5 NCM での証明書の使用

証明書とは、ブラウザに対して Web サーバを識別したり、あるサーバに対して別のサーバを識別したりします。この証明書は、自己署名するか、認証局（CA）の署名を受けることができます。CiscoWorks Network Compliance Manager ソフトウェア（NCM）は次の証明書ファイルを使用します。

- Truecontrol キーストア ファイルには、秘密キーおよび証明書が、それらに対応する公開キーとともに保存されています。これは、次の場所にあります。
  - *Windows の場合*：
    `%NCM_HOME%\server\ext\jboss\server\default\conf\truecontrol.keystore`
  - *UNIX の場合*：
    `$NCM_HOME/server/ext/jboss/server/default/conf/truecontrol.keystore`
- Truecontrol 信頼ストア ファイルには、通信を行う予定の他のパーティーの証明書、または他のパーティーを識別するのに信頼している認証機関からの証明書が含まれています。これは、次の場所にあります。
  - *Windows の場合*：
    `%NCM_HOME%\server\ext\jboss\server\default\conf\truecontrol.truststore`
  - *UNIX の場合*：
    `$NCM_HOME/server/ext/jboss/server/default/conf/truecontrol.truststore`

`truecontrol.truststore` ファイルは、NCM バージョン 1.8 以降最新です。

- また、CAcerts キーストア ファイルには、秘密キーおよび証明書が、それらに対応する公開キーとともに保存されています。これは、NCM とともにインストールされる Java Development Kit（JDK）に含まれ、次の場所にあります。
  - *Windows*：`%NCM_HOME%\jre\lib\security\cacerts`
  - *UNIX*：`$NCM_HOME/jre/lib/security/cacerts`

この章は、次の内容で構成されています。

デフォルトの NCM 証明書

インストール時に、NCM は自己署名の証明書を Truecontrol キーストア、Truecontrol 信頼ストア、および CAcerts キーストアに含めます。NCM が提供する証明書は、すべての NCM サーバ上で同じものです。このような理由から、デフォルトの自己署名証明書を新しい自己署名証明書または CA 署名証明書に交換することをお勧めします。詳細については、「自己署名証明書の NCM への追加」（P.16）または「CA 署名の証明書の NCM への追加」（P.19）を参照してください。

Truecontrol キーストア

`truecontrol.keystore` ファイルには、Web ブラウザが NCM サーバを識別するのに使用する証明書が含まれます。表 2 は、NCM が提供する自己署名証明書の重要なプロパティを示します。プロパティのラベルと値の形式は、Web ブラウザによって異なります。

表 2　　NCM コンソール にアクセスするためのデフォルト証明書のプロパティ

プロパティ	デフォルト値
Issued to and by	localhost, Hewlett Packard Company • CN = localhost • OU = Hewlett Packard Company • O = Hewlett Packard Company • L = Palo Alto • S = CA • C = US
Serial number	48 4e 9d 84
Valid date range	2008/06/10 ～ 2018/06/08
SHA1 fingerprint	05 de dc 68 58 45 ca ea 88 ff 16 05 e7 65 a9 5b 23 29 d7 65
MD5 fingerprint	65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8

デフォルトでは、Web ブラウザは自己署名証明書を信用しません。そのため、NCM コンソール ユーザには、NCM コンソール ログオン ページが表示される前に不明の証明書の警告が表示されます。

Web ブラウザでの Truecontrol 証明書の受諾

Truecontrol 証明書が信頼できる証明書の Web ブラウザのリストに含まれていない場合、Web ブラウザは、証明書の妥当性に関する警告メッセージを表示することがあります。この問題を解決するには、次の手順に従います。

1　証明書の値が予想どおりかどうか確認します。

　デフォルトの NCM が提供する証明書の場合、形式および表示順序は異なる可能性はありますが、値が表 2 の中で説明されている情報に一致する必要があります。

2　Web ブラウザの手順に従い、信頼できる証明書のリストに、検証された証明書を追加します。

Truecontrol キーストアの表示

truecontrol.keystore ファイルの内容をコマンドラインから表示するには、次の手順に従います。

1 truecontrol.keystore および truecontrol.truststore ファイルを含む次のディレクトリに変更します。

- *Windows* : %NCM_HOME%\server\ext\jboss\server\default\conf
- *UNIX* : $NCM_HOME/server/ext/jboss/server/default/conf

