Rigenerazione dei certificati per CUCM

Sommario

Introduzione

In questo documento viene descritta la procedura per rigenerare i certificati in Cisco Unified Communications Manager (CUCM) versione 8.X e successive.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- *Strumento di monitoraggio in tempo reale* (RTMT)
- Certificati CUCM

Componenti usati

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

- CUCM release 8.X 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

In questo documento viene descritta la procedura dettagliata per la rigenerazione dei certificati in Cisco Unified Communications Manager (CUCM) versione 8.X e successive. Tuttavia, ciò non riflette le modifiche successive alla versione 12.0 in ripristino ITL.

Installa RTMT

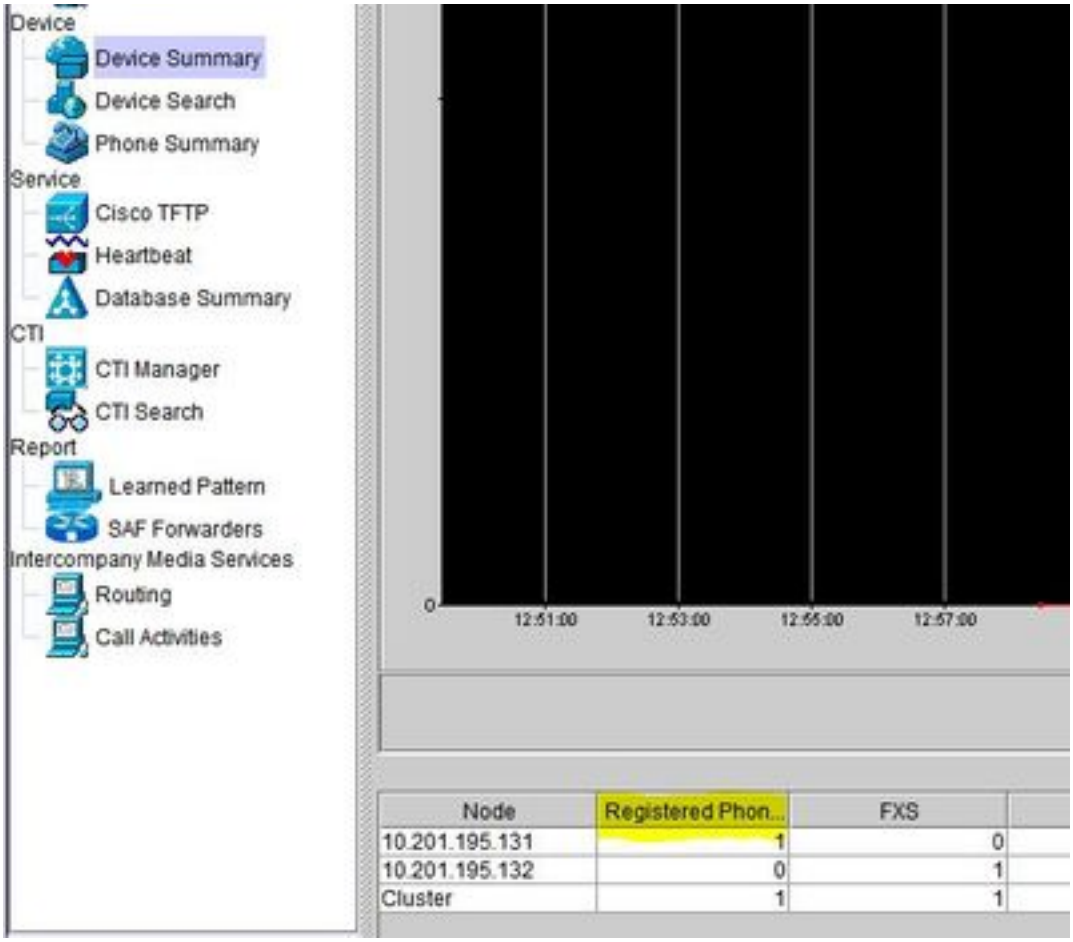
- Scaricare e installare lo strumento RTMT da Call Manager. Passare ad Amministrazione Gestione chiamate (CM): **Applicazione > Plugin > Trova > Strumento di monitoraggio in tempo reale Cisco Unified - Windows > Scarica** Installazione e avvio

