Configuración unificada del cluster de la comunicación con el ejemplo de configuración sujeto multiservidor CA-firmado del nombre alterno

Contenido

Introducción

Este documento describe cómo configurar un cluster unificado de la comunicación con el uso de un Certificate Authority (CA) - el nombre alterno sujeto multiservidor firmado (SAN).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administrador de las Comunicaciones unificadas de Cisco (CUCM)
- CUCM IM y versión 10.5 de la presencia

Antes de que usted intente esta configuración, asegúrese que estos servicios sean ascendentes y funcionales:

- Servicio web administrativo de la Plataforma de Cisco
- Servicio Tomcat de Cisco

Para verificar estos servicios en una interfaz Web, navegue a **Cisco unificó los servicios > el servicio de red de la página de la utilidad > seleccionan un servidor**. Para verificarlos en el CLI, ingrese el **comando list del servicio del utils**.

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

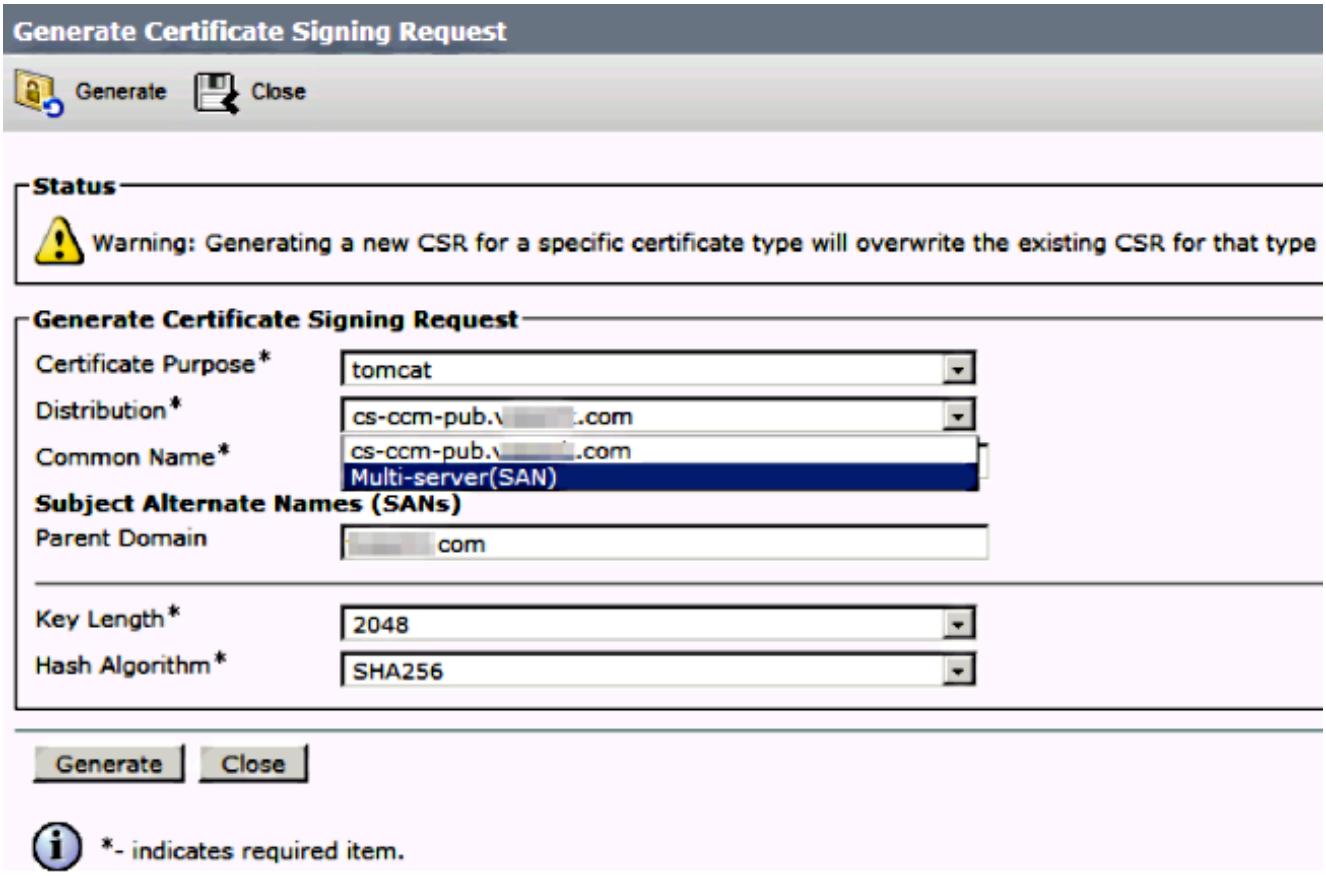
En la versión 10.5 y posterior CUCM, esta petición del pedido de firma de certificado del confianza-almacén (CSR) puede incluir el SAN y los dominios alternos.

