Regenere certificados autofirmados del servicio CUCM IM/P

Contenido

Introducción

Este documento describe un procedimiento paso a paso recomendado sobre cómo regenerar certificados en CUCM IM/P 8.x y versiones posteriores.

Prerequisites

Requirements

Cisco recomienda que conozca los certificados del servicio IM & Presence (IM/P).

Componentes Utilizados

La información de este documento se basa en la versión 8.x y posteriores de IM/P.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos

que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Utilización del almacén de certificados

Certificado de Cisco Unified Presence (CUP)

Se utiliza para conexiones SIP seguras para la federación de SIP, control remoto de llamadas de Microsoft para Lync/OCS/LCS, conexión segura entre Cisco Unified Certificate Manager (CUCM) e IM/P, etc.

Cisco Unified Presence - Certificado de protocolo extensible de mensajería y presencia (CUP-XMPP)

Se utiliza para validar conexiones seguras para clientes XMPP cuando se crea una sesión XMPP.

Cisco Unified Presence - Protocolo extensible de mensajería y presencia - Certificado de servidor a servidor (CUP-XMPP-S2S)

Se utiliza para validar conexiones seguras para federaciones de interdominios XMPP con un sistema XMPP federado externamente.

Certificado de seguridad IP (IPSec)

Se utiliza para:
· Validar una conexión segura para el Sistema de recuperación ante desastres (DRS)/Marco de recuperación ante desastres (DRF)
· Validar una conexión segura para túneles IPsec con Cisco Unified Communications Manager (CUCM) y nodos IM/P del clúster

Certificado Tomcat

Se utiliza para:

· Validar varios accesos web como el acceso a páginas de servicio desde otros nodos del clúster y Jabber Access.
· Validar una conexión segura para el inicio de sesión único (SSO) de SAML.

· Validar conexión segura para Peer Intercluster.

Precaución: si utiliza la función SSO en los servidores de Unified Communication y se vuelven a generar los certificados de Cisco Tomcat, el SSO se debe volver a configurar con los nuevos certificados. El enlace para configurar SSO en CUCM y ADFS 2.0 es: 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: el enlace al proceso de regeneración/renovación de certificados de CUCM es: https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html.

Proceso de regeneración de certificados

Certificado CUP

Paso 1. Abra una interfaz gráfica de usuario (GUI) para cada servidor del clúster. Comience con el editor de IM/P, abra una GUI para cada servidor de suscriptor de IM/P y navegue hasta Cisco Unified OS Administration > Security > Certificate Management.

Paso 2. Comience con la GUI del editor y elija Find mostrar todos los certificados. Elija el cup.pem certificado. Una vez abierta, elija Regenerate y espere hasta que se vea que la operación se ha realizado correctamente antes de que se cierre la ventana emergente.

Paso 3. Continúe con los suscriptores subsiguientes, consulte el mismo procedimiento que en el Paso 2. y complete todos los suscriptores de su clúster.

Paso 4. Después de regenerar el certificado CUP en todos los nodos, se deben reiniciar los servicios.

Nota: si la configuración del grupo de redundancia de presencia tiene activada la opción Activar alta disponibilidad, Uncheck deberá activarla antes de reiniciar los servicios. Se puede acceder a la configuración del grupo de redundancia de presencia en CUCM Pub Administration > System > Presence Redundancy Group. Un reinicio de los servicios provoca una interrupción temporal de IM/P y debe realizarse fuera de las horas de producción.

Reinicie los servicios en este orden:

· Inicie sesión en Serviciabilidad de Cisco Unified del editor:

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

b. Servicio de proxy SIP de Restart Cisco.

c. Una vez que se complete el reinicio del servicio, continúe con los suscriptores y el Restart servicio Cisco SIP Proxy.

d. Comience con el editor y luego continúe con los suscriptores. Restart Servicio Cisco SIP Proxy (también, desdeCisco Unified Serviceability > Tools > Control Center - Feature Services).

· Inicie sesión en Serviciabilidad de Cisco Unified del editor:

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

b. Restart Servicio Cisco Presence Engine.

c. Una vez finalizado el reinicio del servicio, continúe con Restart el servicio de Cisco Presence Engine en los suscriptores.

Nota: si se configura para la federación de SIP, Restart el servicio Cisco XCP SIP Federation Connection Manager (ubicado en Cisco Unified Serviceability > Tools > Control Center - Feature Services). Empiece con el editor y continúe con los suscriptores.