Endpoint monitor con RTMT

- Avviare RTMT e immettere l'indirizzo IP o il nome di dominio completo (FQDN), quindi il nome utente e la password per accedere allo strumento:
- Selezionare la **scheda Voce/video**.Selezionare **Device Summary**. Questa sezione identifica il numero totale di endpoint registrati e il numero di endpoint registrati per ogni nodoMonitoraggio durante la reimpostazione dell'endpoint per garantire la registrazione prima della rigenerazione del certificato successivo

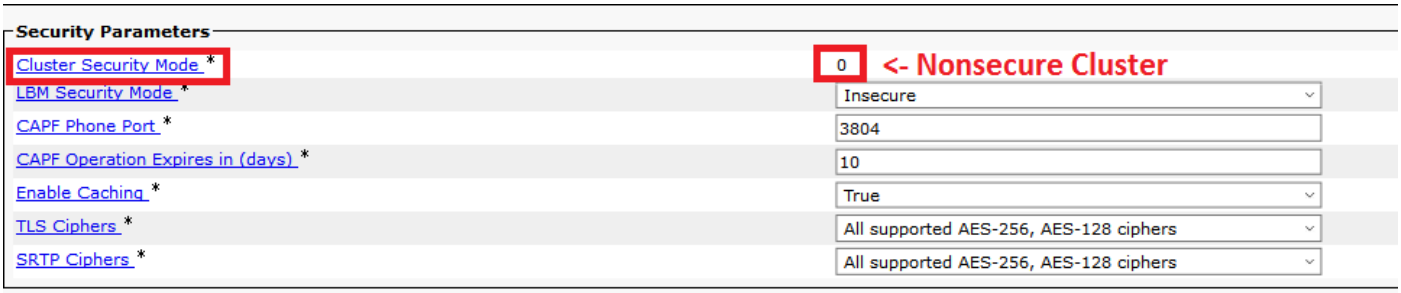
Suggerimento: Il processo di rigenerazione di alcuni certificati può influire sull'endpoint. Considera un piano d'azione dopo il normale orario di lavoro a causa della necessità di riavviare i servizi e i telefoni. Verificare che la registrazione tramite RTMT sia consigliata.

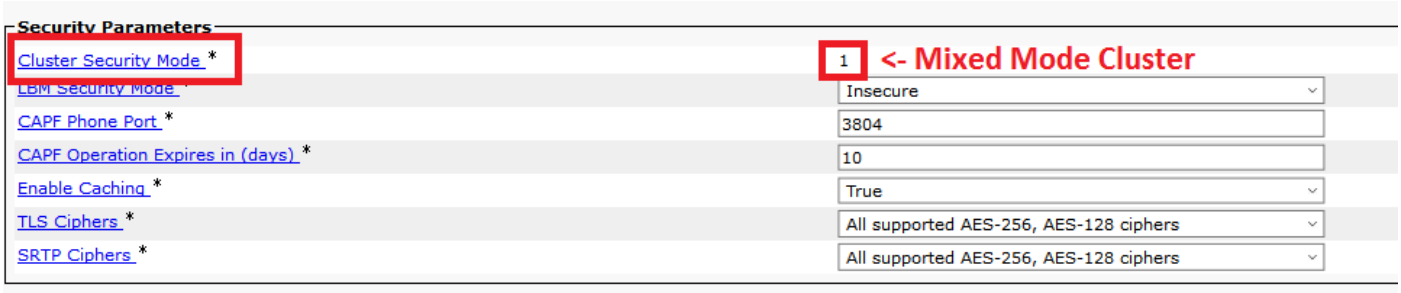
Avviso: Gli endpoint con mancata corrispondenza ITL corrente possono presentare problemi di registrazione dopo questo processo. L'eliminazione dell'ITL sull'endpoint è una tipica soluzione basata su best practice dopo il completamento del processo di rigenerazione e la registrazione di tutti gli altri telefoni.



