



## **SnapCenter**

カスタムプラグインをインストールする準備を  
します

SnapCenter Software 4.6

NetApp  
January 18, 2024

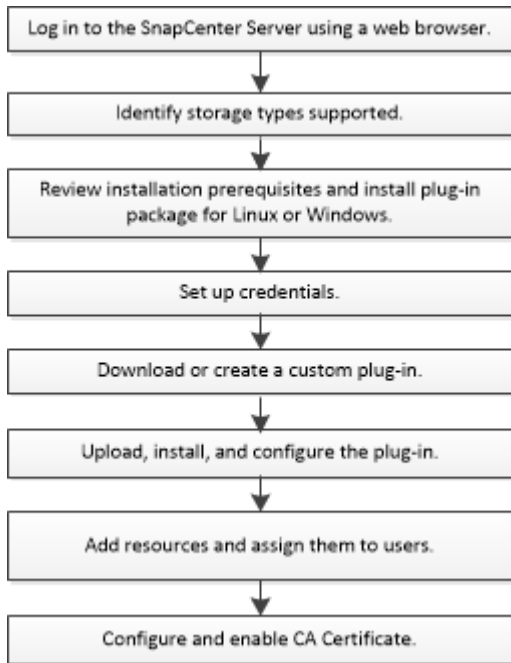
# 目次

SnapCenter カスタムプラグインをインストールする準備をします .....	1
SnapCenter Custom Plug-ins のインストールワークフロー .....	1
ホストを追加して SnapCenter Custom Plug-ins をインストールするための前提条件 .....	1
SnapCenter Plug-ins Package for Windows をインストールするホストの要件 .....	2
SnapCenter Plug-ins Package for Linux をインストールするためのホストの要件 .....	3
SnapCenter Custom Plug-ins のクレデンシャルを設定します .....	4
Windows Server 2012 以降で gMSA を構成します .....	6
SnapCenter Custom Plug-ins をインストールします .....	8
CA 証明書を設定します .....	15

# SnapCenter カスタムプラグインをインストールする準備をします

## SnapCenter Custom Plug-ins のインストールワークフロー

カスタムプラグインリソースを保護する場合は、SnapCenter Custom Plug-ins をインストールしてセットアップする必要があります。



"アプリケーション用のプラグインを開発します"

## ホストを追加して SnapCenter Custom Plug-ins をインストールするための前提条件

ホストを追加してプラグインパッケージをインストールする前に、すべての要件を満たしておく必要があります。Custom Plug-ins は、Windows と Linux のどちらの環境でも使用できます。

- カスタムプラグインを作成しておく必要があります。詳細については、開発者情報を参照してください。

"アプリケーション用のプラグインを開発します"

- MySQL または DB2 アプリケーションを管理する場合は、ネットアップが提供している MySQL および DB2 のカスタムプラグインをダウンロードしておく必要があります。
- Linux ホストまたは Windows ホストに Java 1.8 / 64 ビットをインストール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。

- カスタムプラグインが、ホストの追加処理を実行するクライアントホストにインストールされている必要があります。

## 全般

iSCSI を使用している場合は、iSCSI サービスが実行されている必要があります。

## Windows ホスト

- ローカル管理者権限を持つドメインユーザがあり、リモートホストに対してローカルログイン権限が付与されている必要があります。
- SnapCenter でクラスタノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限を持つユーザが必要です。

## Linux ホスト

- root ユーザまたは root 以外のユーザ用にパスワードベースの SSH 接続を有効にしておく必要があります。
- Linux ホストに Java 1.8 64 ビットがインストールされている必要があります。

SnapCenter Server ホストに Windows 2019 または Windows 2016 を使用している場合は、Java 1.8、64 ビットをインストールする必要があります。要件の最新情報については、Interoperability Matrix Tool (IMT) を参照してください。

"すべてのオペレーティングシステム用の Java のダウンロード"

"NetApp Interoperability Matrix Tool で確認できます"

