Q.A para CERTIFICADOS TELEFÓNICOS CUCM (LSC/MIC)

Contenido

Introducción

Este documento trata algunas de las preguntas y respuestas de los certificados telefónicos de Cisco Unified Communications Manager (CUCM). A continuación se muestra una vista rápida de los certificados telefónicos.

Certificado instalado por el fabricante (MIC):

Como indica el nombre, los teléfonos están preinstalados con el MIC y los administradores no pueden eliminarlo ni modificarlo. Los certificados de la autoridad certificadora (CA) CAP-RTP-001,

CAP-RTP-002, Cisco_Manufacturing_CA y Cisco Manufacturing CA SHA2 están preinstalados en CUCM para confiar en el MIC. El MIC no se puede utilizar una vez que la validez ha caducado, ya que la CA MIC no se puede volver a generar.

Certificado de importancia local (LSC):

El LSC posee la clave pública del teléfono IP de Cisco, que está firmado por la clave privada de la función de proxy de autoridad de certificados (CAPF) de Cisco Unified Communications Manager. No está instalado en el teléfono de forma predeterminada. El administrador tiene control total sobre LSC. El certificado CA de CAPF se puede regenerar, a su vez, puede emitir un nuevo LSC a los teléfonos cuando sea necesario.

¿Cuáles son los usos comunes para los certificados telefónicos?

Estos son algunos de los usos comunes para los certificados telefónicos

Entre CAPF y el teléfono para instalar/actualizar, eliminar o solucionar problemas

El teléfono establece la conexión con CAPF para instalar/actualizar, eliminar o solucionar problemas de certificado en el teléfono. El certificado de teléfono se utiliza para establecer la conexión con CAPF cuando el modo de autenticación se encuentra en Certification Authority Proxy Function (CAPF) Information establecida en By Existing Certificate (Precedence to LSC) o By Existing Certificate (Precedence to MIC).

Por certificado existente (precedencia a LSC): el teléfono utiliza LSC para autenticarse con CAPF. Utilizará MIC si LSC no está instalado. La instalación falla por el motivo "LSC no válido" si hay problemas con el certificado usado. Por ejemplo, la CA firmada para el LSC no está disponible en la CAPF Trust. Actualice el modo de autenticación mediante otro método de certificado o mediante cadena nula para esos casos de error.

Por certificado existente (precedencia a MIC): El teléfono utiliza MIC para autenticarse con CAPF.

Entre CallManager y la conexión de Seguridad de la Capa de Transporte (TLS)

El teléfono utiliza LSC o MIC para establecer la conexión TLS con CallManager. CallManager validará el certificado presentado por el teléfono al marcar CallManager-trust. El certificado CAPF correspondiente debe estar disponible en CallManager-trust para LSC y CA de fabricación de Cisco para MIC.

Entre el teléfono y el servidor de autenticación para autenticación 802.1x

Los certificados de CA CAPF/Manufacturing se cargan en servidores de autenticación como Cisco Secure Access Control Server (ACS) o Identity Services Engine (ISE). El servidor de autenticación utiliza los certificados cargados para autenticar el teléfono cuando presenta su certificado (LSC o MIC).

Para autenticación basada en certificados entre el teléfono y Cisco Adaptive

Security Appliance (ASA) para VPN

Los certificados de CA CAPF/Fabricación se cargan en ASA, cuando el teléfono presente LIC/MIC, ASA los valida comprobando su confianza.

Cuando LSC y MIC están presentes, ¿hay alguna manera de seleccionar LSC o MIC explícitamente para conexiones?

No hay opción para seleccionar si LSC o MIC para las conexiones. Si se instala LSC, el teléfono utiliza LSC. El teléfono utiliza el MIC si LSC no está instalado .

Entrada de consola cuando LSC no está presente:

SECD: -PXY_NO_LSC: No hay LSC para [SCCP], probará MIC

Entrada de consola cuando LSC está presente:

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

La selección de LSC o MIC sólo es posible entre CAPF y el teléfono instalando/actualizando, eliminando o solucionando problemas.

¿Por qué los teléfonos instalados LSC con perfil seguro no se registran al cambiar al nuevo clúster?

Esto puede suceder para los teléfonos que ya tienen un LSC de un clúster antiguo. Cuando están presentes MIC y LSC, se utiliza LSC para establecer la conexión TLS. No se puede establecer TLS porque el nuevo CUCM no tiene la CA para este LSC en su CallManager- trust.

Los registros de la consola muestran qué certificado se utiliza para establecer la TLS. Debajo de la entrada se muestra que se utiliza LSC.

3469 NO 00:01:31.935298 SECD: -PXY_CERT_CIPHER: [SCCP], [TLSv1], cert [LSC], cifra [AES256-SHA:AES128-SHA]

SSL3_Alert con "CA desconocida" para estos casos fallidos en los registros de la consola :-

3486 ERR 00:01:31.938954 SECD: -STATE_SSL3_ALERT: Alerta SSL3 [lectura]:[fatal]:[CA desconocida

Una de las maneras de resolver este problema es registrar el teléfono usando un perfil no seguro y eliminar el LSC existente. Instale el LSC del nuevo clúster y, a continuación, registre el teléfono mediante el perfil seguro. También es posible registrar el teléfono con el perfil seguro mediante MIC sin instalar el LSC.

¿Es necesario tener instalado el LSC para que los teléfonos lo registren usando un perfil seguro autenticado o cifrado?

No. Si LSC no está instalado, el teléfono utiliza MIC para establecer la conexión TLS con CUCM.

4878 WRN 15:47:34.756063 SECD: -PXY_NO_LSC: No hay LSC para [SCCP], prueba MIC.

¿Es obligatorio que el modo de seguridad del dispositivo en el perfil de seguridad del dispositivo respectivo sea autenticado o cifrado para instalar/actualizar/eliminar un LSC?

