CA 証明書を設定します

SnapCenter Software 4.9

NetApp
March 20, 2024

目次

CA 証明書を設定します

CA 証明書 CSR ファイルを生成します

証明書署名要求（ CSR ）を生成し、生成された CSR を使用して認証局（ CA ）から取得できる証明書をインポートできます。証明書には秘密鍵が関連付けられます。

CSR はエンコードされたテキストブロックであり、認証された証明書ベンダーに提供されて署名済み CA 証明書を取得します。

CA証明書RSAキーの長さは3072ビット以上にする必要があります。

CSR の生成方法については、を参照してください "CA 証明書 CSR ファイルの生成方法"。

ドメイン（ * .domain.company.com ）またはシステム（ machine1.domain.company.com ）の CA 証明書を所有している場合、 CA 証明書 CSR ファイルの生成を省略できます。 SnapCenter を使用して既存の CA 証明書を導入できます。

クラスタ構成の場合は、クラスタ名（仮想クラスタ FQDN ）とそれぞれのホスト名を CA 証明書に記載する必要があります。 証明書を更新するには、証明書を調達する前にSubject Alternative Name (SAN)フィールドに値を入力します。 ワイルドカード証明書（ * .domain.company.com ）の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA 証明書をインポートする

Microsoft の管理コンソール（ MMC ）を使用して、 SnapCenter サーバと Windows ホストプラグインに CA 証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、 [* ファイル *] 、 [スナップインの追加と削除] の順にクリックします。
2. [スナップインの追加と削除] ウィンドウで、 [**Certificates**] を選択し、 [**Add**] をクリックします。
3. [証明書] スナップインウィンドウで、 [**Computer account**] オプションを選択し、 [完了 *] をクリックします。
4. [* コンソールルート **>** 証明書–ローカルコンピュータ **>** 信頼されたルート証明機関 **>** 証明書 *] をクリックします。
5. [信頼されたルート証明機関] フォルダを右クリックし、 [すべてのタスク **>*Import**] を選択してインポートウィザードを開始します。
6. 次の手順でウィザードを完了します。

ウィザードウィンドウ	実行する処理
秘密鍵をインポートします	オプション * はい * を選択し、秘密鍵をインポートして、 * 次へ * をクリックします。

ウィザードウィンドウ	実行する処理
インポートファイル形式	変更せずに、 * 次へ * をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、 * Next * をクリックします。
証明書のインポートウィザードを完了しています	概要を確認し、 [完了] をクリックしてインポートを開始します。

証明書のインポートは、秘密鍵にバンドルされている必要があります（サポートされている形式は、**.pfx**、.p12、および*.p7b）。

7. 「 Personal 」フォルダについて、手順 5 を繰り返します。

CA 証明書のサムプリントを取得します

証明書のサムプリントは、証明書を識別する 16 進数の文字列です。サムプリントは、サムプリントアルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUI で次の手順を実行します。
   a. 証明書をダブルクリックします。
   b. [証明書] ダイアログボックスで、 [* 詳細 *] タブをクリックします。
   c. フィールドのリストをスクロールし、 [**Thumbprint**] をクリックします。
   d. ボックスから 16 進文字をコピーします。
   e. 16 進数の間のスペースを削除します。

      たとえば、サムプリントが「 A9 09 50 2D d8 2a 14 33 e6 F8 38 86 b0 0d 42 77 A3 2a 7b 」の場合、スペースを削除すると、「 a909502dd82ae41433e6f83886b00d4277a32a7b 」となります。

