Configurar certificado de servidor UCS para CIMC

Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Informações de Apoio Configurar Gerar CSR Criar certificado autoassinado Verificar Troubleshooting Informações Relacionadas

Introdução

Este documento descreve como gerar uma CSR (Certificate Signing Request, Solicitação de assinatura de certificado) para obter um novo certificado.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Você deve fazer logon como um usuário com privilégios de administrador para configurar certificados.
- Verifique se a hora do CIMC está definida como a hora atual.

Componentes Utilizados

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

- CIMC 1.0 ou posterior
- Openssl

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.

Informações de Apoio

O certificado pode ser carregado no Cisco Integrated Management Controller (CIMC) para substituir o certificado de servidor atual. O certificado do servidor pode ser assinado por uma CA (Autoridade de

Certificação) pública, como Verisign, ou por sua própria autoridade de certificação. O comprimento da chave do certificado gerado é 2048 bits.

Configurar

Etapa 1.	Gere o CSR do CIMC.
Etapa 2.	Envie o arquivo CSR a uma CA para assinar o certificado. Se sua organização gerar seus próprios certificados autoassinados, você poderá usar o arquivo CSR para gerar um certificado autoassinado.
Etapa 3.	Carregue o novo certificado no CIMC.

Observação: o certificado carregado deve ser criado a partir de um CSR gerado pelo CIMC. Não carregue um certificado que não foi criado por este método.

Gerar CSR

Navegue até a guia Admin > Security Management > Certificate Management > Generate Certificate Signing Request (CSR) e preencha os detalhes marcados com um *.

Além disso, consulte o guia Gerando uma solicitação de assinatura de certificado.

ificate Management Secu	ure Key Management Security (Configuration MCTP SPDM	1		
enerate Certificate Signing Reques	st Upload Server Certificate Upload E	xternal Certificate Upload Externa	al Private Key Activate External Certific	ate	
		Generate Certificate Signir	ng Request		0 ×
Current Certificate		* Common Name:	Host01		
and all Monters		Subject Alternate Name:	Subject Alternate Name	dNSName v	+
Subject Information:	: 212DAF6E68B58418158BD0480	* Organization Name:	Cisco		
Country Code (CC) State (S)	: MX : Mexico	Organization Unit:	Cisco		
Locality (L) Organization (O)	: Mexico : Cisco J) : C-Series : HostOl	* Locality:	CA		
Organizational Unit (OU Common Name (CN)		* State Name:	California		
Issuer Information:	: MX : Mexico	* Country Code:	United States	•	
State (S)		Email:	Please enter Valid Email Address	-	
Organization (O) Organizational Unit (OU)	: Cisco) : C-Series	Signature Algorithm:	SHA384	•	
Common Name (CN)	: Host01	Challenge Password:			
Valid From Valid To	: Jun 15 22:47:56 2023 GMT : Sep 17 22:47:56 2025 GMT	String Mask:	Select	•	
		Self Signed Certificate:			
		Selecting this option will prom	pt Cisco IMC to generate Self Signed C	ertificate.	
Certificate Signing Reques	st Status	Communication with the manage	gement controller may be lost moment	tarily and you will ne	ed to re-login.
Status: Not in progre	155.	Even SSH, vKVM and vMedia s	essions will be disconnected.		
			0	BreatMalana	0
External Certificate	External Private Key		Generate CSR	Reset Values	Cancel

Cuidado: use o *Nome alternativo do assunto* para especificar nomes de host adicionais para este servidor. Se o dNSName não for configurado ou excluído do certificado carregado, os navegadores poderão bloquear o acesso à interface do Cisco IMC.

O que fazer em seguida?

