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

SnapCenter Software 5.0

NetApp
October 15, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/snapcenter-50/protect-scw/concept_install_snapcenter_plug_in_for_microsoft_windows.html on October 15, 2025. Always check docs.netapp.com for the latest.

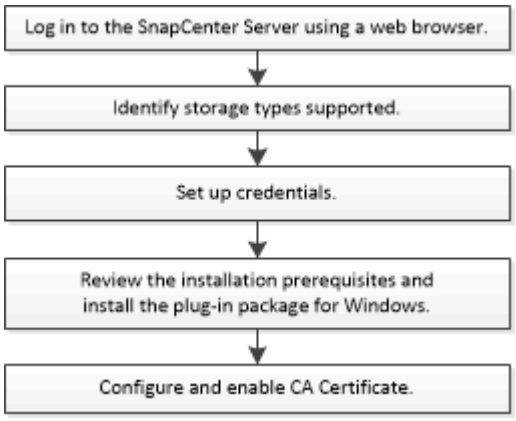
目次

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のクレデンシャルを設定する . . . 2
Windows Server 2012以降でのgMSAの設定 . . . 4
ホストを追加してSnapCenter Plug-in for Microsoft Windowsをインストールする . . . 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
プラグインに対してCA証明書を有効にする . . . 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ときに、組み込みでないクレデンシャルを指定した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、基本的なホストシステムのスペース要件とサイジング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の最新情報については、を参照して "NetApp Interoperability Matrix Tool" ください。
ホスト上のSnapCenterプラグイン用の最小RAM	1 GB
ホスト上のSnapCenterプラグインのインストールと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量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、最近実行した処理の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 4.7.2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 "NetApp Interoperability Matrix Tool" ください。 用。 NET固有のトラブルシューティング情報。を参照してください。 "インターネットに接続されていない従来型システムでは、SnapCenter のアップグレードまたはインストールが失敗します。"

Plug-in for Windowsのクレデンシャルを設定する

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 *
- プラグインをインストールする前に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、リモートホストに対する管理者権限（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 *

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. [Credential]ページで、次の手順を実行します。

フィールド	操作
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。ユーザ名フィールドの有効な形式は次のとおりです。 ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • 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次のとおりです。 `UserName` 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、必要に応じて[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を割り当てることができます。

Windows Server 2012以降でのgMSAの設定

Windows Server 2012以降では、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するグループ管理サービスアカウント（gMSA）を作成できます。

開始する前に

- 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. KDSルートキーを作成して、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. 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。
```

   例えば、

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
. . コマンドを実行し `Get-ADServiceAccount` 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で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。

   選択したプラグインがSnapCenterサーバにインストールされ、指定したgMSAがプラグインのインストール時にサービスのログオンアカウントとして使用されます。

ホストを追加して**SnapCenter Plug-in for Microsoft Windows**をインストールする

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。プラグインのインストールには、この方法を推奨します。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 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ときに、組み込みでないクレデンシャルを指定した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。
- 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
- メッセージキューサービスがrunning状態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 2012以降でのWindowsファイルシステム用のグループ管理サービスアカウントの設定"

タスクの内容

- 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
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
  - 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。

SnapCenterでは、すでにワークグループに属していて別のドメインに変更されたホスト（プラグインホスト）をSnapCenterに追加することはできません。その逆も同様です。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、 * 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]*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	操作
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。

フィールド	操作
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、Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）を入力することを推奨します。 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。
クレデンシャ	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、ホストタイプなどの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、[ホスト追加]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。

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。

   新規導入の場合は、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	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	デフォルトのパスはC：\Program Files\NetApp\SnapCenter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、デフォルトのパスをカスタマイズできます。
クラスタ内のすべてのホストを追加	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。
インストール前チェックをスキップ	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選択します。
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	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選択します。 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、プラグインをインストールするための要件を満たしているかどうかを確認するためにホストが検証されます。 ディスクスペース、RAM、PowerShellのバージョン、 ネットバージョンと場所は、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、該当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、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 `C:\Program Files\NetApp\SnapCenter` 。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。

8. 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、PowerShellコマンドレットを使用し `Install-SmHostPackage` 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、コマンドレットを使用してセッションを確立し `Open-SmConnection` 、クレデンシャルを入力します。
3. 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 `Add-SmHost` 。

   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. 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 `Install-SmHostPackage` ます。

   オプションは、プラグインを手動でインストールしたあとに、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に使用でき `-skipprecheck` 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 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。

開始する前に

- Microsoftがインストールされている必要があります。 Net 4.7.2以降。
- 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. 次のコマンドを入力し、変数をデータに置き換えます。

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

変数	値
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。
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 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時に実行されるプラグインの前提条件に関するチェックの結果が含まれているため、トラブルシューティング情報を取得するには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 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で、SnapCenterサーバ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

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発生していないかどうかを確認できます。

タスクの内容

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
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み

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. [* Monitor*] ページで、 [* Jobs] 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処理のみ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。
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**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"
   ```

プラグインに対して**CA**証明書を有効にする

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、 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. 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

[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、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。
- ** 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。