2 次のコマンドを入力し、Truecontrol キーストア ファイルの内容を調べます。

- *Windows の場合* :
  %NCM_HOME%\jre\bin\keytool.exe -list -keystore truecontrol.keystore
- *UNIX の場合* :
  $NCM_HOME/jre/bin/keytool -list -keystore truecontrol.keystore

キーストアのパスワードの入力を求められたら、「**sentinel**」と入力します。

キーストアは、次の形式で出力されます。

```
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
sentinel, 10-Jun-2008, PrivateKeyEntry,
Certificate fingerprint (MD5): 65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8
```

または、-v（詳細出力）オプションを使用すると、次の形式で詳細に出力されます。

```
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: sentinel
Creation date: 10-Jun-2008
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=localhost, OU=Hewlett Packard Company, O=Hewlett Packard Company, L=Palo Alto, ST=CA,
C=US
Issuer: CN=localhost, OU=Hewlett Packard Company, O=Hewlett Packard Company, L=Palo Alto, ST=CA,
C=US
Serial number: 484e9d84
Valid from: Tue Jun 10 16:28:04 BST 2008 until: Fri Jun 08 16:28:04 BST 2018
Certificate fingerprints:
         MD5:  65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8
         SHA1: 05:DE:DC:68:58:45:CA:EA:88:FF:16:05:E7:65:A9:5B:23:29:D7:65
         Signature algorithm name: SHA1withRSA
         Version: 3
```

Truecontrol 信頼ストア

NCM のインストール時に、truecontrol.truststore ファイルに 1 つの自己署名証明書が含まれます。Secure Sockets Layer（SSL）を越えるアプリケーション間の通信をサポートするために、このファイルに他の製品の証明書を追加できます。

NCM Network Node Manager i Software の証明書を truecontrol.truststore ファイルにインポートするには、『*HP Network Node Manager i Software–Cisco Network Automation Integration Guide*』を参照してください。

自己署名証明書の NCM への追加

ご使用の環境に固有の新しい自己署名証明書を作成できます。新しい自己署名証明書を使用するには、第三者が関与する必要はありませんが、各 NCM コンソール ユーザが新しい自己署名証明書を信頼するように Web ブラウザを設定する必要がある場合があります。

自己署名証明書を作成し、それを NCM に追加するには、次の手順に従います。

1 新しい自己署名証明書を次のように生成します。

a truecontrol.keystore および truecontrol.truststore ファイルを含む次のディレクトリに変更します。

— *Windows* : %NCM_HOME%\server\ext\jboss\server\default\conf

— *UNIX* : $NCM_HOME/server/ext/jboss/server/default/conf

b truecontrol.keystore ファイルのバックアップ コピーを作成します。

c keytool コマンドを使用して Truecontrol キーストア ファイル内に新しい証明書を生成します。次に例を示します。

— *Windows の場合* :

```
%NCM_HOME%\jre\bin\keytool.exe -genkey -keyalg RSA -keysize 2048 \
-validity 3650 -alias nacert -keystore truecontrol.keystore
```

— *UNIX の場合* :

```
$NCM_HOME/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 \
-validity 3650 -alias nacert -keystore truecontrol.keystore
```

キーストアのパスワードの入力を求められたら、「**sentinel**」と入力します。

詳細については、keytool コマンドをオプションなしで実行します。

d 要求された次の情報を入力します。

— 姓と名の入力を求められたら、NCM サーバの識別子を入力します。これは、localhost、短いホスト名、または IP アドレスのいずれかです。

NCM サーバの完全修飾ドメイン名（FQDN）を入力しないでください。

localhost 以外の値を使用すると、NCM サービスの再起動が必要な設定手順が追加されます。

— 組織の情報（たとえば、Is CN=hostname, OU=someOU, O=someORG, L=someCITY, ST=someSTATE, C=AB correct?[no]:）を確認するように求められたら、「**yes**」と入力し、Enter キーを押します。

— パスワードを入力するように求められたら、Enter キーを押します。そうすると、キーストアのパスワードが使用されます。

2 keytool コマンドを使用して、新しく作成された証明書をファイルにエクスポートします。たとえば、truecontrol.keystore および truecontrol.truststore ファイルを含む次のディレクトリに変更します。

- *Windows の場合 :*

```
%NCM_HOME%\jre\bin\keytool.exe -export -alias nacert \
-file nacert.cer -keystore truecontrol.keystore
```

