Generar CSR y aplicar certificados a CMS

Contenido

Introducción

Este documento describe cómo generar la solicitud de firma de certificado (CSR) y cargar certificados firmados en Cisco Meeting Server (CMS).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico del servidor CMS

Componentes Utilizados

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

- Software de masilla o similar
- CMS 2.9 o posterior

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.

Generar el CSR

Hay dos maneras de generar CSR: una es generando CSR directamente en el servidor CMS desde la interfaz de línea de comandos (CLI) con acceso de administrador; la otra es hacerlo con una autoridad de certificación (CA) externa como Open SSL.

En ambos casos, el CSR debe generarse con la sintaxis correcta para que los servicios CMS funcionen correctamente.

Paso 1. Estructura de sintaxis.

```
pki csr <key/cert basename> <CN:value> [OU:<value>] [O:<value>] [ST:<-value>] [C:<value>] [subjectAltNam
```

- <key/cert basename> es una cadena que identifica la nueva clave y el nombre CSR. Puede contener caracteres alfanuméricos, de guión o de subrayado. Este campo es obligatorio.
- <CN:value> es el nombre común. Se trata del nombre de dominio completo (FQDN) que especifica la ubicación exacta del servidor en el sistema de nombres de dominio (DNS). Este campo es obligatorio.
- [OU:<value>] es la unidad organizativa o el nombre del departamento. Por ejemplo, Asistencia, TI, Ingeniero, Finanzas. Este campo es opcional.
- [O:<value>] es el nombre de la organización o la empresa. Por lo general, el nombre legalmente constituido de una empresa. Este campo es opcional.
- [ST:<value>] es la provincia, región, condado o estado. Por ejemplo, Buckinghamshire California. Este campo es opcional.
- [C:<value>] es el país. Código de dos letras de la Organización Internacional de Normalización (ISO) del país en el que se encuentra la organización. Por ejemplo, US, GB, FR. Este campo es opcional.
- [subjectAltName:<value>] es el nombre alternativo del sujeto (SAN). A partir de la versión 3 de X509 (RFC 2459), los certificados SSL (Secure Socket Layers) pueden especificar varios nombres con los que debe coincidir el certificado. Este campo permite que el certificado generado cubra varios dominios. Puede contener direcciones IP, nombres de dominio, direcciones de correo electrónico, nombres de host DNS normales, etc., separados por comas. Si se especifica, también debe incluir el CN en esta lista. Aunque este es un campo opcional, el campo SAN debe completarse para que los clientes de protocolo de presencia y mensajería extensible (XMPP) acepten un certificado; de lo contrario, los clientes XMPP muestran un error de certificado.

Paso 2. Genere callbridge, xmpp, webadmin y webbridge CSR.

1. Acceda a la CLI de CMS con masilla e inicie sesión con la cuenta de administrador.
2. Ejecute los siguientes comandos para crear CSR para cada servicio necesario en CMS. También es aceptable crear un solo certificado que tenga un comodín (*.com) o que tenga el FQDN del clúster como CN, FQDN de cada servidor CMS y unirse a URL si es necesario.

Servicio	Comando
Webadmin	pki csr <cert name> CN:<server FQDN>
Webbridge	pki csr <cert name> CN:<Server FQDN> subjectAltName:<Join Url>,<XMPP domain>
Callbridge GIRAR Equilibrador de carga	pki csr <cert name> CN:<Server FQDN's>

3. En caso de que el CMS esté agrupado, ejecute los siguientes comandos.

Servicio	Comando
Callbridge GIRAR Equilibrador de carga	pki csr <cert name> CN:<cluster FQDN> subjectAltName:<Peer FQDN's>
XMPP	pki csr <cert name> CN:<Cluster FQDN> subjectAltName:<XMPP Domain>,<Peer FQDN's>

Paso 3. Genere la CSR del clúster de base de datos y utilice la CA integrada para firmarla.

Desde CMS 2.7, es necesario tener certificados para el clúster de base de datos. En la versión 2.7, incluimos una CA integrada que se puede utilizar para firmar los certificados de la base de datos.

