証明書の管理

サーバ証明書の管理

ステップ 1 CIMC から CSR を生成します。

ステップ 2 証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。

ステップ 3 新しい証明書を CIMC にアップロードします。

（注） アップロードされた証明書は、CIMC によって生成された CSR から作成される必要があります。この方法で作成されていない証明書はアップロードしないでください。

証明書署名要求の生成

始める前に

証明書を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope certificate**	証明書コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /certificate # **generate-csr**	証明書署名要求（CSR）の生成に関するダイアログを起動します。

証明書署名要求に関して、次の情報の入力を求めるプロンプトが表示されます。

Common Name（CN）	CIMC の完全修飾ホスト名
Organization Name (O)	証明書を要求している組織。
Organization Unit (OU)	組織ユニット
Locality（L）	証明書を要求している会社の本社が存在する市または町。
StateName (S)	証明書を要求している会社の本社が存在する州または行政区分。
Country Code (CC)	会社の本社が存在する国を示す 2 文字の ISO 国コード。
Email	会社の管理用電子メールの連絡先。

要求された情報を入力すると、証明書署名要求が生成され、コンソール出力に表示されます。CSR ファイルは作成されませんが、コンソール出力から CSR 情報をコピーして、テキストファイルに貼り付けることができます。

例

次に、証明書署名要求を生成する例を示します。

```
Server /certificate # generate-csr
Common Name (CN): test.example.com
Organization Name (O): Example, Inc.
Organization Unit (OU): Test Department
Locality (L): San Jose
StateName (S): CA
Country Code (CC): US
Email: user@example.com
[Supported Algorithms: sha1, sha256, sha384, sha512 (Default sha384)]
Signature Algorithm: sha384
Do you want to set Challenge Password ? [y|n] (Default y)n
String Encoding utf8only/nombstr/pkix/default (Enter to skip):
Do you want to enter Subject Alternative Name parameters?[y|n]n
Continue to generate CSR?[y|N]y
Do you want self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]y

Server /certificate # show detail
Certificate Information:
    Serial Number: 3FA8AF325A18359FAFB29C518838A542D945F0EB
    Subject Country Code (CC): US
    Subject State (S): CA
    Subject Locality (L): San Jose
    Subject Organization (O): "Example
    Subject Organizational Unit (OU): Test Department
```

```
Subject Common Name (CN): test.example.com
Issuer Country Code (CC): US
Issuer State (S): CA
Issuer Locality (L): San Jose
Issuer Organization (O): "Example
Issuer Organizational Unit (OU): Test Department
Issuer Common Name (CN): test.example.com
Valid From: Mar 24 04:32:34 2023 GMT
Valid To: Jun 26 04:32:34 2025 GMT
```

次のタスク

次のいずれかの作業を実行します。

- 公共の認証局から証明書を取得したくない場合に、組織が独自の認証局を運用していなければ、CSRから自己署名証明書を内部生成し、すぐにサーバーにアップロードするよう、CIMC を設定できます。この処理を行うには、この例では最後のプロンプトの後に **y** と入力します。
- 組織が自己署名証明書を生成するための独自の証明書サーバーを運用している場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、csr.txt というファイルに貼り付けます。CSR ファイルを証明書サーバーに入力して、自己署名証明書を生成します。
- 公共の認証局から証明書を取得する場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、csr.txt というファイルに貼り付けます。CSR ファイルを認証局に提出して、署名付き証明書を取得します。

CIMC によって自己署名証明書を内部生成し、アップロードする最初のオプションを使用しない場合は、証明書コマンド モードで **upload** コマンドを使用して新しい証明書をアップロードする必要があります。

自己署名証明書の作成

パブリック認証局（CA）を使用してサーバー証明書の生成と署名を行う代わりに、独自のCAを運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。OpenSSL の詳細については「http://www.openssl.org」を参照してください。

（注） これらのコマンドは、CIMC ではなく、OpenSSL パッケージを使用している Linux サーバーで入力します。

始める前に

組織内のサーバーで、証明書サーバーのソフトウェアパッケージを取得してインストールします。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *CA_keyfilenamekeysize* 例： `# openssl genrsa -out ca.key 1024`	このコマンドは、CA によって使用される RSA 秘密キーを生成します。 （注） ユーザ入力なしで CA がキーにアクセスできるように、このコマンドに -des3 オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバーは、アクティブな CA です。
ステップ 3	**echo"nsCertType = server" > openssl.conf** 例： `# echo "nsCertType = server" > openssl.conf`	このコマンドは、証明書がサーバー限定の証明書であることを指定する行を OpenSSL 設定ファイルに追加します。この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType = server" という文が含まれています。
ステップ 4	**openssl x509 -text -noout -in ca.crt** 例： `# openssl x509 -text -noout -in ca.crt`	このコマンドは証明書を表示します。