Identificare se il cluster è in modalità mista o non protetta

- Passare ad Amministrazione CM. **Sistema > Parametri organizzazione > Parametri sicurezza > Modalità di sicurezza cluster**





Impatto dell'archivio certificati

Per una corretta funzionalità di sistema è fondamentale che tutti i certificati vengano aggiornati nel cluster CUCM. Se i certificati sono scaduti o non validi, possono influire in modo significativo sul normale funzionamento del sistema. L'impatto può variare a seconda della configurazione del

sistema. Di seguito è riportato un elenco dei servizi per i certificati specifici non validi o scaduti:

Gestione chiamate.pem

- I telefoni crittografati/autenticati non si registrano
- Il protocollo TFTP (Trivial File Transfer Protocol) non è attendibile (i telefoni non accettano file di configurazione firmati e/o ITL)
- Il problema può riguardare i servizi telefonici
- I trunk SIP (Secure Session Initiation Protocol) o le risorse multimediali (bridge di conferenze, MTP (Media Termination Point), Xcoder e così via) non si registrano o non funzionano.
- Richiesta AXL non riuscita.

Tomcat.pem

- I telefoni non sono in grado di accedere ai servizi HTTP ospitati nel nodo CUCM, ad esempio Directory aziendale
- CUCM può presentare diversi problemi Web, ad esempio l'impossibilità di accedere alle pagine del servizio da altri nodi nel cluster
- Problemi di mobilità delle estensioni (EM) o di mobilità delle estensioni tra cluster
- Single Sign-On (SSO)
- Se UCCX (Unified Contact Center Express) è integrato, a causa del cambiamento della sicurezza rispetto a CCX 12.5 è necessario caricare il certificato CUCM Tomcat (autofirmato) o il certificato radice e intermedio Tomcat (per CA firmato) in UCCX per l'archivio di attendibilità del gatto poiché influisce sugli accessi desktop Finesse.

CAPF.pem

- I telefoni non vengono autenticati per Phone VPN, 802.1x o Phone Proxy
- Impossibile rilasciare certificati LSC (Locally Significant Certificate) per i telefoni.
- I file di configurazione crittografati non funzionano

IPSec.pem

- Il Disaster Recovery System (DRS)/Disaster Recovery Framework (DRF) non funziona correttamente
- I tunnel IPsec da gateway (GW) ad altri cluster CUCM non funzionano

TVS (Trust Verification Service)

Trust Verification Service (TVS) è il componente principale di Security by Default. TVS consente a Cisco Unified IP Phone di autenticare i server applicazioni, come ad esempio i servizi EM, la directory e MIDlet, quando viene stabilito HTTPS.

TVS offre le seguenti funzioni:

- Scalabilità - Il numero di certificati da considerare attendibili non influisce sulle risorse Cisco Unified IP Phone.

- Flessibilità: l'aggiunta o la rimozione di certificati di attendibilità si riflette automaticamente nel sistema.
- Protezione predefinita - Le funzioni di protezione dei segnali e non multimediali fanno parte dell'installazione predefinita e non richiedono l'intervento dell'utente.

ITL e CTL

- ITL contiene il ruolo del certificato per Call Manager TFTP, tutti i certificati TVS nel cluster e la funzione CAPF (Certificate Authority Proxy Function) quando eseguita.
- CTL contiene voci per i servizi SAST (System Administrator Security Token), Cisco CallManager e Cisco TFTP che vengono eseguiti sullo stesso server, CAPF, server TFTP e firewall ASA (Adaptive Security Appliance). Nell'elenco di certificati attendibili (CTL) non viene fatto riferimento a TVS.

Processo di rigenerazione dei certificati

> **Nota:** Tutti gli endpoint devono essere accesi e registrati prima della rigenerazione dei certificati. In caso contrario, i telefoni non collegati richiedono la rimozione dell'ITL.