Certificado CUP-XMPP

Nota: Puesto que Jabber utiliza los certificados de servidor CUCM y IM/P Tomcat y CUP-XMPP para validar las conexiones de Tomcat y los servicios CUP-XMPP, estos certificados CUCM e IM/P suelen estar firmados por CA. Suponga que el dispositivo Jabber no tiene la raíz y un certificado intermedio que forma parte del certificado CUP-XMPP instalado en su almacén de confianza de

---

certificados; en ese caso, el cliente Jabber muestra una ventana emergente de advertencia de seguridad para el certificado no fiable. Si aún no está instalado en el certificado del almacén de confianza del dispositivo Jabber, la raíz y cualquier certificado intermedio deben enviarse al dispositivo Jabber a través de la política de grupo, MDM, correo electrónico, etc., que depende del cliente Jabber.

Nota: Si el certificado CUP-XMMP tiene firma propia, el cliente Jabber muestra una ventana emergente de advertencia de seguridad para el certificado no fiable si el certificado CUP-XMPP no está instalado en el almacén de confianza del certificado del dispositivo Jabber. Si aún no está instalado, el certificado CUP-XMPP autofirmado debe enviarse al dispositivo Jabber a través de la política de grupo, MDM, correo electrónico, etc., que depende del cliente Jabber.

Paso 1. Abra una GUI para cada servidor del clúster. Comience con el editor de IM/P, luego abra una GUI para cada servidor de suscriptor de IM/P y navegue hasta **Cisco Unified OS Administration > Security > Certificate Management**.

Paso 2. Comience con la GUI del editor y elija Find mostrar todos los certificados. En la columna de tipo del cup-xmpp.pem certificado, determine si está firmado por sí mismo o por la CA. Si el cup-xmpp.pem certificado es una distribución de varias redes SAN firmada por terceros (tipo CA-signed), revise este enlace cuando genere una CSR CUP-XMPP de varias redes SAN y envíe a CA un certificado CUP-XMPP firmado por CA; Ejemplo de Configuración de Unified Communication Cluster con CA-Signed Multi-Server Subject Alternate Name Configuration.

Si el cup-xmpp.pem certificado es un nodo único de distribución firmado por terceros (tipo firmado por CA) (el nombre de distribución es igual al nombre común del certificado), revise este enlace cuando genere un CUP-XMPP CSR de nodo único y envíe a CA el certificado CUP-XMPP firmado por CA; Guía de uso de Jabber Complete para la validación de certificados. Si el cup-xmpp.pem certificado está autofirmado, vaya al paso 3.

Paso 3. Elija Find para mostrar todos los certificados y luego elija el cup-xmpp.pem certificado. Una vez abierta, elija Regenerate y espere hasta que se vea que la operación se ha realizado correctamente antes de que se cierre la ventana emergente.

Paso 4. Continúe con los suscriptores subsiguientes; consulte el mismo procedimiento en el paso 2 y complete el procedimiento para todos los suscriptores de su clúster.

Paso 5. Después de regenerar el certificado CUP-XMPP en todos los nodos, se debe reiniciar el servicio del router Cisco XCP en los nodos IM/P.

Nota: si la configuración del grupo de redundancia de presencia tiene activada la opción Activar alta disponibilidad, Uncheck hágalo antes de reiniciar el servicio. Se puede acceder a la configuración del grupo de redundancia de presencia en CUCM Pub Administration > System > Presence Redundancy Group. Un reinicio del servicio provoca una interrupción temporal de IM/P y debe realizarse fuera de las horas de producción.

· Inicie sesión en Serviciabilidad de Cisco Unified del editor:

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

b. Restart el servicio de router Cisco XCP.

c. Una vez que se complete el reinicio del servicio, continúe con el Restart servicio de router Cisco XCP en los suscriptores.

Certificado CUP-XMPP-S2S

Paso 1. Abra una GUI para cada servidor del clúster. Comience con el editor de IM/P, luego abra una GUI para cada servidor de suscriptor de IM/P y navegue hasta Cisco Unified OS Administration > Security > Certificate Management.

Paso 2. Comience con la GUI del editor, elija Find mostrar todos los certificados y elija el cup-xmpp-s2s.pem certificado. Una vez abierta, elija Regenerate y espere hasta que se vea que la operación se ha realizado correctamente antes de que se cierre la ventana emergente.

