

Implementación de la reutilización del certificado Tomcat Multi-SAN para CallManager

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Reutilización del certificado Tomcat para CallManager](#)

[Verificación](#)

Introducción

Este documento describe un proceso paso a paso sobre cómo reutilizar el certificado Tomcat Multi-SAN para CallManager en CUCM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager (CUCM)
- Certificados de CUCM
- Lista de confianza de identidad (ITL)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CUCM versión 15 SU1

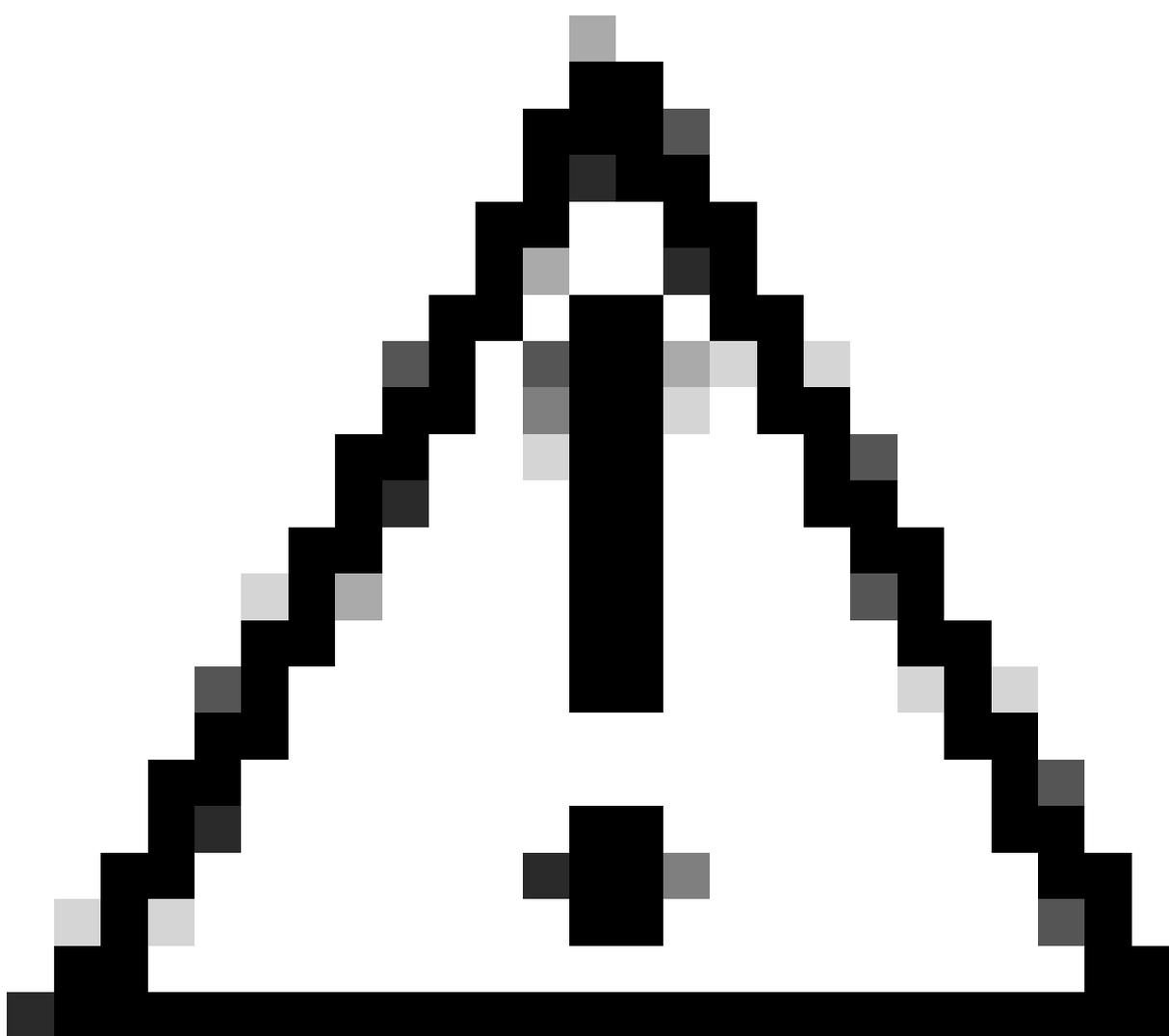
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las versiones anteriores de CUCM utilizaban certificados diferentes para cada servicio del clúster completo, lo que aumentaba el número de certificados y el coste. Esto incluye Cisco Tomcat y Cisco CallManager, que son servicios críticos que se ejecutan en CUCM y que también tienen sus respectivos certificados de identidad.