2. PowerShell で次の手順を実行します。
   a. 次のコマンドを実行して、インストールされている証明書のサムプリントを一覧表示し、最近インストールされた証明書を件名で識別します。

      Get-ChildItem - パス証明書： *\localmachine\My*

   b. サムプリントをコピーします。

Windows ホストプラグインサービスを使用して CA 証明書を設定する

CA 証明書に Windows ホストプラグインサービスを設定して、インストールされたデジタル証明書をアクティブ化する必要があります。

SnapCenter サーバおよび CA 証明書がすでに導入されているすべてのプラグインホストで、次の手順を実行します。

手順

1. 次のコマンドを実行して、 SMCore のデフォルトポート 8145 にバインドされている既存の証明書を削除します。

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   例：

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

   . 次のコマンドを実行して、新しくインストールした証明書を Windows ホストプラグインサービスにバインドします。

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

   例：

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

Linux ホストで SnapCenter Custom Plug-ins サービスの CA 証明書を設定します

カスタムプラグインキーストアとその証明書のパスワードを管理し、CA証明書を設定し、カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定し、インストールされたデジタル証明書をアクティブ化するために、SnapCenterカスタムプラグインサービスを使用してカスタムプラグインの信頼ストアにCA署名キーペアを設定する必要があります。

カスタムプラグインでは、ファイル「 keystore.JKS 」を使用します。このファイルは、信頼ストアおよびキーストアとして _/opt/NetApp/snapcenter / scc /etc/both にあります。

カスタムプラグインのキーストアのパスワード、および使用中の CA 署名済みキーペアのエイリアスを管理します

手順

1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

   キー「 keystore.pass 」に対応する値です。

2. キーストアのパスワードを変更します。

   ```
    keytool -storepasswd -keystore keystore.jks
   ```
   .
   キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   agent.properties ファイル内のキー keystore.pass に対しても同じキーを更新します。

3. パスワードを変更したら、サービスを再起動してください。

> カスタムプラグインキーストアのパスワード、および秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

手順

1. カスタムプラグインキーストアが格納されているフォルダ（/opt/NetApp/snapcenter/scc/etc）に移動します。
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. ルート証明書または中間証明書を追加します。

   ```
    keytool -import -trustcacerts -alias myRootCA -file
   /root/USERTrustRSA_Root.cer -keystore keystore.jks
   ```
   .
   カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動してください。

> ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

手順

1. カスタムプラグインキーストア /opt/NetApp/snapcenter / scc などが含まれているフォルダに移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. キーストアに追加された証明書を表示します。

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. キーストアに、キーストアに追加された新しい CA 証明書に対応するエイリアスが含まれていることを確認します。
7. CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。

   デフォルトのカスタムプラグインキーストアパスワードは、 agent.properties ファイル内のキー keystore.pass の値です。

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   ```
   . CA 証明書のエイリアス名が長く、スペースまたは特殊文字（「 *
   」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   ```
   . agent.properties ファイルの CA 証明書からエイリアス名を設定します。

   この値をキー SCC_CERTIFICATE_ALIAS に更新します。

8. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

SnapCenter Custom Plug-ins の証明書失効リスト（ CRL ）を設定します

このタスクについて

- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、「 /opt/netapp/snapcenter /sscc /etc/crl 」です。

手順

1. agent.properties ファイルのデフォルトディレクトリを、キー crl_path に対して変更および更新できます。

   このディレクトリに複数の CRL ファイルを配置できます。着信証明書は各 CRL に対して検証されます。

Windows ホストで SnapCenter Custom Plug-ins サービスの CA 証明書を設定します

カスタムプラグインキーストアとその証明書のパスワードを管理し、CA証明書を設定し、カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定し、インストールされたデジタル証明書をアクティブ化するために、SnapCenterカスタムプラグインサービスを使用してカスタムプラグインの信頼ストアにCA署名キーペアを設定する必要があります。

カスタムプラグインは、 _ C ： \Program Files\NetApp\SnapManager \Snapcenter Plug-in Creator\etc_both にある file_keystore.JKS_を 信頼ストアおよびキーストアとして使用します。

カスタムプラグインのキーストアのパスワード、および使用中の CA 署名済みキーペアのエイリアスを管理します

手順

1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

   key_keystore.pass_ に対応する値です。

2. キーストアのパスワードを変更します。

   keytool -storepasswd -keystore keystore.JKS

   Windows のコマンドプロンプトで「 keytool 」コマンドが認識されない場合は、 keytool コマンドを完全なパスに置き換えます。

   C ： \Program Files\Java\<JDK_version >\bin\keytool .exe "-storepasswd -keystore keystore.JKS

3. キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアに使用されているパスワードと同じパスワードに変更します。

   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.JKS

   agent.properties ファイル内のキー keystore.pass に対しても同じキーを更新します。

4. パスワードを変更したら、サービスを再起動してください。

   カスタムプラグインキーストアのパスワード、および秘密鍵に関連付けられているすべてのエイリアスパスワードが同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

手順

1. カスタムプラグインkeystore_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_が格納されているフォルダに移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

4. ルート証明書または中間証明書を追加します。

   keytool -import-trustcacerts -alias myRootCA -file/root/USERTrustRSA_Root.cer -keystore keystore.JKS

5. カスタムプラグインの信頼ストアにルート証明書または中間証明書を設定したら、サービスを再起動してください。

ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

CA 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

手順

1. カスタムプラグインの keystore _C ： \Program Files\NetApp\Virtual \SnapCenter \Snapcenter Plug-in Creator\etc\備え ているフォルダに移動します
2. file_keystore.JKS_</Z1> を探します。
3. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

   keytool -importkeystore -srckeystore.root/ snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.JKS -deststoretype JKS

5. キーストアに追加された証明書を表示します。

   keytool -list -v キーストア *.JKS*

6. キーストアに、キーストアに追加された新しい CA 証明書に対応するエイリアスが含まれていることを確認します。
7. CA 証明書用に追加された秘密鍵のパスワードをキーストアのパスワードに変更します。

   デフォルトのカスタムプラグインキーストアパスワードは、 agent.properties ファイル内のキー keystore.pass の値です。

*keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_*

8. *agent.properties* ファイルの CA 証明書からエイリアス名を設定します。

   この値をキー SCC_CERTIFICATE_ALIAS に更新します。

9. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

SnapCenter Custom Plug-ins の証明書失効リスト（ CRL ）を設定します

このタスクについて

- 関連する CA 証明書の最新の CRL ファイルをダウンロードするには、を参照してください "SnapCenter CA 証明書の証明書失効リストファイルを更新する方法"。
- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、 *'C:\Program Files\NetApp\SnapCenter \Snapcenter Plug-in Creator\etc\crl'* です。

手順

1. *agent.properties* ファイルのデフォルトディレクトリを、キー crl_path に対して変更および更新できます。
2. このディレクトリに複数の CRL ファイルを配置できます。

   着信証明書は各 CRL に対して検証されます。

プラグインの CA 証明書を有効にします

CA 証明書を設定し、 SnapCenter サーバと対応するプラグインホストに CA 証明書を導入する必要があります。 プラグインの CA 証明書検証を有効にする必要があります。

作業を開始する前に

- CA 証明書を有効または無効にするには、 run_Set-SmCertificateSetting_cmdlet を使用します。
- このプラグインの証明書ステータスは、 *Get-SmCertificateSettings* を使用して表示できます。

コマンドレットで使用できるパラメータとその説明については、 RUN_Get-Help コマンド *NAME* を実行して参照できます。または、を参照することもできます "SnapCenter ソフトウェアコマンドレットリファレンスガイド"。

手順

1. 左側のナビゲーションペインで、 * Hosts * （ホスト）をクリックします。
2. [Hosts] ページで、 [*Managed Hosts] をクリックします。
3. 1 つまたは複数のプラグインホストを選択します。
4. [* その他のオプション *] をクリックします。
5. [証明書の検証を有効にする] を選択します。

完了後

管理対象ホストタブのホストには鍵が表示され、 SnapCenter サーバとプラグインホストの間の接続のステータスが南京錠の色で示されます。

- は、 CA 証明書が有効になっておらず、プラグインホストにも割り当てられていないことを示します。
- CA 証明書が正常に検証されたことを示します。
- は、 CA 証明書を検証できなかったことを示します。
- 接続情報を取得できなかったことを示します。

ステータスが黄色または緑のときは、データ保護処理が正常に完了しています。

著作権に関する情報

商標に関する情報