Paso 3. Continúe con los suscriptores subsiguientes y consulte el mismo procedimiento en el Paso 2, y complete para todos los suscriptores de su clúster.

Paso 4. Después de regenerar el certificado CUP-XMPP-S2S en todos los nodos, los servicios deben reiniciarse en el orden mencionado.

Nota: si la configuración del grupo de redundancia de presencia tiene activada la opción Activar alta disponibilidad,Uncheck hágalo antes de reiniciar estos servicios. Se puede acceder a la configuración del grupo de redundancia de presencia en CUCM Pub Administration > System > Presence Redundancy Group. Un reinicio de los servicios provoca una interrupción temporal de IM/P y debe realizarse fuera de las horas de producción.

· Inicie sesión en Serviciabilidad de Cisco Unified del editor:

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.
b. Restart el servicio de router Cisco XCP.
c. Una vez que se complete el reinicio del servicio, continúe con Restart del servicio de router Cisco XCP en los suscriptores.

· Inicie sesión en Serviciabilidad de Cisco Unified del editor:

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

b. Restart el servicio Administrador de conexiones de federación XMPP de Cisco.

c. Una vez que se complete el reinicio del servicio, continúe con Restart del servicio Cisco XCP XMPP Federation Connection Manager en los suscriptores.

Certificado IPSec

Nota: el ipsec.pem certificado del editor de CUCM debe ser válido y estar presente en todos los suscriptores (nodos CUCM e IM/P) del almacén de confianza IPSec. El ipsec.pem certificado del suscriptor no está presente en el editor como almacén de confianza IPSec en una implementación estándar. Para verificar la validez, compare los números de serie del ipsec.pem certificado de CUCM-PUB con la confianza IPSec en los suscriptores. Deben coincidir.

Nota: El DRS utiliza una comunicación basada en Secure Socket Layer (SSL) entre el agente de origen y el agente local para la autenticación y el cifrado de datos entre los nodos de clúster de CUCM (nodos de CUCM e IM/P). DRS utiliza los certificados IPSec para el cifrado de clave pública/privada. Tenga en cuenta que si elimina el archivo de almacén de confianza (hostname.pem) IPSEC de la página Administración de certificados, DRS no funcionará como se espera. Si elimina el archivo de confianza IPSEC manualmente, debe asegurarse de cargar el certificado IPSEC en el almacén de confianza IPSEC. Para obtener más información, consulte la página de ayuda de administración de certificados en las guías de seguridad de CUCM.

Paso 1. Abra una GUI para cada servidor del clúster. Comience con el editor de IM/P, luego abra una GUI para cada servidor de suscriptor de IM/P y navegue hasta Cisco Unified OS Administration > Security > Certificate Management.

Paso 2. Comience con la GUI del editor y elija Find mostrar todos los certificados.Choose el ipsec.pem certificado. Una vez abierta, elija Regenerate y espere hasta que se vea que la operación se ha realizado correctamente antes de que se cierre la ventana emergente.

Paso 3. Continúe con los suscriptores subsiguientes y consulte el mismo procedimiento en el Paso 2, y complete para todos los suscriptores de su clúster.

Paso 4. Después de que todos los nodos hayan regenerado el certificado IPSEC, Restart estos servicios. Vaya a Serviciabilidad de Cisco Unified del editor; Cisco Unified Serviceability > Tools > Control Center - Network Services.
a. Elija Restart en el servicio principal de Cisco DRF.
b. Una vez finalizado el reinicio del servicio, seleccione Restart el servicio local de Cisco DRF en el editor y, a continuación, continúe con Restart el servicio local de Cisco DRF en cada suscriptor.

