Configurazione del certificato del server UCS in CIMC

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Configurazione Genera CSR Crea certificato autofirmato Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritto come generare una richiesta di firma di un certificato (CSR) per ottenere un nuovo certificato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Per configurare i certificati, è necessario accedere come utente con privilegi di amministratore.
- Verificare che l'ora CIMC sia impostata sull'ora corrente.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CIMC 1.0 o versioni successive
- Openssl

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il certificato può essere caricato su Cisco Integrated Management Controller (CIMC) per sostituire il certificato del server corrente. Il certificato del server può essere firmato da un'Autorità di certificazione (CA) pubblica, ad esempio Verisign, oppure dall'Autorità di certificazione dell'utente. La lunghezza della

chiave del certificato generata è di 2048 bit.

Configurazione

| Passaggio 1. | Generare il CSR dal CIMC. |
|-----------------|--|
| Passaggio 2. | Inviare il file CSR a una CA per firmare il certificato. Se l'organizzazione genera certificati autofirmati, è possibile utilizzare il file CSR per generare un certificato autofirmato. |
| Passaggio 3. | Caricare il nuovo certificato nel CIMC. |

Nota: il certificato caricato deve essere creato da un CSR generato dal CIMC. Non caricare un certificato non creato con questo metodo.

Genera CSR

Passare alla scheda Amministrazione > Gestione protezione > Gestione certificati > Genera richiesta di firma del certificato (CSR) e immettere i dettagli contrassegnati con un *.

Consultare inoltre la guida Generazione di una richiesta di firma del certificato.

| ficate Management Secu | re Key Management Security C | Configuration MCTP SPDM | 1 | |
|--|--|--------------------------------------|--|--|
| enerate Certificate Signing Reques | t Upload Server Certificate Upload E | xternal Certificate Upload Externa | I Private Key Activate External Certif | icate |
| 0 | | Generate Certificate Signir | ng Request | @ X |
| Surrent Certificate | | * Common Name: | Host01 | |
| Serial Number | · 212DAF6F68B58418158BD0480 | Subject Alternate Name: | Subject Alternate Name | dNSName v + |
| Subject Information: | | * 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: | . wy | * Country Code: | United States | ¥ |
| State (S) Locality (L) | : Mexico : 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: | | Castificate |
| | | WARNING: After successful ce | rtificate generation, the Cisco IMC W | eb GUI will be restarted. |
| Certificate Signing Reques | t Status | Communication with the manag | gement controller may be lost mome | ntarily and you will need to re-login. |
| Status: Not in progre | \$5. | Even SSH, vKVM and vMedia s | essions will be disconnected. | |
| | | | Converte CCC | Reset Volume Ormut |
| External Certificate | External Private Key | | Generate CSR | Reset values Cancel |
| | | | | |

Attenzione: utilizzare il *nome soggetto alternativo* per specificare ulteriori nomi host per il server. La mancata configurazione di dNSName o l'esclusione del file dal certificato caricato potrebbero causare il blocco dell'accesso all'interfaccia Cisco IMC da parte dei browser.

Come procedere?

Eseguire i seguenti task:

- Se non si desidera ottenere un certificato da un'autorità di certificazione pubblica e se l'organizzazione non gestisce la propria autorità di certificazione, è possibile consentire a CIMC di generare internamente un certificato autofirmato dal CSR e caricarlo immediatamente nel server. **Selezionare** la casella **Certificato autofirmato** per eseguire questa operazione.
- Se l'organizzazione dispone di certificati autofirmati, copiare l'output del comando da â€"BEGIN ...per TERMINARE LA RICHIESTA DI CERTIFICATO e incollarla in un file denominato csr.txt. Immettere il file CSR nel server di certificazione per generare un certificato autofirmato.
- Se si ottiene un certificato da un'autorità di certificazione pubblica, copiare l'output del comando da â€"BEGIN ... per TERMINARE LA RICHIESTA DI CERTIFICATO e incollarla in un file denominato csr.txt. Inviare il file CSR all'autorità di certificazione per ottenere un certificato firmato. Verificare che il certificato sia di tipo Server.

Nota: dopo aver generato correttamente il certificato, l'interfaccia utente grafica (GUI) di Cisco IMC Web viene riavviata. La comunicazione con il controller di gestione potrebbe interrompersi momentaneamente ed è necessario effettuare nuovamente l'accesso.

Se non è stata utilizzata la prima opzione, in cui CIMC genera e carica internamente un certificato autofirmato, è necessario creare un nuovo certificato autofirmato e caricarlo nel CIMC.