A partir de la versión 14 de CUCM, se agregó una nueva función para reutilizar el certificado Tomcat de Multi-SAN para el servicio CallManager.

La ventaja de utilizar esta característica es que puede obtener un certificado de la CA y utilizarlo en varias aplicaciones. Esto garantiza la optimización de los costos y una reducción de la gestión y reduce el tamaño del archivo de ITL, reduciendo así los gastos generales.



Precaución: antes de continuar con la configuración de reutilización, asegúrese de que el certificado Tomcat es un certificado SAN multiservidor. El certificado Multi-SAN de Tomcat puede ser de firma automática o de CA.

Configurar

Reutilización del certificado Tomcat para CallManager



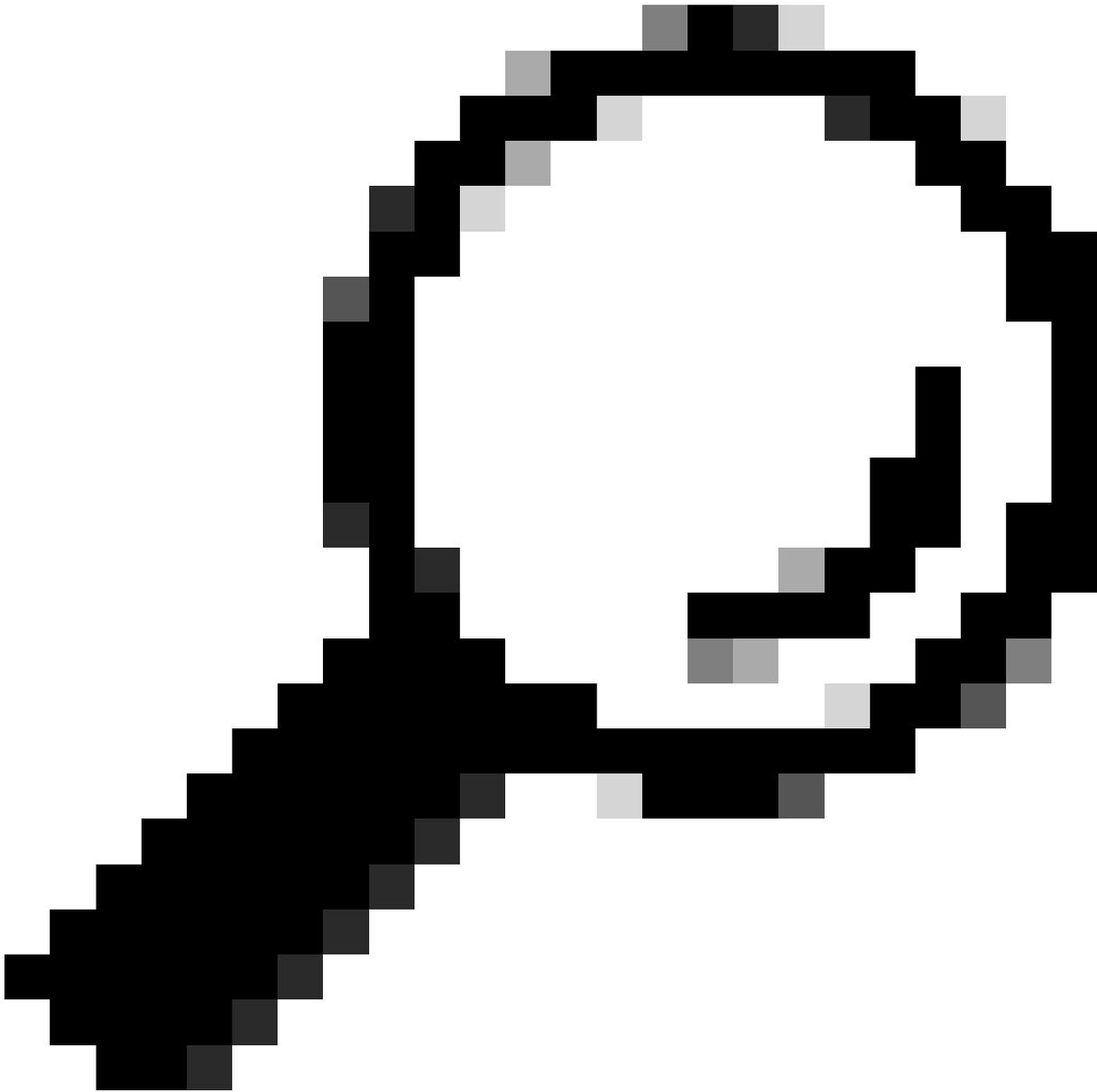
Advertencia: Asegúrese de que ha identificado si el clúster está en modo mixto o en modo no seguro antes de continuar.

