Contenido

Introducción

Este documento describe la característica que mejora la experiencia del usuario y permite el cluster de la cancelacíon del certificado de par en par.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de Cisco unificó el vesion 11.0 del administrador de la comunicación (CUCM) y arriba.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Antecedentes

¿Hay ciertos Certificados en CUCM e IM&P que se repliquen transparente (sin el Admin? conocimiento s). Esto significa que si un certificado es cargado por el Admin en un servidor, está avanzada a los otros servidores dentro del cluster. Esto se hace para soportar la característica del cluster de la cruz de la movilidad de la extensión *(*EMCC).

Previamente, en un cluster enorme si había un requisito de borrar un certificado unrequired, el admin necesario para iniciar sesión en cada uno de los servidores y para borrar el certificado manualmente. Además, si esto no se hace dentro de una ventana estipulada, el certificado borrado pudo reaparecer debido al servicio de CertSync que funciona con cada 30 minutos, que se asegura de que sean las tablas del sistema de archivos y del certificado adentro sincronicen. Para evitar este problema, los clientes inhabilitan hoy el servicio de CertSync en todos los Nodos

seguidos por la cancelacíon del certificado en todos los Nodos. Esto hace que el usuario experimenta muy malo.

Con la mejora de la nueva función tales casos no ocurrirán.

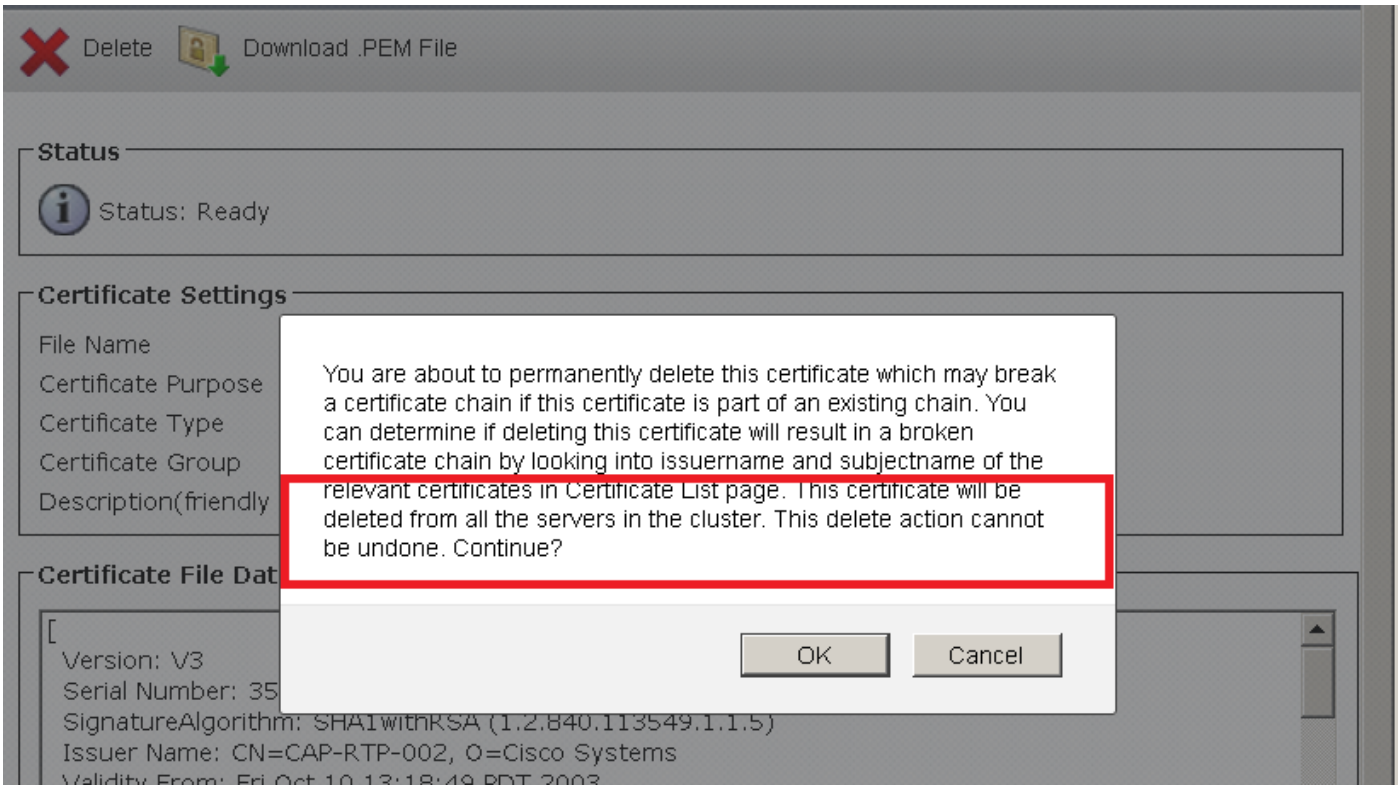
Este ehancement de la característica a la administración de certificados le proporciona la capacidad de borrar automáticamente un certificado de todos los Nodos en el cluster.

