Configuración de Tomcat Certificate Reuse para CallManager en CUCM 14

Contenido

Introducción

Este documento describe cómo reutilizar el certificado Tomcat Multi-SAN para CallManager en un servidor Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- certificados CUCM
- Herramienta de supervisión en tiempo real (RTMT)
- Lista de confianza de identidad (ITL)

Componentes Utilizados

La información de este documento se basa en CUCM 14.0.1.13900-155.

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

Los dos servicios principales para CUCM son Tomcat y CallManager. En las versiones anteriores, se requerían diferentes certificados para cada servicio para el clúster completo. En la versión 14 de CUCM, también se agregó una nueva función para reutilizar el certificado Tomcat Multi-SAN para el servicio CallManager. Las ventajas de utilizar esta función son:

- Reduce el coste de obtener dos certificados firmados por una autoridad de certificación pública (CA) para un clúster de certificados firmados por CA.
- Esta función reduce el tamaño del archivo ITL y, por lo tanto, la sobrecarga.

Low Impact Medium Impact. High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat		-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec		-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF		CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager		CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS		ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery		CTL + ITL	Signer or SAST backup for ITL/CTL	All	

Configurar

⚠ Precaución: Antes de cargar un certificado Tomcat, compruebe que el inicio de sesión único (SSO) está desactivado. En caso de que esté activado, SSO debe desactivarse y volver a activarse una vez que el proceso de regeneración de certificados de Tomcat haya finalizado.

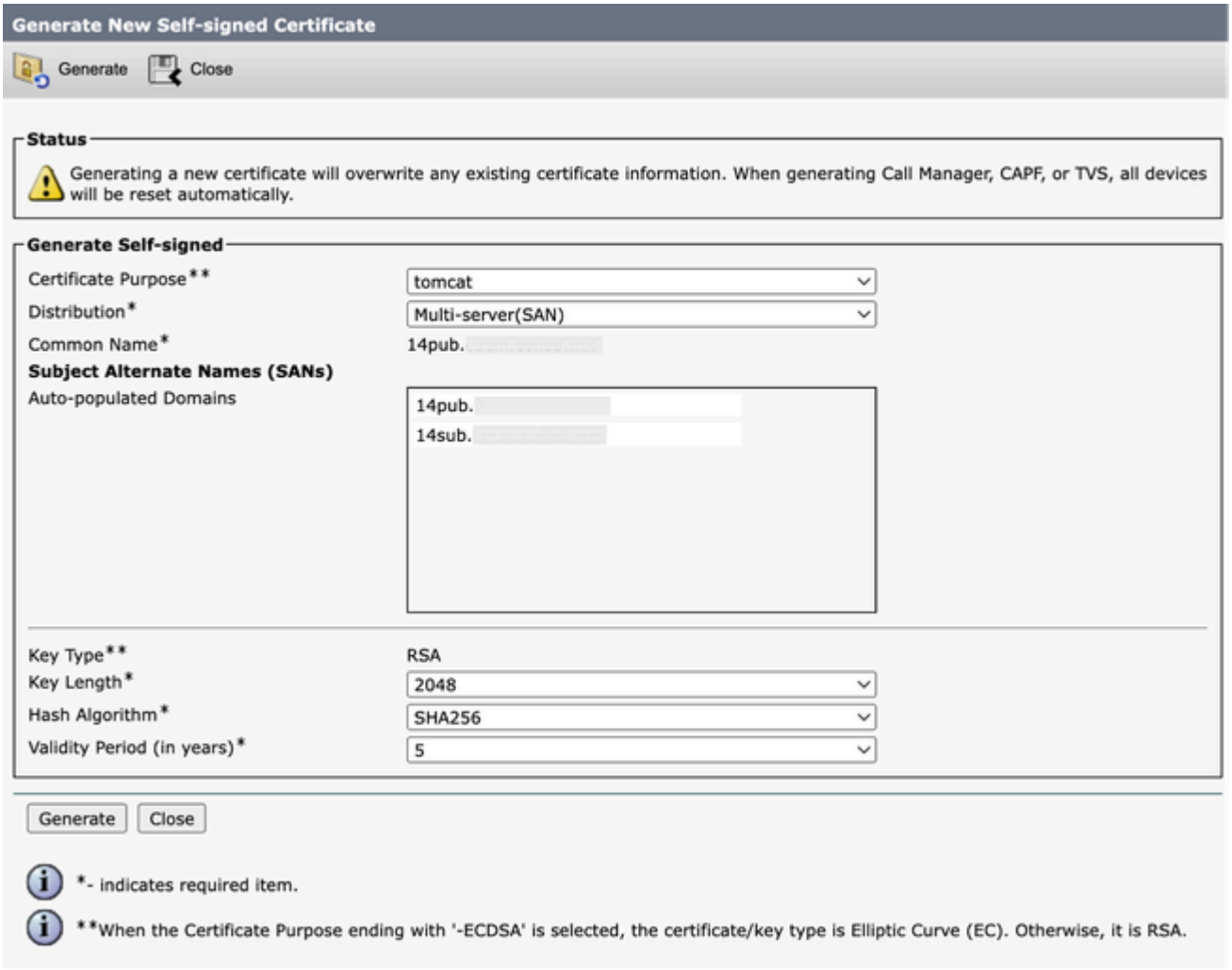
1. Establezca el certificado Tomcat como Multi-SAN Low Impact