1. Tomcat
2. Cisco CallManager (CCM)
3. Cisco unificó la Mensajería y el protocolo Presencia-extensibles de la presencia (CUP-XMPP)
4. Servidor-a-servidor CUP-XMPP (S2S)

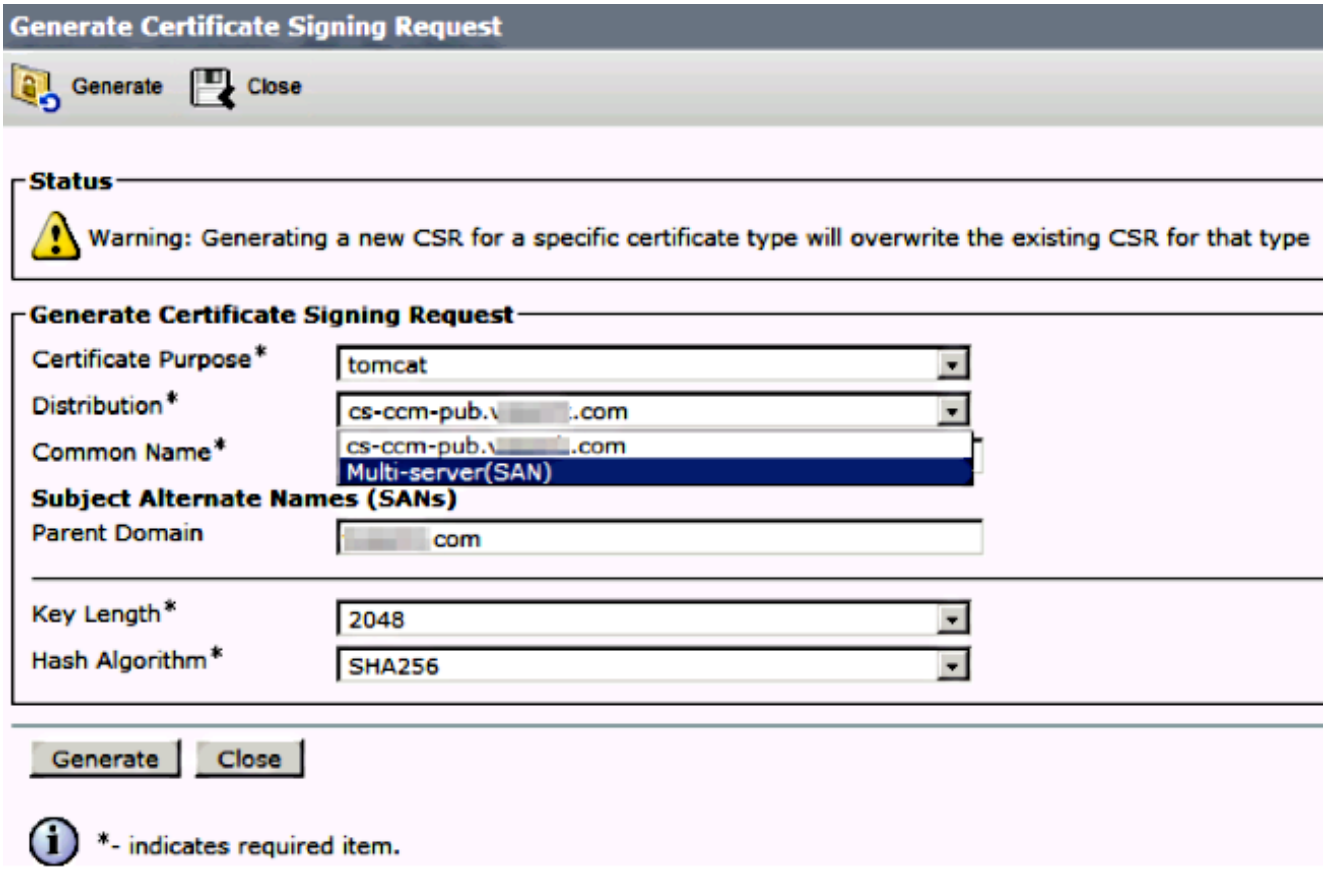
Es más simple obtener a certificado firmado por CA en esta versión. Solamente un CSR se requiere ser firmado por CA bastante que el requisito de obtener un CSR de cada nodo del servidor y después de obtener a certificado firmado por CA para cada CSR y de manejarlos individualmente.