- いくつかのパスにアクセスできるように root 以外のユーザに sudo 権限を設定する必要があります。visudo Linux ユーティリティを使用して、/etc/sudoers ファイルに次の行を追加します。例：

```
Cmnd_Alias SCCMD = /opt/NetApp/snapcenter/scc/bin/scc <non_root_user>  
ALL=(ALL) NOPASSWD:SETENV: SCCMD
```

non\_root\_user は、作成した root 以外のユーザの名前です。

## 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、 <a href="#">を参照してください "NetApp Interoperability Matrix Tool で確認できます"</a> 。
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  <div>  <p>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。</p> </div>
必要なソフトウェアパッケージ	<ul style="list-style-type: none"> <li>• Microsoft .NET Framework 4.5.2 以降</li> <li>• Windows Management Framework （ WMF ） 4.0 以降</li> <li>• PowerShell 4.0 以降</li> </ul> <p>サポートされているバージョンの最新情報については、<a href="#">を参照してください "NetApp Interoperability Matrix Tool で確認できます"</a>。</p>

## SnapCenter Plug-ins Package for Linux をインストールするためのホストの要件

SnapCenter Plug-ins Package for Linux をインストールする前に、ホストが要件を満たしていることを確認する必要があります。

項目	要件
オペレーティングシステム	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux の場合</li> <li>• Oracle Linux の場合</li> <li>• SUSE Linux Enterprise Server （ SLES ）</li> </ul>
ホスト上の SnapCenter プラグインの最小 RAM	1 GB

項目	要件
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	2 GB <div>  <p>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。</p> </div>
必要なソフトウェアパッケージ	Java 1.8 （64 ビット） Oracle Java または OpenJDK <p>Java を最新バージョンにアップグレードした場合は、/var/opt/snapcenter/etc/sp/etc/spl.properties にある JAVA_HOME オプションが正しい Java バージョンに設定されていること、および正しいパスが指定されていることを確認する必要があります。</p>

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"

## SnapCenter Custom Plug-ins 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、およびデータベースや 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 \*
- Linux ホスト

Linux ホストにプラグインをインストールするためのクレデンシャルを設定する必要があります。

プラグインプロセスをインストールして開始するための sudo 権限がある root ユーザまたは root 以外のユーザのクレデンシャルを設定する必要があります。

\* ベストプラクティス：\* ホストを導入してプラグインをインストールしたあとに Linux のクレデンシャルを作成することは可能ですが、SVM を追加したあとで、ホストを導入してプラグインをインストールする前にクレデンシャルを作成することを推奨します。