Execute estas tarefas:

- Se você não quiser obter um certificado de uma autoridade de certificação pública, e se sua organização não operar sua própria autoridade de certificação, você poderá permitir que o CIMC gere internamente um certificado autoassinado do CSR e carregue-o imediatamente no servidor. **Marque** a caixa **Self Signed Certificate** para executar esta tarefa.
- Se sua organização opera seus próprios certificados autoassinados, copie a saída do comando de -----BEGIN ...para END CERTIFICATE REQUEST----- e cole em um arquivo chamado csr.txt. Insira o arquivo CSR no servidor de certificados para gerar um certificado autoassinado.
- Se você obter um certificado de uma autoridade de certificação pública, copie a saída do comando de -----BEGIN ... para END CERTIFICATE REQUEST----- e cole em um arquivo chamado csr.txt. Envie o arquivo CSR à autoridade de certificação para obter um certificado assinado. Certifique-se de que o certificado seja do tipo Servidor.

Observação: após a geração de certificado bem-sucedida, a GUI da Web do Cisco IMC é reiniciada. A comunicação com o controlador de gerenciamento pode ser perdida momentaneamente e um novo login é necessário.

Se você não usou a primeira opção, na qual o CIMC gera e carrega internamente um certificado autoassinado, você deve criar um novo certificado autoassinado e carregá-lo no CIMC.

Criar certificado autoassinado

Como alternativa a uma CA pública e assinar um certificado de servidor, opere sua própria CA e assine seus próprios certificados. Esta seção mostra comandos para criar uma CA e gerar um certificado de servidor com o certificado de servidor OpenSSL. Para obter informações detalhadas sobre o OpenSSL, consulte <u>OpenSSL</u>.

Etapa 1. Gere uma chave privada RSA como mostrado na imagem.

<#root>

[root@redhat ~]#

```
openssl genrsa -out ca.key 1024
```

Etapa 2. Gere um novo certificado autoassinado como mostrado na imagem.

```
<#root>
[root@redhat ~]#
openssl req -new -x509 -days 1095 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [XX]:
US
State or Province Name (full name) []:
California
Locality Name (eg, city) [Default City]:
California
Organization Name (eg, company) [Default Company Ltd]:
Cisco
```

```
Organizational Unit Name (eg, section) []:
Cisco
Common Name (eg, your name or your server's hostname) []:
HostO1
Email Address []:
[root@redhat ~]#
```

Etapa 3. Certifique-se de que o tipo de certificado seja servidor, conforme mostrado na imagem.

```
<#root>
[root@redhat ~]#
echo "nsCertType = server" > openssl.conf
```

Etapa 4. Instrui a CA a usar seu arquivo CSR para gerar um certificado de servidor, como mostrado na imagem.

<#root> [root@redhat ~]# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile

Etapa 5. Verificar se o certificado gerado é do tipo Servidor conforme mostrado na imagem.

```
<#root>
[root@redhat ~]#
openssl x509 -in server.crt -purpose
Certificate purposes:
SSL client : No
SSL client CA : No
SSL server :
Yes
SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
S/MIME signing : No
S/MIME signing CA : No
S/MIME encryption : No
```

```
S/MIME encryption CA : No
CRL signing : Yes
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
Time Stamp signing : No
Time Stamp signing CA : No
----BEGIN CERTIFICATE-----
MIIDFzCCAoCqAwIBAqIBATANBqkqhkiG9w0BAQsFADBoMQswCQYDVQQGEwJVUzET
MBEGA1UECAwKQ2FsaWZvcm5pYTETMBEGA1UEBwwKQ2FsaWZvcm5pYTEOMAwGA1UE
CqwFQ21zY28xDjAMBqNVBAsMBUNpc2NvMQ8wDQYDVQQDDAZIb3N0MDEwHhcNMjMw
NjI3MjI0NDE1WhcNMjQwNjI2MjI0NDE1WjBgMQswCQYDVQQGEwJVUzETMBEGA1UE
CAwKQ2FsaWZvcm5pYTELMAkGA1UEBwwCQ0ExDjAMBqNVBAoMBUNpc2NvMQ4wDAYD
VQQLDAVDaXNjbzEPMA0GA1UEAwwGSG9zdDAxMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAuhJ50V004MZNV3dgQw0Mns9sgzZwjJS8Lv0tHt+GA4uzNf1Z
WKNyZbzD/yLoXiv8ZFgaWJbqEe2yijVzEcguZQTGFRkAWmDecKM9Fieob03B5FNt
pC8M9Dfb3YMkIx29abrZKFEIrYbabbG4gQyfzg0B6D9CK1WuoezsE7zH0oJX4Bcy
ISE0Rs0d9bsXvxyLk2cauS/zvI9hvrWW9P/0g8nF3Y+PGtm/bnfodEnNWFWPLtvF
dGuG5/wBmmMbEb/GbrH9uVcy0z+3HReDcQ+kJde7PoFK3d6Z0dkh7Mmtjpvk5ucQ
NgzaeoCDL0Bn+Z10800/eciSCsGIJKxYD/FY1QIDAQABo1UwUzARBg1ghkgBhvhC
AQEEBAMCBkAwHQYDVR00BBYEFEJ20TeuP27jyCJRiAKKfflNc0hbMB8GA1UdIwQY
MBaAFA4QR965FinE4GrhkiwRV62ziPj/MA0GCSqGSIb3DQEBCwUAA4GBAJuL/Bej
DxenfCt6pBA709GtkltWUS/rEtpQX190hdlahjwbfG/67MYIpIEbidL1BCw55dal
LI7sgu1dnItnIGsJI1L7h6IeFBu/coCvBtopOYUanaBJ1BgxBWhT2FAnmB9wIvYJ
5rMx95vWZXt3KGE8QlP+eGkmAHWA8M0yhwHa
-----END CERTIFICATE-----
[root@redhat ~]#
```