Configurar

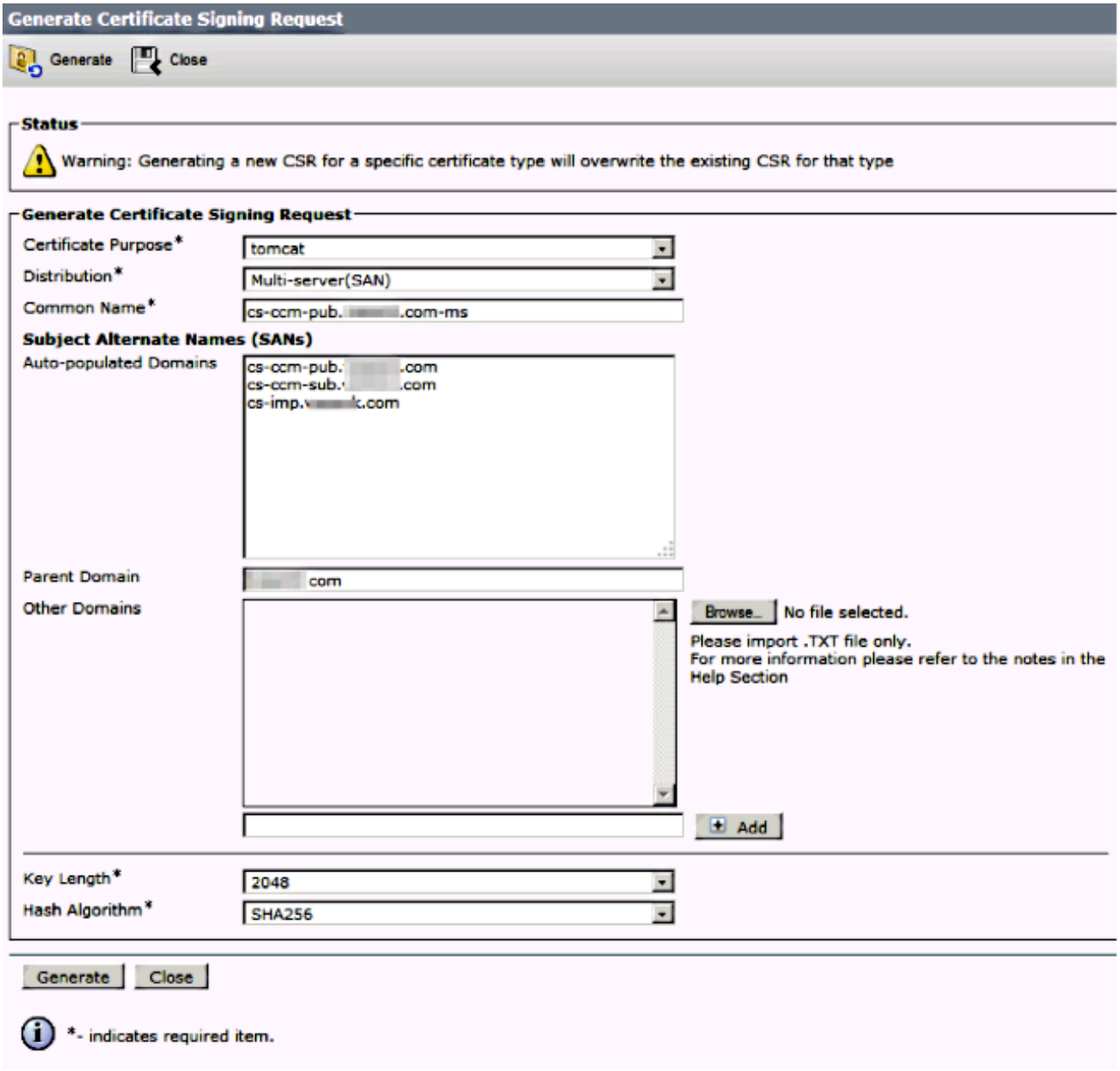
1. Registre en el operating system (OS) la administración y navegue al **Certificate Management (Administración de certificados) de la Seguridad > generan el CSR**.