Cuando un certificado se borra a partir de un nodo en el cluster, conseguirá borrado del resto de los Nodos en el cluster.

Configurar

En el Cisco Call Manager, navegue a **Cisco unificó la administración OS > bajo Certificate Management (Administración de certificados) de la Seguridad**

Seleccione el certificado que las necesidades de ser borrado. Usted verá esto:



Una vez que usted hace clic la **AUTORIZACIÓN**, estos pasos ocurrirán:

1. El certificado será borrado localmente en el servidor.

2. Si el certificado se borra con éxito, después el evento de la plataforma será accionado. Este evento de la plataforma será enviado a todos los servidores en el cluster (CUCM e IM&P). La información presente en el evento de la plataforma es el tipo de unidad (CallManager, Tomcat o Teléfono-SAST) junto con el nombre del certificado (por ejemplo, RootCA.pem). El evento de la plataforma nos da la capacidad de accionar el cluster del evento de la cancelación de par en par.

La operación de eliminación del certificado es solamente aplicable para estos Certificados:

CUCM

1. Tomcat-confianza

2. CallManager-confianza

3. Teléfono-SAST-confianza

Presencia CUCM IM&

1. Tomcat-confianza

Verificación

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

Troubleshooting

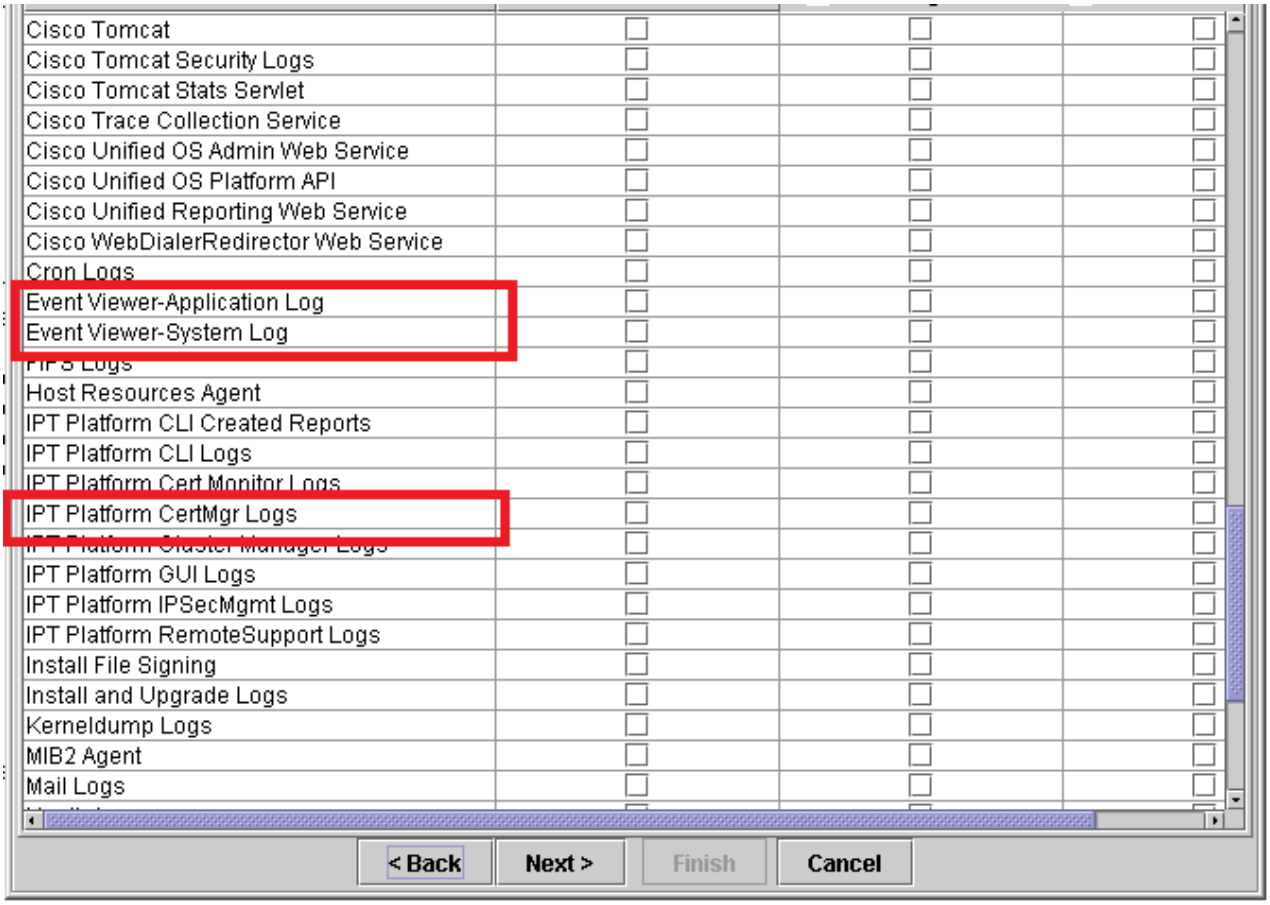
