SnapCenter Plug-in for Microsoft Windows をインストールします

SnapCenter Software 4.6

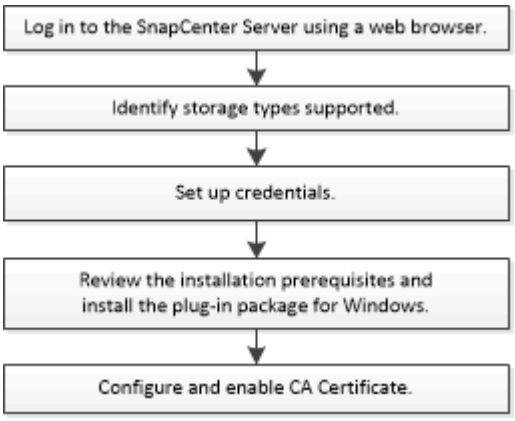
NetApp
August 07, 2024

目次

SnapCenter Plug-in for Microsoft Windows をインストールします

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以外の Windows ファイルを保護する場合は、 SnapCenter Plug-in for Microsoft Windows をインストールしてセットアップ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、一定のインストール要件について理解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 サーバ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 管理者権限が必要です。

  SnapCenter 管理者ロールには管理者権限が必要です。

- SnapCenter サーバ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場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで 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、ホストシステムのいくつかの基本的なスペース要件とサイジング要件を確認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 の場合 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
ホスト上の SnapCenter プラグインの最小 RAM	1 GB
ホスト上の SnapCenter プラグインの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、logs 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、保護する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、最近実行した処理に対してログは作成されません。
必要なソフトウェアパッケージ	• Microsoft .NET Framework 4.5.2 以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 以降 サポートされているバージョンの最新情報については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

Plug-in for Windows のクレデンシャルを設定します

SnapCenter は、クレデンシャルを使用して SnapCenter 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必要なクレデンシャル、および Windows ファイルシステムでデータ保護処理を実行するための追加のクレデンシャルを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 クレデンシャルをセットアップする必要があります。
- リモートホストで、管理者権限を含む管理者権限でクレデンシャル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していて、そのユーザにフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザに割り当てる必要があります。
- 手順 *
  1. 左側のナビゲーションペインで、 * 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. [新規作成（ New ）] をクリックする。

4. [クレデンシャル] ページで、次の操作を実行します。

フィールド	手順
クレデンシャル名	クレデンシャルの名前を入力します。
ユーザ名 / パスワード	認証に使用するユーザ名とパスワードを入力します。 • 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 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。Username フィールドの有効な形式は次のとおりです。 ◦ NETBIOS/USERNAME ◦ 「ドメイン FQDN\ ユーザ名」 ◦ 「 username@UPN 」のようになります • ローカル管理者（ワークグループのみ） 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。Username フィールドの有効な形式は、「 username 」です パスワードに二重引用符（"）またはバックティック（`）を使用しないでください。小なり（<）と感嘆符（！）は使用しないでください。 パスワードに記号を追加します。たとえば、lessthan <！10、lessthan10 <！、backtick 12とします。
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、 [ユーザとアクセス（ User and Access ）] ページで、ユーザまたはユーザグループにクレデンシャルのメンテナンスを割り当てることができます。

Windows Server 2012 以降で gMSA を構成します

Windows Server 2012 以降では、管理ドメインアカウントからサービスアカウントパスワードの自動管理を提供するグループマネージドサービスアカウント（ gMSA ）を作成できます。

- 必要なもの *
- Windows Server 2012 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 2012 以降のホストが必要です。
- 手順 *

1. GMSA のオブジェクトごとに固有のパスワードを生成するには、 KDS ルートキーを作成します。
2. ドメインごとに、 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 -EffectiveImmedient
3. GMSA を作成して構成します。
   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$
.. グループにコンピュータオブジェクトを追加します。
.. 作成したユーザグループを使用して gMSA を作成します。
```

   例：

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. 「 Get-ADServiceAccount
」コマンドを実行して、サービスアカウントを確認します。
```

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。

      そのためには、 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・プロンプトの「 Install-AdServiceAccount <gMSA > 」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