En CUCM 14, el certificado de Tomcat Multi-SAN puede ser de firma automática o de CA. Si su certificado Tomcat ya es Multi-SAN, omita esta sección.

Autofirmado

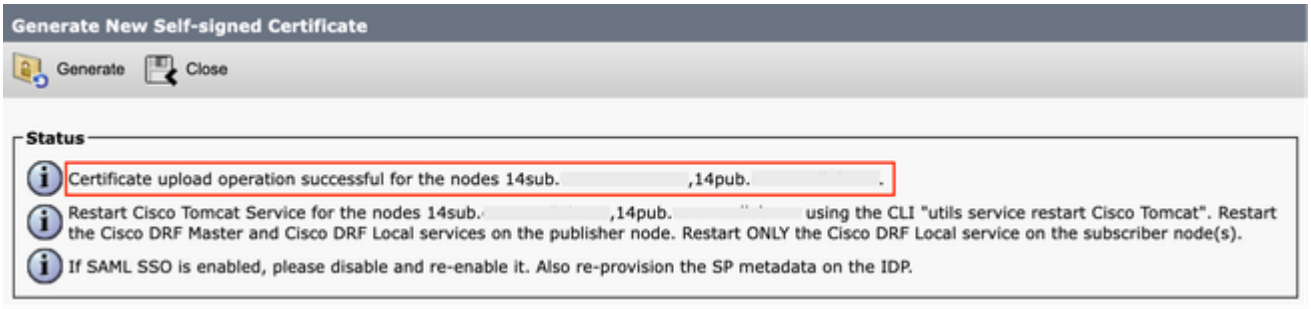
Paso 1. Inicie sesión en Publisher > Operating System (OS) Administration y navegue hasta Security > Certificate Management > Generate Self-Signed.

Paso 2. Seleccione Certificate Purpose: tomcat > Distribution: Multi-Server SAN. Se rellenan automáticamente los dominios SAN y el dominio principal.



Pantalla Generar certificado Tomcat de varias SAN firmado automáticamente

Paso 3. Haga clic en Generate, y valide que todos sus nodos se enumeran bajo el Certificate upload operation successful mensaje. Haga clic en Close.



Generar mensaje de Tomcat Multi-SAN autofirmado correcto

Paso 4. Reinicie el servicio Tomcat, abra una sesión CLI en todos los nodos del clúster y ejecute elutils service restart Cisco Tomcatcomando.