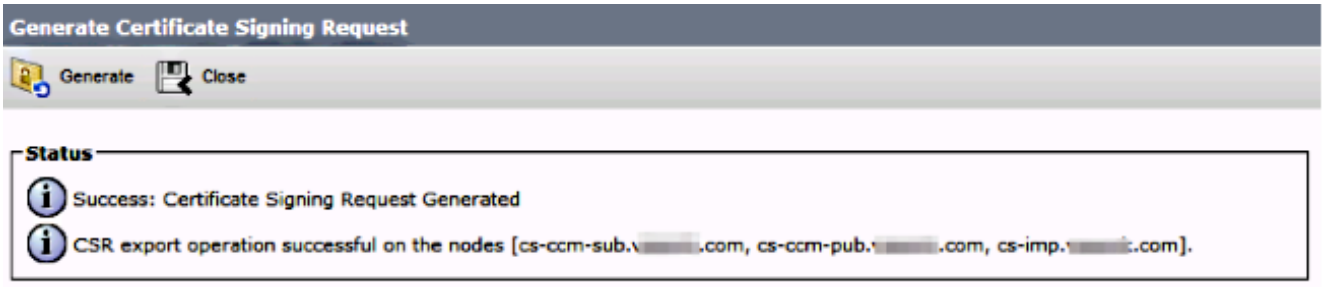
2. Seleccione el **SAN multiservidor** en la distribución.



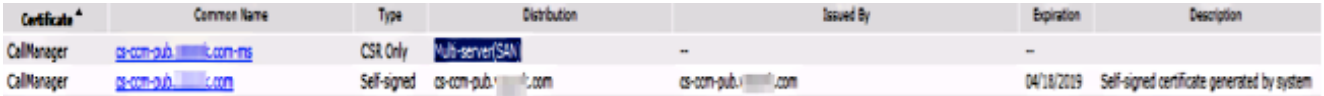
Él autopopulates los dominios SAN y el dominio del padre.



Una vez que se genera, éste visualiza:



En administración de certificados, se genera la petición SAN:

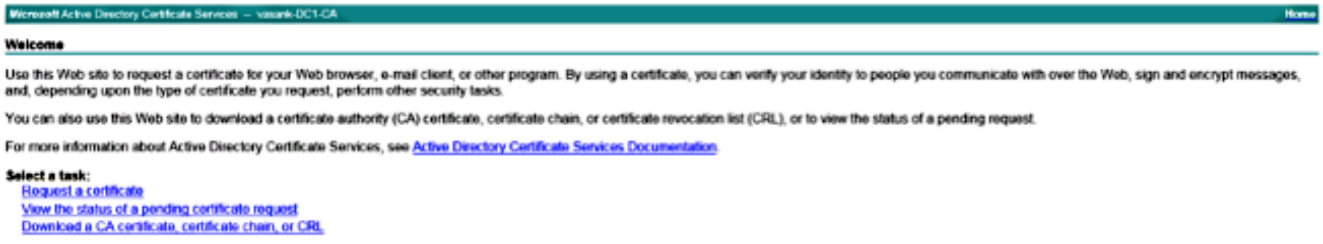


3. Usted puede utilizar CA local o CA externo como Verisign para conseguirlo firmado. Este ejemplo muestra los pasos para la configuración para Microsoft Windows CA basado en el