No es obligatorio, se puede realizar utilizando el perfil no seguro estándar predeterminado también cuando el modo de seguridad del dispositivo no es seguro.

¿Es obligatorio que el clúster se encuentre en modo mixto para instalar el LSC en el teléfono?

No es obligatorio. La instalación/eliminación de LSC se puede realizar incluso cuando el modo de seguridad del clúster no es seguro.

¿Cómo se puede probar rápidamente si hay un problema con el LSC que utiliza el teléfono?

Para eliminar el LSC en uno de los teléfonos, vaya a la página Phone Admin. Esto obliga al teléfono a utilizar MIC. Si todo está bien con MIC, proceda a la resolución de problemas con LSC.

¿Cómo obtener los certificados telefónicos para la resolución de problemas?

Configure la Operación del Certificado para Resolver Problemas en el Dispositivo/Teléfono. Pulse Guardar y, a continuación, Aplicar configuración. Espere para ver el estado de la operación del certificado para **solucionar problemas exitosos**. Recopile registros de **funciones proxy de Cisco Certificate Authority** de Real Time Monitoring Tool (RTMT). Contiene los certificados del teléfono.

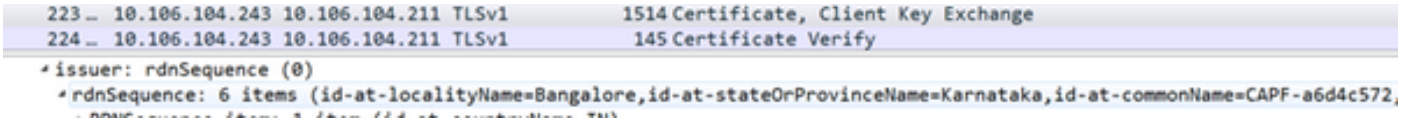
¿Cómo se verifica a partir de capturas de paquetes, si se utiliza LSC o MIC del teléfono para establecer la conexión TLS con CallManager?

Recopile las capturas de paquetes que cubren el reinicio del teléfono.

Verifique el mensaje de intercambio de certificado, clave de cliente. Verifique el certificado enviado desde el teléfono IP.

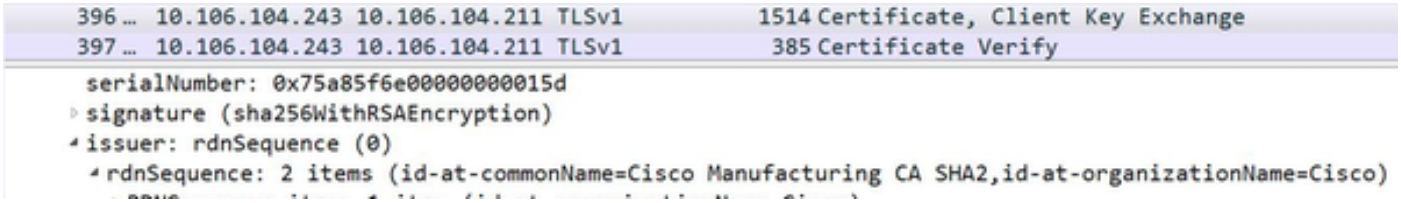
Ejemplo de LSC:

Para el LSC, CAPF CN se ve en el campo emisor. La raíz CAPF correspondiente debe estar presente en CallManager-trust.



Ejemplo de MIC:

Para el MIC, CA de Cisco Manufacturing en el campo emisor. La CA raíz correspondiente debe estar presente en CallManager-trust.



¿Cuál es la importancia del modo de autenticación en la información de la función de proxy de la autoridad de certificación (CAPF)? ¿Tiene algún significado para la conexión TLS entre CUCM y el teléfono?

No es más que un método de autenticación entre el teléfono y CAPF para instalar/actualizar/eliminar y solucionar problemas de operaciones. No tiene ningún significado para la conexión TLS entre CUCM y el teléfono.

¿Cuáles son las operaciones básicas de LSC que deben tener en cuenta los teléfonos después de la regeneración del certificado CAPF?

Esta sección cubre el escenario inactivo donde no se utiliza ninguna CA sin conexión para ejecutar el LSC.

Conexión TLS con CallManager

Asegúrese de instalar el nuevo LSC en el teléfono antes de eliminar el certificado CAPF anterior de CallManager-trust. La eliminación del certificado CAPF anterior seguida de un reinicio del servicio CallManager causa los problemas de registro en los teléfonos que tienen el LSC emitido por este certificado CAPF.

Operaciones LSC con CAPF-Trust

Asegúrese de instalar el nuevo LSC en el teléfono antes de eliminar el certificado CAPF anterior de CAPF-trust. Las operaciones LSC como la instalación/eliminación usando el modo de autenticación **por el certificado existente (Precedencia a LSC)** fallan con el error **LSC no válido** para los teléfonos que tienen el LSC emitido por este certificado CAPF.

Entre el teléfono y el servidor de autenticación para autenticación 802.1x

Asegúrese de no eliminar el certificado CAPF anterior del servidor de autenticación hasta que el nuevo certificado CAPF cargado y el teléfono reciba el LSC emitido por el nuevo CAPF.

Entre ASA y el teléfono

Asegúrese de no eliminar el certificado CAPF anterior del ASA hasta que el teléfono obtenga el nuevo LSC y cargue el nuevo certificado CAPF CA en ASA.

Consulte Regeneración de Certificados para ver los pasos que se deben seguir para regenerar el Certificado CAPF.

Información Relacionada

- Certificados de teléfono IP de Cisco y comunicaciones seguras
- Guía de diseño de telefonía IP para 802.1X
- Guía de seguridad de Cisco Unified Communications Manager