

Gerar CSR e aplicar certificados ao CMS

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Gerar o CSR](#)

[Etapa 1. Estrutura de sintaxe](#)

[Etapa 2. Gerar CSR Callbridge, Smp, Webadmin e Webbridge](#)

[Etapa 3. Gerar o CSR do Cluster do Banco de Dados e Usar a CA Interna para Assiná-los](#)

[Etapa 4. Verificar os certificados assinados](#)

[Etapa 5. Aplicar certificados assinados aos componentes em servidores CMS](#)

[Cadeias e Pacotes de Certificados Confiáveis](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como gerar a CSR (Certificate Signing Request, Solicitação de assinatura de certificado) e carregar certificados assinados para o CMS (Cisco Meeting Server, Servidor de Reunião Cisco).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do servidor CMS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Putty ou software similar
- CMS 2.9 ou posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Gerar o CSR

Há duas maneiras de gerar o CSR: uma delas é gerar o CSR diretamente no servidor CMS a partir da Interface de Linha de Comando (CLI) com acesso de administrador; a outra é fazê-lo com uma Autoridade de Certificação (CA) externa de terceiros, como o Open SSL.

Em ambos os casos, o CSR deve ser gerado com a sintaxe correta para que os serviços CMS funcionem corretamente.

Etapa 1. Estrutura de sintaxe

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

- <key/cert basename> é uma string que identifica a nova chave e o nome do CSR. Ele pode conter caracteres alfanuméricos, de hífen ou de sublinhado. Este é um campo obrigatório.
- <CN:value> é o nome comum. Este é o Nome de Domínio Totalmente Qualificado (FQDN) que especifica o local exato do servidor no Sistema de Nome de Domínio (DNS). Este é um campo obrigatório.
- [OU:<valor>] é a Unidade Organizacional ou o Nome do Departamento. Por exemplo, Suporte, TI, Engenheiro, Finanças. Este é um campo opcional.
- [O:<valor>] é o nome da Empresa ou do Negócio. Normalmente, o nome legalmente incorporado de uma empresa. Este é um campo opcional.
- [ST:<valor>] é a província, a região, o município ou o estado. Por exemplo, Buckinghamshire Califórnia. Este é um campo opcional.
- [C:<valor>] é o País. O código ISO (International Organization for Standardization, Organização Internacional de Padronização) de duas letras para o país onde sua organização está localizada. Por exemplo, EUA, GB, FR. Este é um campo opcional.
- [subjectAltName:<valor>] é o SAN (nome alternativo do assunto). A partir do X509 Versão 3 (RFC 2459), os certificados SSL (Secure Socket Layers) podem especificar vários nomes que o certificado deve corresponder. Este campo permite que o certificado gerado cubra vários domínios. Ele pode conter endereços IP, nomes de domínio, endereços de e-mail, nomes de host DNS regulares etc., separados por vírgulas. Se for especificado, você também deverá incluir o CN nesta lista. Embora esse seja um campo opcional, o campo SAN deve ser preenchido para que os clientes XMPP (Extensible Messaging and Presence Protocol) aceitem um certificado, caso contrário, os clientes XMPP exibirão um erro de certificado.

Etapa 2. Gerar CSR Callbridge, Smp, Webadmin e Webbridge

1. Acesse a CLI do CMS com Putty e faça login com a conta admin.
2. Execute os próximos comandos para criar o CSR para cada serviço necessário no CMS. Também é aceitável criar um único certificado que tenha um curinga (*.com) ou que tenha o FQDN de cluster como CN, FQDNs de cada servidor CMS e URL de junção, se necessário.

Serviço	Comando
Webadmin	<code>pki csr <cert name> CN:<server FQDN></code>
Webbridge	<code>pki csr <cert name> CN:<Server FQDN> subjectAltName:<Join Url>,<XMPP domain></code>
Callbridge TURN Balanceador de carga	<code>pki csr <cert name> CN:<Server FQDN's></code>

3. Caso o CMS esteja em cluster, execute os próximos comandos.

Serviço	Comando
Callbridge TURN Balanceador de carga	<code>pki csr <cert name> CN:<cluster FQDN> subjectAltName:<Peer FQDN's></code>
XMP	<code>pki csr <cert name> CN:<Cluster FQDN> subjectAltName:<XMPP Domain>,<Peer FQDN's></code>

Etapa 3. Gerar o CSR do Cluster do Banco de Dados e Usar a CA Interna para Assiná-los

Desde o CMS 2.7, é necessário ter certificados para o cluster do banco de dados. Na versão 2.7, incluímos uma CA interna que pode ser usada para assinar os certificados do banco de dados.

