DOMANDE FREQUENTI PER CERTIFICATI TELEFONICI CUCM (LSC/MIC)

Sommario

Introduzione
Quali sono gli utilizzi comuni dei certificati telefonici?
Tra CAPF e telefono per l'installazione/aggiornamento, eliminazione o risoluzione dei problemi
Tra CallManager e Phone per la connessione Transport Layer Security (TLS)
Tra telefono e server di autenticazione per autenticazione 802.1x
Per l'autenticazione basata su certificati tra Phone e Cisco Adaptive Security Appliance (ASA) per VPN
Quando sono presenti LSC e MIC, è possibile selezionare in modo esplicito LSC o MIC per le connessioni?
Per quale motivo i telefoni LSC installati con profilo protetto non vengono registrati durante lo spostamento nel nuovo cluster?
È necessario installare LSC per i telefoni per registrarlo utilizzando il profilo autenticato o crittografato protetto?
È obbligatorio che la modalità di sicurezza del dispositivo nel rispettivo profilo di sicurezza del dispositivo sia autenticata o crittografata per installare/aggiornare/eliminare un LSC?
È obbligatorio che il cluster sia in modalità mista per installare LSC nel telefono?
Come verificare rapidamente se si verifica un problema con l'LSC utilizzato dal telefono?
Come ottenere i certificati telefonici per la risoluzione dei problemi?
Come verificare dalle acquisizioni dei pacchetti se si usa LSC o MIC del telefono per stabilire la connessione TLS con CallManager?
Qual è il significato della modalità di autenticazione nelle informazioni CAPF (Certification Authority Proxy Function)? Ha qualche significato per la connessione TLS tra CUCM e Phone?
Quali sono le operazioni LSC di base per i telefoni da prendere in considerazione dopo la rigenerazione del certificato CAPF?
Connessione TLS con CallManager
Operazioni LSC con CAPF-Trust
Tra telefono e server di autenticazione per autenticazione 802.1x
Tra ASA e telefono
Informazioni correlate

Introduzione

Questo documento copre alcune delle domande e delle risposte relative ai certificati telefonici per Cisco Unified Communications Manager (CUCM). Di seguito è riportata una breve panoramica dei certificati telefonici.

Certificato di installazione produttore (MIC):

Come indica il nome, i telefoni sono preinstallati con il MIC e non possono essere eliminati/modificati dagli amministratori. I certificati dell'autorità di certificazione (CA) CAP-RTP-001, CAP-RTP-002, Cisco_Manufacturing_CA e Cisco Manufacturing CA SHA2 sono preinstallati

in CUCM per considerare attendibile il MIC. Non è possibile utilizzare il MIC una volta scaduta la validità in quanto non è possibile rigenerare il CA MIC,

LSC (Locally Significant Certificate):

L'LSC possiede la chiave pubblica per il telefono IP Cisco, firmata dalla chiave privata Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF). Per impostazione predefinita, non è installato nel telefono. L'amministratore ha il controllo completo su LSC. Il certificato CA CAPF può essere rigenerato a sua volta può rilasciare nuove LSC ai telefoni ogni volta che è necessario.

Quali sono gli utilizzi comuni dei certificati telefonici?

Di seguito sono elencati alcuni utilizzi comuni dei certificati telefonici

Tra CAPF e telefono per l'installazione/aggiornamento, eliminazione o risoluzione dei problemi

Il telefono stabilisce la connessione con CAPF per installare/aggiornare, eliminare o risolvere i problemi del certificato sul telefono. Il certificato telefonico viene utilizzato per stabilire la connessione con CAPF quando la modalità di autenticazione è impostata su Informazioni sulla funzione proxy dell'autorità di certificazione (CAPF) impostate su Per certificato esistente (precedenza a LSC) o Per certificato esistente (precedenza a MIC).

Per certificato esistente (precedenza a LSC): Il telefono usa LSC per autenticarsi con CAPF. Se LSC non è installato, verrà utilizzato MIC. L'installazione non riesce con il motivo "LSC non valido" in caso di problemi con il certificato utilizzato. Ad esempio, la CA firmata per l'LSC non è disponibile nel trust CAPF. Aggiornare la modalità di autenticazione utilizzando un altro metodo di certificato o una stringa null per tali casi di errore.

Per certificato esistente (precedenza a MIC): Il telefono usa il MIC per l'autenticazione con CAPF.

Tra CallManager e Phone per la connessione Transport Layer Security (TLS)

Il telefono usa LSC o MIC per stabilire la connessione TLS con CallManager. CallManager convalida il certificato presentato dal telefono verificando CallManager-trust. Il relativo certificato CAPF deve essere disponibile in CallManager-trust per LSC e Cisco Manufacture CA per MIC.

