証明書コマンド

connectorctl generatecert

このコマンドは、新しいセキュアソケットレイヤ（SSL）証明書を生成します。証明書のタイプは Rivest–Shamir–Adleman（RSA）または楕円曲線デジタル署名アルゴリズム（ECDSA）です。自己署名証明書を展開したら、**connectorctl showcert** コマンドを使用して証明書を表示できます。

connectorctl generatecert

コマンド履歴

リリース 2.3.2 より前	Connector SSL 証明書では、CSR の [Subject Alternative Name (SAN)] フィールドに IP アドレスが含まれます。
リリース 2.3.2	2.3.2 以降、コネクタ SSL 証明書では、CSR の [Subject Alternative Name (SAN)] フィールドに完全修飾ドメイン名（FQDN）またはホスト名が含まれます。

使用上のガイドライン

FQDN とホスト名は、CA 署名付き証明書の証明書署名要求（CSR）を設定します。CSR が CA によって署名されている場合、作成された証明書では、[SAN] フィールドに FQDN またはホスト名が含まれます。

CSCvt29826 の場合、IPSec を使用する AAA は、connectorctl generatecert コマンドを使用して生成される、キータイプが楕円曲線デジタル署名アルゴリズム（ECDSA）の Connector で生成される証明書と互換性がありません。https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvx40536

例

次に、以下のコマンドの出力例を示します。

```
[dnasadmin@conn171 ~]$ connectorctl generatecert
Key Type [RSA/ECDSA] [RSA]:
Generating RSA private key, 2048 bit long modulus
.
........
e is 65537 (0x10001)
generatecert successful.
Note: Rsyslog service is enabled with TLS protocol.
You may need to deploy connector's CA certificate into Remote Syslog Server.
You can use "connectorctl exportcacert" command to extract the CA certitifcate.
Afterwards, you may need to restart rsyslog service. using "connectorctl rsyslogconfig
restart"
```