1. Em todos os núcleos, execute `database cluster remove`.
2. Na Principal, execute `pki selfsigned dbca CN`. Exemplo: `Pki dbca autoassinado CN:tplab.local`
3. No Primário, execute `pki csr dbserver CN:cmscore1.example.com subjectAltName`. Exemplo: `cmscore2.example.com,cmscore3.example.com`.
4. No Primário, crie um certificado para o banco de dados `clientpki csr dbclient CN:postgres`.
5. No Primário, use `dbca` para assinar o `dbserver cert` `pki sign dbserver dbca`.
6. No Principal, use `dbca` para assinar o `dbclient cert` `pki sign dbclient dbca`.

7. Copie o dbclient.crt para todos os servidores que precisam se conectar a um nó de banco de dados
8. Copie o arquivo dbserver.crt para todos os servidores que foram adicionados ao banco de dados (nós que formam o cluster de banco de dados).
9. Copie o arquivo dbca.crt para todos os servidores.
10. No servidor de BD primário, execute certificados de cluster de banco de dados dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt. Isso usa o dbca.crt como raiz ca-cert.
11. No servidor de BD primário, execute o cluster de banco de dados localnode a.
12. No servidor do BD Primário, execute database cluster initialize.
13. No servidor do BD Primário, execute o status do cluster do banco de dados. Deve ver Nodes: (me): Connected Primary.
14. Em todos os outros núcleos que estão Associados ao cluster de banco de dados, execute database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt.
15. Em todos os núcleos conectados (não colocados com um banco de dados) ao cluster de banco de dados, execute database cluster certs dbclient.key dbclient.crt dbca.crt.

- Nos núcleos que estão unidos (co-localizados com um banco de dados):

- execute o **cluster de banco de dados localnode a**.
- execute **junção de cluster de banco de dados**.

- NOS núcleos conectados (não colocados em um banco de dados):

- executar **cluster de banco de dados localnode a**.
- executar **conexão de cluster de banco de dados**.

Etapa 4. Verificar os certificados assinados

- A validade do certificado (data de expiração) pode ser verificada com a inspeção do certificado, execute o comando **pki inspect <filename>**.
- Você pode validar se um certificado corresponde a uma chave privada; execute o comando **pki match <keyfile> <certificate file>**.
- Para validar que um certificado é assinado pela CA e que o pacote de certificados pode ser usado para declará-lo, execute o comando **pki verify <cert> <certificate bundle/Root CA>**.

Etapa 5. Aplicar certificados assinados aos componentes em servidores CMS

- Para aplicar certificados ao Webadmin, execute os próximos comandos:

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

- Para aplicar certificados ao Callbridge, execute os próximos comandos:

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

- Para aplicar certificados ao Webbridge, execute os próximos comandos:

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

- Para aplicar certificados ao XMPP, execute os próximos comandos:

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

- Para aplicar certificados ao banco de dados ou substituir certificados expirados no cluster do banco de dados atual, execute os próximos comandos:

```
database cluster remove (on all servers, noting who was primary before beginning) database cluster certs <server_key> <server_certificate> <client_key> <client_certificate>
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 cluster)
```

- Para aplicar certificados ao TURN, execute os próximos comandos:

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

Cadeias e Pacotes de Certificados Confiáveis

Desde o CMS 3.0, você deve usar cadeias de certificados confiáveis ou relações de confiança de cadeia completa. Além disso, é importante para qualquer serviço que você reconheça como os certificados devem ser criados quando você cria pacotes.

Quando você cria uma cadeia de certificados confiáveis, conforme exigido pela Web bridge 3, você deve criá-la conforme mostrado na imagem, com o certificado de entidade na parte superior, os intermediários no meio, a CA raiz na parte inferior e, em seguida, um único retorno de carro.

```
-----BEGIN CERTIFICATE-----
Entity cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
root cert
-----END CERTIFICATE-----
single carriage return at end
```

Sempre que você criar um pacote, o certificado deverá ter apenas um retorno de carro no final.

Os pacotes de CA seriam os mesmos mostrados na imagem, mas, é claro, não haveria certificado de entidade.