- Windows ホスト

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。

リモートホストに対する管理者権限を含む、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。

- Custom Plug-ins アプリケーション

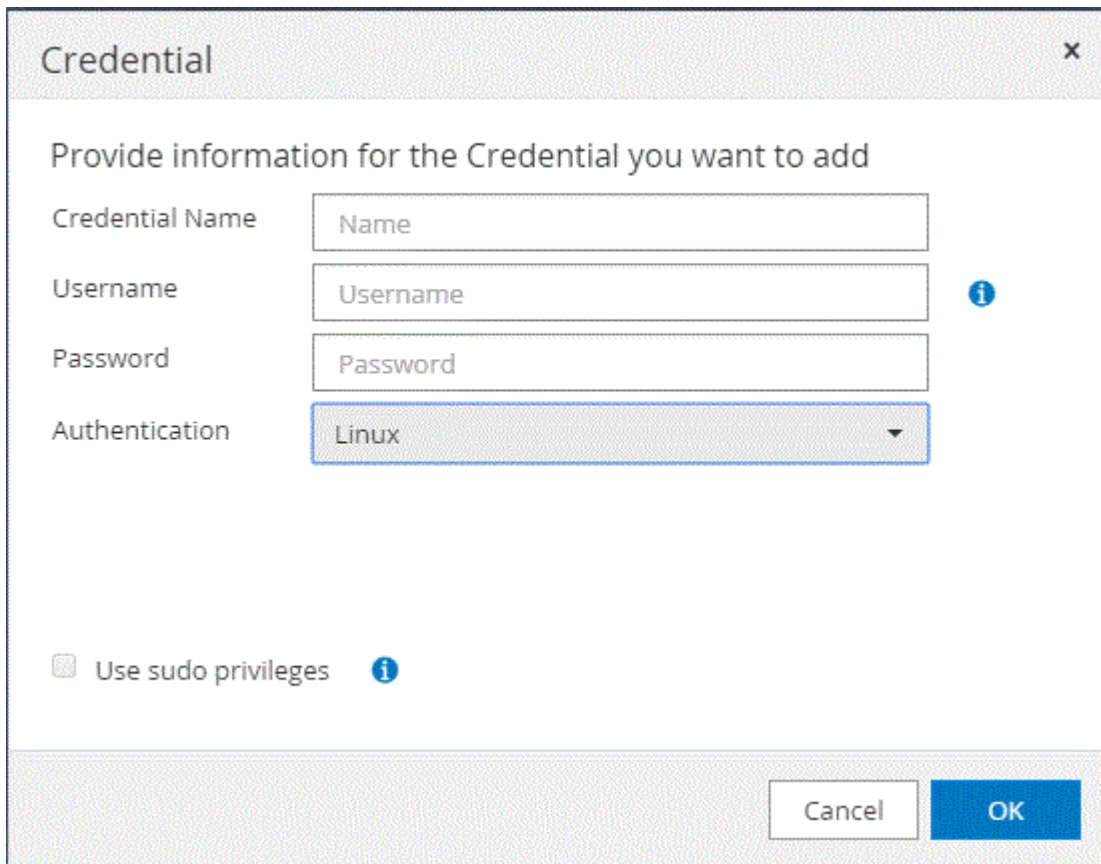
プラグインは、リソースの追加時に選択または作成されたクレデンシャルを使用します。データ保護処理中にクレデンシャルが不要なリソースの場合は、クレデンシャルを「\* なし」に設定できます。

- このタスクについて \*

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、ユーザ名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名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. [Credential] ページで、クレデンシャルの設定に必要な情報を指定します。

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。

フィールド	手順
ユーザ名	<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。Username 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>◦ _ドメイン FQDN\ ユーザ名_</li> </ul> <ul style="list-style-type: none"> <li>ローカル管理者（ワークグループのみ）</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。Username フィールドの有効な形式は、<i>username</i> 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。
認証モード	使用する認証モードを選択します。
sudo 権限を使用する	<p>root 以外のユーザのクレデンシャルを作成する場合は、「* sudo 権限を使用する *」チェックボックスをオンにします。</p> <div>  Linux ユーザのみに該当します。 </div>

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 -EffectivelyImmedient
  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.

- ホストを再起動します。
- 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
- 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>
  - 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。
  - 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。

## SnapCenter Custom Plug-ins をインストールします

ホストを追加し、プラグインパッケージをリモートホストにインストールする

ホストを追加するには、SnapCenterAdd Host ページを使用して、プラグインパッケージをインストールする必要があります。プラグインは、自動的にリモートホストにインストールされます。ホストの追加とプラグインパッケージのインストールは、個々のホストまたはクラスタに対して実行できます。

- 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。
- メッセージキューサービスが実行されていることを確認してください。
- 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。

"カスタムアプリケーション用に、 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。

クラスタ（WSFC）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プラグインがインストールされます。


- 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] タブ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、次の操作を実行します。



フィールド	手順
ホストタイプ	<p>ホストタイプを選択します。</p> <ul style="list-style-type: none"><li>• Windows の場合</li><li>• Linux の場合</li></ul> <div><p>カスタムプラグインは、Windows と Linux のどちらの環境でも使用できます。</p></div>
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 は、DNS の適切な設定によって異なります。そのため、FQDN を入力することを推奨します。</p> <p>Windows 環境の場合、信頼されていないドメインホストの IP アドレスは、FQDN に解決される場合にのみサポートされます。</p> <p>スタンドアロンホストの IP アドレスまたは FQDN を入力できます。</p> <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>