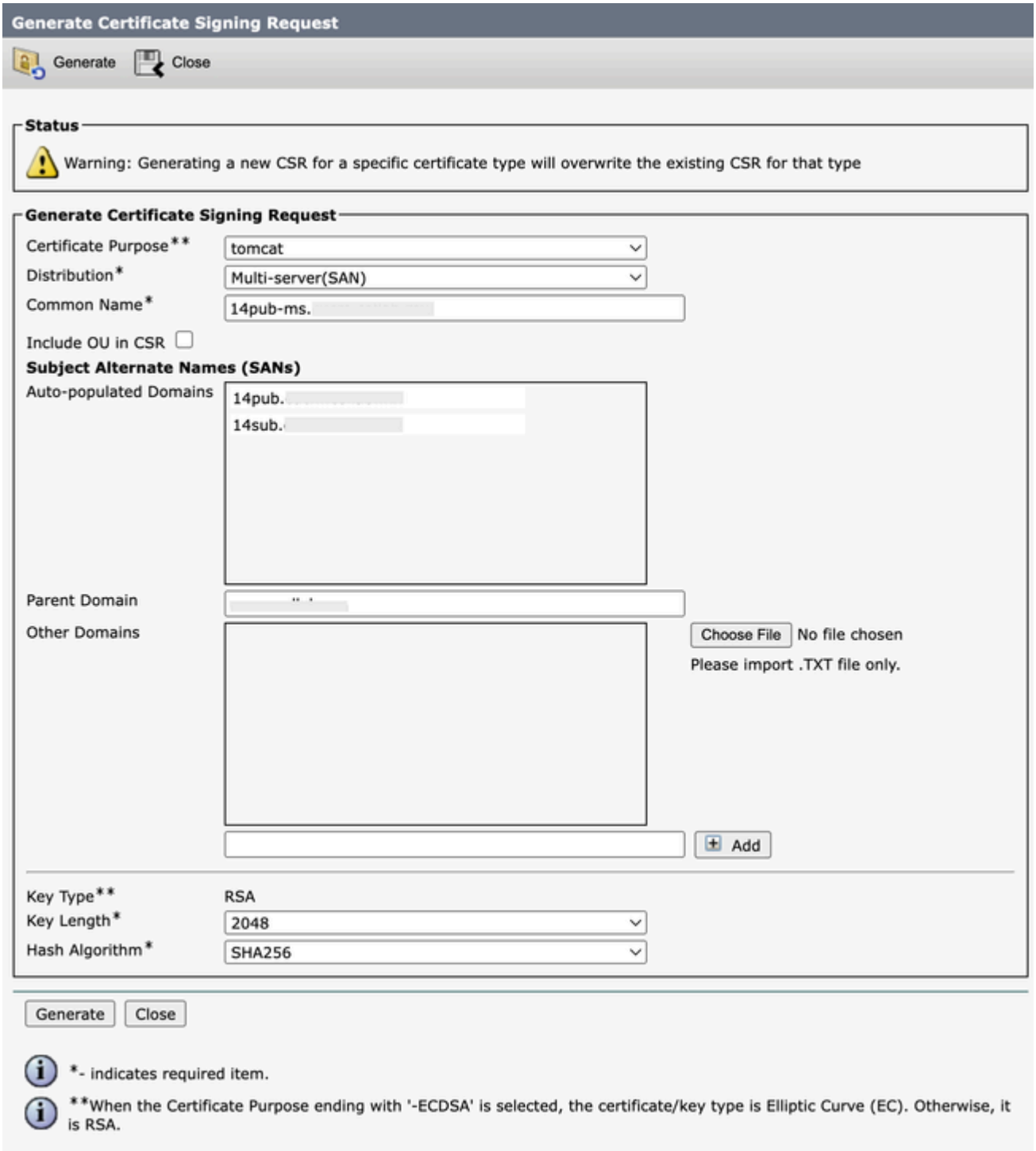
Paso 5. Desplácese hasta el Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services y reinicie el Cisco DRF Master Service y Cisco DRF Local Service.

