WindowsホストのCA証明書の設定

SnapCenter software

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/snapcenter/install/reference_generate_CA_certificate_CSR_file.html on January 09, 2026. Always check docs.netapp.com for the latest.

目次

Windowsホストの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
- SnapCenterサイトでCA証明書を設定 . . . 3
- SnapCenterのCA証明書を有効にする . . . 4

Windowsホストの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RSAキーの長さは3072ビット以上にする必要があります。

CSRを生成する方法については、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、クラスタ名（仮想クラスタFQDN）、および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。証明書を更新するには、証明書を取得する前に 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証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenterサーバおよび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	操作
秘密キーのインポート	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	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、 * Next * 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。

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」フォルダに対して手順5を繰り返します。

CA証明書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、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から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 - 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を使用して既存の証明書バインディングを削除します。

   ```
   > 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ホストの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：

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

SnapCenterサイトでCA証明書を設定

WindowsホストのSnapCenterサイトでCA証明書を設定する必要があります。

- 手順 *

  1. SnapCenter がインストールされている Windows サーバーで IIS マネージャーを開きます。
  2. 左側のナビゲーションペインで、 * 接続 * をクリックします。
  3. サーバー名と * Sites * を展開します。
  4. SSL証明書をインストールするSnapCenter Webサイトを選択します。
  5. [* アクション * （ Actions * ）] > [* サイトの編集 * （ * Edit Site * ）] に移動し、 [* バインド * （ Bind
  6. バインディングページで、「 https * のバインディング」を選択します。
  7. [編集（ Edit ）] をクリックします。

8. [SSL証明書]ドロップダウンリストから、最近インポートしたSSL証明書を選択します。
9. [OK]*をクリックします。

SnapCenterスケジューラサイト（デフォルトポート：8154、HTTPS）には自己署名証明書が設定されています。このポートはSnapCenterサーバホスト内で通信しており、CA証明書を使用してを設定する必要はありません。ただし、CA証明書の使用が必要な環境の場合は、SnapCenterスケジューラサイトを使用して手順5から9を繰り返します。

最近導入したCA証明書がドロップダウンメニューに表示されない場合は、CA証明書が秘密鍵に関連付けられているかどうかを確認します。

証明書が次のパスを使用して追加されていることを確認します。 * 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 * 。

SnapCenterのCA証明書を有効にする

CA証明書を設定し、SnapCenterサーバに対して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

- CA証明書を有効または無効にするには、Set-SmCertificateSettingsコマンドレットを使用します。
- SnapCenterサーバの証明書のステータスは、Get-SmCertificateSettingsコマンドレット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、を参照して "SnapCenter ソフトウェアコマンドレットリファレンスガイド"ください。

- 手順 *
  1. 設定ページで、 * 設定 * > * グローバル設定 * > * CA 証明書設定 * と進みます。
  2. [証明書の検証を有効にする] を選択します。
  3. [適用（ Apply ）] をクリックします。
- 終了後 *

[管理対象ホスト]タブのホストには南京錠が表示され、南京錠の色はSnapCenterサーバ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、有効になっているかプラグインホストに割り当てられているCA証明書が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 © 2026 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権を有し、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権については、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。