- *UNIX の場合* :
  ```
  $NCM_HOME/jre/bin/keytool -export -alias nacert -file nacert.cer \
  -keystore truecontrol.keystore
  ```

キーストアのパスワードの入力を求められたら、「**sentinel**」と入力します。

ステップ 1（P.16）で証明書を生成するときに使用した別名を指定します。

出力ファイル（たとえば、nacert.cer）は、コマンドが実行される場所に作成されます。

コマンドは、次の形式で出力されます。

```
Certificate stored in file nacert.cer
```

3 次のように、エクスポートされた証明書を CAcerts キーストアにインポートします。

a エクスポート ファイルを現在の場所から cacerts ファイルを含むディレクトリに移動します。たとえば、truecontrol.keystore および truecontrol.truststore ファイルを含む次のディレクトリに変更します。

— *Windows* : `move nacert.cer %NCM_HOME%\jre\lib\security`

— *UNIX* : `mv nacert.cer $NCM_HOME/jre/lib/security`

b 次の手順で cacerts ファイルを含むディレクトリに変更します。

— *Windows* : `%NCM_HOME%\jre\lib\security`

— *UNIX* : `$NCM_HOME/jre/lib/security`

c cacerts ファイルのバックアップ コピーを作成します。

d keytool コマンドを使用して CAcerts キーストア ファイルに新しい証明書をインポートします。次に例を示します。

— *Windows の場合* :
```
%NCM_HOME%\jre\bin\keytool.exe -import -alias nacert \
-file nacert.cer -keystore cacerts
```

— *UNIX の場合* :
```
$NCM_HOME/jre/bin/keytool -import -alias nacert -file nacert.cer \
-keystore cacerts
```

キーストアのパスワードの入力を求められたら、「**changeit**」と入力します。

証明書を信頼するか求められたら、「**yes**」と入力し、Enter キーを押します。

ステップ 2（P.16）で作成されたファイル（たとえば、nacert.cer）を指定します。

エイリアスは、cacerts ファイル内の新しい証明書の識別子です。truecontrol.keystore ファイル内のエイリアスに一致する必要はありません。

コマンドは、次の形式で出力されます。

```
Owner: CN=myhost, OU=Some OU, O=Some O, L=Mytown, ST=My State, C=AB
Issuer: CN=myhost, OU=Some OU, O=Some O, L=Mytown, ST=My State, C=AB
Serial number: 4e79d241
Valid from: Wed Sep 21 13:02:09 BST 2011 until: Sat Sep 18 13:02:09 BST 2021
Certificate fingerprints:
         MD5: FA:B1:86:18:18:47:43:30:8B:38:38:E6:8E:73:DB:84
         SHA1: CC:F2:69:F3:2C:7E:8E:03:BE:EC:F2:18:78:80:41:0A:BA:95:48:F8
         Signature algorithm name: SHA1withRSA
         Version: 3
Trust this certificate?[no] yes
Certificate was added to keystore
```

4 NCM に新しい証明書を強制的に使用させるには、次のように NCM が提供する証明書を Truecontrol キーストアから削除します。

a truecontrol.keystore および truecontrol.truststore ファイルを含む次のディレクトリに変更します。

— *Windows* : %NCM_HOME%\server\ext\jboss\server\default\conf

— *UNIX* : $NCM_HOME/server/ext/jboss/server/default/conf

b keytool コマンドを使用して、sentinel の証明書をバックアップ ファイルにエクスポートします。次に例を示します。

— *Windows の場合* :

```
%NCM_HOME%\jre\bin\keytool.exe -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

— *UNIX の場合* :

```
$NCM_HOME/jre/bin/keytool -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

キーストアのパスワードの入力を求められたら、「**sentinel**」と入力します。

コマンドは、次の形式で出力されます。

```
Certificate stored in file sentinel_from_truecontrol_keystore.cer
```

c バックアップ ファイル（たとえば、sentinel_from_truecontrol_keystore.cer）を安全な場所に移動します。

d keytool コマンドを使用して Truecontrol キーストアから既存の sentinel の証明書を削除します。次に例を示します。

— *Windows の場合* :

```
%NCM_HOME%\jre\bin\keytool.exe -delete -alias sentinel \
-keystore truecontrol.keystore
```

— *UNIX の場合* :

```
$NCM_HOME/jre/bin/keytool -delete -alias sentinel \
-keystore truecontrol.keystore
```