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 >

   1. ホスト上で設定されている gMSA に管理者権限を割り当てます。

   2. SnapCenter サーバで設定済みの gMSA アカウントを指定して、 Windows ホストを追加します。

      SnapCenter サーバーは選択されたプラグインをホストにインストールし、指定された gMSA はプラグインのインストール時にサービスログオンアカウントとして使用されます。

Windows Server 2012 以降で gMSA を構成します

Windows Server 2012 以降では、管理ドメインアカウントからサービスアカウントパスワードの自動管理を提供するグループマネージドサービスアカウント（ gMSA ）を作成できます。

- 必要なもの *
- Windows Server 2012 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 2012 以降のホストが必要です。
- 手順 *

1. GMSA のオブジェクトごとに固有のパスワードを生成するには、 KDS ルートキーを作成します。
2. ドメインごとに、 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 -EffectiveImmedient
3. GMSA を作成して構成します。

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

例：

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. 「 Get-ADServiceAccount
」コマンドを実行して、サービスアカウントを確認します。
```

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。

      そのためには、 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・プロンプトの「 Install-AdServiceAccount <gMSA > 」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
   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 >
      1. ホスト上で設定されている gMSA に管理者権限を割り当てます。
      2. SnapCenter サーバで設定済みの gMSA アカウントを指定して、 Windows ホストを追加します。

SnapCenter サーバーは選択されたプラグインをホストにインストールし、指定された gMSA はプラグインのインストール時にサービスログオンアカウントとして使用されます。

ホストを追加し、 SnapCenter Plug-in for Microsoft Windows をインストールします

SnapCenter のホストの追加ページを使用して、 Windows ホストを追加できます。指定したホストには、 SnapCenter Plug-in for Microsoft Windows が自動的にインストールされます。これはプラグインのインストールに推奨される方法です。ホストを追加してプラグインをインストールするには、個々のホストまたはクラスタを使用します。

- 必要なもの *
- 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必要です。
- Windows ホストにプラグインをインストールする場合、ビルトインでないクレデンシャルを指定する場合、またはユーザがローカルワークグループユーザに属している場合は、ホストで UAC を無効にする必要があります。
- SnapCenter ユーザーは '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
- メッセージキューイングサービスが実行中状態であることを確認する必要があります。
- Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用している場合は、管理者権限を持つ gMSA を設定する必要があります。

  "Windows ファイルシステム用に、 Windows Server 2012 以降のグループマネージドサービスアカウントを設定します"

- このタスクについて *
- SnapCenter サーバをプラグインホストとして別の SnapCenter サーバに追加することはできません。
- Windows プラグイン
  - Microsoft Windows の場合
  - Microsoft Exchange Server の略
  - Microsoft SQL Server の場合
  - SAP HANA のサポート
  - カスタムプラグイン
- 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と、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。

- 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. 上部で [Managed Hosts] が選択されていることを確認します。
3. [追加（ Add ）] をクリックします。
4. Hosts ページで、次の手順を実行します。

フィールド	手順
ホストタイプ	Windows * タイプのホストを選択します。 SnapCenter Server によってホストが追加され、Plug-in for Windows がまだホストにインストールされていない場合はインストールされます。
ホスト名	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。 SnapCenter は、 DNS の適切な設定によって異なります。そのため、ベストプラクティスは Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を入力することです。 次のいずれかの IP アドレスまたは FQDN を入力できます。 • スタンドアロンホスト • Windows Server フェイルオーバークラスタリング（ WSFC ） 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。

フィールド	手順
クレデンシャル	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。 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。 ユーザ名、ドメイン、ホストタイプなど、クレデンシャルの詳細は、指定したクレデンシャル名にカーソルを合わせると表示されます。 認証モードは、ホストの追加ウィザードで指定したホストタイプによって決まります。

5. インストールするプラグインの選択セクションで、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	手順
ポート	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。 デフォルトのポート番号は 8145 です。SnapCenter サーバ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。 プラグインを手動でインストールし、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、処理は失敗します。
インストールパス	デフォルトパスは C ： \Program Files\NetApp\SnapManager です。 必要に応じて、パスをカスタマイズできます。SnapCenter Plug-ins Package for Windows のデフォルトパスは C ： \Program Files\NetApp\SnapManager です。ただし、必要に応じて、デフォルトパスをカスタマイズできます。

フィールド	手順
クラスタ内のすべてのホストを追加します	WSFC 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選択します。
インストール前のチェックをスキップします	プラグインを手動でインストール済みで、プラグインのインストール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選択します。
プラグインサービスを実行するには、 Group Managed Service Account （ gMSA ；グループ管理サービスアカウント）を使用します	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。 gMSA 名を *domainName\accountName$* の形式で指定します。 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。

7. [Submit （送信）] をクリックします。

   「 * 事前確認をスキップ」チェックボックスを選択していない場合、プラグインのインストール要件をホストが満たしているかどうかが検証されます。ディスクスペース、 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は、対応するエラーまたは警告メッセージが表示されます。

   エラーがディスクスペースまたは RAM に関連している場合は、「 C ： \Program Files\NetApp\SnapCenter ' WebApp 」にある web.config ファイルを更新して、デフォルト値を変更できます。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 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。

1. インストールの進行状況を監視します。

PowerShell コマンドレットを使用して、複数のリモートホストに SnapCenter Plug-in for Microsoft Windows をインストールします

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 コマンドレットを使用します。

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 サーバ・ホストで 'Open-SmConnection' コマンドレットを使用してセッションを確立し ' 認証情報を入力します
3. 「 Add-SmHost 」コマンドレットと必要なパラメータを使用して、スタンドアロン・ホストまたはクラスタを SnapCenter に追加します。

   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"。

4. Install-SmHostPackage コマンドレットと必要なパラメータを使用して、複数のホストにプラグインをインストールします。

   プラグインを手動でインストールし ' 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 '-skipprecheck オプションを使用できます

コマンドラインから **SnapCenter Plug-in for Microsoft Windows** をサイレントにインストールします

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

- 必要なもの *
- Microsoft .NET Framework 4.5.2 以降がインストールされている必要があります。
- PowerShell 4.0 以降がインストールされている必要があります。
- Windows メッセージキューをオンにしておく必要があります。
- ホストのローカル管理者である必要があります。
- 手順 *

1. 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 サーバ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。

2. 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。
3. コマンドプロンプトで、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。
4. 変数を実際のデータに置き換えて、次のコマンドを入力します。

   「 snapcenter _windows_host_plugin.exe 」 /silent/debuglog 「 /log 」 by_SNAPCENTER_port=SUIT_INSTALLDIR="by_ServiceAccount=BI_SERVICEPWD=ISFeatureInstal

I=SCW`

例：

