



証明書

- [の証明書管理 \(1 ページ\)](#)

の証明書管理



(注) このセクションでは、DCNM OVA/ISO の展開にのみ適用されます。

リリース 11.2(1) 以降、Cisco DCNM では新しい方法と新しい CLI で、システム上で証明書のインストール、アップグレード後の復元、検証が可能です。アクティブノードからスタンバイノードに証明書をエクスポートして、ネイティブ HA セットアップの両方のピアに同じ証明書があることを確認できます。

Cisco DCNM ネイティブ HA セットアップでは、アクティブノードに CA 証明書をインストールし、サービスを開始すると、証明書はスタンバイノードと自動的に同期されます。アクティブノードとスタンバイノードの両方で同じ内部証明書が必要な場合は、アクティブノードからスタンバイノードに証明書をエクスポートする必要があります。これにより、Cisco ネイティブ HA セットアップの両方のピアの証明書が同じになります。



(注) リリース 11.3(1) 以降では、証明書の管理に **sysadmin** ロールを使用する必要があります。

Cisco DCNM は、次の 2 つの証明書を保存します。

- 自己署名証明書 (Cisco DCNM サーバとさまざまなアプリケーション間の内部通信用)
- Web UI などの外部世界と通信するための CA (認証局) 署名付き証明書。



(注) CA 署名付き証明書をインストールするまで、Cisco DCNM は外部ネットワークと通信するため自己署名証明書を保持します。

証明書管理のベストプラクティス

Cisco DCNM での証明書管理のガイドラインとベストプラクティスを次に示します。

- Cisco DCNM は、証明書を表示、インストール、復元、およびエクスポートまたはインポートするための CLI ベースのユーティリティを提供します。これらの CLI は SSH コンソールから使用でき、**sysadmin** ユーザーのみがこれらのタスクを実行できます。
- Cisco DCNM をインストールするとき、デフォルトで自己署名付き証明書がインストールされています。この証明書は、外部との通信に使用されます。Cisco DCNM のインストール後に、CA 署名付き証明書をシステムにインストールする必要があります。
- Cisco DCNM ネイティブ HA セットアップでは、DCNM アクティブ ノードに CA 署名付き証明書をインストールすることを推奨します。CA 署名付き証明書は、自動的にスタンバイ ノードと同期されます。ただし、アクティブ ノードとスタンバイ ノードの両方で同じ内部および CA 署名付き証明書を保持する場合は、アクティブ ノードから証明書をエクスポートして、スタンバイ ノードにインポートする必要があります。アクティブ ノードとスタンバイ ノードの両方に同じ証明書セットがあります。



(注) コンピューティング ノードは内部的に管理された証明書を使用するため、クラスタ展開のコンピューティング ノードには何のアクションも必要ありません。

- CN (共通名) を使用して Cisco DCNM で CSR を生成します。CN として VIP FQDN (仮想 IP アドレス FQDN) を指定して、CA 署名付き証明書をインストールします。FQDN は、Cisco DCNM Web UI にアクセスするために使用される管理サブネット VIP (eth0 の VIP) インターフェイスの完全修飾ドメイン名です。
- Cisco DCNM をアップグレードする前に CA 署名付き証明書がインストールされている場合は、Cisco DCNM をアップグレードした後に、CA 署名付き証明書を復元する必要があります。