キーストアのパスワードの入力を求められたら、「**sentinel**」と入力します。

コマンドは、次の形式で出力されます。

```
[Storing truecontrol.keystore]
```

5 *（任意）*ステップ 1（P.16）で、NCM サーバの識別子が localhost でない場合は、NCM 設定を次のように更新します。

a 次の手順で .rcx ファイルを含むディレクトリに変更します。

— *Windows* : %NCM_HOME%\jre

— *UNIX* : $NCM_HOME/jre

b adjustable_options.rcx ファイルを <NCM_HOME> ディレクトリ以外の場所にバックアップします。

c adjustable_options.rcx ファイルの中に次の行を追加します。

```
<option name="startup/precompile/http.prefix">http://"hostname"/</option>
```

d 新しい行の中で、hostname をステップ 1（P.16）のステップ d で姓と名に入力した識別子に置き換えます。

e adjustable_options.rcx ファイルを保存します。

この手順を完了すると、NCM コンソール 内の新規ページごとの待ち時間がなくなるので、NCM コンソール のユーザ エクスペリエンスが向上します。

6 次のように、すべての NCM サービスを再起動します。

- *Windows* : [Services] コントロール パネルを開きます。サービスのリストの中で、次の各サービスを右クリックし、[Restart] をクリックします。
  - **TrueControl Management Engine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX* : 次のコマンドを実行します。

```
/etc/init.d/truecontrol restart
```

7 各 NCM コンソール ユーザに、それぞれの Web ブラウザの信頼できる証明書のリストに新しい証明書を追加するように指示します。

CA 署名の証明書の NCM への追加

新しい CA 署名証明書を使用するには、第三者とやりとりする必要がありますが、各 NCM コンソール ユーザが新しい自己署名証明書を信頼するように Web ブラウザを設定する必要はありません。

CA 署名証明書を要求し、それを NCM に追加するには、次の手順に従います。

1 新しいローカル証明書を次のように生成します。

a truecontrol.keystore および truecontrol.truststore ファイルを含む次のディレクトリに変更します。

- *Windows* : %NCM_HOME%\server\ext\jboss\server\default\conf
- *UNIX* : $NCM_HOME/server/ext/jboss/server/default/conf

b truecontrol.keystore ファイルのバックアップ コピーを作成します。

c keytool コマンドを使用して Truecontrol キーストア ファイル内に新しい証明書を生成します。次に例を示します。

- *Windows の場合* :

```
%NCM_HOME%\jre\bin\keytool.exe -genkey -keyalg RSA -keysize 2048 \
-validity 3650 -alias nacacert -keystore truecontrol.keystore
```

- *UNIX の場合* :

```
$NCM_HOME/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 \
-validity 3650 -alias nacacert -keystore truecontrol.keystore
```

キーストアのパスワードの入力を求められたら、「**sentinel**」と入力します。

詳細については、keytool コマンドをオプションなしで実行します。

d 要求された次の情報を入力します。

— 姓と名を入力するように求められたら、NCM サーバの完全修飾ドメイン名（FQDN）を入力してください。

— 組織の情報（たとえば、Is CN=hostname, OU=someOU, O=someORG, L=someCITY, ST=someSTATE, C=AB correct?[no]:）を確認するように求められたら、「**yes**」と入力し、Enter キーを押します。

— パスワードを入力するように求められたら、Enter キーを押します。そうすると、キーストアのパスワードが使用されます。

2 keytool コマンドを使用し、新しいローカル証明書から証明書署名要求（CSR）を作成します。たとえば、truecontrol.keystore および truecontrol.truststore ファイルを含む次のディレクトリに変更します。

- *Windows の場合*：
```
%NCM_HOME%\jre\bin\keytool.exe -certreq -alias nacacert \
-file narequest.csr -keystore truecontrol.keystore
```
- *UNIX の場合*：
```
$NCM_HOME/jre/bin/keytool -certreq -alias nacacert -file narequest.csr \
-keystore truecontrol.keystore
```

