Vencimiento y cancelacíon del certificado CER

ID del Documento: 117566

Actualizado: De marcha el 05 de 2014

Contribuido por Guillermo Ryan Bennett, ingeniero de Cisco TAC.

Productos Relacionados

- Certificados

Contenido

Introducción

Este documento describe un problema con el Cisco Emergency Responder (CER) donde usted recibe el **CertExpiryEmergency: Certifique el** mensaje de alarma del **vencimiento EMERGENCY_ALARM del** CLI y ofrece una solución al problema.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de las versiones 2.x CER con 9.x.

Además, esta configuración requiere que su sistema:

- No contiene ninguna configuración del Domain Name Server (DNS)
- Tiene un servidor CER instalado y certifcates que estén a punto de expirar

Note: El IP Address del sistema no importa si usted ingresa los **nuevos** o **regenerados** comandos de la **generación** después de que usted haya cambiado el nombre de host o el IP Address.

Componentes Utilizados

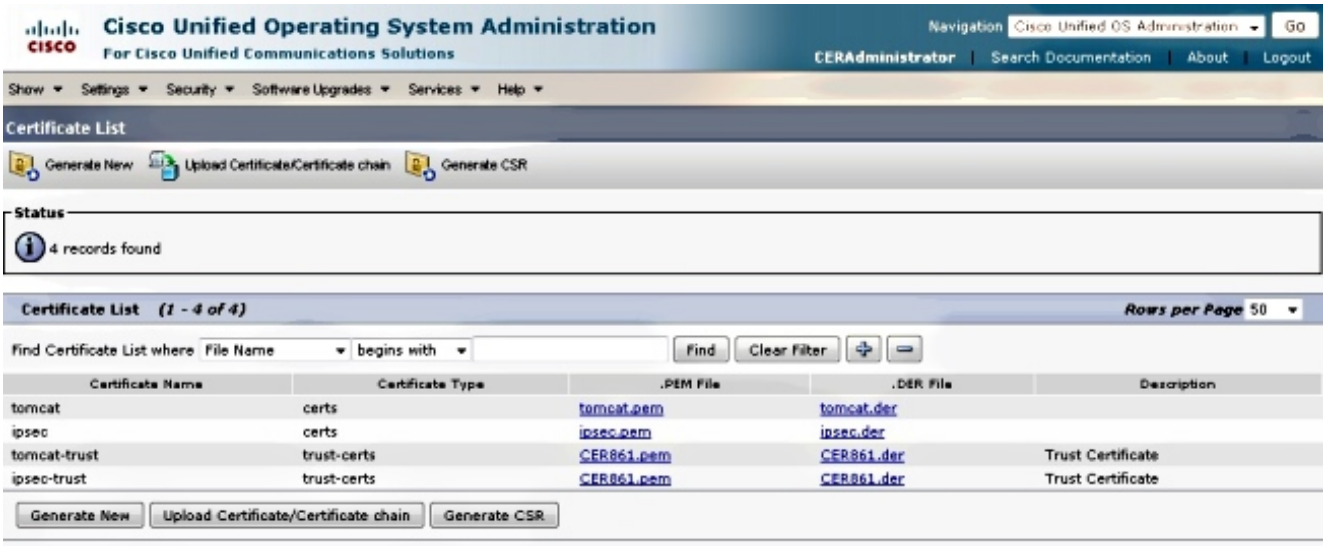
La información en este documento se basa en la versión 9.x CER.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