(注) インラインアップグレードまたはバックアップと復元を実行する場合は、証明書のバックアップを取得する必要はありません。

インストールされた証明書の表示

次のコマンドを使用して、インストールされた証明書の詳細を表示できます。

appmgr afw show-cert-details

appmgr afw show-cert-details コマンドの次のサンプル出力では、**CERTIFICATE 1** は外部ネットワークおよび Web ブラウザに提供されている証明書を示します。**CEERTIFICATE 2** は内部で使用されている証明書を示します。

```

dcnm# appmgr afw show-cert-details

****CERTIFICATE 1****
[Certificate available to web gateway. This certificate is offered to webclients]:
-----Web gateway certificate-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4202 (0x106a)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=IN, ST=KA, L=BGL, O=xyz, OU=ABC, CN=<FQDN/IP>
    Validity
      Not Before: Jun  4 13:55:25 2019 GMT
      Not After : Jun  3 13:55:25 2020 GMT
    Subject: C=IN, ST=KA9, L=BGL9, O=XYZ123, OU=ABC123, CN=<FQDN/IP>
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:bb:52:1e:7f:24:d7:2e:24:62:5a:83:cc:e4:88:
-----Certificate output is truncated to first 15 lines-----

****CERTIFICATE 2****
[Certificate available in keystore(jks). CA signed certificate is installed here till
DCNM version 11.1.x]
If you have upgraded from DCNM version 11.1.x to later version please see installation
guide to restore
CA signed certificate to upgraded version.
-----Keystore certificate-----
alias = sme, storepass = <<storepass-pwd>>
Alias name: sme
Creation date: Oct 14, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=localhost, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Issuer: CN=dcnmca, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Serial number: 62044620
Valid from: Sun Oct 14 20:39:39 PDT 2018 until: Fri Oct 13 20:39:39 PDT 2023
Certificate fingerprints:
  MD5:  E5:F8:AD:17:4D:43:2A:C9:EE:35:5F:BE:D8:22:7D:9C
  SHA1: 38:66:F1:CD:10:61:27:E7:43:85:10:41:3D:A3:4B:5C:C9:CC:17:5E
  SHA256:
E0:87:D8:34:71:18:FE:8C:AB:18:0B:D7:85:B1:91:A8:4B:75:A3:91:BA:90:83:46:72:87:FE:FE:FE:04:F0:E1
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
-----Certificate output is truncated to first 15 lines-----
dcnm#

```



(注) <<storepass-pwd>> は、DCNM サーバをインストールする間に生成されるパスワードです。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。storepass-pwd の dcnm.fmserver.token の値を取得します。

インストール後、Web UI は **CERTIFICATE 1** を参照します。**CERTIFICATE 1** が利用できない場合、次のコマンドを使用して、すべてのアプリケーションを停止し再起動する必要があります。



- (注) Cisco DCNM で同じ一連のコマンドに従い、このシナリオをトラブルシューティングするようにしてください。

Cisco DCNM スタンドアロン アプライアンスで、次のコマンドを実行して、すべてのアプリケーションを停止および開始し、**CERTIFICATE 1** をトラブルシューティングします。

```
dcnm# appmgr stop all /* stop all the applications running on Cisco DCNM */
dcnm# appmgr start all /* start all the applications running on Cisco DCNM */
```

Cisco DCNM ネイティブ HA アプライアンスで、次のコマンドを実行して、すべてのアプリケーションを停止および開始し、**CERTIFICATE 1** をトラブルシューティングします。

例えば、**dcnm1** でアクティブ ノードを示し、**dcnm2** でスタンバイ ノードを示します。

両方のノードで実行しているアプリケーションを停止します。

```
dcnm2# appmgr stop all /* stop all the applications running on Cisco DCNM Standby Node */
dcnm1# appmgr stop all /* stop all the applications running on Cisco DCNM Active Node */
```

両方のノードでアプリケーションを開始します。

```
dcnm1# appmgr start all /* start all the applications running on Cisco DCNM Active Node*/
dcnm2# appmgr start all /* start all the applications running on Cisco DCNM Standby Node*/
```



- (注) 管理 IP アドレスを使用して、Cisco DCNM Web UI を起動する前にブラウザ キャッシュを消去します。

CERTIFICATE 1 は、ブラウザのセキュリティ設定に表示されます。

CA 署名付き証明書のインストール

標準のセキュリティ慣行として CA 署名付き証明書をインストールすることをお勧めします。CA 署名付き証明書が認識され、ブラウザによって検証されます。CA 署名付き証明書を手動で検証することもできます。