フィールド	手順
クレデンシャル	<p>作成したクレデンシャル名を選択するか、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>クレデンシャルの詳細を表示するには、指定したクレデンシャル名にカーソルを合わせます。</p> <div>  <p>クレデンシャル認証モードは、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。</p> </div>

5. [インストールするプラグインを選択してください\*] 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。
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	<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 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。</p> <div>  <p>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。</p> </div>

フィールド	手順
インストールパス	<p>カスタムプラグインは、Windows システムと Linux システムのどちらにもインストールできます。</p> <ul style="list-style-type: none"> <li>Windows 用 SnapCenter Plug-ins パッケージのデフォルトパスは C : \Program Files\NetApp\SnapManager です。</li> </ul> <p>必要に応じて、パスをカスタマイズできます。</p> <ul style="list-style-type: none"> <li>SnapCenter Plug-ins Package for Linux のデフォルトパスは /opt/NetApp/SnapCenter です。</li> </ul> <p>必要に応じて、パスをカスタマイズできます。</p> <ul style="list-style-type: none"> <li>SnapCenter Custom Plug-ins の場合： <ul style="list-style-type: none"> <li>i. Custom Plug-ins （カスタムプラグイン）セクションで * Browse （参照） * をクリックし、zip 形式のカスタムプラグインフォルダーを選択します。</li> </ul> <p>zip 形式のフォルダには、カスタムプラグインコードと DESCRIPTOR .xml ファイルが含まれています。</p> <p>Storage Plug-In の場合は、_C : \ProgramData\NetApp\SnapCenter \Package Repository_ に移動し、「Storage.zip」フォルダを選択します。</p> <li>ii. [ アップロード ] をクリックします。</li> </li></ul> <p>パッケージをアップロードする前に zip 形式のカスタムプラグインフォルダ内の記述子 .xml ファイルが検証されます。</p> <p>SnapCenter サーバにアップロードされたカスタムプラグインが表示されます。</p> <p>MySQL または DB2 アプリケーションを管理する場合は、ネットアップが提供している MySQL および DB2 のカスタムプラグインを使用できます。MySQL と DB2 のカスタムプラグインについては、を参照してください  <a href="#">"NetApp Automation Store の略"</a></p>

フィールド	手順
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	<p>Windows ホストの場合、プラグインサービスの実行にグループ管理サービスアカウント（gMSA）を使用する場合は、このチェックボックスをオンにします。</p> <div>  <p>gMSA 名を domainName\accountName\$ の形式で指定します。</p> </div> <div>  <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> </div>

## 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、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、場所（Windows プラグインの場合）、および Java のバージョン（Linux プラグインの場合）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\SnapManager WebApp にある web.config ファイルを更新してデフォルト値を変更することができます。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. ホストタイプが Linux の場合は、フィンガープリントを確認し、\* Confirm and Submit \* をクリックします。



同じホストを以前に SnapCenter に追加し、フィンガープリントを確認した場合でも、フィンガープリントの検証は必須です。

## 2. インストールの進行状況を監視します。

インストール固有のログファイルは、/custom\_location/snapcenter /logs にあります。

コマンドレットを使用して、複数のリモートホストに **Linux** または **Windows** 用の **SnapCenter** プラグインパッケージをインストールします

Install-SmHostPackage PowerShell コマンドレットを使用すると、複数のホストに Linux または Windows 向け SnapCenter プラグインパッケージを同時にインストールできます。

- 必要なもの \*

ホストを追加するユーザには、ホストに対する管理者権限が必要です。

- 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、クレデンシャルを入力します。
3. 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。