1. En todos los núcleos, ejecute database cluster remove .

- En el menú Primario, ejecute pki selfsigned dbca CN . Ejemplo: **Pki selfsigned dbca CN:tplab.local**

- En el Primary, ejecute pki csr dbserver CN:cmscore1.example.com subjectAltName . Ejemplo: cmscore2.example.com,cmscore3.example.com

- En el menú Primario, cree un certificado para el cliente pki csr dbclient CN:postgres de base de datos.

- En el servidor principal, utilice dbca para firmar el certificado dbserver **pki sign dbserver dbca** .

- En el Primary, utilice dbca para firmar el certificado dbclient pki sign dbclient dbca .

- Copie dbclient.crt en todos los servidores que necesiten conectarse a un nodo de base de datos

- Copie el archivo dbserver.crt en todos los servidores que se han unido a la base de datos (nodos que forman el clúster de base de datos)

- Copie el archivo dbca.crt en todos los servidores.

- En el servidor de base de datos principal, ejecute database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt . Esto utiliza dbca.crt como root ca-cert .

- En el servidor de base de datos principal, ejecute database cluster localnode a .

- En el servidor de base de datos principal, ejecute database cluster initialize .

- En el servidor de base de datos principal, ejecute database cluster status . Debe ver Nodos: (me): Conectado principal.

- En todos los demás núcleos que estén unidos al clúster de base de datos, ejecute database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt .

- En todos los núcleos que estén conectados (no ubicados en una base de datos) al clúster de base de datos, ejecute **database cluster certs dbclient.key cbclient.crt dbca.crt** .

- En los núcleos que se han unido (se encuentran junto con una base de datos):

    - ejecute. database cluster localnode a

        - ejecute.database cluster join

- EN núcleos conectados (no ubicados en una base de datos):

    - ru n database cluster localnode a .

        - ejecute. database cluster connect

Paso 4. Verifique los certificados firmados.

- La validez del certificado (fecha de vencimiento) se puede verificar con la inspección de certificados, ejecute el comando **pki inspect <filename>** .

  - Puede validar que un certificado coincide con una clave privada, ejecute el comando pki match <keyfile> <certificate file> .

  - Para validar que un certificado está firmado por la CA y que el paquete de certificados se puede utilizar para afirmarlo, ejecute el comando pki verify <cert> <certificate bundle/Root CA> .

Paso 5. Aplique certificados firmados a los componentes de los servidores CMS.

1. Para aplicar certificados a Webadmin, ejecute los siguientes comandos:

```
webadmin disable
webadmin certs <keyfile> <certificate file> <certificate bundle/Root CA>
webadmin enable
```

2. Para aplicar certificados a Callbridge, ejecute los siguientes comandos:

```
callbridge certs <keyfile> <certificate file> <certificate bundle/Root CA>
callbridge restart
```

3. Para aplicar certificados a Webbridge, ejecute los siguientes comandos:

```
webbridge disable
webbridge certs <keyfile> <certificate file> <certificate bundle/Root CA>
webbridge enable
```

4. Para aplicar certificados a XMPP, ejecute los siguientes comandos:

```
xmpp disable
xmpp certs <keyfile> <certificate file> <certificate bundle/Root CA>
xmpp enable
```

5. Para aplicar certificados a la base de datos o reemplazar certificados caducados en el clúster de base de datos actual, ejecute los siguientes comandos:

```
database cluster remove (on all servers, noting who was primary before beginning)
database cluster certs <server_key> <server_certificate> <client_key> <client_certificate> <Root ca_crt
database cluster initialize     (only on primary node)
database cluster join <FQDN or IP of primary>    (only on slave node)
database cluster connect <FQDN or IP of primary> (only on nodes that are not part of the database clust
```

