



証明書ベースの認証を設定します

SnapCenter Software 5.0

NetApp
July 18, 2024

目次

証明書ベースの認証を設定します	1
SnapCenterサーバから認証局（CA）証明書をエクスポートします	1
認証局（CA）証明書をWindowsプラグインホストにインポートします	1
CA証明書をUNIXホストプラグインにインポートし、ルート証明書または中間証明書をSPL trust-storeに設定します	2
証明書ベースの認証を有効にします	4

証明書ベースの認証を設定します

SnapCenterサーバから認証局（CA）証明書をエクスポートします

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバからプラグインホストにCA証明書をエクスポートする必要があります。

開始する前に

双方向SSLを設定しておく必要があります。

• 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*オプションを選択し、[完了]*をクリックします。
4. >[証明書-ローカルコンピュータ]>[個人]>[証明書]*をクリックします。
5. SnapCenterサーバで使用される調達CA証明書を右クリックし、[すべてのタスク]>*[エクスポート]*を選択してエクスポートウィザードを開始します。
6. ウィザードで次の操作を実行します。

オプション	操作
秘密キーのエクスポート	を選択し、[次へ]*をクリックします。
エクスポートファイル形式	「* 次へ *」をクリックします。
ファイル名	をクリックし、証明書を保存するファイルパスを指定して[次へ]*をクリックします。
証明書のエクスポートウィザードの完了	概要を確認し、* 完了 * をクリックしてエクスポートを開始します。



証明書ベースの認証は、SnapCenter HA構成およびSnapCenter Plug-in for VMware vSphereではサポートされません。

認証局（CA）証明書をWindowsプラグインホストにインポートします

エクスポートしたSnapCenterサーバCA証明書を使用するには、Microsoft管理コンソール（MMC）を使用して、関連する証明書をSnapCenter Windowsプラグインホストに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*オプションを選択し、[完了]*をクリックします。
4. >[証明書-ローカルコンピュータ]>[個人]>[証明書]*をクリックします。
5. 「個人」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開始します。
6. ウィザードで次の操作を実行します。

オプション	操作
ストアの場所	「* 次へ *」をクリックします。
インポートするファイル	拡張子.cerで終わるSnapCenterサーバ証明書を選択します。
証明書ストア	「* 次へ *」をクリックします。
証明書のエクス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。

CA証明書をUNIXホストプラグインにインポートし、ルート証明書または中間証明書をSPL trust-storeに設定します

CA証明書をUNIXプラグインホストにインポートします

CA証明書をUNIXプラグインホストにインポートする必要があります。

• このタスクについて *

- SPLキーストアのパスワード、および使用中のCA署名キーペアのエイリアスを管理できます。
- SPLキーストアのパスワードと、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は同じである必要があります。

• 手順 *

1. SPLキーストアのデフォルトパスワードは、SPLプロパティファイルから取得できます。キーに対応する値です SPL_KEYSTORE_PASS。
2. キーストアのパスワードを変更します。\$ keytool -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、キーストアと同じパスワードに変更します。\$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
4. ファイルのSPL_KEYSTORE_PASSキーについても同じ内容を更新し spl.properties` ます。

5. パスワードを変更したら、サービスを再起動します。

spl trust-storeに対するルート証明書または中間証明書の設定

ルート証明書または中間証明書をspl trust-storeに設定する必要があります。ルートCA証明書のあとに中間CA証明書を追加する必要があります。

• 手順 *

1. SPLキーストアが格納されているフォルダに移動します `/var/opt/snapcenter/spl/etc`。
2. ファイルを探します `keystore.jks`。
3. キーストアに追加された証明書を一覧表示します。 `$ 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 <AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. spl trust-store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ます。

SPL trust-storeへのCA署名済みキーペアの設定

SPL trust-storeにCA署名付きキーペアを設定する必要があります。

• 手順 *

1. SPLのキーストアが格納されているフォルダに移動し ``var/opt/snapcenter/spl/etc``ます。
2. ファイルを探します `keystore.jks``。
3. キーストアに追加された証明書を一覧表示します。 `$ keytool -list -v -keystore keystore.jks`
4. 秘密鍵と公開鍵の両方が設定されたCA証明書を追加します。 `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. キーストアに追加された証明書を一覧表示します。 `$ 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SPLキーストアパスワードは、ファイル内のキー`spl_keystore_pass`の値です `spl.properties`。

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
```

1. 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 "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks``

2. ファイルにあるキーストアからエイリアス名を設定し `spl.properties` ます。この値を `SPL_CERTIFICATE_ALIAS` キーに対して更新します。
3. SPL trust-storeにCA署名キーペアを設定したら、サービスを再起動します。

証明書ベースの認証を有効にします

SnapCenter ServerおよびWindowsプラグインホストに対して証明書ベースの認証を有効にするには、次のPowerShellコマンドレットを実行します。Linuxプラグインホストで双方向SSLを有効にすると、証明書ベースの認証が有効になります。

- クライアント証明書ベースの認証を有効にするには：

```
Set-SmConfigSettings -Agent -configSettings  
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- クライアント証明書ベースの認証を無効にするには：

```
Set-SmConfigSettings -Agent -configSettings  
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

著作権に関する情報

Copyright © 2024 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。