Certificato Tomcat

Indica se i certificati di terze parti sono in uso:

1. Passare a ogni server del cluster (in schede separate del browser Web) iniziando dall'editore, seguito da ogni sottoscrittore. Passare a **Cisco Unified OS Administration > Security > Certificate Management > Find (Amministrazione Cisco Unified SO > Protezione > Gestione certificati > Trova)**.
   Osservare nella colonna Descrizione se Tomcat indica un certificato autofirmato generato dal sistema. Se Tomcat è firmato da terze parti, seguire il collegamento fornito ed eseguire questi passaggi dopo la rigenerazione di Tomcat.Per i certificati firmati da terze parti, vedere Caricamento di certificati CUCMdmin Web GUI.
2. Per visualizzare tutti i certificati, selezionare **Trova**: Selezionare il certificato **Tomcat pem**.Una volta aperto, selezionate **Rigenera (Regenerate)** e attendete fino a quando non viene visualizzata la finestra a comparsa Successo (Success), quindi chiudete la finestra a comparsa o tornate indietro e selezionate **Trova/Lista (Find/List)**.
3. Continuare con ogni Sottoscrittore successivo, seguire la stessa procedura nel passaggio 2 e completare su tutti i Sottoscrittori del cluster.
4. Dopo che tutti i nodi hanno rigenerato il certificato Tomcat, riavviare il servizio Tomcat su tutti i nodi. Iniziare con l'autore e quindi con i sottoscrittori. Per riavviare Tomcat, è necessario aprire una sessione CLI per ciascun nodo ed eseguire il comando **utils service restart Cisco Tomcat**.

5. Se applicabile, è necessario eseguire le seguenti operazioni dall'ambiente CCX:

- Se viene utilizzato un certificato autofirmato, caricare i certificati Tomcat da tutti i nodi del cluster CUCM nell'archivio attendibile Unified CCX Tomcat.
- Se si utilizza un certificato CA firmato o privato firmato dalla CA, caricare il certificato CA radice di CUCM nell'archivio attendibile Unified CCX Tomcat.
- Riavviare i server come indicato nel documento di rigenerazione dei certificati per CCX.

Ulteriori riferimenti:

- Guida alla gestione dei certificati della soluzione UCCX
- Unified CCX Health Check Utility

Certificato IPSEC

Nota: CUCM/Messaggistica immediata e presenza (IM&P) prima della versione 10.X del DRF Master L'agente viene eseguito sia su CUCM Publisher che su IM&P Publisher. Il servizio locale DRF viene eseguito rispettivamente sui sottoscrittori. Versioni 10.X e successive, DRF Master L'agente viene eseguito solo sull'editore CUCM e il servizio locale DRF sui sottoscrittori CUCM e sull'editore e i sottoscrittori IM&P.

Nota: Il sistema di disaster recovery utilizza una comunicazione SSL (Secure Sockets Layer) tra Master Agente e Agente locale per l'autenticazione e la crittografia dei dati tra i nodi del cluster CUCM. DRS utilizza i certificati IPSec per la crittografia a chiave pubblica/privata. Tenere presente che se si elimina il file truststore IPSEC (hostname.pem) dalla pagina di gestione dei certificati, il funzionamento di DRS non sarà quello previsto. Se si elimina il file di trust IPSEC 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 di Cisco Unified Communications Manager.

1. Passare a ogni server del cluster (in schede separate del browser Web) iniziando dall'editore, seguito da ogni sottoscrittore. Passare a **Cisco Unified OS Administration > Security > Certificate Management > Find (Amministrazione Cisco Unified SO > Sicurezza > Gestione certificati > Trova)**:
   Selezionare il certificato **pem IPSEC**.Una volta aperto, selezionate **Rigenera (Regenerate)** e attendete fino a quando non viene visualizzata la finestra a comparsa Successo (Success), quindi chiudete la finestra a comparsa o tornate indietro e selezionate **Trova/Lista (Find/List)**.
2. Continuare con gli abbonati successivi; seguire la stessa procedura al passaggio 1 e completare in tutti i sottoscrittori del cluster.
3. Dopo che tutti i nodi hanno rigenerato il certificato IPSEC, riavviare i servizi.
   Passare al server di pubblicazione **Cisco Unified Serviceability**. **Cisco Unified Serviceability > Strumenti > Control Center - Servizi di rete**.Selezionare **Riavvia** il **Cisco DRF Master**servizio.Al termine del riavvio del servizio, selezionare **Restart** (Riavvia) sul **servizio locale Cisco DRF**

nel server di pubblicazione, quindi continuare con i sottoscrittori e selezionare **Restart** (Riavvia) sul **servizio locale Cisco DRF**.