ステップ 1（P.19）でローカル証明書を生成するときに使用した別名を指定します。

出力ファイル（たとえば、narequest.csr）は、コマンドが実行される場所に作成されます。

3 CSR を CA に送信します。オプションが選べる場合は、新しい証明書が Tomcat 互換または Apache 互換の形式になるように要求してください。

CA は次のいずれかを返します。

- 署名証明書のファイルを 1 つ。この手順では server.crt と呼ばれます。

  server.crt ファイルは、サーバ証明書（ファイルに含まれる最上位の証明書）と 1 つ以上の CA 証明書（ファイルに含まれる最後の証明書）

  WordPad または vi のようなテキスト エディタで、CA 証明書の内容を CA.crt という新しいファイルの中にコピーします。

  サーバ証明書を truecontrol.keystore ファイルにインポートするには、server.crt ファイルを使用し、CA 証明書を truecontrol.truststore ファイルにインポートするには、CA.crt を使用します。

- ファイルを 2 つ。この手順では、server.crt および CA.crt と呼ばれます。

  WordPad または vi のようなテキスト エディタで、CA.crt ファイルの内容を server.crt ファイルの最後に追加します。

  サーバ証明書を truecontrol.keystore ファイルにインポートするには、変更された server.crt ファイルを使用し、CA 証明書を truecontrol.truststore ファイルにインポートするには、CA.crt を使用します。

次の例は、CA が提供するファイルがどのような内容かを示しています。

サーバ証明書と CA 証明書を 1 つのファイルに結合：

```
-----BEGIN CERTIFICATE-----
Sample1/VQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
.....
.....
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Sample2/Gh0dHA6Ly9jb3JwMWRjc2cyLnNnLmludC5wc2FnbG9iYWwuY29tL0Nlc
RaOCApwwggKYMB0GA1UdDgQWBBSqaWZzCRcpvJWOFPZ/Be9b+QSPyDAfBgNVHSMC
.....
.....
Wp5Lz1ZJAOu1VHbPVdQnXnlBkx7V65niLoaT90Eqd6laliVlJHj7GBriJ90uvVGu
BQagggEChoG9bGRhcDovLy9DTj1jb3JwMWRjc2cyL==
-----END CERTIFICATE-----
```

サーバ証明書と CA 証明書のファイルを分離：

```
-----BEGIN CERTIFICATE-----
Sample/AVQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
.....
.....
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
```

4 次のように、変更された（必要な場合）server.crt および CA.crt ファイルを Truecontrol キーストアにインポートします。

a 次のように、server.crt および CA.crt ファイルを truecontrol.keystore および truecontrol.truststore ファイルを含むディレクトリにコピーします。

— *Windows*：%NCM_HOME%\server\ext\jboss\server\default\conf

— *UNIX*：$NCM_HOME/server/ext/jboss/server/default/conf

b truecontrol.keystore および truecontrol.truststore ファイルを含む次のディレクトリに変更します。

— *Windows*：%NCM_HOME%\server\ext\jboss\server\default\conf

— *UNIX*：$NCM_HOME/server/ext/jboss/server/default/conf

c truecontrol.keystore ファイルのバックアップ コピーを作成します。

d server.crt および CA.crt のそれぞれのファイルに対して、keytool コマンドを使用して Truecontrol キーストア ファイルに新しい証明書をインポートします。次に例を示します。

— *Windows の場合*：

```
%NCM_HOME%\jre\bin\keytool.exe -import -trustcacerts \
-alias nacacert -file server.crt -keystore truecontrol.keystore

%NCM_HOME%\jre\bin\keytool.exe -import -trustcacerts \
-alias nacacert -file CA.crt -keystore truecontrol.keystore
```

— *UNIX の場合* :

```
$NCM_HOME/jre/bin/keytool -import -trustcacerts -alias nacert \
-file server.crt -keystore truecontrol.keystore

$NCM_HOME/jre/bin/keytool -import -trustcacerts -alias nacert \
-file CA.crt -keystore truecontrol.keystore
```

キーストアのパスワードの入力を求められたら、「**sentinel**」と入力します。

証明書を信頼するか求められたら、「**yes**」と入力し、Enter キーを押します。

エイリアスは、各ファイル内の新しい証明書の識別子です。これは、ステップ 2（P.20）で要求される証明書を生成するのに使用されるエイリアスと通常一致します。

コマンドは、次の形式で出力されます。

```
Owner: CN=NCM_server.example.com
Issuer: CN=NCM_server.example.com
Serial number: 4e79d241
Valid from: Wed Sep 21 13:02:09 BST 2011 until: Sat Sep 18 13:02:09 BST 2021
Certificate fingerprints:
         MD5: FA:B1:86:18:18:47:43:30:8B:38:38:E6:8E:73:DB:84
         SHA1: CC:F2:69:F3:2C:7E:8E:03:BE:EC:F2:18:78:80:41:0A:BA:95:48:F8
         Signature algorithm name: SHA1withRSA
         Version: 3
Trust this certificate?[no] yes
Certificate was added to keystore
```

