Rigenera certificati autofirmati servizio IM/IP CUCM

Sommario

Introduzione

In questo documento viene descritta una procedura dettagliata consigliata per la rigenerazione dei certificati in CUCM IM/P 8.x e versioni successive.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei certificati del servizio IM & Presence (IM/P).

Componenti usati

Le informazioni fornite in questo documento si basano sulla versione 8.x di IM/P e successive.

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

Utilizzo archivio certificati

Certificato Cisco Unified Presence (CUP)

Utilizzato per connessioni SIP sicure per la federazione SIP, il controllo delle chiamate remote di Microsoft per Lync/OCS/LCS, le connessioni sicure tra Cisco Unified Certificate Manager (CUCM) e IM/P e così via.

Cisco Unified Presence - Certificato CUP-XMPP (Extensible Messaging and Presence Protocol)

Utilizzato per convalidare le connessioni protette per i client XMPP quando viene creata una sessione XMPP.

Cisco Unified Presence - Extensible Messaging and Presence Protocol - Certificato da server a server (CUP-XMPP-S2S)

Utilizzato per convalidare le connessioni protette per le federazioni tra domini XMPP con un sistema XMPP federato esternamente.

Certificato di protezione IP (IPSec)

Utilizzato per:
· Convalida di una connessione sicura per Disaster Recovery System (DRS)/Disaster Recovery Framework (DRF)
· Convalidare la connessione sicura per i tunnel IPsec ai nodi Cisco Unified Communications Manager (CUCM) e IM/P nel cluster

Certificato Tomcat

Utilizzato per:

· Convalidare vari accessi Web, ad esempio l'accesso alle pagine dei servizi da altri nodi nel cluster e Jabber Access.
· Convalida della connessione protetta per SAML Single Sign-On (SSO).

· Convalidare la connessione protetta per il peer intercluster.

Attenzione: se si utilizza la funzione SSO sui server Unified Communications e i certificati Cisco Tomcat vengono rigenerati, l'SSO deve essere riconfigurato con i nuovi certificati. Il collegamento per la configurazione dell'SSO su CUCM e ADFS 2.0 è: https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html.

Nota: il collegamento al processo di rigenerazione/rinnovo dei certificati CUCM è: https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html.

Processo di rigenerazione dei certificati

Certificato CUP

Passaggio 1. Aprire un'interfaccia grafica utente (GUI) per ogni server del cluster. Iniziare con l'editore IM/P, quindi aprire una GUI per ogni server di sottoscrizione IM/P e passare a Cisco Unified OS Administration > Security > Certificate Management.

Passaggio 2. Iniziare dalla GUI dell'editore e scegliere Find di visualizzare tutti i certificati. Scegliere il certificatocup.pem. Una volta aperto, scegliere Regenerate e attendere fino a quando non si vede il successo prima che il popup è chiuso.

Passaggio 3. Continuare con i sottoscrittori successivi, seguire la stessa procedura descritta al passaggio 2 e completare tutti i sottoscrittori del cluster.

Passaggio 4. Dopo la rigenerazione del certificato CUP su tutti i nodi, è necessario riavviare i servizi.

Nota: se per la configurazione del gruppo di ridondanza di presenza è selezionata l'opzione Abilita alta disponibilità, Uncheck questa opzione viene selezionata prima del riavvio dei servizi. La configurazione del gruppo di ridondanza di presenza è accessibile all'indirizzo CUCM Pub Administration > System > Presence Redundancy Group. Il riavvio dei servizi provoca un'interruzione temporanea di IM/P e deve essere eseguito al di fuori dell'orario di produzione.

Riavviare i servizi nell'ordine seguente:

· Accedere a Cisco Unified Serviceability del server di pubblicazione:

r. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Servizio proxy Restart Cisco SIP.

c. Al termine del riavvio del servizio, continuare con i sottoscrittori e il servizio proxy SIP di CiscoRestart.

d. Iniziare con l'autore e quindi continuare con i sottoscrittori. Restart Cisco SIP Proxy Service (anche da Cisco Unified Serviceability > Tools > Control Center - Feature Services).

