



# **SnapCenter Plug-in for Microsoft Windowsのインストール**

## **SnapCenter software**

NetApp  
November 06, 2025

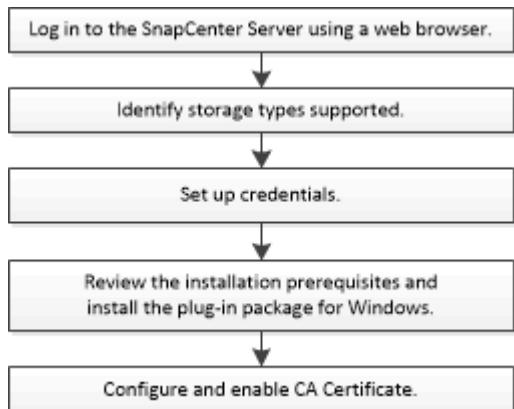
# 目次

SnapCenter Plug-in for Microsoft Windowsのインストール	1
SnapCenter Plug-in for Microsoft Windowsのインストール ワークフロー	1
SnapCenter Plug-in for Microsoft Windowsのインストール要件	1
SnapCenter Plug-ins Package for Windowsをインストールするホストの要件	1
Plug-in for Windowsのクレデンシャルの設定	2
Windows Server 2016以降でのgMSAの設定	4
ホストの追加とSnapCenter Plug-in for Microsoft Windowsのインストール	5
PowerShellコマンドレットを使用した複数のリモート ホストへのSnapCenter Plug-in for Microsoft Windowsのインストール	9
コマンドラインからのSnapCenter Plug-in for Microsoft Windowsのサイレント インストール	9
SnapCenterプラグイン パッケージのインストール ステータスの監視	11
CA証明書の設定	12
CA証明書CSRファイルの生成	12
CA証明書のインポート	12
CA証明書のサムプリントの取得	13
Windowsホスト プラグイン サービスでのCA証明書の設定	14
プラグインのCA証明書の有効化	14

# SnapCenter Plug-in for Microsoft Windowsのインストール

## SnapCenter Plug-in for Microsoft Windowsのインストール ワークフロー

データベース ファイルではない Windows ファイルを保護する場合は、Microsoft Windows 用のSnapCenterプラグインをインストールして設定する必要があります。



## SnapCenter Plug-in for Microsoft Windowsのインストール要件

Plug-in for Windowsをインストールする前に、特定のインストール要件を確認しておく必要があります。

ユーザがPlug-in for Windowsの使用を開始するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- Plug-in for Windowsをインストールするには、SnapCenter admin権限が必要です。  
SnapCenter adminロールには管理者権限が必要です。
- SnapCenter Serverをインストールして設定しておく必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- バックアップ レプリケーションが必要な場合は、SnapMirrorとSnapVaultをセットアップする必要があります。

## SnapCenter Plug-ins Package for Windowsをインストールするホストの要件

SnapCenter Plug-ins Package for Windowsをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、 " <a href="#">NetApp Interoperability Matrix Tool</a> "。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB  十分なディスク スペースを割り当て、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	<ul style="list-style-type: none"> <li>ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル</li> <li>PowerShell Core 7.4.2</li> </ul> <p>サポートされているバージョンに関する最新情報については、 "<a href="#">NetApp Interoperability Matrix Tool</a>"。</p>

## Plug-in for Windowsのクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、Windowsファイルシステムでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

### 必要なもの

- プラグインのインストール前にWindowsクレデンシャルを設定する必要があります。
- このクレデンシャルには、管理者権限（リモート ホストに対する管理者権限を含む）を設定する必要があります。
- 個々のリソース グループのクレデンシャルを設定する場合で、ユーザに完全なadmin権限が割り当てられない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

### 手順

- 左側のナビゲーション ペインで、[設定] をクリックします。

2. [設定]ページで、[資格情報]をクリックします。
3. \*新規\*をクリックします。
4. [Credential]ページで次の操作を実行します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。
ユーザー名/パスワード	<p>認証に使用するユーザ名とパスワードを入力します。</p> <ul style="list-style-type: none"> <li>• ドメイン管理者または管理者グループの任意のメンバー</li> </ul> <p>ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。</p> <ul style="list-style-type: none"> <li>◦ NetBIOS\UserName</li> <li>◦ Domain FQDN\UserName</li> <li>◦ UserName@upn</li> </ul> <ul style="list-style-type: none"> <li>• ローカル管理者（ワークグループの場合のみ）</li> </ul> <p>ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザ名フィールドの有効な形式は次のとおりです。</p> <p>UserName</p> <p>パスワードには二重引用符 ("") やバッククオート (`) を使用しないでください。未満記号 (&lt;) と感嘆符 (!) を組み合わせて使用したりしないでください。たとえば、less than &lt;!10 、less than 10&lt;!、バックティック `12 などです。</p>
パスワード	認証に使用するパスワードを入力します。