Certificado Tomcat

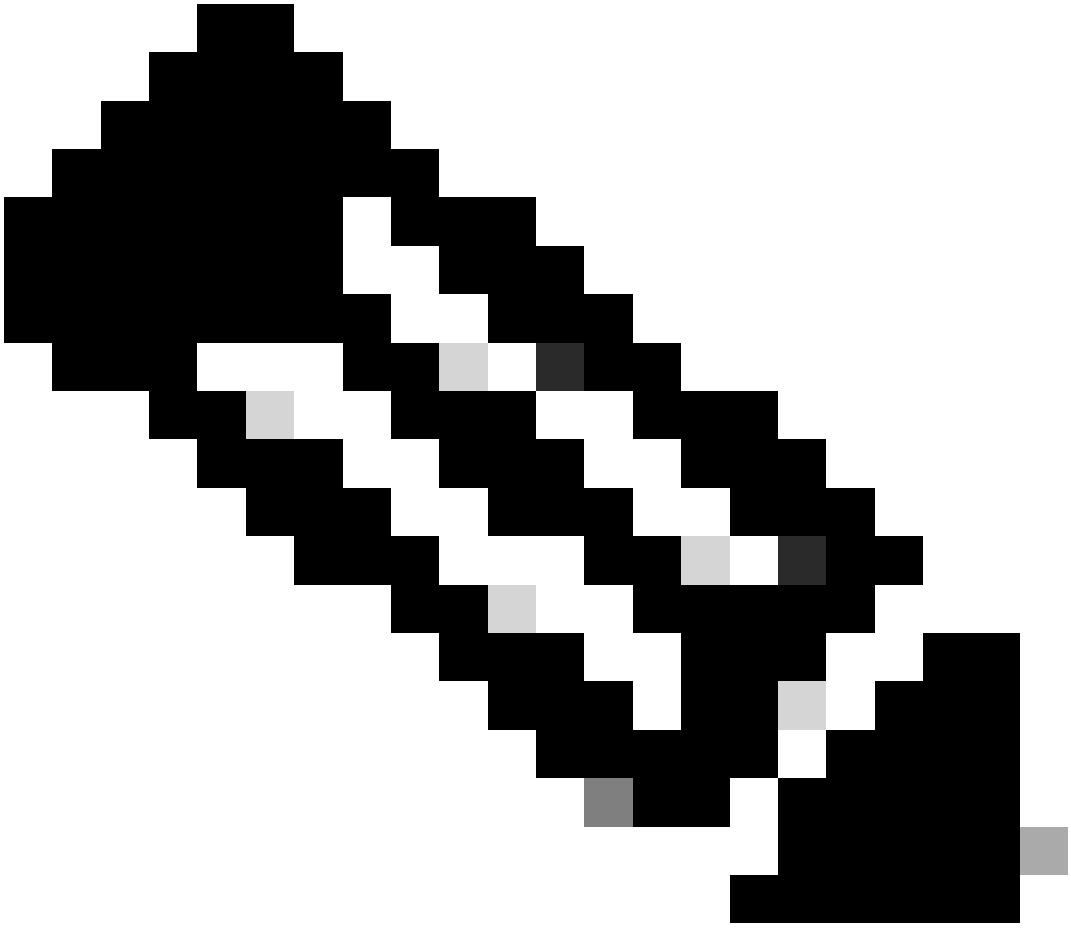
Nota: puesto que Jabber utiliza los certificados de servidor Tomcat y Tomcat IM/P y CUP-XMPP de CUCM para validar las conexiones de los servicios Tomcat y CUP-XMPP, estos certificados CUCM e IM/P suelen estar firmados por CA. Suponga que el dispositivo Jabber no tiene la raíz ni ningún certificado intermedio que forme parte del certificado Tomcat instalado en su almacén de confianza de certificados. En ese caso, el cliente Jabber muestra una ventana emergente de advertencia de seguridad para el certificado no confiable. Si aún no está instalado en el almacén de confianza de certificados del dispositivo Jabber, la raíz y cualquier certificado intermedio deben enviarse al dispositivo Jabber a través de la política de grupo, MDM, correo electrónico, etc., que depende del cliente Jabber.

Nota: Si el certificado Tomcat está autofirmado, el cliente Jabber muestra una ventana emergente de advertencia de seguridad para el certificado no fiable, si el certificado Tomcat no está instalado en el almacén de confianza de certificados del dispositivo Jabber. Si aún no está instalado en el almacén de confianza de certificados del dispositivo Jabber, el certificado CUP-XMPP autofirmado debe enviarse al dispositivo Jabber a través de la política de grupo, MDM, correo electrónico, etc., que depende del cliente Jabber.

Paso 1. Abra una GUI para cada servidor del clúster. Comience con el editor de IM/P, luego abra una GUI para cada servidor de suscriptor de IM/P y navegue hasta Cisco Unified OS Administration > Security > Certificate Management.