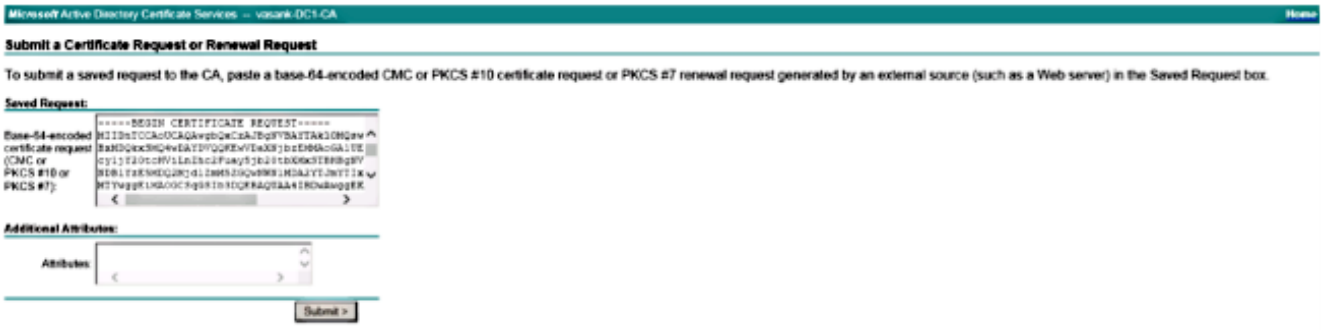
servidor.

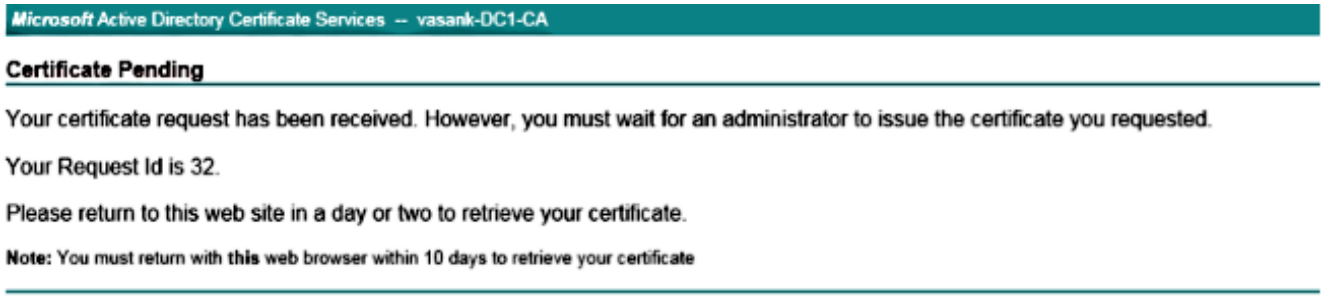
Registre en https:// <windowsserveripaddress>/certsrv/

Seleccione la **petición un certificado > avanzó el pedido de certificado**.