Il certificato IPSEC.pem nel server di pubblicazione deve essere valido e deve essere presente in tutti i sottoscrittori come truststore IPSEC. Il certificato IPSEC.pem dei sottoscrittori non è presente nel server di pubblicazione come truststore IPSEC in una distribuzione standard. Per verificare la validità, confrontare i numeri di serie nel certificato IPSEC.pem del PUB con il trust IPSEC nei SUB. Devono corrispondere.

Certificato CAPF

Avviso: Prima di procedere, verificare di aver identificato se il cluster è in modalità mista. Fare riferimento alla sezione **Identificare se il cluster è in modalità mista o non protetta**.

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 su 1. Se il valore è 0, il cluster è in modalità non protetta. Se è 1, il cluster è in modalità mista ed è necessario aggiornare il file CTL prima del riavvio dei servizi. Vedere Collegamenti Token e Token.
2. Passare a ogni server del cluster (in schede separate del browser Web) iniziando dal server di pubblicazione, quindi da ogni sottoscrittore. Passare a **Cisco Unified OS Administration > Security > Certificate Management > Find (Amministrazione Cisco Unified SO > Protezione > Gestione certificati > Trova)**.
   Selezionare il certificato **PEM CAPF**.Una volta aperto, selezionate **Rigenera** (Regenerate) e attendete fino a quando non viene visualizzata la finestra a comparsa Successo (Success), quindi chiudete la finestra a comparsa o tornate indietro e selezionate **Trova/Lista (Find/List)**
3. Continuare con gli abbonati successivi; seguire la stessa procedura al passaggio 2 e completare su tutti i sottoscrittori del cluster. Se il cluster è solo in modalità mista e il file CAPF è stato rigenerato, aggiornare il CTL prima di procedere con Token - Token.Se il cluster è in modalità mista, è necessario riavviare anche il servizio Gestione chiamate prima di riavviare altri servizi.
4. Dopo che tutti i nodi hanno rigenerato il certificato CAPF, riavviare i servizi.
   Passare a **Cisco Unified Serviceability** di **Cisco**. **Cisco Unified Serviceability > Strumenti > Control Center - Feature Services**.Iniziare con l'autore e selezionare **Riavvia** nel **servizio funzione proxy Autorità di certificazione Cisco** solo se attivo.
5. Selezionare **Cisco Unified Serviceability > Tools > Control Center - Network Services (Servizi di rete unificati Cisco > Strumenti > Control Center -** Servizi di rete). Iniziare con l'autore, quindi continuare con i sottoscrittori e selezionare **Riavvia** sul **servizio di verifica dell'attendibilità Cisco**. Selezionare **Cisco Unified Serviceability > Tools > Control Center - Feature Services (Servizi unificati Cisco > Strumenti > Control Center - Servizi funzionalità)**.Iniziare con l'autore, quindi continuare con i sottoscrittori, riavviare il **servizio Cisco TFTP** solo se attivo.
6. Riavvia tutti i telefoni: **Cisco Unified CM Amministrazione > Sistema > Parametri Enterprise**Selezionare **Reset** quindi viene visualizzata una schermata di popup con l'istruzione **You are about to reset all devices in the system. L'operazione non può essere annullata. Continuare?,** selezionare **OK** e quindi **Reset**.

I telefoni sono stati ripristinati. Monitorare le azioni eseguite tramite lo strumento RTMT per

verificare che il ripristino sia stato eseguito correttamente e che i dispositivi vengano registrati nuovamente in CUCM. Attendere il completamento della registrazione telefonica prima di procedere con il certificato successivo. Questo processo di registrazione dei telefoni può richiedere del tempo. Tenere presente che i dispositivi con ITL errati prima del processo di rigenerazione non vengono registrati nuovamente nel cluster fino a quando non vengono rimossi.

Certificato CallManager

> **Avviso:** Prima di procedere, verificare di aver identificato se il cluster è in modalità mista. Fare riferimento alla sezione **Identificare se il cluster è in modalità mista o non protetta**.