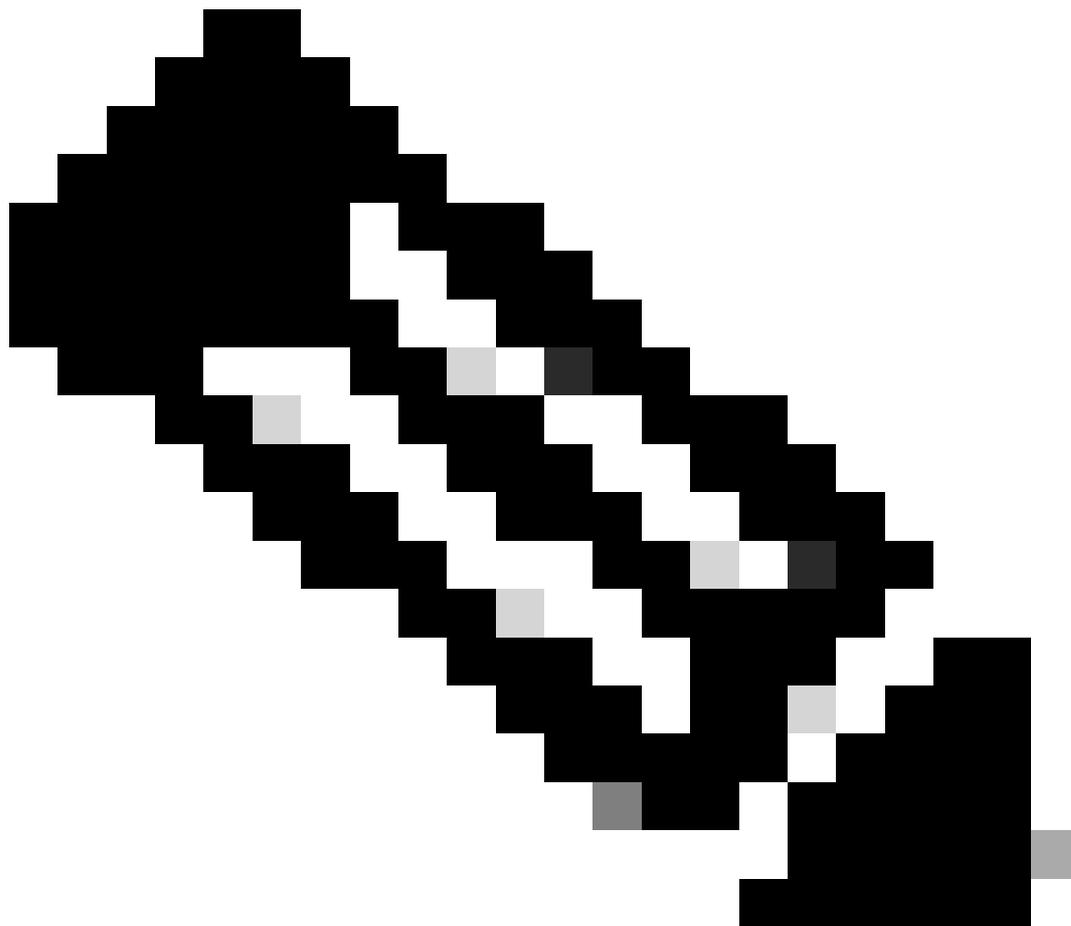
Troubleshooting

Se você precisar substituir um certificado expirado para todos os serviços, exceto certificados de banco de dados, o método mais fácil é carregar novos certificados com o MESMO nome dos certificados antigos. Se você fizer isso, o serviço precisará ser reiniciado e você não precisará

reconfigurar o serviço.

Se você executar **pki csr ...** e esse nome de certificado corresponder a uma chave atual, ele interromperá imediatamente o serviço. Se a produção estiver ativa e você criar proativamente um novo CSR e uma nova chave, use um novo nome. Você pode renomear o nome atualmente ativo antes de carregar o novo certificado nos servidores.

Se os certificados do banco de dados tiverem expirado, você precisará verificar com o **status do cluster do banco de dados** quem é o banco de dados Primário e, em todos os nós, executar o comando **database cluster remove**. Em seguida, você poderá usar as instruções da Etapa 3. Gere o cluster de banco de dados CSR e use uma CA interna para assiná-los.



Observação: caso você precise renovar os certificados do Cisco Meeting Manager (CMM), consulte o próximo vídeo: [Atualizando o certificado SSL do Cisco Meeting Management](#).

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.