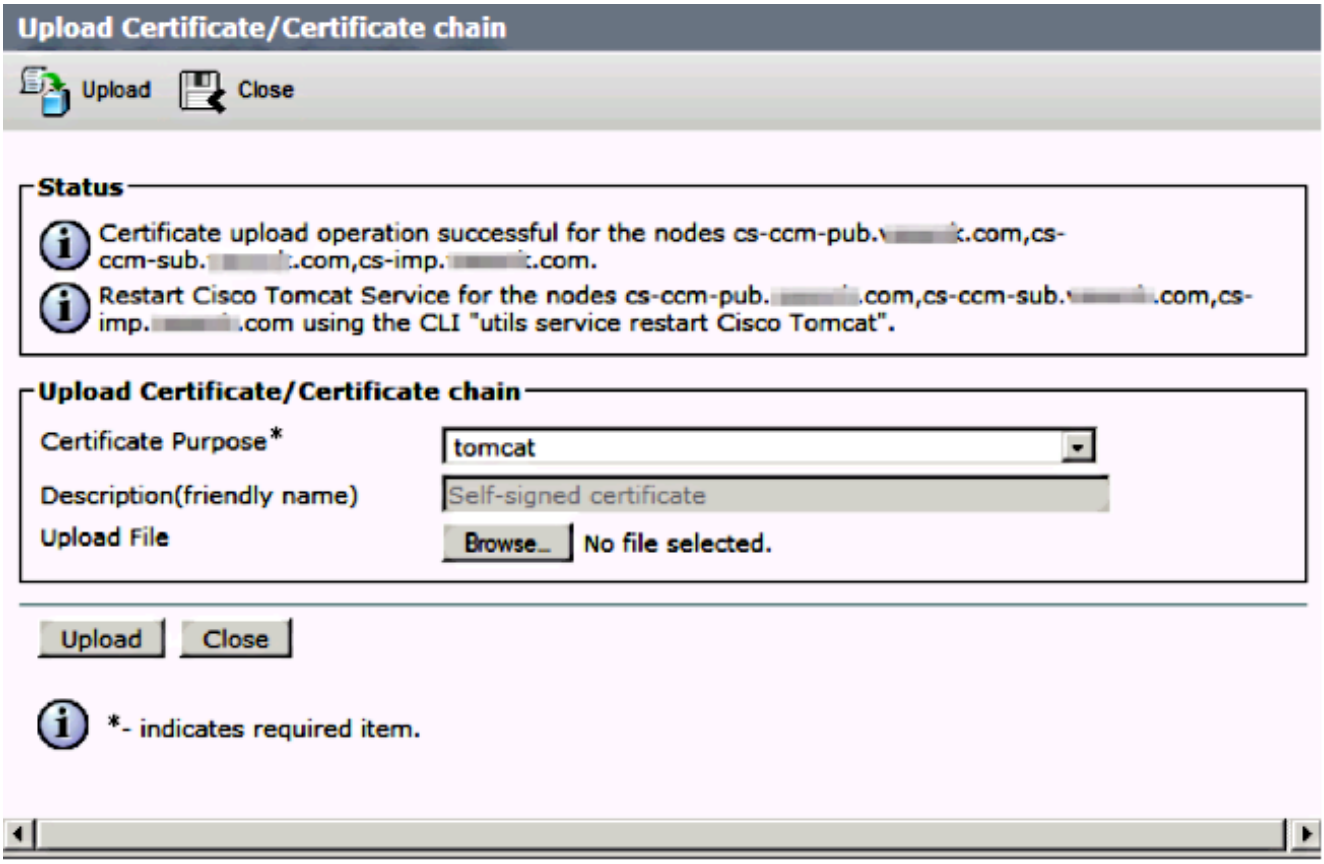


4. Someta la petición CSR como se muestra aquí.

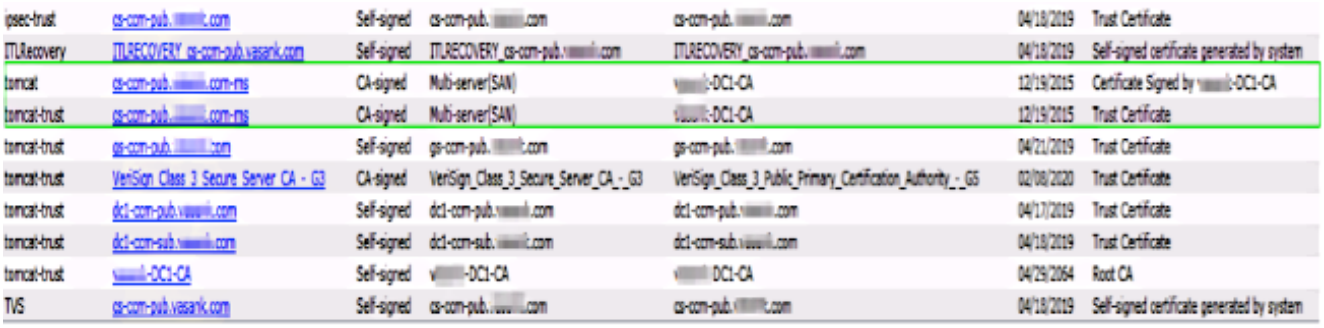




5. Una vez que usted obtiene el certificado, usted debe cargar el certificado de CA como Tomcat-confianza y después cargar certificado firmado por CA como tomcat.