· Accedere a Cisco Unified Serviceability del server di pubblicazione:

r. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Servizio Cisco Presence Engine.

c. Al termine del riavvio del servizio, continuare con Cisco Presence Engine Service Restart nei sottoscrittori.

Nota: se configurato per la federazione SIP, Restart il servizio Cisco XCP SIP Federation Connection Manager (disponibile all'indirizzo Cisco Unified Serviceability > Tools > Control Center - Feature Services). Iniziare con l'autore e quindi continuare con i sottoscrittori.

Certificato CUP-XMPP

Nota: poiché Jabber utilizza i certificati CUCM e IM/P Tomcat e i certificati server CUP-XMPP per convalidare le connessioni per Tomcat e i servizi CUP-XMPP, nella maggior parte dei casi questi certificati CUCM e IM/P sono firmati da CA. Si supponga che il dispositivo Jabber non disponga della radice e di un certificato intermedio che fa parte del certificato CUP-XMPP installato nell'archivio

---

di certificati attendibili. In questo caso, il client Jabber visualizza un messaggio di avviso di protezione per il certificato non attendibile. Se non è già installato nel certificato dell'archivio di attendibilità del dispositivo Jabber, la radice e gli eventuali certificati intermedi devono essere inviati al dispositivo Jabber tramite Criteri di gruppo, MDM, posta elettronica e così via, che dipendono dal client Jabber.

Nota: se il certificato CUP-XMMP è autofirmato, il client Jabber visualizza un messaggio di avviso di protezione per il certificato non attendibile se il certificato CUP-XMPP non è installato nell'archivio attendibile del certificato del dispositivo Jabber. Se non è già installato, il certificato CUP-XMPP autofirmato deve essere inviato al dispositivo Jabber tramite Criteri di gruppo, MDM, posta elettronica e così via, che dipende dal client Jabber.

Passaggio 1. Aprire una GUI per ogni server del cluster. Iniziare con l'editore IM/P, quindi aprire una GUI per ogni server di sottoscrizione IM/P e passare a **Cisco Unified OS Administration > Security > Certificate Management**.

Passaggio 2. Iniziare dalla GUI dell'editore e scegliere Find di visualizzare tutti i certificati. Nella colonna Tipo del cup-xmpp.pem certificato determinare se il certificato è autofirmato o firmato dall'autorità di certificazione. Se il cup-xmpp.pem certificato è una distribuzione multiSAN firmata da terze parti (di tipo con firma CA), esaminare questo collegamento quando si genera un CSR Multi-SAN CUP-XMPP e si invia all'autorità di certificazione per il certificato CUP-XMPP firmato dall'autorità di certificazione; Esempio di configurazione di un cluster di comunicazioni unificato con nome soggetto multiserver con firma CA.

Se il cup-xmpp.pem certificato è una distribuzione a nodo singolo firmata da terze parti (tipo con firma CA) (il nome della distribuzione è uguale al nome comune del certificato), esaminare questo collegamento quando si genera un CUP-XMPP CSR a nodo singolo e si invia a CA per il certificato CUP-XMPP firmato da CA; Guida procedurale Jabber Complete per la convalida dei certificati. Se il cup-xmpp.pem certificato è autofirmato, passare al punto 3.

Passaggio 3. Scegliere Find per visualizzare tutti i certificati, quindi scegliere il cup-xmpp.pem certificato. Una volta aperto, scegliere Regenerate e attendere fino a quando non si vede il successo prima che il popup è chiuso.

Passaggio 4. Continuare con i sottoscrittori successivi; fare riferimento alla stessa procedura nel passaggio 2 e completarla per tutti i sottoscrittori nel cluster.