Tra telefono e server di autenticazione per autenticazione 802.1x

I certificati CAPF/CA di produzione vengono caricati in server di autenticazione come Cisco Secure Access Control Server (ACS) o Identity Services Engine (ISE). Il server di autenticazione utilizza i certificati caricati per autenticare il telefono quando presenta il proprio certificato (LSC o MIC).

Per l'autenticazione basata su certificati tra Phone e Cisco Adaptive Security Appliance (ASA) per VPN

I certificati CAPF/CA di produzione vengono caricati nell'appliance ASA e vengono convalidati dall'appliance ASA quando il telefono presenta il dispositivo LIC/MIC.

Quando sono presenti LSC e MIC, è possibile selezionare in modo esplicito LSC o MIC per le connessioni?

Nessuna opzione per selezionare se utilizzare LSC o MIC per le connessioni. Se è installato LSC, il telefono usa LSC. Il telefono usa il microfono se LSC non è installato.

Voce della console quando LSC non è presente:

SECONDO: -PXY_NO_LSC: Nessun LSC per [SCCP]. Verrà eseguito un tentativo con MIC

Voce della console quando è presente LSC:

SECONDO: -PXY_CERT_CIPHER: [SCCP], [TLSv1], cert [LSC]

La selezione di LSC o MIC è possibile solo tra CAPF e Phone installazione/aggiornamento, eliminazione o risoluzione dei problemi.

Per quale motivo i telefoni LSC installati con profilo protetto non vengono registrati durante lo spostamento nel nuovo cluster?

Ciò può accadere per i telefoni che dispongono già di una scheda LSC da VECCHIO cluster. Se sono presenti sia MIC che LSC, LSC viene utilizzato per stabilire la connessione TLS. Impossibile stabilire TLS. Il nuovo CUCM non dispone della CA per questo LSC nel trust CallManager-.

Nei log della console viene visualizzato il certificato utilizzato per stabilire il TLS. La voce seguente mostra l'utilizzo di LSC.

3469 NON 00:01:31.935298 SECONDI: -PXY_CERT_CIPHER: [SCCP], [TLSv1], cert [LSC], cifratura [AES256-SHA:AES128-SHA]

SSL3_Alert con "CA sconosciuta" per casi non riusciti nei log della console:-

3486 ERR 00:01:31,938954 SECD: -STATE_SSL3_ALERT: Avviso SSL3 [lettura]:[errore irreversibile]:[CA sconosciuta

Per risolvere il problema, è possibile registrare il telefono utilizzando un profilo non protetto ed eliminare la scheda LSC esistente. Installare LSC dal nuovo cluster, quindi registrare il telefono utilizzando il profilo protetto. È inoltre possibile registrare il telefono con profilo protetto utilizzando il microfono senza installare LSC.

Ènecessario installare LSC per i telefoni per registrarlo utilizzando il profilo autenticato o crittografato protetto?

No. Se LSC non è installato, Phone utilizza MIC per stabilire la connessione TLS a CUCM.

4878 WRN 15:47:34,756063 SECD: -PXY_NO_LSC: Nessun LSC per [SCCP], prova MIC.

Èobbligatorio che la modalità di sicurezza del dispositivo nel rispettivo profilo di sicurezza del dispositivo sia autenticata o crittografata per installare/aggiornare/eliminare un LSC?

Non è obbligatorio, può essere fatto utilizzando il profilo standard predefinito Non-Secure anche dove in modalità di sicurezza del dispositivo non è sicuro.

Èobbligatorio che il cluster sia in modalità mista per installare LSC nel telefono?

Non è obbligatorio. È possibile eseguire l'installazione o l'eliminazione di LSC anche quando la modalità di protezione del cluster non è protetta.

Come verificare rapidamente se si verifica un problema con l'LSC utilizzato dal telefono?

Eliminare l'LSC in uno del telefono andando alla pagina Phone Admin. In questo modo il telefono deve utilizzare il microfono. Se tutto funziona correttamente con MIC, procedere alla risoluzione dei problemi con LSC.

Come ottenere i certificati telefonici per la risoluzione dei problemi?

Impostare Operazione certificato su Risoluzione dei problemi nella periferica o nel telefono. Selezionare Save (Salva), quindi Apply Config (Applica configurazione). Attendere per visualizzare lo stato dell'operazione certificato per **risolvere i problemi**. Raccogliere i log delle **funzioni proxy di Cisco Certificate Authority** da Real Time Monitoring Tool (RTMT). Contiene i certificati del telefono.