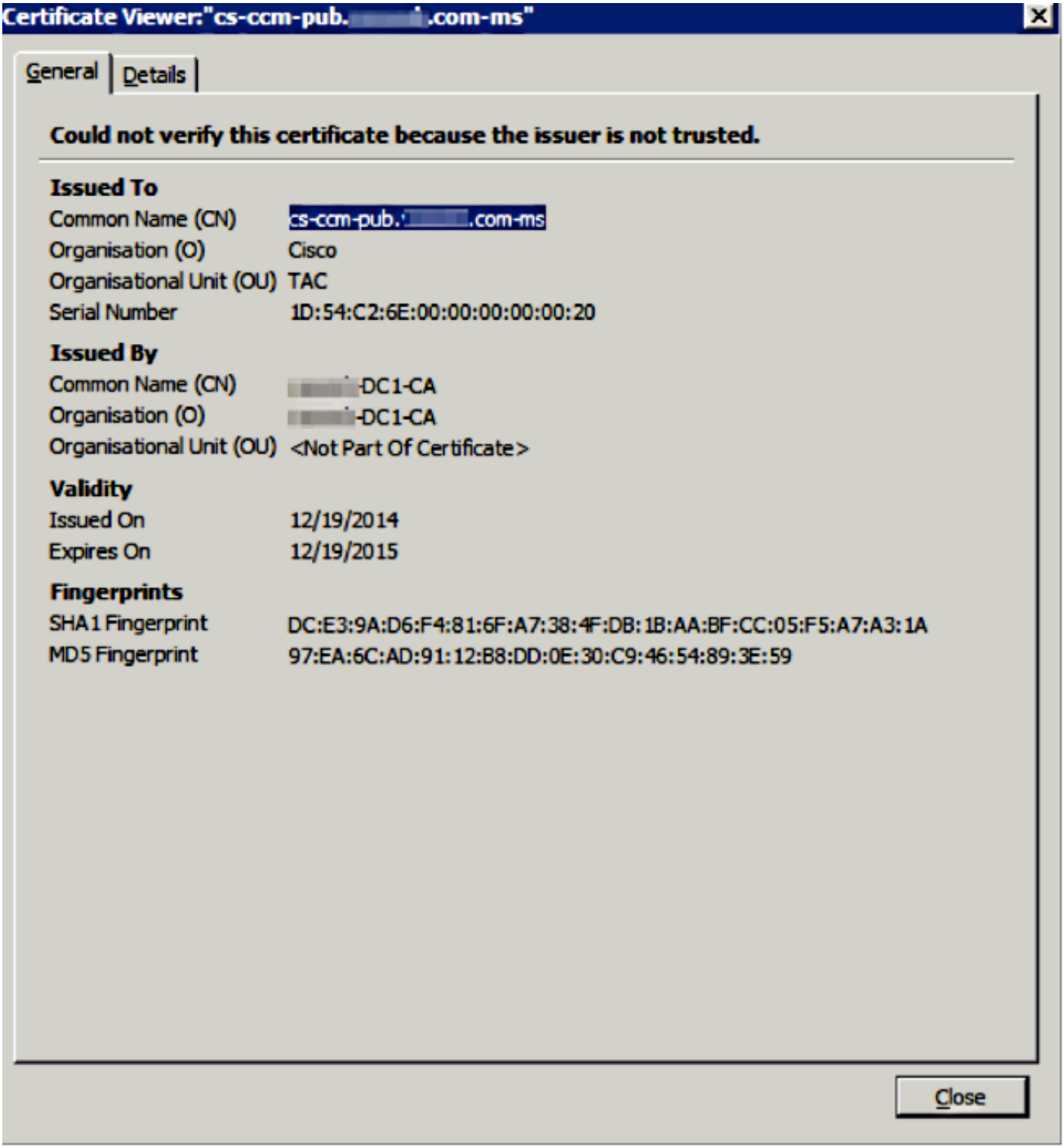
6. Asegúrese que el servicio esté recomenzado en todos los Nodos en la lista SAN, que incluye el nodo donde está cargada. Usted ve el SAN multiservidor enumerado en administración de certificados.