Passaggio 5. Dopo aver rigenerato il certificato CUP-XMPP su tutti i nodi, è necessario riavviare il servizio router Cisco XCP sui nodi IM/P.

Nota: se per la configurazione del gruppo di ridondanza di presenza è selezionata l'opzione Abilita alta disponibilità, Uncheck prima del riavvio del servizio. La configurazione del gruppo di ridondanza di presenza è accessibile all'indirizzo CUCM Pub Administration > System > Presence Redundancy Group. Il riavvio del servizio provoca un'interruzione temporanea del servizio di messaggistica immediata e deve essere eseguito al di fuori dell'orario di produzione.

· Accedere a Cisco Unified Serviceability del server di pubblicazione:

r. Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart il servizio Cisco XCP Router.

c. Al termine del riavvio del servizio, continuare con Restart il servizio Cisco XCP Router sugli utenti.

Certificato CUP-XMPP-S2S

Passaggio 1. Aprire una GUI per ogni server del cluster. Iniziare con l'editore IM/P, quindi aprire una GUI per ciascun server di sottoscrizione IM/P e passare a Cisco Unified OS Administration > Security > Certificate Management.

Passaggio 2. Iniziare con l'interfaccia utente grafica dell'autore, scegliere Find di visualizzare tutti i certificati e scegliere il cup-xmpp-s2s.pem certificato. Una volta aperto, scegliere Regenerate e attendere fino a quando non si vede il successo prima che il popup è chiuso.

Passaggio 3. Continuare con i sottoscrittori successivi e fare riferimento alla stessa procedura nel passaggio 2 e completare per tutti i sottoscrittori nel cluster.

Passaggio 4. Dopo la rigenerazione del certificato CUP-XMPP-S2S su tutti i nodi, è necessario riavviare i servizi nell'ordine indicato.

Nota: se per la configurazione del gruppo di ridondanza di presenza è selezionata l'opzione Abilita alta disponibilità,Uncheck prima del riavvio di questi servizi. È possibile accedere alla configurazione del gruppo di ridondanza di presenza su CUCM Pub Administration > System > Presence Redundancy Group. Il riavvio dei servizi provoca un'interruzione temporanea di IM/P e deve essere eseguito al di fuori dell'orario di produzione.

· Accedere a Cisco Unified Serviceability del server di pubblicazione:

r. Cisco Unified Serviceability > Tools > Control Center - Network Services.
b. Restart il servizio Cisco XCP Router.
c. Al termine del riavvio del servizio, continuare con il servizio Restart del router Cisco XCP sugli utenti.

· Accedere a Cisco Unified Serviceability del server di pubblicazione:

r. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart il servizio Cisco XCP XMPP Federation Connection Manager.

c. Al termine del riavvio del servizio, continuare con Restart il servizio Cisco XCP XMPP Federation Connection Manager sui sottoscrittori.

Certificato IPSec

Nota: il ipsec.pem certificato nell'editore CUCM deve essere valido e presente in tutti i sottoscrittori (nodi CUCM e IM/P) nell'archivio attendibilità IPSec. Il ipsec.pem certificato del sottoscrittore non è presente nel server di pubblicazione come archivio di attendibilità IPSec in una distribuzione standard. Per verificare la validità, confrontare i numeri di serie nel ipsec.pem certificato del CUCM-PUB con quelli dell'IPSec-trust degli utenti. Devono corrispondere.

Nota: DRS utilizza una comunicazione basata su SSL (Secure Socket Layer) tra l'agente di origine e l'agente locale per l'autenticazione e la crittografia dei dati tra i nodi cluster CUCM (nodi CUCM e IM/P). DRS utilizza i certificati IPSec per la crittografia a chiave pubblica/privata. Tenere presente che se si elimina il file dell'archivio attendibilità IPSEC (hostname.pem) dalla pagina Gestione certificati, DRS non funziona come previsto. Se il file di trust IPSEC viene eliminato manualmente, è necessario assicurarsi di caricare il certificato IPSEC nell'archivio trust IPSEC. Per ulteriori informazioni, vedere la pagina della Guida alla gestione dei certificati nelle Guide alla sicurezza CUCM.