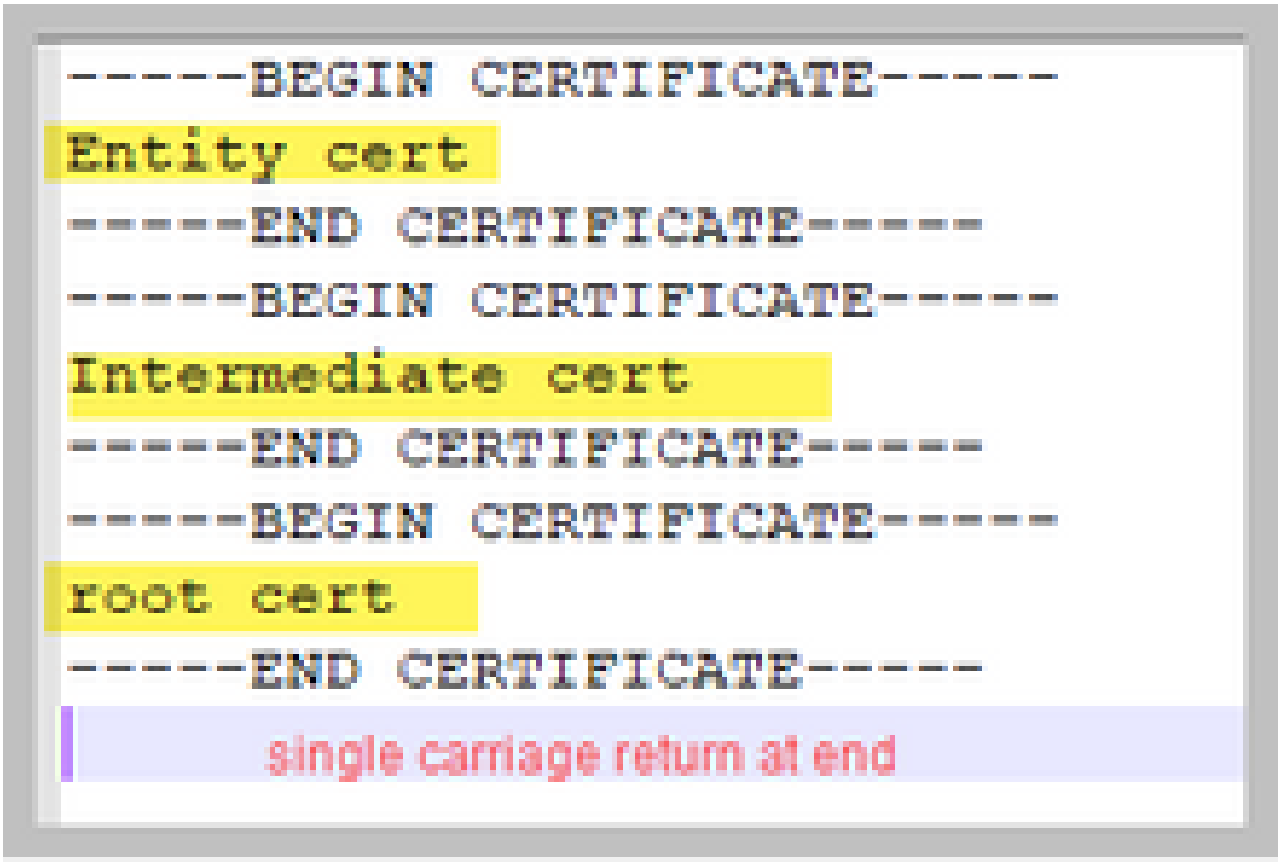
6. Para aplicar certificados a TURN, ejecute los siguientes comandos:

```
turn disable
turn certs <keyfile> <certificate file> <certificate bundle/Root CA>
turn enable
```

Cadenas y paquetes de confianza de certificados

Desde CMS 3.0, es necesario utilizar cadenas de confianza de certificados o confianzas de cadena completa. Además, es importante para cualquier servicio que reconozca cómo deben crearse los certificados cuando crea paquetes.

Cuando crea una cadena de confianza de certificados, como se requiere para el puente web 3, debe crearla como se muestra en la imagen, con certificado de entidad en la parte superior e intermedios en el medio, y CA raíz en la parte inferior, y luego un único retorno de carro.



Cada vez que cree un conjunto, el certificado sólo debe tener un retorno de carro al final.