ipsec-trust	cs-ccm-pub.[redacted].com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY_cs-ccm-pub.vasank.com	Self-signed	ITLRECOVERY_cs-ccm-pub.[redacted].com	ITLRECOVERY_cs-ccm-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-ccm-pub.[redacted].com-ms	CA-signed	Multi-server(SAN)	[redacted]-DC1-CA	12/19/2015	Certificate Signed by [redacted]-DC1-CA
tomcat-trust	cs-ccm-pub.[redacted].com-ms	CA-signed	Multi-server(SAN)	[redacted]-DC1-CA	12/19/2015	Trust Certificate
tomcat-trust	cs-ccm-pub.[redacted].com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/21/2019	Trust Certificate
tomcat-trust	VeriSign_Class_3_Secure_Server_CA_-_G3	CA-signed	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/08/2020	Trust Certificate
tomcat-trust	dc1-ccm-pub.[redacted].com	Self-signed	dc1-ccm-pub.[redacted].com	dc1-ccm-pub.[redacted].com	04/17/2019	Trust Certificate
tomcat-trust	dc1-ccm-sub.[redacted].com	Self-signed	dc1-ccm-sub.[redacted].com	dc1-ccm-sub.[redacted].com	04/18/2019	Trust Certificate
tomcat-trust	[redacted]-DC1-CA	Self-signed	[redacted]-DC1-CA	[redacted]-DC1-CA	04/29/2064	Root CA
TVS	cs-ccm-pub.vasank.com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system

Verificación

Registro en http://<fqdnofccm>:8443/ccmadmin para asegurarse de que el nuevo certificado esté utilizado.



Certificado multiservidor del CallManager SAN

Un procedimiento similar se puede seguir para el certificado del CallManager. En este caso, los dominios autopopulated son todos los Nodos del CallManager. Si no se ejecuta, usted puede elegir guardarlo de la lista SAN o quitarlo de allí.

Después de que usted instale el certificado publicado por CA, usted debe recomenzar el servicio de CallManager en todos los Nodos.

Antes de que usted consiga el certificado CA-firmado SAN para CUCM, asegure eso:

- El teléfono del IP puede confiar en el servicio de la verificación de la confianza (TV). Esto

puede ser verificada si usted accede algún servicio HTTPS del teléfono. Por ejemplo, si Corporate Directory (Directorio corporativo) el acceso trabaja, después significa que el teléfono confía en el servicio TV.
- Si es un cluster seguro, asegúrese de que Certificate Trust List (Lista de confianza del certificado) volver a efectuar se cree el cliente (CTL) para un nuevo archivo CTL y se reinicia el cluster.

Troubleshooting

Estos registros deben ayudar al Centro de Asistencia Técnica de Cisco para identificar cualquier problema relacionado con la generación SAN CSR y la carga multiservidoras CA-Firmar Certficate.

- Cisco unificó la Plataforma OS API
- Cisco Tomcat
- Registros de CertMgr de la plataforma IPT

En un Certifcate multiservidor existente CUCM, si el nombre de host del servidor cambia, se recomienda para generar una petición multiservidora SAN CSR según lo explicado previamente para conseguir el certificado firmado por CA.