Passaggio 1. Aprire una GUI per ogni server del cluster. Iniziare con l'editore IM/P, quindi aprire una GUI per ciascun server di sottoscrizione IM/P e passare a Cisco Unified OS Administration > Security > Certificate Management.

Passaggio 2. Iniziare con l'interfaccia utente dell'editore e scegliere Find di visualizzare tutti i certificati.Choose ipsec.pem il certificato. Una volta aperto, scegliere Regenerate e attendere fino a quando non si vede il successo prima che il popup è chiuso.

Passaggio 3. Continuare con i sottoscrittori successivi e fare riferimento alla stessa procedura nel passaggio 2 e completare per tutti i sottoscrittori nel cluster.

Passaggio 4. Dopo che tutti i nodi hanno rigenerato il certificato IPSEC, eseguire quindiRestart questi servizi. Passare alla pagina Cisco Unified Serviceability del server di pubblicazione; Cisco Unified Serviceability > Tools > Control Center - Network Services.
a. Scegliere Restart il servizio primario Cisco DRF.
b. Una volta completato il riavvio del servizio, scegliereRestart il servizio locale DRF di Cisco nell'editore, quindi continuare con Restart il servizio locale DRF di Cisco in ogni sottoscrittore.

Certificato Tomcat

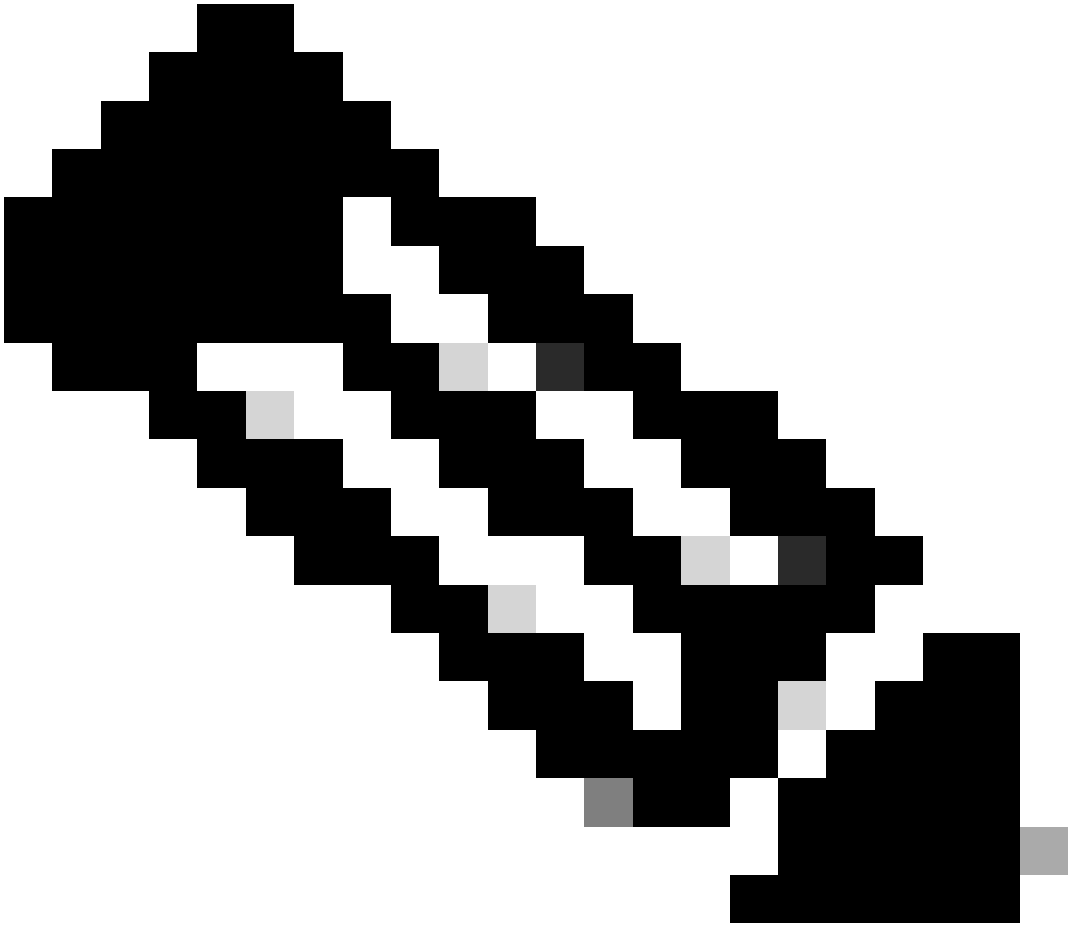
Nota: poiché Jabber utilizza i certificati server CUCM Tomcat e IM/P Tomcat e CUP-XMPP per convalidare le connessioni per i servizi Tomcat e CUP-XMPP, nella maggior parte dei casi questi certificati CUCM e IM/P sono firmati da CA. Si supponga che il dispositivo Jabber non disponga della radice e di eventuali certificati intermedi che fanno parte del certificato Tomcat installato nel relativo archivio certificati attendibili. In tal caso, il client Jabber visualizza un messaggio di avviso di protezione per il certificato non attendibile. Se non è già installato nell'archivio di certificati attendibili del dispositivo Jabber, la radice e gli eventuali certificati intermedi devono essere inviati al dispositivo Jabber tramite Criteri di gruppo, MDM, posta elettronica e così via, che dipendono dal client Jabber.