Paso 6. Desplácese hasta cada Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services y reinicie Cisco DRF Local Service.

Firmado por CA

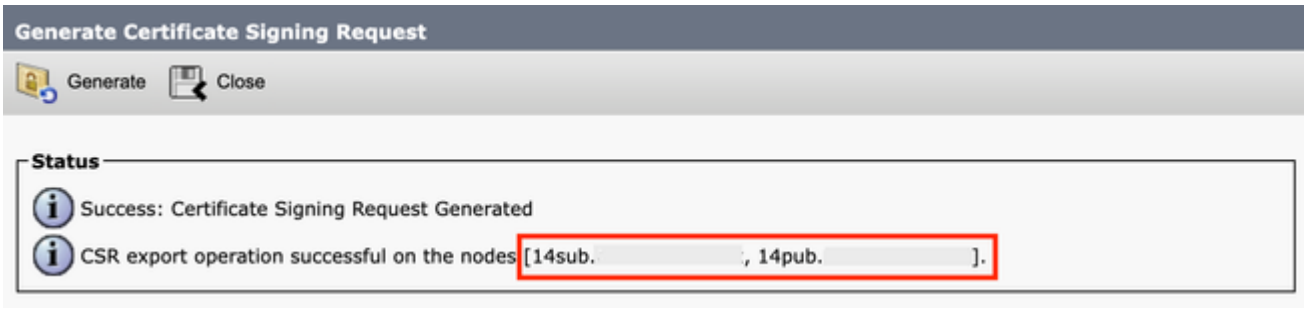
Paso 1. Inicie sesión en Publisher > Operating System (OS) Administration y navegue hasta Security > Certificate Management > Generate CSR.

Paso 2. Seleccione Certificate Purpose: tomcat > Distribution: Multi-Server SAN. Se rellenan automáticamente los dominios SAN y el dominio principal.



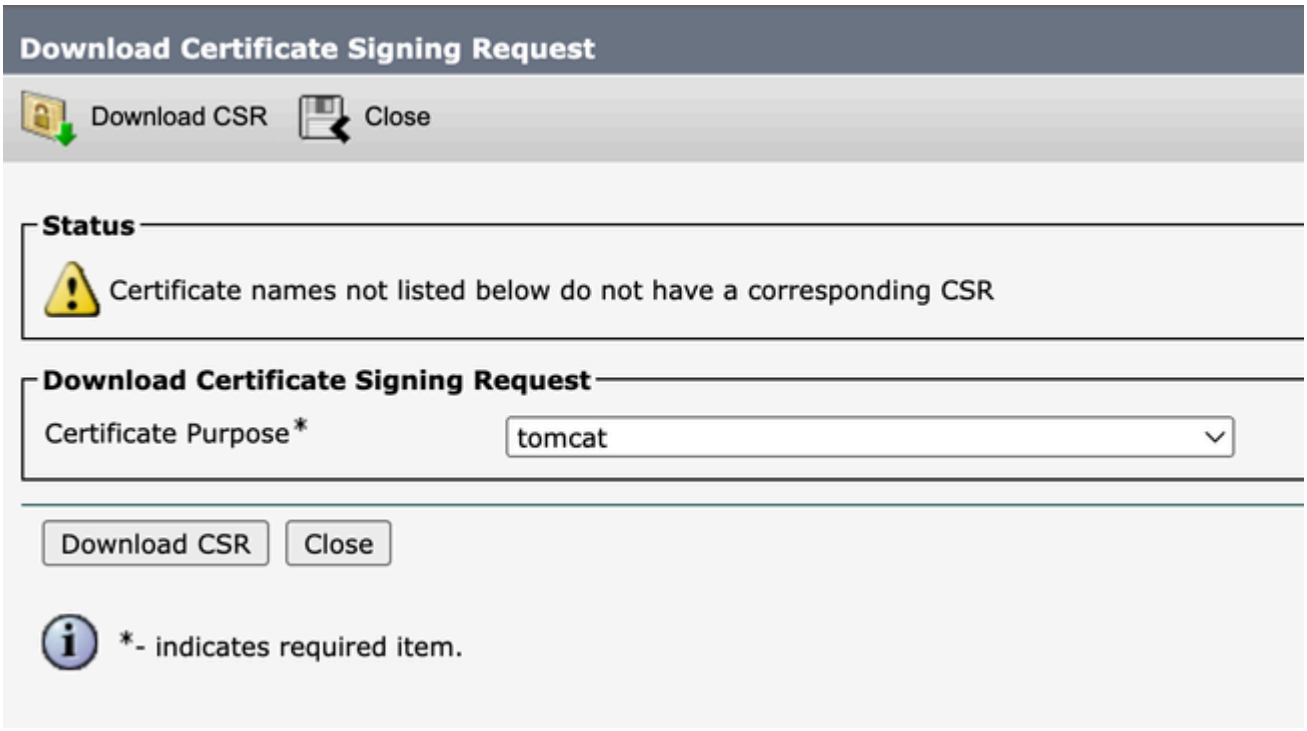
Pantalla Generate Multi-SAN CSR for Tomcat Certificate