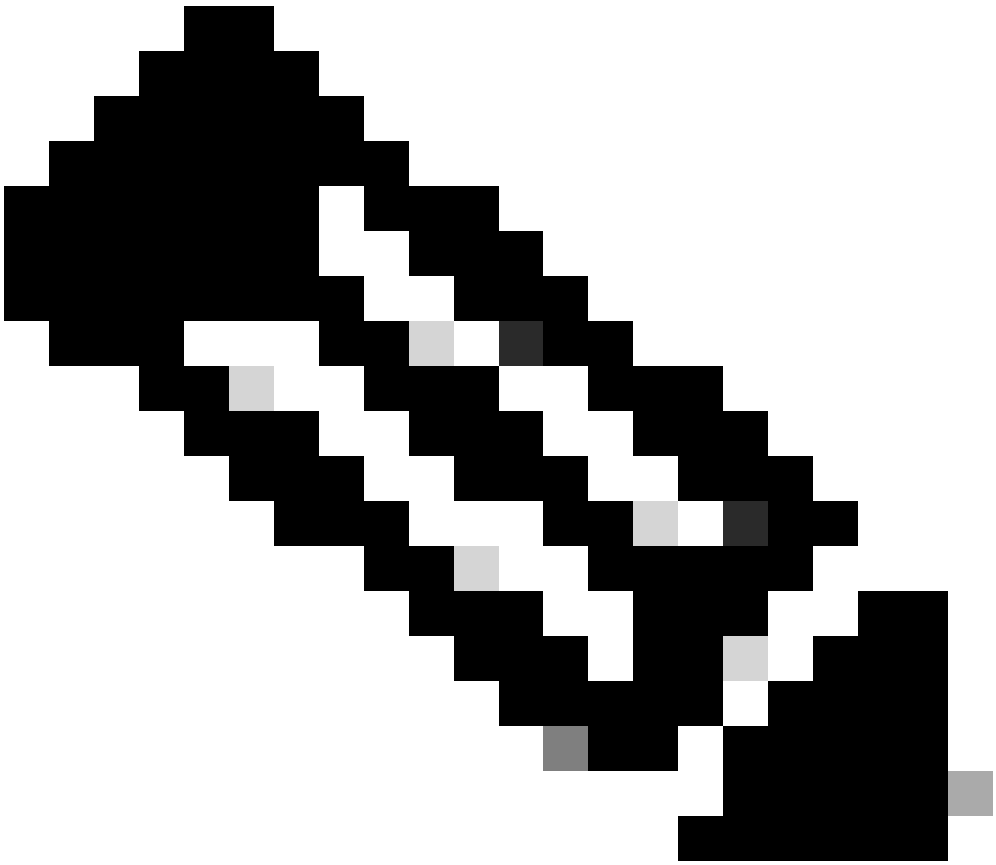
Los paquetes de CA serían los mismos que se muestran en la imagen; solo que, por supuesto, no habría ningún certificado de entidad.

Troubleshoot

Si necesita reemplazar un certificado caducado para todos los servicios, excepto los certificados de base de datos, el método más sencillo consiste en cargar certificados nuevos con el MISMO nombre que los certificados antiguos. Si hace esto, el servicio solo debe reiniciarse y no es necesario volver a configurar el servicio.

Si realiza pki csr ... y el nombre del certificado coincide con una clave actual, el servicio se interrumpirá inmediatamente. Si la producción está activa y crea de forma proactiva una nueva CSR y clave, utilice un nuevo nombre. Puede cambiar el nombre del nombre activo antes de cargar el nuevo certificado en los servidores.

Si los certificados de la base de datos han caducado, debe comprobar **database cluster status** quién es el principal de la base de datos y, en todos los nodos, ejecutar el comando database cluster remove . A continuación, puede utilizar las instrucciones del paso 3. Genere la CSR del clúster de base de datos y utilice la CA integrada para firmarla**.**



Nota: en caso de que necesite renovar los certificados de Cisco Meeting Manager (CMM), consulte el siguiente vídeo: Actualización del certificado SSL de Cisco Meeting Management

---

Información Relacionada

- **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).