Nota: se il certificato Tomcat è autofirmato, il client Jabber visualizza un messaggio di avviso di protezione per il certificato non attendibile, se il certificato Tomcat non è installato nell'archivio di certificati attendibili del dispositivo Jabber. Se non è già installato nell'archivio di certificati attendibili del dispositivo Jabber, il certificato CUP-XMPP autofirmato deve essere inviato al dispositivo Jabber tramite Criteri di gruppo, MDM, posta elettronica e così via, che dipendono dal client Jabber.

Passaggio 1. Aprire una GUI per ogni server del cluster. Iniziare con l'editore IM/P, quindi aprire una GUI per ciascun server di sottoscrizione IM/P e passare a Cisco Unified OS Administration > Security > Certificate Management.

Passaggio 2. Iniziare dalla GUI dell'editore e scegliere Find di visualizzare tutti i certificati.
· Dalla colonna Tipo del tomcat.pem certificato, determinare se è autofirmato o firmato dalla CA.

· Se il tomcat.pem certificato è una distribuzione multisito firmata da terze parti (di tipo con firma CA), vedere questo collegamento per informazioni su come generare un CSR Tomcat multisSAN e inoltrare a CA un certificato Tomcat firmato da CA, Esempio di configurazione di Unified Communication Cluster Setup con nome alternativo soggetto multiserver con firma CA



Nota: il CSR Tomcat multi-SAN viene generato nell'editore CUCM e viene distribuito a tutti i nodi CUCM e IM/P nel cluster.

· Se il tomcat.pem certificato è una distribuzione a nodo singolo firmata da terze parti (il nome di distribuzione è uguale al nome comune del certificato), esaminare questo collegamento per generare un CSR CUP-XMPP a nodo singolo e inviarlo all'autorità di certificazione per il certificato CUP-XMPP firmato dall'autorità di certificazione, Jabber Complete How-To Guide for Certificate Validation

· Se il tomcat.pem certificato è autofirmato, passare al punto 3

Passaggio 3. Scegliere Find per visualizzare tutti i certificati:

· Scegliere il certificatotomcat.pem.