- (注) 認証局は、企業の署名機関でもかまいません。

Cisco DCNM スタンドアロン セットアップで CA 署名済み証明書をインストールする

Cisco DCNM に CA 署名付き証明書をインストールするには、次の手順を実行します。

Procedure

ステップ 1 SSH 端末を経由して DCNM サーバにログオンします。

ステップ 2 `appmgr afw gen-csr` コマンドを使用して、CISCO DCNM サーバで CSR を生成します。

Note CSR は Cisco DCNM に固有のものであり、対応する CSR 署名付き証明書のみが所定の Cisco DCNM にインストールされている必要があります。

```
dcnm# appmgr afw gen-csr
Generating CSR....
..
...
-----
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]:Cisco
Organizational Unit Name (eg, section) []:DCBG
Common Name (eg, your name or your server's hostname) []:dcnmhost.cisco.com
Email Address []:dcnm@cisco.com

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []: /* This field is not mandatory */
An optional company name []: /* This field is not mandatory */
...

CSR ファイル dcnmweb.csr が /var/tmp/ ディレクトリに作成されます。

***** CA certificate installation not completed yet. Please do followings. *****
CSR is generated and placed at /var/tmp/dcnmweb.csr.
Please download or copy the content to your certificate signing server.
```

ステップ 3 この CSR を証明書署名サーバに送信します。

Note CA 署名サーバは、組織に対してローカルです。

ステップ 4 認証局によって署名された証明書を取得します。

認証局 (CA) は、プライマリ、中間 (Issuing/Subordinate) 証明書、およびルート証明書の 3 つの証明書を返します。3 つの証明書すべてを `one.pem` ファイルに結合し、DCNM にインポートします。

ステップ 5 新しい CA 署名付き証明書を Cisco DCNM サーバにコピーします。

証明書が Cisco DCNM サーバの `/var/tmp` ディレクトリにあることを確認します。

ステップ 6 次のコマンドを使用して、Cisco DCNM に CA 署名付き証明書をインストールします。

Note 以下に示すように、同じ順序で次のコマンドを実行することを推奨します。

```
dcnm# appmgr stop all /* Stop all applications running on Cisco DCNM
dcnm# appmgr afw install-CA-signed-cert <CA-signed certificate directory>
/* CA-signed certificate with full or relative path */
Making the signed certificate available to web gateway....

CA signed certificate CA-signed-cert.pem is installed. Please start all applications as
```

```

followings:
On standalone setup execute: 'appmgr start all'

```

ステップ 7 **appmgr start all** コマンドを使用して、Cisco DCNM で新しい証明書ですべてのアプリケーションを再起動します。

```
dcnm# appmgr start all
```

ステップ 8 **appmgr afw show-cert-details** コマンドを使用して、新しくインストールした CA 署名証明書を確認します。

システムは、CA 証明書を用意しており、ブラウザで確認できます。

Note CSR は Cisco DCNM に固有のものであり、対応する CSR 署名付き証明書のみが所定の Cisco DCNM にインストールされている必要があります。

DCNM ネイティブ HA セットアップで CA 署名済み証明書をインストールする

Cisco DCNM に CA 署名付き証明書をインストールするには、次の手順を実行します。



Note 以下に示すように、同じ順序で次のコマンドを実行することを推奨します。

Procedure

ステップ 1 アクティブ ノードで、SSH 端末を経由して DCNM サーバにログオンします。

Note 例えば、Cisco DCNM アクティブおよびスタンバイ アプライアンスを **dcnm1** および **dcnm2** に個別に示します。

ステップ 2 **appmgr afw gen-csr** コマンドを使用して、CISCO DCNM サーバで CSR を生成します。

Note CSR は Cisco DCNM に固有のものであり、対応する CSR 署名付き証明書のみが所定の Cisco DCNM にインストールされている必要があります。

```

dcnm1# appmgr afw gen-csr
Generating CSR....
..
...
-----
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]:Cisco
Organizational Unit Name (eg, section) []:DCBG
Common Name (eg, your name or your server's hostname) []:dcnmhost.cisco.com
/* Provide a VIP FQDN name of the eth0 interface*/
Email Address []:dcnm@cisco.com