Paso 3. Haga clic Generate, y validar todos sus nodos se enumeran bajo el CSR export operation successful mensaje. Haga clic en Close.



Generar mensaje CSR Tomcat correcto de Multi-SAN

Paso 4. Haga clic en Download CSR > Certificate Purpose: tomcat > Download



Descargar la pantalla CSR de Tomcat

Paso 5. Envíe el CSR a la CA para su firma.

Paso 6. Para cargar la cadena de confianza de la CA, navegue por Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust. Establezca la descripción del certificado y explore los archivos de la cadena de confianza.

Paso 7. Cargue el certificado firmado por la CA y vaya a Certificate Management > Upload certificate > Certificate Purpose: tomcat. Establezca la descripción del certificado y examine el archivo de certificado firmado por la CA.

Paso 8. Reinicie el servicio Tomcat, abra una sesión CLI en todos los nodos del clúster y ejecute el utils service restart Cisco Tomcat comando.

Paso 9. Desplácese hasta el Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services y reinicie

el Cisco DRF Master Service y Cisco DRF Local Service.

Paso 10. Desplácese hasta cada uno Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services y reinicie Cisco DRF Local Service.

2. Reutilice el certificado Tomcat para CallManager

⚠ Precaución: Para CUCM 14, se introduce un nuevo parámetro Phone Interaction on Certificate Update empresarial. Utilice este campo para restablecer los teléfonos de forma manual o automática según corresponda cuando se actualice uno de los certificados TVS, CAPF o TFTP (CallManager/ITLRecrecovery). Este parámetro se establece de forma predeterminada en reset the phones automatically. Después de la regeneración, eliminación y actualización de certificados, asegúrese de reiniciar los servicios adecuados.