例

この例は、CA の作成方法、および新規に作成された CA が署名するサーバー証明書の生成方法を示します。これらのコマンドは、OpenSSL を実行している Linux サーバーで入力します。

```
[root@localhost ~]# openssl genrsa -out ca.key 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
...........+++++
......+++++
e is 65537 (0x010001)
[root@localhost ~]# openssl req -new -x509 -days 365 -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) []:CA
Locality Name (eg, city) [Default City]:San Jose
Organization Name (eg, company) [Default Company Ltd]:Example
Organizational Unit Name (eg, section) []:Test Department
Common Name (eg, your name or your server's hostname) []:test.example.com
Email Address []:user@example.com
[root@localhost ~]#
[root@localhost ~]# echo "nsCertType = server" > openssl.conf
[root@localhost ~]# openssl x509 -text -noout -in ca.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            33:52:14:5a:12:8d:12:9c:c1:fa:77:13:a5:0c:eb:af:83:bd:6b:68
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = CA, L = San Jose, O = Example, OU = Test Department, CN =
test.example.com, emailAddress = user@example.com
        Validity
            Not Before: Mar 28 23:15:11 2023 GMT
            Not After : Mar 27 23:15:11 2024 GMT
        Subject: C = US, ST = CA, L = San Jose, O = Example, OU = Test Department, CN =
 test.example.com, emailAddress = user@example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (1024 bit)
                Modulus:
                    00:b9:a6:16:7d:bf:74:d0:10:e2:61:af:56:55:ee:
                    60:e6:57:c0:74:bd:b0:0b:7d:64:54:75:74:d8:f8:
                    7b:3e:1a:5b:cf:d4:76:6d:fb:01:92:07:d0:3b:45:
                    9c:49:22:7d:22:55:75:05:d9:94:d2:f2:7d:4b:14:
                    96:5e:fc:26:12:30:6f:1f:54:a8:40:25:e2:1a:62:
                    f8:ec:f8:be:e2:b0:fc:85:21:9b:cb:78:f7:6d:0e:
                    00:01:50:a9:07:e8:de:c2:b5:44:c5:41:c1:3a:0b:
                    93:4f:e9:94:c6:82:df:76:15:de:42:1f:b3:86:de:
                    96:0c:52:27:10:25:25:75:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                71:84:61:C4:AF:E7:57:2C:B4:BB:19:22:D7:DC:7A:7F:80:E8:58:A3
            X509v3 Authority Key Identifier:
                keyid:71:84:61:C4:AF:E7:57:2C:B4:BB:19:22:D7:DC:7A:7F:80:E8:58:A3

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         89:6d:7f:72:89:29:4e:8b:da:74:ec:8b:10:78:ca:86:68:be:
         88:c2:25:79:cd:a1:dc:7d:ac:32:18:be:7d:54:6e:12:c9:53:
         de:c3:dc:b3:e7:52:1e:14:c5:1c:10:95:3f:e3:df:04:82:27:
         19:56:55:c6:96:e1:0c:cc:0a:81:05:aa:3f:a3:29:52:b3:bb:
         66:78:55:2b:b0:c5:f9:f7:bc:fb:e4:fd:30:f2:16:73:65:88:
         38:ea:6f:dc:34:44:50:ef:3b:a8:ac:22:98:34:11:bb:e8:27:
         6d:da:5d:ff:18:b9:e4:4f:22:54:b9:ab:51:1f:41:51:00:4e:
         25:f6
[root@localhost ~]#
```

次のタスク

新しい証明書を CIMC にアップロードします。

サーバー証明書のアップロード

始める前に

証明書をアップロードするには、admin 権限を持つユーザーとしてログインする必要があります。

アップロードする証明書は、読み取り可能テキストとして使用できる必要があります。アップロード手順で、証明書テキストをコピーして CLI に貼り付けます。

（注） 最初に、CIMC 証明書管理 CSR の生成手順を使用して CSR を生成し、その CSR を使用してアップロード用の証明書を取得する必要があります。この方法で取得されていない証明書はアップロードしないでください。

（注） 新しいサーバー証明書がアップロードされると、現在の HTTPS および SSH セッションはすべて切断されます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope certificate**	証明書コマンド モードを開始します。
ステップ 2	Server /certificate # **upload**	新しいサーバー証明書を入力してアップロードするためのダイアログが起動します。

プロンプトが表示されたら、証明書テキストをコピーしてコンソールに貼り付け、CTRL を押した状態で D を押して証明書をアップロードします。

例

次に、新しい証明書をサーバーにアップロードする例を示します。

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
```

```
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。