```

Please enter the following 'extra' attributes to be sent with your certificate request

```
A challenge password []: /* This field is not mandatory */
An optional company name []: /* This field is not mandatory */
...
```

Note アクティブ ノードで CSR を生成するケースでは、プロンプトで共通名を促される場合に、eth0 インターフェイスの VIP FQDN 名を提供することをお勧めします。

この FQDN は、Cisco DCNM Web UI を起動するためにブラウザで入力した Web サーバアドレスである必要があります。

CSR ファイル dcnmweb.csr が /var/tmp/ ディレクトリに作成されます。

```
***** CA certificate installation not completed yet. Please do followings. *****
CSR is generated and placed at /var/tmp/dcnmweb.csr.
Please download or copy the content to your certificate signing server.
```

ステップ 3 この CSR を証明書署名サーバに送信します。

Note CA 署名サーバは、組織に対してローカルです。

CA 署名サーバは、組織内の CA 署名期間または組織のローカル CA にすることができます。

ステップ 4 認証局によって署名された証明書を取得します。

ステップ 5 新しい CA 署名付き証明書を Cisco DCNM サーバにコピーします。

証明書が Cisco DCNM サーバの /var/tmp ディレクトリにあることを確認します。

ステップ 6 スタンバイ ノードで、SSH 端末を経由して DCNM サーバにログオンします。

ステップ 7 スタンバイ ノードで、**appmgr stop all** コマンドを使用してすべてのアプリケーションを停止します。

```
dcnm2# appmgr stop all /* Stop all applications running on Cisco DCNM Standby Node
dcnm2#
```

ステップ 8 アクティブ ノードで、**appmgr stop all** コマンドを使用してすべてのアプリケーションを停止します。

```
dcnm1# appmgr stop all /* Stop all applications running on Cisco DCNM Active Node
dcnm2#
```

ステップ 9 アクティブ ノードで、**appmgr afw install-CA-signed-cert** コマンドを使用して Cisco DCNM に CA 署名付き証明書をインストールします。

```
dcnm1# appmgr afw install-CA-signed-cert <CA-signed certificate directory>
/* CA-signed certificate with full or relative path */
Making the signed certificate available to web gateway....
```

```
CA signed certificate CA-signed-cert.pem is installed. Please start all applications as
followings:
On standalone setup execute: 'appmgr start all'
```

ステップ 10 アクティブ ノードで、**appmgr start all** コマンドを使用して、Cisco DCNM 上で新しい証明書とともにすべてのアプリケーションを再起動します。

```
dcnm1# appmgr start all /* Start all applications running on Cisco DCNM Active Node
```

先に進む前に、Cisco DCNM アクティブノードのすべてのサービスが動作していることを確認します。

Note Cisco DCNM Web UI にログオンし、証明書の詳細が正しいことを確認します。

- ステップ 11** スタンバイノードで、**appmgr start all** コマンドを使用して、Cisco DCNM 上で新しい証明書とともにすべてのアプリケーションを再起動します。

```
dcnm2# appmgr start all /* Start all applications running on Cisco DCNM Standby Node
```

これにより、スタンバイノードはアクティブノードと新しいピア関係を確立できます。したがって、アクティブノードに新しくインストールされている CA 署名付き証明書は、スタンバイノードで同期されます。

- ステップ 12** アクティブおよびスタンバイノードの両方で **appmgr afw show-cert-details** コマンドを使用して、新しくインストールした CA 署名証明書を確認します。

システムは、CA 証明書を用意しており、ブラウザで確認できます。

Note 証明書情報が表示されない場合、数分待機することをお勧めします。セカンダリノードは、アクティブノードとの同期に少し時間がかかります。

ネイティブ HA セットアップの両方のピアで、同じ内部および CA 署名付き証明書を保持する場合、最初にアクティブノードの証明書をインストールします。アクティブノードに証明書をインストールした後、アクティブノードから証明書をエクスポートし、同じ証明書をスタンバイノードにインポートします。