Crea certificato autofirmato

In alternativa a una CA pubblica e alla firma di un certificato server, è possibile utilizzare la propria CA e firmare i propri certificati. Questa sezione illustra i comandi per creare una CA e generare un certificato server con il certificato server OpenSSL. Per informazioni dettagliate su OpenSSL, vedere <u>OpenSSL</u>.

Passaggio 1. Generare la chiave privata RSA come mostrato nell'immagine.

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

Passaggio 2. Generare un nuovo certificato autofirmato come mostrato nell'immagine.

<#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]:

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) []:
Host01
Email Address []:
[root@redhat ~]#
```

Passaggio 3. Verificare che il tipo di certificato sia server, come illustrato nell'immagine.

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

Passaggio 4. Indica all'autorità di certificazione di utilizzare il file CSR per generare un certificato server, come mostrato nell'immagine.

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

Passaggio 5. Verifica se il certificato generato è di tipo Server come mostrato nell'immagine.

```
<#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
CgwFQ21zY28xDjAMBgNVBAsMBUNpc2NvMQ8wDQYDVQQDDAZIb3N0MDEwHhcNMjMw
NjI3MjI0NDE1WhcNMjQwNjI2MjI0NDE1WjBqMQswCQYDVQQGEwJVUzETMBEGA1UE
CAwKQ2FsaWZvcm5pYTELMAkGA1UEBwwCQ0ExDjAMBqNVBAoMBUNpc2NvMQ4wDAYD
VQQLDAVDaXNjbzEPMA0GA1UEAwwGSG9zdDAxMIIBIjANBgkghkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAuhJ50V004MZNV3dgQw0Mns9sgzZwjJS8Lv0tHt+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
LI7squ1dnItnIGsJIlL7h6IeFBu/coCvBtopOYUanaBJ1BqxBWhT2FAnmB9wIvYJ
5rMx95vWZXt3KGE8Q1P+eGkmAHWA8M0yhwHa
----END CERTIFICATE-----
[root@redhat ~]#
```

Passaggio 6. Caricare il certificato del server come mostrato nell'immagine.

| 😸 📲 diale Cisco Integra | ted Management C | Controller | External Certificate uploaded successfully | ÷ |
|--|--|--|--|---------------------|
| / / Security Managem Certificate Management Sec | ent / Certificate M | anagement 🚖 | ок | Refresh Host Powe |
| Generate Certificate Signing Reque | st Upload Server Certifical | e Upload External Certificate Uplo | oad External Private Key Activate External Certificate | |
| Serial Number Subject Information: Country Code (CC) State (S) Locality (L) 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) : C-Series : Host01 : Jun 15 22:47:56 : Sep 17 22:47:56 | 158BD04804D64B2C5EE08B6B 2023 GMT 2025 GMT | | |
| Certificate Signing Reque Status: Not in progr External Certificate | st Status ess. ▶ External Private I | (ey | | |

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Passare a **Amministrazione > Gestione certificati** e verificare il certificato corrente come mostrato nell'immagine.

| rtificate Management | Secure Key Management | Security Configuration | MCTP SPDM | | |
|---|--|-----------------------------------|----------------------|---|---|
| Senerate Certificate Signing | Request Upload Server Certifica | ate Upload External Certificate | Upload External Priv | ate Key Activate External Certificate | , |
| Current Certificate | | | | | |
| Serial Number | : 01 | | | | |
| Subject Informatic Country Code (CC) | i US | | | | |
| State (S) Locality (L) | : California : CA | | | | |
| Organization (0) Organizational Uni | : Cisco it (OU) : Cisco | | | | |
| Common Name (CN) | : Host01 | | | | |
| Issuer Information Country Code (CC) | i: : US | | | | |
| State (S) Locality (L) | : California : California | | | | |
| Organization (O) Organizational Uni | : Cisco it (OU) : Cisco | | | | |
| Common Name (CN) | : Host01 | | | | |
| Valid From Valid To | : Jun 27 22:44:15 : Jun 26 22:44:15 | 2023 GMT 2024 GMT | | | |
| | | | | | |
| | | | | | |
| Certificate Signing I | Request Status | | | | |
| | | | | | |
| Status: Not | in progress. | | | | |

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per risolvere i problemi relativi a questa configurazione.

Informazioni correlate

- <u>ID bug Cisco CSCup26248</u> Impossibile caricare il certificato SSL dell'autorità di certificazione di terze parti in CIMC 2.0(1a).
- Documentazione e supporto tecnico â€" Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).