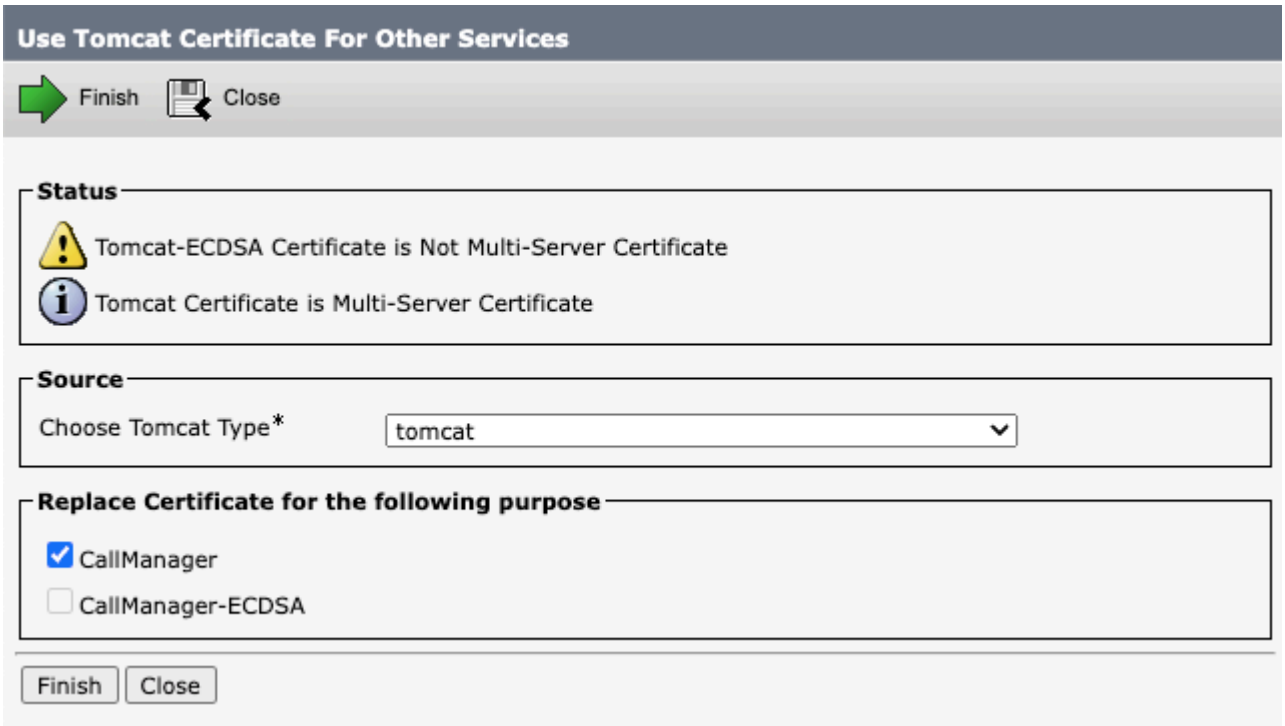
Es necesario reiniciar los servicios para una regeneración de certificado de CallManager normal. Marque Regenerar Certificados En Unified Communications Manager.

Paso 1. Vaya al editor de CUCM y, a continuación, a Cisco Unified OS Administration > Security > Certificate Management.

Paso 2. Haga clic en Reuse Certificate

Paso 3. En la lista choose **Tomcat type** desplegable, seleccione tomcat.

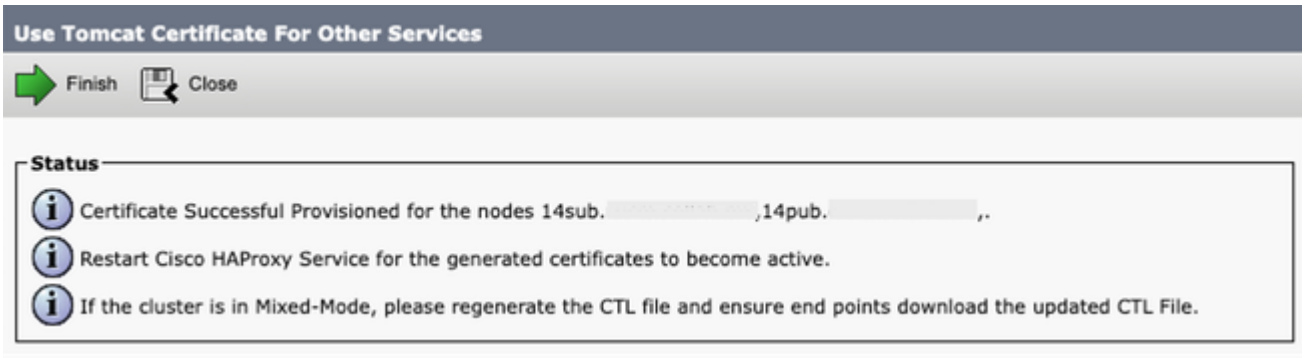
Paso 4. Desde el Replace Certificate for the following purpose panel, marque la CallManager casilla de verificación.