5. [OK]をクリックします。

クレデンシャルの設定が完了したら、必要に応じて[User and Access]ページでユーザやユーザ グループにクレデンシャルを割り当てるすることができます。

## Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、作成したグループ管理サービス アカウント（gMSA）を通じて、管理対象ドメインアカウントからサービス アカウントのパスワードを自動管理できます。

開始する前に

- Windows Server 2016以降のドメイン コントローラが必要です。
- ドメインのメンバーであるWindows Server 2016以降のホストが必要です。

手順

1. KDSルート キーを作成し、gMSA内のオブジェクトごとに一意のパスワードを生成します。
2. 各ドメインについて、Windows ドメインコントローラから次のコマンドを実行します: Add-KDSRootKey -EffectiveImmediately
3. gMSAを作成して設定します。
  - a. 次の形式でユーザ グループ アカウントを作成します。

```
domainName\accountName$  
.. コンピュータ オブジェクトをグループに追加します。  
.. 作成したユーザ グループを使用してgMSAを作成します。
```

次に例を示します。

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 走る `Get-ADServiceAccount` サービス アカウントを確認するコマンド。
```

4. ホストでgMSAを設定します。

- a. gMSAアカウントを使用するホストで、Windows PowerShell用のActive Directoryモジュールを有効にします。

これを行うには、PowerShellから次のコマンドを実行します。

```

PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name           Name           Install State
-----
[ ] Active Directory Domain Services   AD-Domain-Services Available

PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
----- ----- ----- -----
True    No          Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.

```

- a. ホストを再起動します。
  - b. PowerShell コマンド プロンプトから次のコマンドを実行して、ホストに gMSA をインストールします。 `Install-AdServiceAccount <gMSA>`
  - c. 次のコマンドを実行して、gMSA アカウントを確認します。 `Test-AdServiceAccount <gMSA>`
5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
6. SnapCenter Serverで設定済みのgMSAアカウントを指定してWindowsホストを追加します。

SnapCenter Serverにより、選択したプラグインがホストにインストールされ、プラグインのインストール時には指定したgMSAがサービスのログオン アカウントとして使用されます。

## ホストの追加とSnapCenter Plug-in for Microsoft Windowsのインストール

SnapCenterの[Add Host]ページを使用して、Windowsホストを追加できます。SnapCenter Plug-in for Microsoft Windowsは、指定したホストに自動的にインストールされます。これは推奨されるプラグインのインストール方法です。ホストの追加とプラグインのインストールは、ホストごとまたはクラスタごとに実行できます。

開始する前に

- SnapCenter Serverホストのオペレーティング システムがWindows 2019で、プラグイン ホストのオペレーティング システムがWindows 2022の場合は、次の手順を実行する必要があります。
  - Windows Server 2019 (OSビルド17763.5936) 以降にアップグレードする
  - Windows Server 2022 (OSビルド20348.2402) 以降にアップグレードする
- この処理は、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。

- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザーがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- SnapCenterユーザーを、Windows Server の「サービスとしてログオン」ロールに追加する必要があります。
- メッセージ キュー サービスが実行中であることを確認する必要があります。
- グループ管理サービス アカウント (gMSA) を使用する場合は、管理者権限でgMSAを設定する必要があります。

["Windows Server 2016以降でWindowsファイルシステム用にグループ管理サービス アカウントを設定する"](#)

## タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。
- Windowsプラグイン
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
- クラスタへのプラグインのインストール

クラスタ (WSFC、Oracle RAC、またはExchange DAG) にプラグインをインストールする場合、プラグインはクラスタのすべてのノードにインストールされます。

- Eシリーズ ストレージ

Eシリーズ ストレージに接続されたWindowsホストにPlug-in for Windowsをインストールすることはできません。



SnapCenterでは、同じホスト（プラグイン ホスト）をSnapCenterに追加することはできません。そのホストがすでにワークグループに属していて、ドメインを別のものに変更しても（またはその逆をしても）、追加することはできません。同じホストを追加する場合は、SnapCenterからホストを削除して再度追加する必要があります。

## 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. 上部で\*管理対象ホスト\*が選択されていることを確認します。
3. \*[追加]\*をクリックします。
4. [Hosts]ページで次の操作を実行します。

フィールド	操作
ホストタイプ	<p><b>Windows</b> タイプのホストを選択します。</p> <p>SnapCenter Serverがホストを追加し、Plug-in for Windowsをホストにインストールします（プラグインがまだインストールされていない場合）。</p>
ホスト名	<p>ホストの完全修飾ドメイン名 (FQDN) またはIPアドレスを入力します。</p> <p>SnapCenterが機能するためには、DNSが適切に設定されている必要があります。したがって、ベストプラクティスはFQDNを入力することです。</p> <p>次のいずれかのIPアドレスまたはFQDNを入力できます。</p> <ul style="list-style-type: none"> <li>• スタンドアロン ホスト</li> <li>• Windows Serverフェイルオーバー クラスタリング (WSFC)</li> </ul> <p>SnapCenterを使用してホストを追加する際、ホストがサブドメインの一部である場合は、FQDNを指定する必要があります。</p>
Credentials	<p>作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。</p> <p>このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。</p> <p>ユーザ名、ドメイン、およびホスト タイプを含むクレデンシャルの詳細は、指定したクレデンシャルの名前にカーソルを合わせると表示されます。</p> <div style="display: flex; align-items: center;"> <span style="font-size: 2em; margin-right: 10px;">i</span> <p>認証モードは、[Add Host] ウィザードで指定するホスト タイプによって決まります。</p> </div>

5. [Select Plug-ins to Install] セクションで、インストールするプラグインを選択します。

新規導入の場合、プラグイン パッケージは表示されません。

6. (オプション) [その他のオプション] をクリックします。

フィールド	操作
ポート	<p>デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。</p> <p>デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。</p> <p> プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。</p>
Installation Path	<p>デフォルトのパスはC:\Program Files\NetApp\SnapCenterです。</p> <p>必要に応じて変更できます。SnapCenter Plug-ins Package for Windowsの場合、デフォルト パスはC:\Program Files\NetApp\SnapCenterです。ただし、必要に応じて、デフォルト パスはカスタマイズできます。</p>
クラスター内のすべてのホストを追加する	WSFC内のすべてのクラスタ ノードを追加するには、このチェック ボックスをオンにします。
Skip preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェック ボックスをオンにします。
Use group Managed Service Account (gMSA) to run the plug-in services	<p>グループ管理サービス アカウント (gMSA) を使用してプラグイン サービスを実行する場合は、このチェック ボックスをオンにします。</p> <p>gMSA 名を次の形式で指定します: <i>domainName\accountName\$</i></p> <p> gMSAは、SnapCenter Plug-in for Windowsサービスのログオン サービス アカウントとしてのみ使用されます。</p>

7. \*送信\*をクリックします。

「事前チェックをスキップ」 チェックボックスを選択していない場合、ホストがプラグインのインストール要件を満たしているかどうかが検証されます。ディスク容量、RAM、PowerShellのバージョン、.NETのバージョン、および場所が最小要件に照らして検証されます。最小要件を満たしていない場合、対応す

るエラーまたは警告メッセージが表示されます。

エラーがディスク容量またはRAMに関連している場合は、次の場所にあるweb.configファイルを更新できます。`C:\Program Files\NetApp\SnapCenter`デフォルト値を変更する WebApp。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HAのセットアップでweb.configファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

#### 8. インストールの進捗状況を監視します。

## PowerShellコマンドレットを使用した複数のリモート ホストへのSnapCenter Plug-in for Microsoft Windowsのインストール

SnapCenter Plug-in for Microsoft Windowsを複数のホストに一度にインストールする場合は、`Install-SmHostPackage` PowerShell コマンドレット。

プラグインをインストールする各ホストで、ローカル管理者の権限を持つドメイン ユーザとしてSnapCenterにログインしている必要があります。

### 手順

1. PowerShellを起動します。
2. SnapCenter Serverホストで、`Open-SmConnection`コマンドレットを実行し、資格情報を入力します。
3. スタンドアロンホストまたはクラスタをSnapCenterに追加するには、`Add-SmHost`コマンドレットと必要なパラメータ。

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"](#)。

4. 複数のホストにプラグインをインストールするには、`Install-SmHostPackage`コマンドレットと必要なパラメータ。

使用することができます`-skiprecheck`プラグインを手動でインストールし、ホストがプラグインのインストール要件を満たしているかどうかを検証たくない場合は、このオプションを選択します。

## コマンドラインからのSnapCenter Plug-in for Microsoft Windowsのサイレント インストール

SnapCenter GUIからリモートでインストールできない場合は、Windowsホスト上でローカルにSnapCenter Plug-in for Microsoft Windowsをインストールできます。Windowsのコマンドラインから、SnapCenter Plug-in for Microsoft Windowsのインストール プログラムをサイレント モードで自動的に実行できます。

### 開始する前に

- ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドルがイン

ストールされている必要があります。

- PowerShell 7.4.2以降がインストールされている必要があります。
- ホストのローカル管理者である必要があります。

#### 手順

- インストールの場所から、SnapCenter Plug-in for Microsoft Windowsをダウンロードします。

たとえば、デフォルトのインストール パスはC:\ProgramData\NetApp\SnapCenter\Package Repositoryです。

このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

- プラグインをインストールするホストにインストール ファイルをコピーします。
- コマンド プロンプトから、インストール ファイルをダウンロードしたディレクトリに移動します。
- 以下のコマンドを、変数を実際のデータに置き換えて入力します。

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""  
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=  
ISFeatureInstall=SCW
```