> **Avviso:** Non rigenerare contemporaneamente i certificati CallManager.PEM e TVS.PEM. Ciò causa una mancata corrispondenza irreversibile con l'ITL installato sugli endpoint che richiedono la rimozione dell'ITL da TUTTI gli endpoint nel cluster. Completare l'intero processo per CallManager.PEM e, una volta registrati nuovamente i telefoni, avviare il processo per TVS.PEM.

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 su 1. Se il valore è 0, il cluster è in modalità non protetta. Se è 1, il cluster è in modalità mista ed è necessario aggiornare il file CTL prima del riavvio dei servizi. Vedere Collegamenti Token e Token.
2. Passare a ogni server del cluster (in schede separate del browser Web) iniziando dal server di pubblicazione, quindi da ogni sottoscrittore. Passare a **Cisco Unified OS Administration > Security > Certificate Management > Find (Amministrazione Cisco Unified SO > Protezione > Gestione certificati > Trova)**.
   Selezionare il certificato peer CallManager.Una volta aperto, selezionate **Rigenera (Regenerate)** e attendete fino a quando non viene visualizzata la finestra a comparsa Successo (Success), quindi chiudete la finestra a comparsa o tornate indietro e selezionate **Trova/Lista (Find/List)**.
3. Continuare con gli abbonati successivi; seguire la stessa procedura al passaggio 2 e completare su tutti i sottoscrittori del cluster. Se il cluster è solo in modalità mista e il certificato di CallManager è stato rigenerato, aggiornare l'elenco di certificati attendibili prima di procedere con il token - senza token
4. Accedere a Publisher Cisco Unified Serviceability: Selezionare **Cisco Unified Serviceability > Tools > Control Center - Feature Services (Servizi unificati Cisco > Strumenti > Control Center - Servizi funzionalità)**.Iniziare con l'autore, quindi continuare con i sottoscrittori e riavviare il **servizio Cisco CallManager**, se attivo.
5. Passare a **Cisco Unified Serviceability > Strumenti > Control Center - Feature Services**
   Iniziare con il server di pubblicazione, quindi continuare con i sottoscrittori, riavviare il **servizio Cisco CTIManager** solo se attivo.
6. Selezionare **Cisco Unified Serviceability > Tools > Control Center - Network Services (Servizi di rete unificati Cisco > Strumenti > Control Center -Servizi di rete)**.
   Iniziare con il server di pubblicazione, quindi continuare con i sottoscrittori e riavviare il **servizio di verifica del trust Cisco**.
7. Selezionare **Cisco Unified Serviceability > Tools > Control Center - Feature Services (Servizi unificati Cisco > Strumenti > Control Center - Servizi funzionalità)**.

Iniziare con il server di pubblicazione, quindi continuare con i sottoscrittori, riavviare il **servizio Cisco TFTP** solo se attivo.

8. Riavvia tutti i telefoni: **Cisco Unified CM Amministrazione > Sistema > Parametri Enterprise**Selezionare **Reset** quindi viene visualizzata una schermata di popup con l'istruzione **You are about to reset all devices in the system. L'operazione non può essere annullata. Continuare?,** selezionare **OK** e quindi **Reset**

I telefoni sono stati ripristinati. Monitorare le azioni eseguite tramite lo strumento RTMT per verificare che il ripristino sia stato eseguito correttamente e che i dispositivi vengano registrati nuovamente in CUCM. Attendere il completamento della registrazione telefonica prima di procedere con il certificato successivo. Questo processo di registrazione dei telefoni può richiedere del tempo. Tenere presente che i dispositivi con ITL errati prima del processo di rigenerazione non si registrano nuovamente nel cluster finché non viene rimosso ITL.

Certificato TV

Avviso: Non rigenerare contemporaneamente i certificati CallManager.PEM e TVS.PEM. Ciò causa una mancata corrispondenza irreversibile con l'ITL installato sugli endpoint che richiedono la rimozione dell'ITL da TUTTI gli endpoint nel cluster.

Nota: TVS autentica i certificati per conto di Call Manager. Rigenerare il certificato per ultimo.