En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Si los Certificados en los otros Nodos en el cluster no se borran, recoja estos registros de RTMT, para resolver problemas este problema.

1. Registro de la aplicación del visor de eventos

2. Registro del Visualizador-sistema del evento

3. Registros de CertMgr de la plataforma IPT



Mensaje de ejemplo:

6 de julio ilog_impl del usuario CM11 6 de 03:12:05: Pedido recibido el plataforma-evento (--plataforma-evento-clusterwide-certificado-cancelación HOSTNAME=CM11Sub UNIT=tomcat-trust Type=certs-trust NAME=testcert.pem de la ninguno-espera).

Este registro indica que un evento ha sido recibido por los otros Nodos en el cluster para borrar el testcert del certificado, cuando el certificado se borra en un nodo.

De los registros del certMgmt para la operación de eliminación:

Este registro muestra que el mgmt CERT ha recibido el pedido la cancelacíon del certificado certificate.pem en el tomcat_trust:

decodifique: verdad

de Op. Sys.: cancelación

unidad: Tomcat-confianza

keystoreUnit: Tomcat-confianza

fichero de diario: /var/log/active/platform/log/cert-mgmt.log

resultFile: /var/log/active/platform/log/certde-info.xml

keyDir: /usr/local/cm/.security/tomcat/keys

certDir: /usr/local/cm/.security/tomcat/trust-certs/Certificate.pem

Este registro muestra que los Certificados están borrados de la base de datos:

2016-07-06 [MAIN] DE LA INFORMACIÓN DE 01:31:55,374 - EN -- CertDBAction.java - deleteCertificateInDB(certInfo) -