関連トピック

connectorctl showcert （3 ページ）
connectorctl rsyslogconfig restart

connectorctl showcert

このコマンドは、展開された証明書の詳細を表示します。

connectorctl showcert

コマンド履歴

リリース 2.2	このコマンドが導入されました。

例

次に、以下のコマンドの出力例を示します。

```
dnasadmin@conn171 ~]$ connectorctl showcert

Certificate details
================================================================================================
                                        Certificate
================================================================================================
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            a2:b6:8f:39:9e:b3:e5:19
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=CA, L=San Jose, O=Cisco, CN=conn171
        Validity
            Not Before: Aug 17 21:29:13 2021 GMT
            Not After : Aug 17 21:29:13 2023 GMT
        Subject: C=US, ST=CA, L=San Jose, O=Cisco, CN=conn171
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:aa:2f:26:cb:37:d0:d9:d8:bc:83:42:ea:fe:fc:
                    e3:21:62:12:57:40:4e:73:fa:6d:82:8c:eb:00:37:
                    43:60:5b:70:30:09:a5:33:57:71:13:33:62:3d:de:
                    bb:51:39:b5:0b:f2:bc:2d:fc:20:38:b7:8c:ca:1b:
                    6a:9c:d3:84:dc:7d:ed:31:ca:96:e7:7e:dd:59:b5:
                    ee:ea:4b:f2:ec:9a:9a:58:65:8f:f6:05:ef:ee:40:
                    4f:78:37:09:a5:6b:79:e8:4a:df:17:2e:84:76:8c:
                    c4:59:30:6c:a3:9e:63:f5:f2:a0:5e:e0:0e:38:bd:
                    86:e2:f7:48:fb:7a:85:06:2f:37:a2:e8:c9:f0:b4:
                    85:99:65:91:a0:8d:ab:55:b0:cd:0a:69:26:9f:d3:
                    39:11:66:ea:1e:22:ce:59:3e:a2:c4:25:d6:07:74:
                    71:71:f1:1b:78:36:4d:28:57:2c:fd:5d:0d:f0:20:
                    3b:d4:bb:c7:90:4a:02:d1:f5:0d:49:1d:7a:10:7d:
                    ca:c3:ae:43:bc:7f:cf:a3:84:8f:0d:0f:b3:2e:48:
                    c8:61:d5:18:7e:d6:27:e7:e2:b2:17:d2:2e:57:05:
                    d1:22:c6:74:23:ee:d9:6e:c6:9f:cc:30:0a:be:f3:
                    b2:03:bf:bb:e7:ea:b1:e1:53:01:62:5b:ca:05:98:
                    e8:db
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                DA:2E:75:E3:F1:64:F4:35:5F:4C:B6:63:E2:E1:F1:E5:03:89:D3:CA
            X509v3 Authority Key Identifier:
                keyid:DA:2E:75:E3:F1:64:F4:35:5F:4C:B6:63:E2:E1:F1:E5:03:89:D3:CA

            X509v3 Basic Constraints:
                CA:TRUE
```

```
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Subject Alternative Name:
                DNS:conn171
    Signature Algorithm: sha256WithRSAEncryption
         4c:63:b0:f7:37:24:7c:b5:5d:f9:b0:c2:3e:dc:8b:c9:27:ab:
         7e:e9:00:1b:b3:49:9e:62:de:e1:eb:1c:8c:46:ad:96:ed:82:
         04:e4:f9:02:39:7f:6d:b6:4f:cb:49:87:03:aa:2c:75:37:0f:
         52:03:85:66:37:23:29:16:68:65:4a:f6:c7:8a:9e:df:c7:a9:
         e8:43:96:cc:4b:47:69:b7:ff:17:f6:8f:82:05:b2:d8:51:84:
         b4:56:85:99:31:7b:3a:ee:c5:e4:dd:f1:24:7a:d8:6d:b1:79:
         86:a8:1e:08:cf:be:3e:0d:2a:78:9b:23:7c:12:68:ce:c9:fd:
         49:39:5b:74:80:98:d0:cb:6f:7e:5a:5b:f2:65:77:04:22:3f:
         99:fe:cb:7e:08:bd:76:3b:91:3f:5f:a8:fa:8b:06:6f:f7:57:
         46:2f:73:ac:22:00:3a:e1:49:3c:dc:71:c2:db:e6:8a:00:de:
         d2:56:12:7b:ca:15:f7:29:89:11:8d:71:64:87:e0:75:7b:9e:
         a0:35:12:48:76:8f:11:9f:d5:3c:28:6b:e7:8a:d4:10:50:b1:
         b8:92:5e:61:98:d5:ac:56:82:75:38:cb:58:d3:3e:e4:13:27:
         b3:60:7a:b3:19:c7:6c:a8:76:0c:b2:0f:c8:a8:9a:a2:59:5c:
         26:b7:64:eb
================================================================================
                            Certificate for IOT interface
================================================================================
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cc:68:8e:6e:a7:26:a7:66
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=CA, L=San Jose, O=Cisco, CN=conn171
        Validity
            Not Before: Jul 15 20:28:15 2021 GMT
            Not After : Jul 15 20:28:15 2023 GMT
        Subject: C=US, ST=CA, L=San Jose, O=Cisco, CN=conn171
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:8b:30:3b:f5:6d:33:60:3f:63:0b:be:a4:b0:49:
                    b3:7f:bc:69:d3:ea:ab:e3:be:0b:43:da:f6:2c:40:
                    4e:7f:41:70:62:83:ae:cf:e5:ab:35:b5:e5:99:8a:
                    61:03:89:0f:c7:6f:26:d6:d4:b7:aa:d9:98:23:f3:
                    a4:da:8a:6b:59:0d:05:cf:17:3f:06:e2:41:10:f4:
                    4a:f6:96:99:58:57:27:b7:0a:4e:b5:5d:93:55:26:
                    fd:f6:51:f1:17:c5:a6:44:42:ae:18:1e:73:41:16:
                    ab:68:83:26:7f:45:3f:c1:b8:5e:0c:eb:a6:03:16:
                    64:41:95:92:b2:d8:a2:df:05:92:22:68:ec:dc:28:
                    85:5a:0c:aa:63:b6:e3:a1:41:08:04:5b:99:46:51:
                    c2:79:3d:8f:4c:b1:e8:f1:12:9c:45:a5:11:8b:40:
                    ff:dd:7f:ba:07:5e:d8:b9:0a:87:f9:81:4b:ed:f6:
                    ae:8d:52:e6:4c:85:66:ee:1c:a4:f8:a3:c8:af:3a:
                    5d:70:f3:26:a7:09:9f:b3:4f:5c:ac:04:35:44:6b:
                    ff:d5:31:07:d3:f7:27:c8:5a:34:93:77:bb:97:d4:
                    88:7c:fa:01:6b:32:6b:be:7a:ab:8e:fd:bf:15:10:
                    2b:66:46:b4:0d:43:2b:63:3e:9e:c1:7b:ad:dc:61:
                    d4:13
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                A9:52:B9:CF:B9:F5:24:2F:02:DE:EC:65:5C:94:31:44:C0:C2:16:A9
            X509v3 Authority Key Identifier:
                keyid:A9:52:B9:CF:B9:F5:24:2F:02:DE:EC:65:5C:94:31:44:C0:C2:16:A9

            X509v3 Basic Constraints:
```

```
                CA:TRUE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Subject Alternative Name:
                IP Address:10.x.x.x    Signature Algorithm: sha256WithRSAEncryption
        13:1d:a7:31:54:b4:b4:6c:de:7f:2a:7a:27:c7:46:6a:bf:2a:
        61:6d:0e:7e:23:c1:2c:b6:15:35:a6:79:86:59:85:8e:39:ff:
        9e:fc:a9:95:6b:99:23:78:e2:24:46:a3:bc:18:b8:df:b9:bc:
        80:2a:42:90:56:56:55:a7:3f:34:90:8a:f4:48:13:5a:af:36:
        7f:8b:71:57:97:76:3f:59:2d:be:8a:28:e9:0d:58:53:16:d0:
        a1:24:bb:be:32:67:e3:98:9b:f2:93:50:b3:c1:b3:56:e4:dc:
        e8:a3:35:63:51:a1:2c:ce:9f:99:fb:7a:51:92:2c:30:e0:17:
        1c:28:b4:2d:ad:1d:ca:0a:53:1f:da:d9:c5:ad:0d:24:a9:53:
        fa:18:f5:5d:17:d1:3c:cb:0c:be:04:7b:1a:d6:96:ce:6c:6b:
        21:a1:ba:2f:9a:5c:8e:5f:f3:8d:1f:69:bd:e1:8b:73:53:d8:
        f1:69:b2:bf:23:bb:af:f5:87:b4:66:5c:e1:47:a7:3f:12:aa:
        4b:55:35:78:04:e5:f7:ae:76:9c:ba:4a:15:c2:85:60:2a:b3:
        a8:00:51:bf:23:82:b8:95:eb:f9:75:4c:ba:31:43:dc:98:dd:
        a3:ab:f3:60:7a:e0:60:cc:d8:8b:91:90:8e:56:2c:d1:16:1a:
        6c:a5:c7:79
================================================================================
No Certificate available for WSA interface.
================================================================================
```