アクティブノードからスタンバイノードへ証明書をエクスポートする

次の手順は Cisco DCNM ネイティブ HA セットアップのみに適用されます。アクティブノードにインストールされている CA 署名付き証明書は、常にスタンバイノードに同期されています。ただし、内部の証明書はアクティブノードとスタンバイノードの両方で異なります。両方のピアで同じ証明書セットを保持する場合、このセクションで説明されている手順を実行する必要があります。



Note 内部証明書はシステム内部のため、証明書をエクスポートしないように選択できます。これらの証明書は、機能に影響を与えることなく、アクティブノードおよびスタンバイノードで別に行うことができます。

アクティブノードから CA 署名付き証明書をエクスポートし、スタンバイノードに証明書をインポートするには、次の手順を実行します。

Procedure

ステップ 1 アクティブ ノードで、SSH 端末を経由して DCNM サーバにログオンします。

ステップ 2 `appmgr afw export-import-cert-ha-peer export` コマンドを使用して、証明書バンドルを作成します。

```
dcnm1# appmgr afw export-import-cert-ha-peer export
```

ステップ 3 証明書バンドルをスタンバイ ノードをコピーします。

Note スタンバイ ノード上の証明書を、SSH 端末で指定されている場所にコピーしていることを確認します。

ステップ 4 スタンバイ ノードで、`appmgr stop all` コマンドを使用してすべてのアプリケーションを停止します。

```
dcnm2# appmgr stop all /* Stop all applications running on Cisco DCNM Standby Node  
dcnm2#
```

ステップ 5 `appmgr afw export-import-cert-ha-peer import` コマンドを使用して、スタンバイ ノードに証明書をインポートします。

証明書バンドルがインポートされ、スタンバイ ノードにインストールされます。

ステップ 6

ステップ 7 スタンバイ ノードで、`appmgr start all` コマンドを使用して、Cisco DCNM 上で新しい証明書とともにすべてのアプリケーションを再起動します。

```
dcnm2# appmgr start all /* Start all applications running on Cisco DCNM Standby Node
```

これにより、スタンバイ ノードでアプリケーションが起動したときに、新しいインポートされた証明書が有効になります。

ステップ 8 スタンバイ ノードで、`appmgr afw show-cert-details` コマンドを使用して、新しくインポートされた CA 署名付き証明書を確認します。

これで、システムはアクティブ ノードとスタンバイ ノードの両方で同じ証明書を使用できるようになりました。

アップグレード後に証明書を復元する

このメカニズムは、インラインアップグレードプロセスのみを使用した Cisco DCNM アップグレード手順に適用されます。この手順は、同じバージョンの Cisco DCNM アプライアンスでのデータのバックアップと復元には必要ありません。

証明書の復元は破壊的なメカニズムであることに注意してください。アプリケーションを停止して再起動する必要があります。復元は、アップグレードされたシステムが安定している際のみ実行する必要があります。つまり、Cisco DCNM Web UI にログインできる必要があります。

す。Cisco DCNM ネイティブ HA セットアップでは、アクティブ ノードとスタンバイ ノードの両方でピア関係が確立されている必要があります。



(注) 証明書は、次の状況でのみ復元する必要があります。

- アップグレード前に CA 署名付き証明書がシステムにインストールされている場合。
- 11.2(1) より前のバージョンからバージョン 11.2(1) 以降にアップグレードしている場合。

Cisco DCNM をアップグレードした後は、復元する前に **CERTIFICATE 1** が CA 署名付き証明書であるか必ず証明書を確認する必要があります。それ以外の場合は、証明書を復元する必要があります。