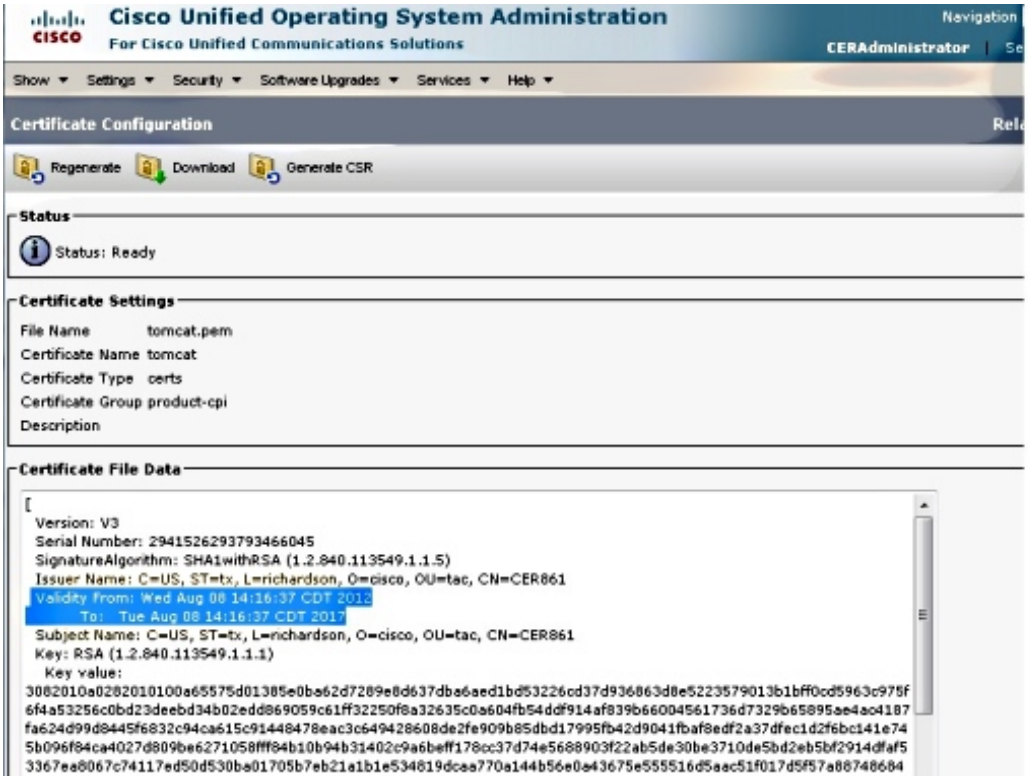
Genere un nuevo certificado

1. Vaya al GUI en la página de administración del operating system (OS) y seleccione la página del **Certificate Management (Administración de certificados) de la Seguridad**.

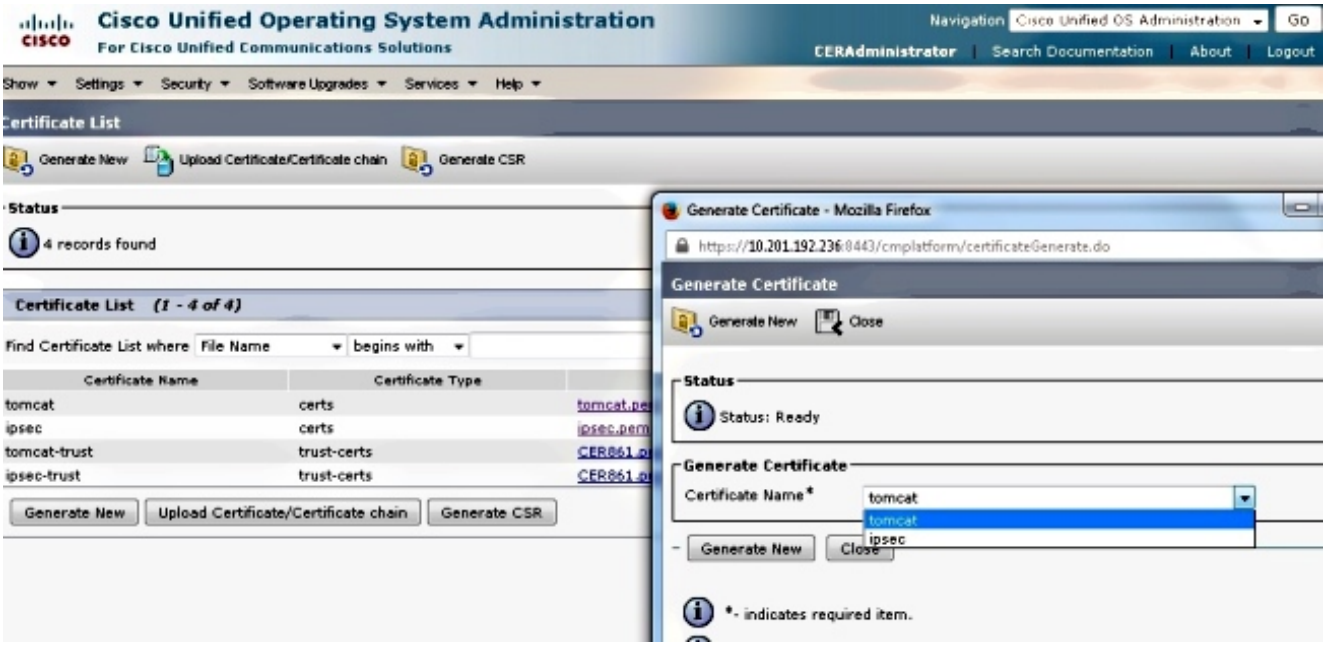
2. Para visualizar la lista de Certificados, haga clic el **botón Find Button**.



