UCS Server-certificaat configureren naar CIMC

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren MVO genereren Zelfondertekend certificaat maken Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u een aanvraag voor het ondertekenen van een certificaat (CSR) genereert om een nieuw certificaat te verkrijgen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- U moet inloggen als gebruiker met beheerdersrechten om certificaten te configureren.
- Zorg ervoor dat de CIMC-tijd is ingesteld op de huidige tijd.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CIMC 1.0 of hoger
- OpenSSL

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het certificaat kan worden geüpload naar de Cisco Integrated Management Controller (CIMC) om het huidige servercertificaat te vervangen. Het servercertificaat kan worden ondertekend door een openbare certificeringsinstantie (CA), zoals Verisign, of door uw eigen certificeringsinstantie. De gegenereerde certificaatsleutellengte is 2048 bits.

Configureren

Stap 1.	Genereert de CSR via de CIMC.
Stap 2.	Leg het CSR-bestand voor aan een CA om het certificaat te ondertekenen. Als uw organisatie eigen zelfondertekende certificaten genereert, kunt u het CSR-bestand gebruiken om een zelfondertekend certificaat te genereren.
Stap 3.	Upload het nieuwe certificaat naar de CIMC.

Opmerking: het geüploade certificaat moet worden aangemaakt op basis van een CSR dat door de CIMC wordt gegenereerd. Upload geen certificaat dat niet met deze methode is gemaakt.

MVO genereren

Navigeer naar het tabblad **Beheerder** > **Beveiligingsbeheer** > **Certificaatbeheer** > **Certificaatondertekeningsaanvraag** (CSR) genereren en vul de gegevens in die zijn gemarkeerd met een *.

Raadpleeg ook de handleiding voor het genereren van een aanvraag voor certificaatondertekening.

ficate Management Secu	are Key Management Security	Configuration MCTP SPDN	t			
enerate Certificate Signing Reques	t Upload Server Certificate Upload	External Certificate Upload Externa	al Private Key Activate External Certifi	cate		
		Generate Certificate Signi	ng Request			0 ×
Current Certificate		* Common Name:	Host01			
and al Number		Subject Alternate Name:	Subject Alternate Name	dNSName	v +	ĭ l
Subject Information:	: 212DAF6E68B58418158BD048	* Organization Name:	Cisco			
Country Code (CC) State (S)	: MX : Mexico	Organization Unit:	Cisco			
Locality (L) Organization (O)	: Mexico : Cisco	* Locality:	CA			
Organizational Unit (OU) Common Name (CN)	: C-Series : Host01	* State Name:	California			
Issuer Information:		* Country Code:	United States	•		
State (S)	: MX : Mexico	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	Certificate.	rtad	
ertificate Signing Reques	t Status	Communication with the mana	gement controller may be lost momen	ntarily and you will	need to r	e-login.
Status: Not in progre	65.	Even SSH, vKVM and vMedia s	essions will be disconnected.			
External Certificate	External Private Key		Generate CSR	Reset Values	Ca	ncel

Waarschuwing: gebruik de *alternatieve onderwerpnaam* om extra hostnamen voor deze server op te geven. Het niet configureren van NSName of het uitsluiten van het geüploade certificaat kan resulteren in browsers die de toegang tot de Cisco IMC-interface blokkeren.

Wat nu?

Voer de volgende taken uit:

- Als u geen certificaat van een openbare certificeringsinstantie wilt verkrijgen en uw organisatie geen eigen certificeringsinstantie beheert, kunt u CIMC toestaan intern een zelfondertekend certificaat van de CSR te genereren en het onmiddellijk naar de server te uploaden. **Controleer** het vakje **Zelfondertekend certificaat** om deze taak uit te voeren.
- Als uw organisatie zelf ondertekende certificaten gebruikt, kopieert u de opdrachtoutput van -----BEGIN ...om HET CERTIFICAAT AAN TE VRAGEN----- en te plakken op een bestand met de naam csr.txt. Voer het CSR-bestand in op uw certificaatserver om een zelfondertekend certificaat te genereren.
- Als u een certificaat verkrijgt van een openbare certificeringsinstantie, kopieert u de opdrachtoutput van -----BEGIN ... om HET CERTIFICAAT AAN TE VRAGEN----- en te plakken op een bestand met de naam csr.txt. Leg het MVO-bestand voor aan de certificeringsinstantie om een ondertekend

certificaat te verkrijgen. Zorg ervoor dat het certificaat van het type Server is.

Opmerking: na een succesvolle certificaatgeneratie wordt de Cisco IMC Web GUI opnieuw gestart. De communicatie met de managementcontroller kan tijdelijk verloren gaan en opnieuw inloggen is vereist.

Als u de eerste optie niet hebt gebruikt, waarin CIMC intern een zelf-ondertekend certificaat genereert en uploadt, moet u een nieuw zelf-ondertekend certificaat maken en uploaden naar de CIMC.

Zelfondertekend certificaat maken

Als alternatief voor een openbare CA en onderteken een servercertificaat, beheer uw eigen CA en onderteken uw eigen certificaten. Deze sectie toont opdrachten om een CA te maken en een servercertificaat te genereren met het OpenSSL-servercertificaat. Zie <u>OpenSSL</u> voor meer informatie over OpenSSL.