Passare a ogni server del cluster (in schede separate del browser Web) iniziando dal server di pubblicazione, quindi da ogni sottoscrittore. Passare a **Cisco Unified OS Administration > Security > Certificate Management > Find**:

- Selezionare il certificato **peer TVS**.
- Una volta aperto, selezionate **Rigenera (Regenerate)** e attendete fino a quando non viene visualizzata la finestra a comparsa Successo (Success), quindi chiudete la finestra a comparsa o tornate indietro e selezionate **Trova/Lista (Find/List)**.

1. Continuare con gli abbonati successivi; seguire la stessa procedura al passaggio 1 e completare in tutti i sottoscrittori del cluster. Dopo che tutti i nodi hanno rigenerato il certificato TVS, riavviare i servizi: Accedere a Publisher **Cisco Unified Serviceability**. Selezionare **Cisco Unified Serviceability > Tools > Control Center - Network Services (Servizi di rete unificati Cisco > Strumenti > Control Center -Servizi di rete)**.Nel server di pubblicazione selezionare **Riavvia** il **servizio di verifica dell'attendibilità Cisco**.Una volta completato il riavvio del servizio, continuare con i sottoscrittori e riavviare il **servizio di verifica del trust Cisco**.
2. Iniziare con il server di pubblicazione, quindi continuare con i sottoscrittori, riavviare il **servizio Cisco TFTP** solo se attivo.
3. Riavvia tutti i telefoni: **Amministrazione Cisco Unified CM > Sistema > Parametri Enterprise**.Selezionare **Reset** quindi viene visualizzata una schermata di popup con l'istruzione **You are about to reset all devices in the system. L'operazione non può essere annullata. Continuare?,** selezionare **OK** e quindi **Reset**.

I telefoni sono stati ripristinati. Monitorare le azioni eseguite tramite lo strumento RTMT per verificare che il ripristino sia stato eseguito correttamente e che i dispositivi vengano registrati nuovamente in CUCM. Attendere il completamento della registrazione telefonica prima di

procedere con il certificato successivo. Questo processo di registrazione dei telefoni può richiedere del tempo. Tenere presente che i dispositivi con ITL errati prima del processo di rigenerazione non si registrano nuovamente nel cluster finché non viene rimosso ITL.

Certificato di recupero ITLR

> **Nota:** Il certificato ITLRecovery viene utilizzato quando i dispositivi perdono lo stato di attendibilità. Il certificato viene visualizzato sia in ITL che in CTL (quando il provider CTL è attivo).
> Se i dispositivi perdono lo stato di attendibilità, è possibile utilizzare il comando **utils itl reset localkey** per i cluster non protetti e il comando **utils ctl reset localkey** per i cluster in modalità mista. Leggere la guida alla protezione per la versione di Call Manager in uso per acquisire familiarità con l'utilizzo del certificato ITLRecovery e con il processo richiesto per recuperare lo stato di attendibilità.
> Se il cluster è stato aggiornato a una versione che supporta una lunghezza di chiave pari a 2048 e i certificati del server cluster sono stati rigenerati a 2048 e ITLRecovery non è stato rigenerato ed è attualmente lungo 1024 chiavi, il comando ITL recovery ha esito negativo e il metodo ITLRecovery non è utilizzato.

