager-ECDSA viene abilitato come tipo sostitutivo.

Passaggio 7. Fare clic su Fine per sostituire il certificato CallManager con il certificato SAN multiserver tomcat.

Use Tomcat Certificate For Other Services

→ Finish ↩ Close

Status

- i** Certificate Successful Provisioned for the nodes cucmpub15. . . , cucmsub15. . . .
- i** Restart Cisco HAProxy Service for the generated certificates to become active.
- i** If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

Passaggio 8. Riavviare il servizio Cisco HAProxy su tutti i nodi del cluster eseguendo il comando `utils service restart Cisco HAProxy` tramite CLI.

```
admin:utils service restart Cisco HAProxy
Stopping Cisco HAProxy...

Cisco HAProxy [STOPPED] Service Activated
Starting Cisco HAProxy...
Cisco HAProxy [STARTED]
admin:█
```

Passaggio 9. Se il cluster è in modalità mista, aggiornare il file CTL eseguendo il comando `utils ctl update CTLFile` via CLI di CUCM Publisher e procedere con il ripristino dei telefoni per ottenere il nuovo file CTL.

Verifica



Nota: il certificato CallManager non viene visualizzato sulla GUI quando si riutilizza il certificato.

È possibile eseguire il comando dalla CLI per verificare che CallManager riutilizzi il certificato Tomcat.

- mostra elenco certificati proprio

```
admin:show cert list own  
  
tomcat/tomcat.pem: Certificate Signed by AKASH-WINSERVLAB-CA  
tomcat-ECDSA/tomcat-ECDSA.pem: Self-signed certificate generated by system  
ipsec/ipsec.pem: Self-signed certificate generated by system  
ITLRecovery/ITLRecovery.pem:  
CallManager-ECDSA/CallManager-ECDSA.pem: Self-signed certificate generated by system  
CallManager/CallManager.pem: Reusing tomcat certificate for CallManager  
TVS/TVS.pem: Self-signed certificate generated by system  
  
admin:█
```


Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).