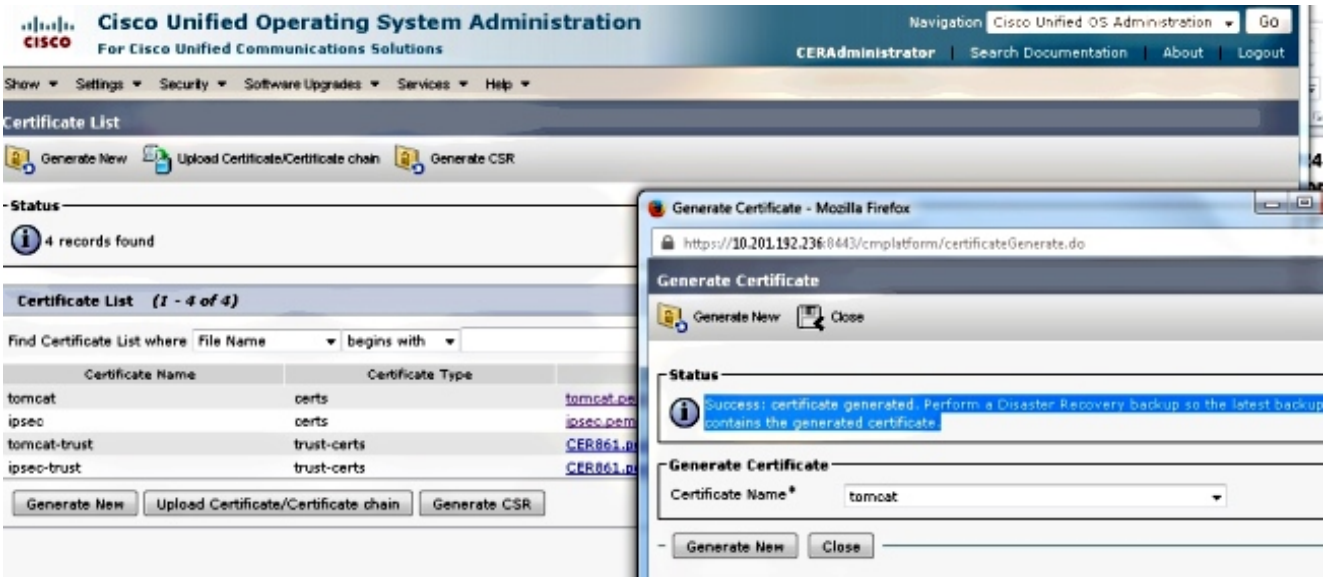
Esta captura de pantalla muestra el **certificado tomcat.pem**, y se resalta el Validitydate. Si el certificado está a punto de expirar, complete los pasos próximos.



3. Navegue a la página previa y haga clic el **nuevo** icono de la **generación**. Este pantallas emergentes para arriba:



4. Para regenerar el certificado, el tecleo **genera nuevo** en la ventana emergente. Visualizaciones de un Mensaje de éxito para anunciar que el certificado está regenerado.



5. Usted debe recomenzar Tomcat o el servicio de la seguridad de protocolos en Internet (IPSec) (si usted regeneró los Certificados del IPSec). Para recomenzar el tomcat, abrir un CLI en el nodo y ingresar el comando del **tomcat de Cisco del reinicio del servicio del utils**. La página web indica para una descarga del nuevo certificado una vez que la página está detrás en línea.

Certificados vencidos de la cancelación

NOTAS IMPORTANTES sobre la cancelacíon del certificado:

- Asegúrese de que los Certificados que se fijan para la cancelacíon sean no más funcionando o estén expirados realmente.
- Marque siempre toda la información en el certificado, porque no puede ser guardado después de que se borre.

Revise todos los Certificados con la extensión del **.pem** y verifiquelos que son todos dentro de un rango de tiempo válido. Si no son, después pueden ser borrados.

Si los servidores múltiples están en el cluster, usted debe ir a la dirección IP de cada uno de los servidores. Entonces, dentro de la página de administración OS, usted puede completar los pasos enumerados en la sección de la configuración.

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre los convenios usados en este documento.

Actualizado: De marcha el 05 de 2014
ID del Documento: 117566