Paso 2. Comience con la GUI del editor y elija Find mostrar todos los certificados.
· En la columna Tipo del tomcat.pem certificado, determine si está autofirmado o firmado por CA.

· Si el tomcat.pem certificado es una distribución de varias redes SAN firmada por terceros (tipo CA-signed), revise este enlace sobre cómo generar una CSR Tomcat de varias redes SAN y enviar a CA un certificado Tomcat firmado por CA, Ejemplo de Configuración de Unified Communication Cluster con Nombre Alternativo de Asunto de Varios Servidores Firmado por CA



Nota: el CSR de Tomcat de varias SAN se genera en el editor de CUCM y se distribuye a todos los nodos de CUCM e IM/P del clúster.

· Si el tomcat.pem certificado es un nodo único de distribución firmado por terceros (tipo firmado por CA) (el nombre de distribución es igual al nombre común del certificado), revise este enlace para generar un CSR CUP-XMPP de nodo único y envíelo a CA para obtener el certificado CUP-XMPP firmado por CA, guía de uso de Jabber Complete para la validación de certificados

· Si el tomcat.pem certificado está autofirmado, vaya al paso 3

Paso 3. Elija Find para mostrar todos los certificados:

· Elija el tomcat.pem certificado.

· Una vez abierta, elija Regenerate y espere hasta que aparezca la ventana emergente de éxito antes de que se cierre la ventana emergente.

Paso 4. Continúe con cada suscriptor subsiguiente, consulte el procedimiento del paso 2 y complete todos los suscriptores de su clúster.

Paso 5. Después de que todos los nodos hayan regenerado el certificado Tomcat, Restart el servicio Tomcat en todos los nodos. Empiece por el editor, seguido por los suscriptores.

· Para activar el Restart servicio Tomcat, debe abrir una sesión CLI para cada nodo y ejecutar el comando hasta que el servicio reinicie Cisco Tomcat, como se muestra en la imagen:

```
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:
```

Eliminar certificados de confianza caducados

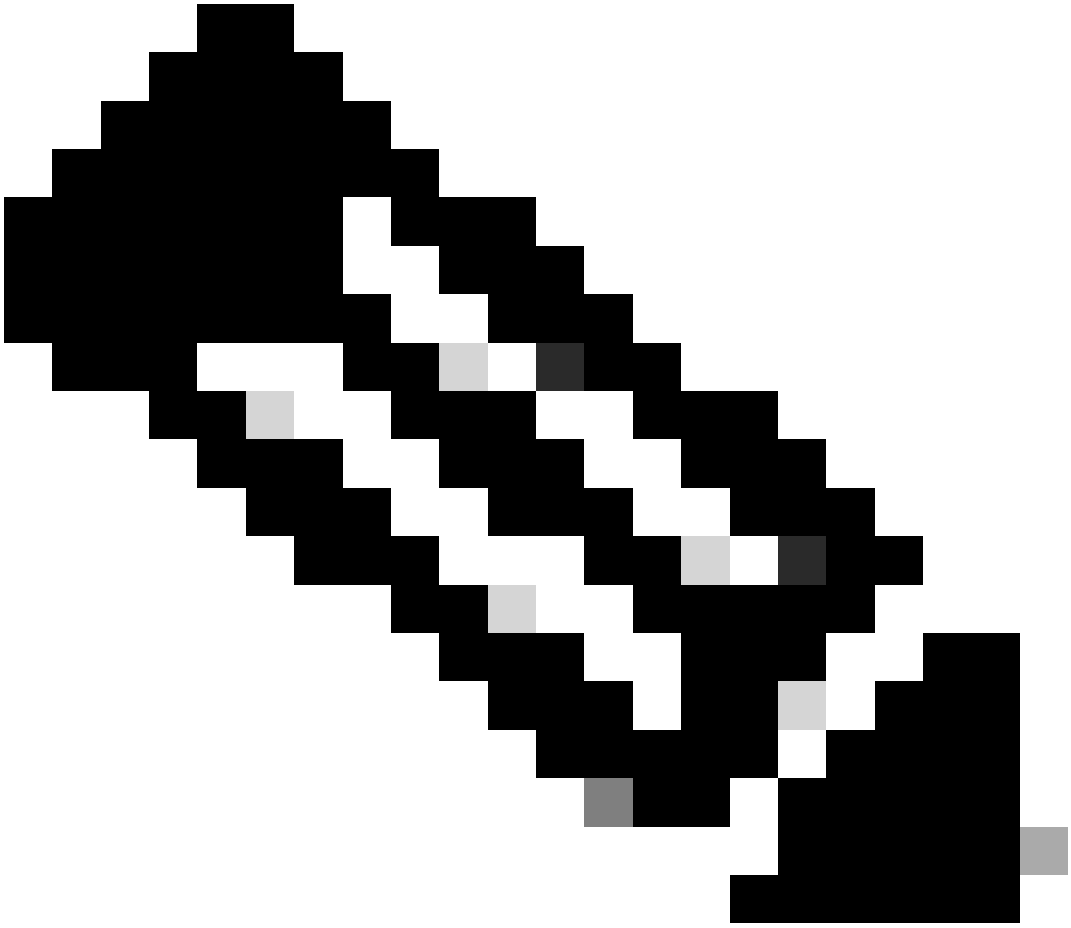
Nota: los certificados de confianza (que terminan en -trust) se pueden eliminar cuando sea apropiado. Los certificados de confianza que se pueden eliminar son aquellos que ya no son necesarios, que han caducado o que están obsoletos. No elimine los cinco certificados de identidad: cup.pem , cup-xmpp.pem , cup-xmpp-s2s.pem , ipsec.pem , y tomcat.pem certificados. Los reinicios del servicio, como se muestra, están diseñados para borrar cualquier información en memoria de estos certificados heredados dentro de esos servicios.