· Una volta aperto, scegliere Regenerate e attendere fino a quando non viene visualizzato il pop-up di successo prima che il pop-up sia chiuso.

Passaggio 4. Continuare con ogni sottoscrittore successivo, fare riferimento alla procedura descritta nel passaggio 2 e completare tutti i sottoscrittori del cluster.

Passaggio 5. Dopo che tutti i nodi hanno rigenerato il certificato Tomcat, Restart il servizio Tomcat su tutti i nodi. Iniziare con l'editore, seguito dai sottoscrittori.

· Per eseguire il servizio Tomcat, è necessario aprire una sessione CLI per ciascun nodo ed eseguire il comando finché il servizio nonRestart riavvia Cisco Tomcat, come mostrato nell'immagine:

```
admin:
admin:utils service restart Cisco Tomcat
 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

Elimina certificati di attendibilità scaduti

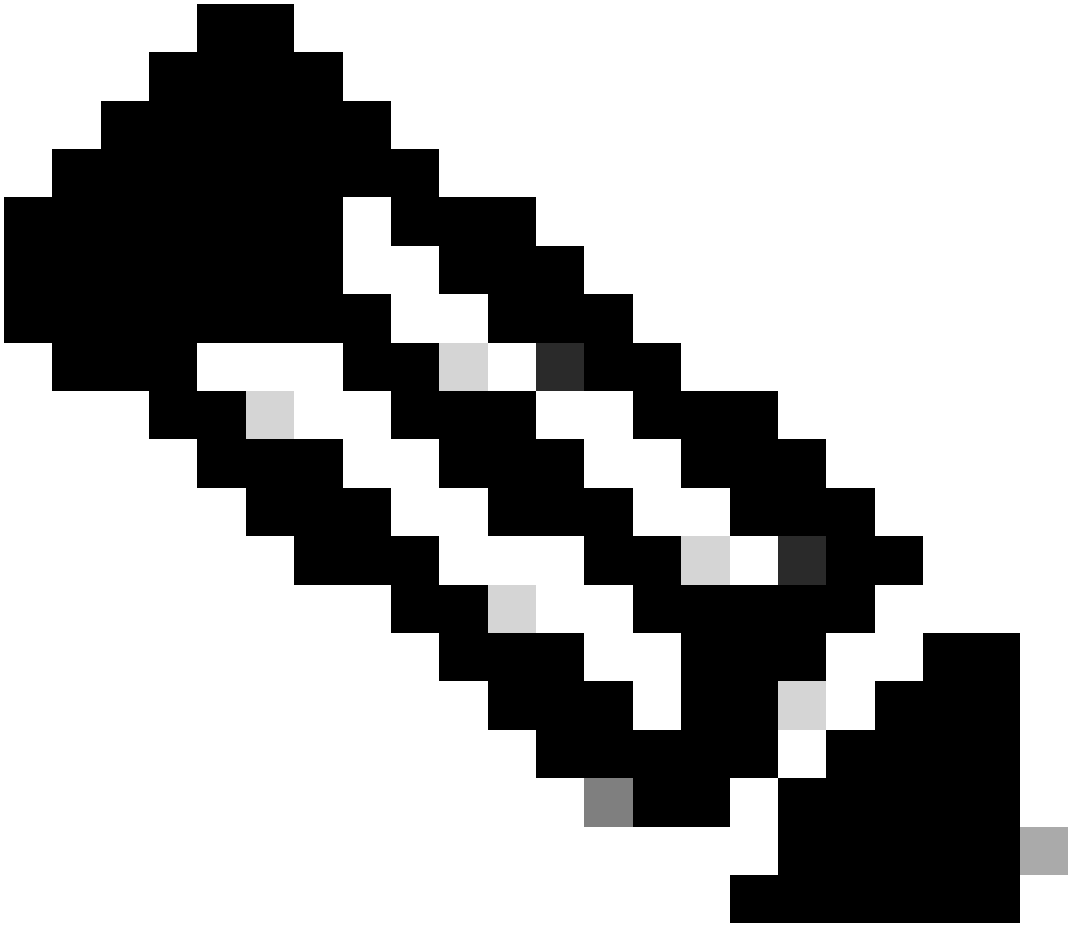
Nota: è possibile eliminare i certificati di attendibilità (che terminano con -trust) quando necessario. I certificati di attendibilità che è possibile eliminare sono quelli non più necessari, scaduti o obsoleti. Non eliminare i cinque certificati di identità: cup.pem , cup-xmpp.pem , cup-xmpp-s2s.pem , ipsec.pem , e tomcat.pem certificati. I riavvii del servizio, come illustrato, sono progettati per cancellare qualsiasi informazione in memoria di questi certificati legacy all'interno di tali servizi.

Nota: se per la configurazione del gruppo di ridondanza di presenza è selezionata l'opzione Abilita alta disponibilità, Uncheck ciò avviene prima che un servizio sia Stopped/Started o Restarted. La configurazione del gruppo di ridondanza di presenza è accessibile all'indirizzo CUCM Pub Administration > System > Presence Redundancy Group. Il riavvio di alcuni servizi, come illustrato, provoca un'interruzione temporanea di messaggistica istantanea/processo e deve essere eseguito al di fuori dell'orario di produzione.

Passaggio 1. Accedere a:Cisco Unified Serviceability > Tools > Control Center - Network Services

· Dal menu a discesa, scegliere l'editore IM/IP, scegliere Stop da Cisco Certificate Expiry Monitor, quindi Stop in Cisco Intercluster Sync Agent.