関連トピック

connectorctl generatecert （2 ページ）
connectorctl createcsr （6 ページ）

connectorctl createcsr

このコマンドは、新しいセキュアソケットレイヤ（SSL）証明書の証明書署名要求（CSR）を作成します。認証局（CA）によって署名されたCSRを取得し、CA署名付きSSL証明書を取得できます。CA署名付き証明書を展開したら、**connectorctl showcert**コマンドを使用して証明書を表示できます。

connectorctl createcsr

コマンド履歴

リリース 2.3.2 より前	コネクタSSL証明書では、CSRの[Subject Alternative Name (SAN)]フィールドにIPアドレスが含まれます。
リリース 2.3.2	2.3.2以降、コネクタSSL証明書では、CSRの[Subject Alternative Name (SAN)]フィールドに完全修飾ドメイン名（FQDN）またはホスト名が含まれます。

使用上のガイドライン

FQDNとホスト名は、CA署名付き証明書の証明書署名要求（CSR）を設定します。CSRがCAによって署名されている場合、作成された証明書では、[SAN]フィールドにFQDNまたはホスト名が含まれます。

例

次に、以下のコマンドの出力例を示します。

```
[[cmxadmin@cmxnew ~]$ connectorctl createcsr

Creating Certificate Signing Request (CSR)

[For SAN field of CSR, enter IP Address for CMX server []: 10.x.x.x
Keytype is RSA, so generating RSA key with length 2048

Generating RSA private key, 2048 bit long modulus

e is 65537 (0x10001)
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) [AU]:US
[State or Province Name (full name) [Some-State]:CA
[Locality Name (eg, city) []:San Jose
Organization Name (eg, company) []:Cisco Systems Inc.
Organizational Unit Name (eg, section) []:DNA_Spaces_Connector_01
[Common Name (e.g. server FQDN or YOUR name) [10.x.x.x]:
[Email Address []:
Please enter the following 'extra' attributes
 to be sent with your certificate request

[A challenge password []:
[An optional company name []:
The CSR is stored in : /etc/ssl/private/dnaspacescsr.pem
```

```
The Private key is stored in: /etc/ssl/private/dnaspaceskey.pem
Certificate Signing Request created successfully
```