次のサンプル出力に示すように、**appmgr afw show-cert-details** を使用して証明書を確認します。

```

dcnm# appmgr afw show-cert-details
****CERTIFICATE 1****
[Certificate available to web gateway. This certificate is offered to webclients]:
-----Web gateway certificate-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1575924977762797464 (0x15decf6aec378798)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=CA, L=San Jose, O=Enterprise CA inc, OU=Data Center,
CN=dcnm1.ca.com
    Validity
      Not Before: Dec  9 20:56:17 2019 GMT
      Not After : Dec  9 20:56:17 2024 GMT
    Subject: C=US, ST=CA, L=San Jose, O= Enterprise CA inc, OU=Data Center,
CN=dcnm1.ca.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:cf:6e:cd:c6:a9:30:08:df:92:98:38:49:9c:2a:
-----Certificate output is truncated to first 15 lines-----

****CERTIFICATE 2****
[Certificate available in keystore(jks). CA signed certificate is installed here till
DCNM version 11.1.x]
If you have upgraded from DCNM version 11.1.x to later version please see installation
guide to restore
CA signed certificate to upgraded version.
-----Keystore certificate-----
Alias name: sme
Creation date: Oct 14, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=localhost, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Issuer: CN=dcnmca, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Serial number: 62044620
Valid from: Sun Oct 14 20:39:39 PDT 2018 until: Fri Oct 13 20:39:39 PDT 2023
Certificate fingerprints:
  SHA1: 38:66:F1:CD:10:61:27:E7:43:85:10:41:3D:A3:4B:5C:C9:CC:17:5E
  SHA256:

```

```
E0:87:D8:34:71:18:FE:8C:AB:18:0B:D7:85:B1:91:A8:4B:75:A3:91:BA:90:83:46:72:87:FE:FE:FE:04:F0:E1
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
-----Certificate output is truncated to first 15 lines-----
dcnm#
```

アップグレード後に Cisco DCNM スタンドアロン セットアップで証明書を復元する

Cisco DCNM スタンドアロン展開をリリース にアップグレードした後に証明書を復元するには、次の手順を実行します。

Procedure

ステップ 1 Note リリース にアップグレードすると、CA 署名付き証明書のバックアップが作成されません。

Cisco DCNM スタンドアロンアプライアンスが正常にアップグレードされたら、SSH を使用して DCNM サーバにログインします。

ステップ 2 次のコマンドを使用して、すべてのアプリケーションを停止します。

```
appmgr stop all
```

ステップ 3 次のコマンドを使用して、証明書を復元します。

```
appmgr afw restore-CA-signed-cert
```

ステップ 4 [はい (yes)] と入力し、以前インストールした証明書を復元することを確認します。

ステップ 5 次のコマンドを使用して、すべてのアプリケーションを開始します。

```
appmgr start all
```

ステップ 6 appmgr afw show-cert-details コマンドを使用して、新しくインストールした CA 署名証明書を confirms します。

システムは、CA 証明書を用意しており、ブラウザで確認できます。

アップグレード後に Cisco DCNM ネイティブ HA セットアップで証明書を復元する

Cisco DCNM ネイティブ HA セットアップでは、証明書はアクティブ ノードとスタンバイ ノードの両方にインストールされます。アクティブ ノードでのみ証明書を復元する必要があります。証明書はスタンバイ ノードと自動的に同期されます。

Cisco DCNM スタンドアロン展開をリリース にアップグレードした後に証明書を復元するには、次の手順を実行します。

Procedure

ステップ 1 SSH を使用して Cisco DCNM サーバにログインします。

Note 例えば、アクティブおよびスタンバイ アプライアンスを **dcnm1** および **dcnm2** に個別に示します。

ステップ 2 スタンバイ ノードで、**appmgr stop all** コマンドを使用してすべてのアプリケーションを停止します。

```
dcnm2# appmgr stop all /* Stop all applications running on Cisco DCNM Standby Node
```

ステップ 3 アクティブ ノードで、**appmgr stop all** コマンドを使用してすべてのアプリケーションを停止します。

```
dcnm1# appmgr stop all /* Stop all applications running on Cisco DCNM Active Node
```