Pantalla Reutilizar certificado Tomcat para otros servicios

Nota: Si elige Tomcat como tipo de certificado, CallManager se habilita como reemplazo. Si elige tomcat-ECDSA como tipo de certificado, CallManager-ECDSA se habilita como reemplazo.

Paso 5. Haga clic Finish para reemplazar el certificado de CallManager con el certificado de Tomcat Multi-SAN.



Mensaje de reutilización correcta del certificado Tomcat

Paso 6. Reinicie el servicio Cisco HAProxy, abra una sesión CLI en todos los nodos del clúster y ejecute el utils service restart Cisco HAProxy comando.

Nota: Para determinar si el clúster está en modo mixto, navegue hasta Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == No seguro; 1 == Mixed Mode [Modo mixto]).

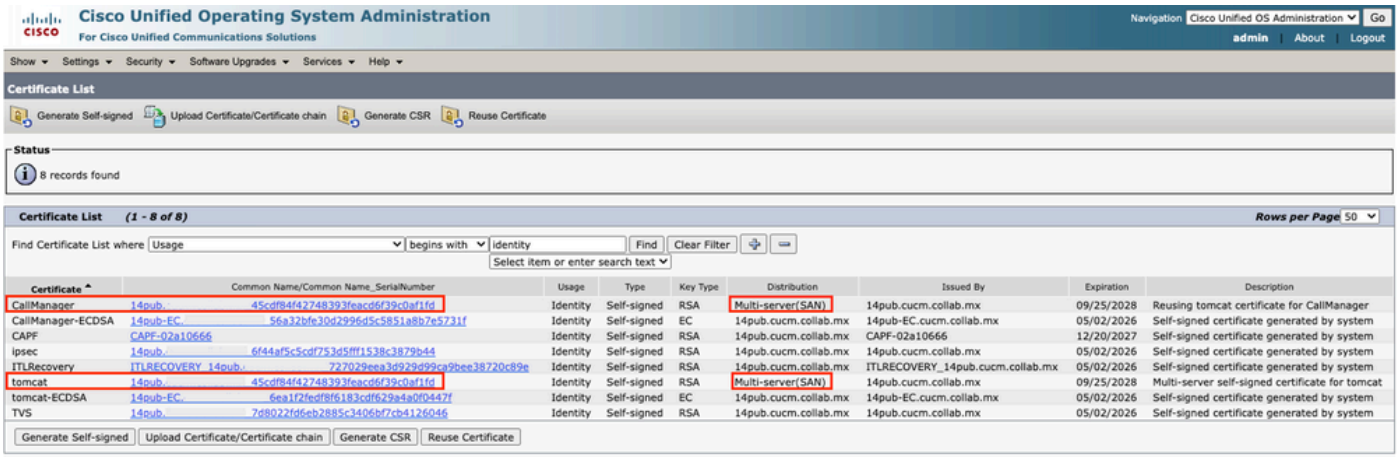
Paso 7. Si el clúster está en modo mixto, abra una sesión CLI en el nodo del editor, ejecute el **utils ctl update CTLFile** comando y restablezca todos los teléfonos del clúster para que se apliquen las actualizaciones del archivo CTL.

Verificación

Paso 1. Vaya al editor de CUCM y, a continuación, a Cisco Unified OS Administration > Security > Certificate Management.

Paso 2. Filtre por Find Certificate List where: Usage > begins with: identity y haga clic en Find.

Paso 3. Los certificados de CallManager y Tomcat deben terminar con el mismo Common Name_Serial Number valor.



Verificar reutilización de certificado Tomcat para CallManager

Nota: A partir de SU4, con la reutilización de certificados habilitada, el certificado de Call Manager no se muestra en la GUI, mientras que ambos certificados están visibles en SU2 y SU3.

Información Relacionada

- Guía de seguridad de Cisco Unified Communications Manager 14
- Soporte técnico y descargas de Cisco

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).