1. Passare a ogni server del cluster (in schede separate del browser Web) iniziando dal server di pubblicazione, quindi da ogni sottoscrittore. Passare a **Cisco Unified OS Administration > Security > Certificate Management > Find (Amministrazione Cisco Unified SO > Sicurezza > Gestione certificati > Trova)**:
   Selezionare il certificato **ITLRecovery pem**.Una volta aperto, selezionate **Rigenera (Regenerate)** e attendete fino a quando non viene visualizzata la finestra a comparsa Successo (Success), quindi chiudete la finestra a comparsa o tornate indietro e selezionate **Trova/Lista (Find/List)**.
2. Continuare con gli abbonati successivi; seguire la stessa procedura al passaggio 2 e completare su tutti i sottoscrittori del cluster.
3. Dopo che tutti i nodi hanno rigenerato il certificato ITLRecovery, è necessario riavviare i servizi nell'ordine seguente: Se è attiva la modalità mista, aggiornare il CTL prima di procedere con Token - Token.Accedere a Publisher **Cisco Unified Serviceability**. Selezionare **Cisco Unified Serviceability > Tools > Control Center - Network Services (Servizi di rete unificati Cisco > Strumenti > Control Center -Servizi di rete)**.Nel server di pubblicazione selezionare **Riavvia** il **servizio di verifica dell'attendibilità Cisco**. Una volta completato il riavvio del servizio, continuare con i sottoscrittori e riavviare il **servizio di verifica del trust Cisco**.
4. Iniziare con il server di pubblicazione, quindi continuare con i sottoscrittori, riavviare il **servizio Cisco TFTP** solo se attivo.
5. Riavvia tutti i telefoni: **Cisco Unified CM Amministrazione > Sistema > Parametri Enterprise**Selezionare **Reset** quindi viene visualizzata una schermata di popup con l'istruzione **You are about to reset all devices in the system. L'operazione non può essere annullata. Continuare?,** selezionare **OK** e quindi **Reset**.
6. I telefoni caricano il nuovo ITL/CTL mentre vengono reimpostati.

Elimina certificati di attendibilità scaduti

Nota: Identificare i certificati di attendibilità da eliminare, non più necessari o scaduti. Non eliminare i cinque certificati di base che includono CallManager.pem, tomcat.pem, ipsec.pem, CAPF.pem e TVS.pem. Se necessario, è possibile eliminare i certificati di attendibilità. Il servizio successivo che viene riavviato è progettato per cancellare le informazioni sui certificati legacy all'interno di tali servizi.

1. Selezionare **Cisco Unified Serviceability > Tools > Control Center - Network Services (Servizi di rete unificati Cisco > Strumenti > Control Center -** Servizi di rete). Dal menu a discesa selezionare CUCM Publisher.Selezionare **Interrompi notifica di modifica certificato**.Ripetere l'operazione per ogni nodo Gestione chiamate del cluster.Se si dispone di un server IMP: Dal menu a discesa selezionare i server IMP uno alla volta e selezionare **Arresta Platform Administration Web Services e Cisco Intercluster Sync Agent**.
2. Passare a **Cisco Unified OS Administration > Security > Certificate Management > Find (Amministrazione Cisco Unified SO > Protezione > Gestione certificati > Trova)**. Trovare i certificati di attendibilità scaduti. Per le versioni 10.X e successive è possibile filtrare in base alla scadenza. Per le versioni precedenti alla 10.0 è necessario identificare i certificati specifici manualmente o tramite gli avvisi RTMT, se ricevuti.)Lo stesso certificato di trust può essere visualizzato in più nodi. Deve essere eliminato singolarmente da ogni nodo.Selezionare il certificato di attendibilità da eliminare (a seconda della versione in uso, è possibile visualizzare un popup o passare al certificato nella stessa pagina) Selezionare **Elimina**. (Viene visualizzata una schermata di popup che inizia con "si sta per eliminare definitivamente questo certificato".*)*Selezionare **OK**.
3. Ripetere la procedura per ogni certificato di attendibilità da eliminare.
4. Al completamento, è necessario riavviare i servizi direttamente correlati ai certificati eliminati. In questa sezione non è necessario riavviare i telefoni. Il Call Manager e il CAPF possono influire sull'endpoint. Tomcat-trust: riavviare il servizio Tomcat dalla riga di comando (vedere la sezione Tomcat)trust CAPF: riavviare la funzione proxy di Cisco Certificate Authority (vedere la sezione CAPF) Non riavviare gli endpoint.Trust CallManager: Servizio CallManager/CTIManager (vedere la sezione CallManager) Non riavviare gli endpoint. Impatto sugli endpoint e conseguente riavvio.Trust IPSEC: DRF Master/DRF Locale (vedere la sezione IPSEC).TVS (autofirmato) non dispone di certificati di attendibilità.
5. Riavviare i servizi precedentemente arrestati nel passaggio 1.

Verifica

Procedura di verifica non disponibile per questa configurazione.

Risoluzione dei problemi

Procedure di risoluzione dei problemi non disponibili per 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).