ステップ 4 **appmgr afw restore-CA-signed-cert** コマンドを使用して、アクティブ ノードの証明書を復元します。

```
dcnm1# appmgr afw restore-CA-signed-cert
```

ステップ 5 **[はい (yes)]** と入力し、以前インストールした証明書を復元することを確認します。

ステップ 6 アクティブ ノードで、**appmgr start all** コマンドを使用してすべてのアプリケーションを起動します。

```
dcnm1# appmgr start all /* Start all applications running on Cisco DCNM Active Node
```

先に進む前に、Cisco DCNM アクティブ ノードのすべてのサービスが動作していることを確認します。

Note Cisco DCNM Web UI にログオンし、証明書の詳細が正しいことを確認します。

ステップ 7 スタンバイ ノードで、**appmgr start all** コマンドを使用してすべてのアプリケーションを起動します。

```
dcnm2# appmgr start all /* Start all applications running on Cisco DCNM Standby Node
```

しばらく待ってから、スタンバイ ノードがアクティブ ノードと同期します。

ステップ 8 アクティブおよびスタンバイ ノードの両方で **appmgr afw show-cert-details** コマンドを使用して、新しくインストールした CA 署名証明書を確認します。

システムは、CA 証明書を用意しており、ブラウザで確認できます。

以前にインストールされた CA 署名付き証明書の回復と復元

CA 署名付き証明書のインストール、復元、管理は、サードパーティの署名サーバが関係しているため、時間がかかるプロセスです。これにより、誤った証明書をインストールすることと

なるミスが生じる場合があります。このようなシナリオでは、最新のインストールまたはアップグレードの前にインストールされた証明書を復元することをお勧めします。

以前にインストールされた CA 署名付き証明書を回復して復元するには、次の手順を実行します。

手順

ステップ 1 SSH 端末を経由して DCNM サーバにログオンします。

ステップ 2 `/var/lib/dcnm/afw/apigateway/` ディレクトリに移動します。

```
dcnm# cd /var/lib/dcnm/afw/apigateway/
dcnm# ls -ltr /* View the contents of the folder
total 128
-rw----- 1 root root 1844 Nov 18 13:14 dcnmweb.key.2019-11-20T132939-08:00
-rw-r--r-- 1 root root 1532 Nov 18 13:14 dcnmweb.crt.2019-11-20T132939-08:00
-rw----- 1 root root 1844 Nov 20 10:15 dcnmweb.key.2019-11-20T132950-08:00
-rw-r--r-- 1 root root 1532 Nov 20 10:15 dcnmweb.crt.2019-11-20T132950-08:00
-rw----- 1 root root 1844 Dec 22 13:59 dcnmweb.key
-rw-r--r-- 1 root root 1532 Dec 22 13:59 dcnmweb.crt

.
..
...
```

dcnmweb と **dcnmweb** は、現在、システムにインストールされているキーと証明書ファイルです。同様のファイル名は、タイムスタンプサフィックスを使用して、最近のアップグレードまたは復元の前にインストールされているキーと証明書のペアを識別するのに役立ちます。

ステップ 3 `appmgr stop all` コマンドを使用して、Cisco DCNM 上で実行されているすべてのアプリケーションを停止します。

ステップ 4 `dcnmweb.key` および `dcnmweb.crt` ファイルのバックアップをとります。

ステップ 5 復元する古いキーと証明書のペアを特定します。

ステップ 6 キーと証明書のペアを **dcnmweb.key** および **dcnmweb.crt** として (タイムスタンプ サフィックスなしで) コピーします。

ステップ 7 `appmgr start all` コマンドを使用して、Cisco DCNM 上で実行されているすべてのアプリケーションを開始します。

ステップ 8 `appmgr afw show-cert-details` コマンドを使用して、証明書の詳細を確認します。CERTIFICATE 1 は CA 署名付き証明書です。