Nota: Si la configuración del grupo de redundancia de presencia tiene activada la opción Activar alta disponibilidad, Uncheck esto se realiza antes de que un servicio sea Stopped/Started o Restarted. Se puede acceder a la configuración del grupo de redundancia de presencia en CUCM Pub Administration > System > Presence Redundancy Group. El reinicio de algunos de los servicios, como se muestra, provoca una interrupción temporal de IM/P y debe realizarse fuera de las horas de producción.

Paso 1. Navegue hasta:Cisco Unified Serviceability > Tools > Control Center - Network Services

· En el menú desplegable, elija su editor de IM/P, elija Stop en Cisco Certificate Expiry Monitor, seguido de Stop en Cisco Intercluster Sync Agent.

· Repita Stop para estos servicios para cada nodo IM/P del clúster.



Nota: si se debe eliminar el certificado de confianza de Tomcat, desplácese hasta Cisco Unified Serviceability > Tools > Control Center - Network Services de la publicación de CUCM.

· En el menú desplegable, seleccione el editor de CUCM.

· Elija Stop de Cisco Certificate Expiry Monitor, seguido de Stop en Cisco Certificate Change Notification.

· Repita este procedimiento para cada nodo de CUCM del clúster.

Paso 2. Desplácese hasta Cisco Unified OS Administration > Security > Certificate Management > Find.

· Busque los certificados de confianza caducados (para las versiones 10.x y posteriores, puede filtrar por Caducidad. En las versiones anteriores a la 10.0, debe identificar los certificados específicos manualmente o a través de las alertas de RTMT (si se reciben).

· El mismo certificado de confianza puede aparecer en múltiples nodos, debe eliminarse individualmente de cada nodo.

· Elija el certificado de confianza que desea eliminar (en función de la versión, obtendrá una ventana emergente o accederá al certificado en la misma página).

· Elija Delete (aparece una ventana emergente que comienza con "va a eliminar permanentemente este certificado...").
· Haga clic OK.

Paso 3. Repita el proceso para cada certificado de confianza que desee eliminar.

Paso 4. Al finalizar, se deben reiniciar los servicios que estén directamente relacionados con los certificados eliminados.

· Cup-trust: Cisco SIP Proxy, Cisco Presence Engine y, si se ha configurado para la federación de SIP, Cisco XCP SIP Federation Connection Manager (consulte la sección Certificado CUP)
· CUP-XMPP-trust: router Cisco XCP (consulte la sección de certificados CUP-XMPP)
· CUP-XMPP-S2S-trust: router Cisco XCP y administrador de conexiones de federación Cisco XCP XMPP
· IPSec-trust: DRF Source/DRF Local (consulte la sección de certificados IPSec)
· Tomcat-trust: Reinicie el servicio Tomcat mediante la línea de comandos (consulte la sección de certificados de Tomcat)

Paso 5. Se detuvieron los servicios de reinicio en el paso 1.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).