Paso 1. Vaya a Administración de Cisco Unified CM > Sistema > Parámetros de empresa:

Verifique la sección Parámetros de seguridad y verifique si el Modo de seguridad del clúster está configurado en 0 o 1. Si el valor es 0, el clúster está en modo no seguro. Si es 1, el clúster está en modo mixto y debe actualizar el archivo CTL antes de reiniciar los servicios.

Paso 2. Navegue hasta su editor de CUCM y luego hasta Administración de Cisco Unified OS > Seguridad > Administración de certificados.

Paso 3. Cargue la cadena de certificados CA de Multi-SAN Tomcat en el almacén de confianza de CallManager.



Sugerencia: Si utiliza el certificado SAN multiservidor de firma automática para Tomcat, puede omitir este paso.

Antes de reutilizar los certificados, asegúrese de cargar manualmente la cadena de certificados de CA (que firmó el certificado de identidad tomcat) en el almacén de confianza de CallManager.

Reinicie estos servicios cuando cargue la cadena de certificados tomcat en la confianza de CallManager.

- CallManager: servicio Cisco HAProxy
- CallManager-ECDSA: Cisco CallManager Service y Cisco HAProxy Service

Paso 4. Haga clic en Reutilizar certificado. Aparecerá la página Utilizar certificados Tomcat para otros servicios.

Use Tomcat Certificate For Other Services



Finish



Close

Status



Tomcat-ECDSA Certificate is Not Multi-Server Certificate



Tomcat Certificate is Multi-Server Certificate

Source

Choose Tomcat Type*

tomcat



Replace Certificate for the following purpose



CallManager



CallManager-ECDSA

Finish

Close

Paso 5. En la lista desplegable Tipo de Tomcat, elija Tomcat o Tomcat-ECDSA.

Paso 6. En el panel Reemplazar certificado para el siguiente propósito, marque la casilla de verificación CallManager o CallManager-ECDSA basada en el certificado seleccionado en el paso anterior.



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 7. Haga clic en Finish para reemplazar el certificado de CallManager con el certificado SAN multiservidor tomcat.

Use Tomcat Certificate For Other Services

 Finish  Close

Status

-  Certificate Successful Provisioned for the nodes cucmpub15. , cucmsub15. .
-  Restart Cisco HAProxy Service for the generated certificates to become active.
-  If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

Paso 8. Reinicie el servicio Cisco HAProxy en todos los nodos del clúster mediante la ejecución del comando `utils service restart Cisco HAProxy` a través de CLI.

```
admin:utils service restart Cisco HAProxy
Stopping Cisco HAProxy...

Cisco HAProxy [STOPPED] Service Activated
Starting Cisco HAProxy...
Cisco HAProxy [STARTED]
admin: █
```

Paso 9. Si el clúster está en modo mixto, actualice el archivo CTL ejecutando el comando `utils ctl update CTLFile` a través de CLI de CUCM Publisher y proceda a restablecer los teléfonos para obtener el nuevo archivo CTL.

Verificación

Nota: El certificado de CallManager no se muestra en la GUI cuando se reutiliza el certificado.

Puede ejecutar el comando desde la CLI para confirmar que CallManager reutiliza el certificado Tomcat.

- show cert list own

```
admin:show cert list own  
  
tomcat/tomcat.pem: Certificate Signed by AKASH-WINSERVLAB-CA  
tomcat-ECDSA/tomcat-ECDSA.pem: Self-signed certificate generated by system  
ipsec/ipsec.pem: Self-signed certificate generated by system  
ITLRecovery/ITLRecovery.pem:  
CallManager-ECDSA/CallManager-ECDSA.pem: Self-signed certificate generated by system  
CallManager/CallManager.pem: Reusing tomcat certificate for CallManager  
TVS/TVS.pem: Self-signed certificate generated by system  
  
admin:█
```

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).