```
`"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 のインストール中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。

次の変数の値を入力します。

変数（ **Variable** ）	価値
	インストーラのログファイルの名前と場所を次のように指定します。 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。
BY_ServiceAccount の場合	SnapCenter Plug-in for Microsoft Windows の Web サービスアカウントを指定します。
BI_SERVVICEPWD	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 によってリモートホストに導入される解決策を指定します。

_debuglog_parameter 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方法としてこのログファイルに書き込むことを推奨します。

必要に応じて、 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確認できます。パッケージのログファイルは、 *%Temp_folder* に（最も古いものから）一覧表示されます（例： *_C ： \temp* ）。

Plug-in for Windows をインストールすると、 SnapCenter サーバではなくホストにプラグインが登録されます。SnapCenter サーバにプラグインを登録するには、 SnapCenter GUI または PowerShell コマンドレットを使用してホストを追加します。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を監視する

SnapCenter プラグインパッケージのインストールの進捗状況は、 Jobs ページで監視できます。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あるかどうかを確認できます。

- このタスクについて *

以下のアイコンがジョブページに表示され、操作の状態を示します。

- 実行中です
- 正常に完了しました
- 失敗しました
- 警告で終了したか、警告が原因で起動できませんでした
- キューに登録され
- 手順 *
  1. 左側のナビゲーションペインで、 **Monitor** 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だけが表示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 * （ Filter * ）] をクリック
     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、インストールステータスを選択します。
     e. [適用（ Apply ）] 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。

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。
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、*.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 sslcertipport=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 sslcertipport=0.0.0.0:_<SMCore Port>_certthash=$cert
appid="$GUID"
```

例：

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

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。

- 必要なもの *
- 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。
- 終了後 *

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。