



CA証明書の設定

SnapCenter software

NetApp
November 06, 2025

目次

CA証明書の設定	1
CA証明書CSRファイルの生成	1
CA証明書のインポート	1
CA証明書のサムプリントの取得	2
Windowsホスト プラグイン サービスでのCA証明書の設定	2
LinuxホストでのNetAppがサポートしているプラグイン サービスのCA証明書の設定	3
プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する	3
ルート証明書または中間証明書をプラグイン信頼ストアに設定する	4
プラグイン信頼ストアにCA署名キーペアを構成する	4
プラグインの証明書失効リスト（CRL）を構成する	5
WindowsホストでのNetAppがサポートしているプラグイン サービスのCA証明書の設定	6
プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する	6
ルート証明書または中間証明書をプラグイン信頼ストアに設定する	6
プラグイン信頼ストアにCA署名キーペアを構成する	7
SnapCenterプラグインの証明書失効リスト（CRL）を構成する	8
プラグインのCA証明書の有効化	8

CA証明書の設定

CA証明書CSRファイルの生成

証明書署名要求 (CSR) を生成し、生成したCSRを使用して認証局 (CA) から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。



CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、["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は、CA 証明書 CSR ファイルの生成をスキップできます。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、クラスタ名 (仮想クラスタFQDN) と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。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証明書のインポート

Microsoft管理コンソール (MMC) を使用して、SnapCenter Server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] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] 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 コンピューター > 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]>[インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。

ウィザード ウィンドウ	操作
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、[次へ] をクリックします。
証明書のインポート ウィザードの完了	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。



インポートする証明書は秘密キーと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 です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための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て、「拇印」をクリックします。
 - d. ボックスから16進数の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、拇印が「a9 09 50 2d d8 2a e4 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」になります。

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表示し、最近インストールされた証明書をサブジェクト名で識別します。

```
Get-ChildItem -Path 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 サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラグイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、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、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

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

例えば：

```
> 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
サービスとバインドします。
```

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

例えば：

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

LinuxホストでのNetAppがサポートしているプラグイン サービスのCA証明書の設定

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には、SnapCenterプラグイン サービスを使用して、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 証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成 し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、`/opt/NetApp/snapcenter/scc/etc`にあるファイル「`keystore.jks`」を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

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キー
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 ファイルのキー KEYSTORE_PASS も同様に更新します。

3. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは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プラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグイン キーストアが含まれるフォルダーに移動します: /opt/ NetApp/snapcenter/scc/etc。
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

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

4. ルート証明書か中間証明書を追加します。

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

・ ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。
。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアにCA署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグイン キーストア `/opt/NetApp/snapcenter/scc/etc` が含まれるフォルダーに移動します。
2. 「`keystore.jks`」ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

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

4. 秘密キーと公開キーの両方が設定された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の一覧を表示します。

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

6. 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、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、`agent.properties` ファイルのキー `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、スペースや特殊文字（「*」、「」）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_ALIASES` に対して更新します。

8. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

プラグインの証明書失効リスト（CRL）を構成する

タスク概要

- ・ SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- ・ SnapCenter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/scc/etc/crl`」です。

手順

1. キー `CRL_PATH` に対して、`agent.properties` ファイルのデフォルト ディレクトリを変更、更新できます。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれ

のCRLに対して検証が行われます。

WindowsホストでのNetAppがサポートしているプラグインサービスのCA証明書の設定

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には、SnapCenterプラグインサービスを使用して、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証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、`C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`にあるファイル `keystore.jks` を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

これはキー `_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
```



Windows 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キー エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "証明書内のエイリアス名" -keystore keystore.jks
```

`agent.properties` ファイルのキー `KEYSTORE_PASS` も同様に更新します。

4. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは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プラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `_C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_` に移動します。
2. 「`keystore.jks`」ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

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

4. ルート証明書か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. ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアに**CA**署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `_C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_` に移動します。
2. ファイル `keystore.jks` を見つけます。
3. キーストアに追加された証明書の一覧を表示します。

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

4. 秘密キーと公開キーの両方が設定された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の一覧を表示します。

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

6. 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、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、`agent.properties` ファイルのキー `KEYSTORE_PASS` の値です。

```
keytool -keypasswd -alias "CA証明書のエイリアス名" -keystore keystore.jks
```

8. `agent.properties` ファイル内の 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` に対して更新します。

9. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

SnapCenterプラグインの証明書失効リスト (CRL) を構成する

タスク概要

- 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、"[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プラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter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. キー `CRL_PATH` に対して、`agent.properties` ファイル内のデフォルト ディレクトリを変更および更新できます。
2. このディレクトリには、複数のCRLファイルを格納できます。

受信する証明書については、それぞれのCRLに対して検証が行われます。

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 `Set-SmCertificateSettings` コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで使用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[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、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
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。

終了後の操作

[Managed Hosts] タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- *  * は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。

- *  * は 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。
- *  * は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場合は、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

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。