· Ripetere la proceduraStop per questi servizi per ogni nodo IM/P del cluster.



Nota: se è necessario eliminare il certificato Tomcat-trust, passare alla pagina Cisco Unified Serviceability > Tools > Control Center - Network Services dell'editore CUCM.

· Scegliere l'editore CUCM dall'elenco a discesa.

· Scegliere Stopda Cisco Certificate Expiry Monitor, quindi digitare Stop in Notifica di modifica del certificato Cisco.

· Ripetere l'operazione per ogni nodo CUCM del cluster.

Passaggio 2. Passare a Cisco Unified OS Administration > Security > Certificate Management > Find.

· Individuare i certificati di attendibilità scaduti (per le versioni 10.x e successive, è possibile filtrare in base alla scadenza). Nelle versioni precedenti alla 10.0 è necessario identificare i certificati specifici manualmente o tramite gli avvisi RTMT, se ricevuti.

· Lo stesso certificato di attendibilità può apparire in più nodi, ma deve essere eliminato singolarmente da ogni nodo.

· Scegliere il certificato di attendibilità da eliminare (in base alla versione, viene visualizzata una schermata popup o viene visualizzato il certificato nella stessa pagina).

· Scegliere Delete (viene visualizzato un popup che inizia con "si sta per eliminare definitivamente questo certificato...").
•Fare clic su OK.

Passaggio 3. Ripetere la procedura per ogni certificato di attendibilità da eliminare.

Passaggio 4. Al termine, è necessario riavviare i servizi direttamente correlati ai certificati eliminati.

· CUP-trust: Cisco SIP Proxy, Cisco Presence Engine e, se configurato per la federazione SIP, Cisco XCP SIP Federation Connection Manager (vedere la sezione Certificato CUP)
· CUP-XMPP-trust: router Cisco XCP (vedere la sezione relativa ai certificati CUP-XMPP)
· CUP-XMPP-S2S-trust: router Cisco XCP e Cisco XCP XMPP Federation Connection Manager
· IPSec-trust: origine DRF/locale DRF (vedere la sezione relativa ai certificati IPSec)
· Tomcat-trust: riavviare il servizio Tomcat dalla riga di comando (vedere la sezione relativa ai certificati Tomcat)

Passaggio 5. Riavviare i servizi arrestati nel passaggio 1.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

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).