関連トピック

connectorctl showcert （3 ページ）

connectorctl setproxycert

このコマンドは、HTTPS プロキシの証明書を設定します。

パラメータ

証明書のファイル名。

connectorctl setproxycert *filename*

構文の説明

filename	証明書のファイル名。

使用上のガイドライン

コマンドを実行する前に、まず証明書ファイルを dnasadmin ユーザーがアクセスできる（Cisco Unified Computing System（Cisco UCS） 上の）任意のフォルダにコピーする必要があります。

```
[cmxadmin@connector ~]$ connectorctl setproxycert cert.pem
New cert exists.
Restarting connector container ...
Connector container was restarted.
setProxyCert successful.
```

connectorctl validatecert

このコマンドは、認証局（CA） によって署名された証明書を検証します。

connectorctl validatecert *{ CA_certificate | root_certificate }*

構文の説明

CA_certificate	CA 証明書
root_certificate	ルート証明書

例

次に、 コマンドの出力例を示します。

```
[cmxadmin@cmxnew ~]$ connectorctl validatecert 10.22.244.80.cert.pem
root-cal-ca2-chain.cert.pem

Validating certificate
root-cal-ca2-chain.cert.pem amd 10.22.244.80.cert.pern exists

Validation of server certificate is successful

[cmxadmin@cmxnew ~]$
```

connectorctl importcacert

このコマンドは、署名付き証明書を コネクタ の正確な場所にインポートし、 コネクタ との接続のセキュリティを確保します。

connectorctl createcsr では、認証局（CA） による署名が必要な証明書が作成されます。この署名付き証明書は、connectorctl validatecert コマンドを使用して検証できます。署名付き証明書をインポートするには、connectorctl importcacert コマンドを使用できます。この手順により、コネクタ GUI にログインしようとしたときに表示される「Your connection is not private」というメッセージも削除されます。

connectorctl importcacert *certificate*

構文の説明

certificate	署名および検証済みの証明書。

コマンド履歴

リリース 2.2	このコマンドが導入されました。

例

次に、以下のコマンドの出力例を示します。

```
[cmxadminÇcmxnew ~]$ connectorctl importcacert 10.x.x.x.cert.pem
Importing CA certificate
10.x.x.x.cert.pem exists

Certificate Imported Successfully!
Restarting HAProxy...
HA Proxy restarted successfully!
CA certificate import process executed successfully
```

使用上のガイドライン

CSCvy62400 では、サードパーティ CA による証明書またはデバイス証明書をインポートできない場合があります。https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy62400このような場合、証明書のインポートにいくつかのエラーが発生し、GUI が終了することがあります。次の出力が表示されます。

```
[dnasadmin@dnasc-1 ~]$ connectorctl importcacert 20210609-063645839_Roche_G3_Root_CA.pem
Importing CA certificate.....
20210609-063645839_Roche_G3_Root_CA.pem exists
Certificate Imported Successfully!
Restarting HAProxy...
Job for haproxy.service failed because the control process exited with error code. See
"systemctl status haproxy.service" and "journalctl -xe" for details.
HAProxy restarted successfully!
CA certificate import process executed successfully

[dnasadmin@dnasc-1 ~]$ su -
Password:
Last login: Wed Jun  9 13:10:35 CDT 2021 on pts/0
```

この問題は、connectorctl generatecert コマンドを使用して自己署名証明書を再生成することで解決できます。この手順により、互換性のない証明書形式に関連する問題がすべて解消されます。

関連トピック

connectorctl validatecert （9 ページ）
connectorctl createcsr （6 ページ）
connectorctl generatecert （2 ページ）

connectorctl dockersubnet

デフォルトでは、コネクタ の Docker コンテナには 172.17.0.0/16 サブネットの IP アドレスが割り当てられます。サブネットがアドレス空間と重複している場合は、connectorctl dockersubnet コマンドを使用して、Docker サブネットを追加または削除できます。

connectorctl dockersubnet

例

次に、 コマンドの出力例を示します。

```
[cmxadminQcmxnew ~]$ connectorctl dockersubnet
Do you want to add or remove the subnet? [Insert a to add, r to remove] [a]: a

Please insert the Netmask IP: 10.22.244.1
Please insert CIDR [1-32] [16]:
Successfully changed the docker subnet
[cmxadminpcmxnew ~]$
```