Etapa 6. Carregue o certificado do servidor conforme mostrado na imagem.

÷Ē	cisco Cisco Inte	grated Management (Controller	External Certificate uploaded successfully	÷
h / Certif	/ Security Manag	ement / Certificate N Secure Key Management	Anagement 🚖		Refresh Host Powe
Ger	erate Certificate Signing R	equest Upload Server Certifica	ate Upload External Certificate Uploa	ad External Private Key Activate External Certificate	
с	urrent Certificate				
S SOSLOCOO HOSLOCOO VV	erial Number Subject Information: Sountry Code (CC) itate (S) Socality (L) organizational Unit Common Name (CN) Subject (CC) State (S) Socality (L) Organizational Unit Sommon Name (CN) Vrganizational Unit Sommon Name (CN) Valid From Valid From	: 212DAF6E68B5841 : MX : Mexico : Mexico : C-Series : Host01 : MX : Mexico : Mexico : Mexico : Mexico : Cisco (OU) : C-Series : Host01 : Jun 15 22:47:56 : Sep 17 22:47:56	8158BD04804D64B2C5EE08B6B 2023 GMT 2025 GMT		
c	ertificate Signing Re Status: Not in p External Certificate	quest Status progress.	Кеу		

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Navegue até **Admin > Gerenciamento de Certificado** e verifique o Certificado Atual conforme mostrado na imagem.

ificate Management	Secure Key Management	Security Configuration	MCTP SPDM	1	
anouto munugomon	occure noy munugement	occurry comparation	MOTT OF DM		
enerate Certificate Signing	Request Upload Server Certifica	ate Upload External Certificate	Upload External F	Private Key Activate External Certific	ate
Current Certificate					
Serial Number	: 01				
Subject Informatio Country Code (CC)	n: : US				
State (S) Locality (L)	: California : CA				
Organization (O) Organizational Uni Common Name (CN)	t (OU) : Cisco t (OU) : Fost01				
Issuer Information	:				
Country Code (CC) State (S)	: US : California				
Locality (L) Organization (O)	: California : Cisco				
Common Name (CN)	t (OU) : Cisco : Host01				
Valid From Valid To	: Jun 27 22:44:15 : Jun 26 22:44:15	2023 GMT 2024 GMT			
Certificate Signing R	equest Status				
Status: Not i	n progress.				

Troubleshooting

No momento, não há informações específicas disponíveis para solucionar esse problema de configuração.

Informações Relacionadas

- <u>ID de bug Cisco CSCup26248</u> Não é possível carregar o certificado SSL de CA de terceiros no CIMC 2.0.(1a)
- Suporte Técnico e Documentação Cisco Systems

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.