例えば：

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository  
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:  
\HPPW_SCW_Install.log" /log"C:\\" BI_SNAPCENTER_PORT=8145  
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW`
```



Plug-in for Windowsのインストール時に渡されるすべてのパラメータでは、大文字と小文字が区別されます。

以下の変数に値を入力します。

変数	Value
/debuglog"<デバッグルogパス>	次の例のように、スイート インストーラ ログ ファイルの名前と場所を指定します: Setup.exe /debuglog"C:\PathToLog\setupexe.log"。
BI_SNAPCENTER_PORT	SnapCenterがSMCoreと通信するポートを指定します。
SUITE_INSTALLDIR	ホストのプラグイン パッケージのインストール ディレクトリを指定します。

変数	Value
BI_SERVICEACCOUNT	SnapCenter Plug-in for Microsoft WindowsのWebサービス アカウントを指定します。
BI_SERVICEPWD	SnapCenter Plug-in for Microsoft WindowsのWebサービス アカウントのパスワードを指定します。
ISFeatureInstall	SnapCenterでリモート ホストに導入するソリューションを指定します。

*debuglog* パラメータには、 SnapCenterのログ ファイルのパスが含まれます。このログ ファイルにはインストールで実行されるプラグインの前提条件に関するチェック結果が記録されるため、トラブルシューティング情報を入手する手段としてこのログ ファイルに書き込むことを推奨します。

必要な場合、 SnapCenter for Windowsパッケージのログ ファイルでその他のトラブルシューティング情報を探して確認できます。パッケージのログ ファイルは、 %Temp% フォルダー (例: C:\temp\ ) に (古いものから順に) リストされます。



Plug-in for Windowsをインストールすると、 SnapCenter Serverではなくホストにプラグインが登録されます。 SnapCenter GUIまたはPowerShellコマンドレットを使用してホストを追加することにより、 SnapCenter Serverにプラグインを登録できます。ホストを追加すると、 プラグインが自動的に検出されます。

## SnapCenter プラグイン パッケージのインストール ステータス の監視

[Jobs]ページを使用して、 SnapCenter プラグイン パッケージのインストールの進捗状況を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

### タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録

### 手順

1. 左側のナビゲーションペインで、 [モニター] をクリックします。
2. \*モニター\*ページで、 \*ジョブ\*をクリックします。

3. ジョブ ページで、プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、次の手順を実行します。
  - a. \*フィルター\*をクリックします。
  - b. オプション：開始日と終了日を指定します。
  - c. [タイプ] ドロップダウン メニューから、[プラグインのインストール] を選択します。
  - d. [Status] ドロップダウン メニューから、インストールのステータスを選択します。
  - e. \*適用\*をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. \*ジョブの詳細\*ページで、\*ログの表示\*をクリックします。

## 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。
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"
```

## 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隨時、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 5225.227-19（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。