(注) CA 署名付き証明書が Cisco DCNM Web UI に表示されない場合、または DCNM サーバがエラーメッセージを送信した場合は、システムを再起動する必要があります。

インストールした証明書の確認

`appmgr afw show-cert-details` コマンドを使用してインストールした証明書を確認でき、Web ブラウザによって証明書が有効か否か確認します。Cisco DCNM はすべての標準ブラウザ (Chrome、



IE、Safari、Firefox)をサポートします。しかし、各ブラウザでは証明書情報が異なって表示されます。

ブラウザのプロバイダ Web サイトで、ブラウザの固有情報を参照することをお勧めします。

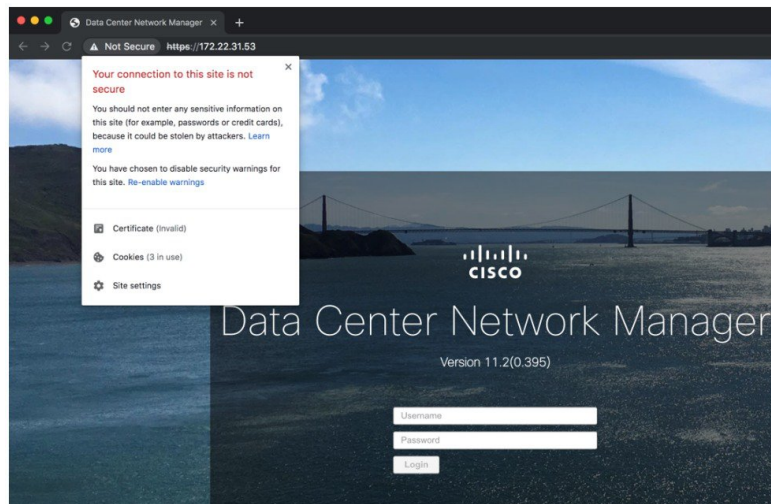
次のスニペットは、証明書を確認するための Chrome ブラウザバージョン 74.0.3729.169 の例です。

1. URL **https://<dcnm-ip-address>** または **https://<FQDN>** をブラウザのアドレスバーに入力します。

Return キーを押します。

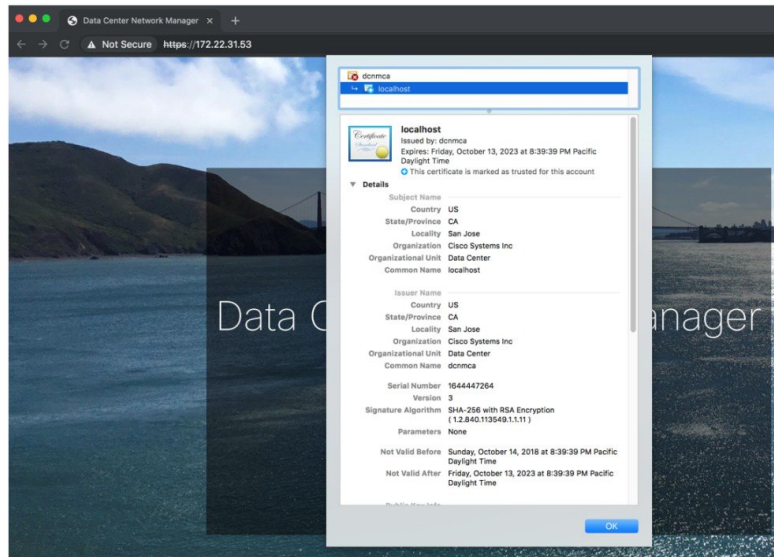
2. 証明書の種類に基づき、URL フィールドの左側のアイコンにロックアイコン [] またはアラートアイコン [] が表示されます。

アイコンをクリックします。



3. カードで、[証明書 (Certificate)] フィールドをクリックします。

証明書の情報が示されます。



表示されている情報は、**appmgr afw show-cert-details** を使用して証明書の詳細を確認したときに、証明書 1 に表示されている詳細と一致している必要があります。