Stap 1. Genereert RSA private key zoals in de afbeelding.

```
<#root>
[root@redhat ~]#
openssl genrsa -out ca.key 1024
```

Stap 2. Genereer nieuw zelfondertekend certificaat zoals in de afbeelding.

```
<#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 ~]#
```

Stap 3. Zorg ervoor dat het certificaattype een server is zoals in de afbeelding.

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

Stap 4. Leidt de CA om uw CSR-bestand te gebruiken om een servercertificaat te genereren zoals in de afbeelding.

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

Stap 5. Controleer of het gegenereerde certificaat van type is Server zoals in de afbeelding.

```
<#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 : 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
CAwKQ2FsaWZvcm5pYTELMAkGA1UEBwwCQ0ExDjAMBgNVBAoMBUNpc2NvMQ4wDAYD
VQQLDAVDaXNjbzEPMA0GA1UEAwwGSG9zdDAxMIIBIjANBqkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAuhJ50V004MZNV3dgQwOMns9sgzZwjJS8LvOtHt+GA4uzNf1Z
WKNyZbzD/yLoXiv8ZFgaWJbqEe2yijVzEcguZQTGFRkAWmDecKM9Fieob03B5FNt
pC8M9Dfb3YMkIx29abrZKFEIrYbabbG4qQyfzq0B6D9CK1WuoezsE7zH0oJX4Bcy
ISE0Rs0d9bsXvxyLk2cauS/zvI9hvrWW9P/0g8nF3Y+PGtm/bnfodEnNWFWPLtvF
dGuG5/wBmmMbEb/GbrH9uVcy0z+3HReDcQ+kJde7PoFK3d6Z0dkh7Mmtjpvk5ucQ
NgzaeoCDL0Bn+Z10800/eciSCsGIJKxYD/FY1QIDAQABo1UwUzARBg1ghkgBhvhC
AQEEBAMCBkAwHQYDVR00BBYEFEJ20TeuP27jyCJRiAKKfflNc0hbMB8GA1UdIwQY
MBaAFA4QR965FinE4GrhkiwRV62ziPj/MA0GCSqGSIb3DQEBCwUAA4GBAJuL/Bej
DxenfCt6pBA709GtkltWUS/rEtpQX190hdlahjwbfG/67MYIpIEbidL1BCw55dal
LI7sgu1dnItnIGsJI1L7h6IeFBu/coCvBtopOYUanaBJ1BgxBWhT2FAnmB9wIvYJ
5rMx95vWZXt3KGE8Q1P+eGkmAHWA8M0yhwHa
-----END CERTIFICATE-----
[root@redhat ~]#
```

Stap 6. Servercertificaat uploaden zoals in de afbeelding.

÷E	cisco Integrat	ed Management (Controller	External Certificate uploaded successfully	*
∩ / Cert	/ Security Manageme	ent / Certificate M ure Key Management	Security Configuration	ок	Refresh Host Powe
G	enerate Certificate Signing Reques	t Upload Server Certifica	te Upload External Certificate Uploa	d External Private Key Activate External Certificate	
_	Current Certificate				
	Serial Number Subject Information: Country Code (CC) State (S) Locality (L) Organization (O) Organizational Unit (OU) Common Name (CN) Issuer Information: Country Code (CC) State (S) Locality (L) Organization (O) Organizational Unit (OU) Common Name (CN) Valid From Valid To	: 212DAF6E68B58418 : MX : Mexico : Cisco : C-Series : Host01 : MX : Mexico : Cisco : Cisco : C-Series : Host01 : Jun 15 22:47:56 : Sep 17 22:47:56	2023 GNT 2025 GNT		
	Certificate Signing Reques Status: Not in progre	st Status			
•	External Certificate	► External Private I	Кеу		

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Navigeer naar **Beheer > Certificaatbeheer** en controleer het huidige certificaat zoals in de afbeelding.

tificate Management	Secure Key Management	Security Configuration	MCTP SPDM		
enerate Certificate Signing	Request Upload Server Certifica	ate Upload External Certificate	Upload External Priv	vate Key Activate External Certificate	
Current Certificate					
Serial Number Subject Informatic Country Code (CC) State (S) Locality (L) Organization (O) Organizational Uni Common Name (CN)	: 01 : US : California : CA : Cisco : Cisco : Host01				
Issuer Information Country Code (CC) State (S) Locality (L) Organization (O) Organizational Uni Common Name (CN)	: US : California : California : Cisco t (OU) : Cisco : Host01				
Valid From Valid To	: Jun 27 22:44:15 : Jun 26 22:44:15	2023 GMT 2024 GMT			
Certificate Signing F	Request Status				
Status: Not	in progress.				

Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar om deze configuratie problemen op te lossen.

Gerelateerde informatie

- <u>Cisco bug-id CSCup26248</u> CA SSL-certificaat van derden kan niet naar CIMC 2.0 worden geüpload.(1a)
- <u>Technische ondersteuning en documentatie Cisco Systems</u>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.