e CA が提供するすべての証明書が truecontrol.keystore ファイルにインポートされるまでステップ d を繰り返します。

5 NCM に新しい証明書を強制的に使用させるには、次のように NCM が提供する証明書を Truecontrol キーストアから削除します。

a truecontrol.keystore および truecontrol.truststore ファイルを含む次のディレクトリに変更します。

— *Windows* : %NCM_HOME%\server\ext\jboss\server\default\conf

— *UNIX* : $NCM_HOME/server/ext/jboss/server/default/conf

b keytool コマンドを使用して、sentinel の証明書をバックアップ ファイルにエクスポートします。次に例を示します。

— *Windows の場合* :

```
%NCM_HOME%\jre\bin\keytool.exe -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

— *UNIX の場合* :

```
$NCM_HOME/jre/bin/keytool -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

キーストアのパスワードの入力を求められたら、「**sentinel**」と入力します。

コマンドは、次の形式で出力されます。

```
Certificate stored in file sentinel_from_truecontrol_keystore.cer
```

c バックアップ ファイル（たとえば、sentinel_from_truecontrol_keystore.cer）を安全な場所に移動します。

d keytool コマンドを使用して Truecontrol キーストアから既存の sentinel の証明書を削除します。次に例を示します。

— *Windows の場合* :

```
%NCM_HOME%\jre\bin\keytool.exe -delete -alias sentinel \
-keystore truecontrol.keystore
```

— *UNIX の場合* :

```
$NCM_HOME/jre/bin/keytool -delete -alias sentinel \
-keystore truecontrol.keystore
```

キーストアのパスワードの入力を求められたら、「**sentinel**」と入力します。

コマンドは、次の形式で出力されます。

```
[Storing truecontrol.keystore]
```

6 次のように NCM の設定を更新します。

a 次の手順で .rcx ファイルを含むディレクトリに変更します。

— *Windows* : %NCM_HOME%\jre

— *UNIX* : $NCM_HOME/jre

b adjustable_options.rcx ファイルを <NCM_HOME> ディレクトリ以外の場所にバックアップします。

c adjustable_options.rcx ファイルの中に次の行を追加します。

```
<option name="startup/precompile/http.prefix">http://"hostname"/</option>
```

d 新しい行の中で、hostname をステップ 1（P.19）のステップ d で姓と名に入力した識別子に置き換えます。

e adjustable_options.rcx ファイルを保存します。

この手順を完了すると、NCM コンソール 内の新規ページごとの待ち時間がなくなるので、NCM コンソール のユーザ エクスペリエンスが向上します。

7 次のように、すべての NCM サービスを再起動します。

- *Windows* : [Services] コントロール パネルを開きます。サービスのリストの中で、次の各サービスを右クリックし、[Restart] をクリックします。
  - **TrueControl Management Engine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX* : 次のコマンドを実行します。

```
/etc/init.d/truecontrol restart
```

8 NCM コンソール にログインし、新しい証明書をテストします。Web ブラウザが CA を信頼している場合、警告メッセージを生成することなく NCM コンソール への接続を信頼します。

トラブルシューティング

このセクションには、NCM で証明書を使用する際に表示される可能性のあるエラー メッセージに関する情報が含まれます。

Incorrect Magic

RedHat Linux のような一部のオペレーティング システムには、keytool ユーティリティが含まれます。オペレーティング システムに付属する keytool のバージョンが NCM JRE バージョンと一致しない場合、次のようなエラー メッセージが表示されます。

```
keytool error: gnu.javax.crypto.keyring.MalformedKeyringException: incorrect
magic
```

この場合、NCM で提供される keytool ユーティリティを使用します。

- *Windows*：`%NCM_HOME%\jre\bin\keytool.exe`
- *UNIX*：`$NCM_HOME/jre/bin/keytool`

httpmonitor のエラー

証明書を変更し、それを CAcerts キーストアにインポートしていない場合、httpmonitor エラーが表示されます。

この問題を解決するには、「自己署名証明書の NCM への追加」（P.16）で説明されているように、新しい証明書を NCM キーストアにインポートします。