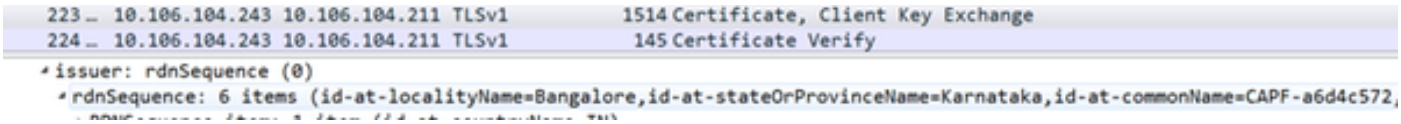
Come verificare dalle acquisizioni dei pacchetti se si usa LSC o MIC del telefono per stabilire la connessione TLS con CallManager?

Raccogliere le acquisizioni di pacchetti che coprono il riavvio del telefono.

Controllare il certificato, il messaggio di scambio chiave client. Verificare il certificato inviato dal telefono IP.

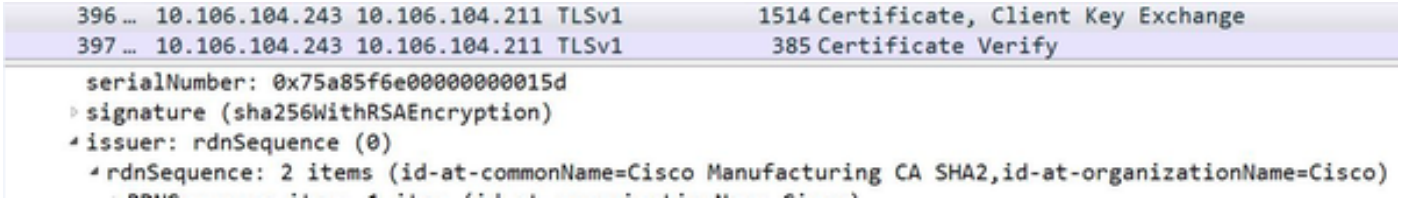
Esempio di LSC:

Per il sistema LSC, la sigla CAPF CN viene visualizzata nel campo issuer (emittente). La radice CAPF corrispondente deve essere presente in CallManager-trust.



Esempio di MIC:

Per il MIC, Cisco Manufacturing CA nel campo dell'emittente. La CA radice corrispondente deve essere presente in CallManager-trust.



Qual è il significato della modalità di autenticazione nelle informazioni CAPF (Certification Authority Proxy Function)? Ha qualche significato per la connessione TLS tra CUCM e Phone?

Non è altro che un metodo di autenticazione tra Phone e CAPF per l'installazione/aggiornamento/eliminazione e le operazioni di risoluzione dei problemi. Non ha alcun significato per la connessione TLS tra CUCM e Phone.

Quali sono le operazioni LSC di base per i telefoni da prendere in considerazione dopo la rigenerazione del certificato CAPF?

In questa sezione viene descritto lo scenario di inattività in cui non viene utilizzata alcuna CA offline per emettere il certificato LSC.

Connessione TLS con CallManager

Prima di eliminare il certificato CAPF precedente da CallManager-trust, accertarsi di installare il nuovo LSC sul telefono. L'eliminazione del precedente certificato CAPF seguita dal riavvio del servizio CallManager causa problemi di registrazione ai telefoni in cui è stato rilasciato il certificato CAPF.

Operazioni LSC con CAPF-Trust

Prima di eliminare il certificato CAPF precedente da CAPF-trust, accertarsi di installare il nuovo LSC nel telefono. Operazioni LSC come installazione/eliminazione utilizzando la modalità di autenticazione **da certificato esistente (precedenza a LSC)** non riescono con l'errore **LSC non valido** per i telefoni che hanno LSC rilasciato da questo certificato CAPF.

Tra telefono e server di autenticazione per autenticazione 802.1x

Assicurarsi di non eliminare il certificato CAPF precedente dal server di autenticazione fino a quando il nuovo certificato CAPF non viene caricato e Phone non ottiene il LSC rilasciato dal nuovo CAPF.

Tra ASA e telefono

Accertarsi di non eliminare il certificato CAPF precedente dall'appliance ASA finché il telefono non riceve il nuovo LSC e non carica il nuovo certificato CAPF CA nell'appliance ASA.

Per ulteriori informazioni sulla rigenerazione del certificato CAPF, fare riferimento a Rigenerazione certificato.

Informazioni correlate

- Certificati per telefoni IP e comunicazioni sicure Cisco
- Guida alla progettazione di IP Telephony per 802.1X
- Guida alla sicurezza di Cisco Unified Communications Manager