コマンドレットで利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](#)"。

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。

1. リモートインストールのクレデンシャルを入力します。

コマンドラインインターフェイスを使用して、**Linux** ホストに **SnapCenter** カスタムプラグインをインストールします

SnapCenter カスタムプラグインは、SnapCenter ユーザインターフェイス（UI）を使用してインストールする必要があります。環境内で SnapCenter UI からプラグインのリモートインストールが許可されていない場合は、カスタムプラグインをコンソールモードまたはサイレントモードでインストールできます。そのためには、コマンドラインインターフェイス（CLI）を使用します。

- 手順 \*

1. SnapCenter Plug-ins Package for Linux のインストールファイル（snapcenter linux\_host\_plugin.bin）を C : \ProgramData\NetApp\SnapCenter \Package Repository から、カスタムプラグインをインストールするホストにコピーします。

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. コマンドプロンプトで、インストールファイルをコピーしたディレクトリに移動します。
3. プラグインをインストールします。'path-to\_installation\_bin\_file/ snapcenter\_linux\_host\_plugin.bin -i silent -dport=port\_number\_for\_host-DSEVER\_IP=server\_name\_or\_IP\_address -DSEVER\_HTTPS\_port=port\_number\_for\_server

- -dport には、SMCore HTTPS 通信ポートを指定します。
- -DSERVER\_IP は、SnapCenter サーバの IP アドレスを指定します。
- -DSERVER\_HTTPS\_PORT には、SnapCenter サーバの HTTPS ポートを指定します。
- -duser\_install\_DIR - SnapCenter Plug-ins Package for Linux をインストールするディレクトリを指定します
- DINSTALL\_LOG\_name は、ログファイルの名前を指定します。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Add-Smhost コマンドレットと必要なパラメータを使用して、ホストを SnapCenter サーバに追加します。

コマンドで利用できるパラメータとその説明については、`RUNNING Get Help command_name _` を使用して参照できます。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"](#)。

5. SnapCenter にログインし、UI または PowerShell コマンドレットを使用してカスタムプラグインをアップロードします。

カスタムプラグインを UI からアップロードする方法については、を参照してください ["ホストを追加し、プラグインパッケージをリモートホストにインストールする"](#) セクション。

PowerShell コマンドレットの詳細については、SnapCenter のコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。






["SnapCenter ソフトウェアコマンドレットリファレンスガイド"](#)。

## カスタムプラグインのインストールの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。

- b. サンプルをコピーします。

## 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 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 sslcert ipport=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"
```

## Linux ホストで SnapCenter Custom Plug-ins サービスの CA 証明書を設定します

カスタムプラグインキーストアとその証明書のパスワードの管理、CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

カスタムプラグインでは、ファイル「keystore.JKS」を使用します。このファイルは、信頼ストアおよびキーストアとして `_/opt/NetApp/snapcenter / scc /etc/both` にあります。

カスタムプラグインのキーストアのパスワード、および使用中の **CA** 署名済みキーペアのエイリアスを管理します

• 手順 \*

1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

キー「keystore.pass」に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```

・  
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、キーストアに使用されているパスワードと同じパスワードに変更します。

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

*agent.properties* ファイル内のキー keystore.pass に対しても同じキーを更新します。

3. パスワードを変更したら、サービスを再起動してください。



カスタムプラグインキーストアのパスワード、および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が同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

• 手順 \*

1. カスタムプラグインキーストアを含むフォルダ（/opt/NetApp/snapcenter / scc など）に移動します
2. ファイル 'keystore.jks' を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .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 myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

・  
カスタムプラグインの信頼ストア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てください。



ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

## CA 署名キーペアをカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

### • 手順 \*

1. カスタムプラグインキーストア /opt/NetApp/snapcenter / scc などが含まれているフォルダに移動します
2. ファイル 'keystore.jkS' を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .jks
```

4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

```
keytool -importkeystore -srckeystore.root/ snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.JKS -deststoretype JKS `
```

5. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .jks
```

6. キーストアに、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含まれていることを確認します。
7. CA 証明書用に追加され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。

デフォルトのカスタムプラグインキーストアパスワードは、agent.properties ファイル内のキー keystore.pass の値です。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

・ 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 "long_alias_name" -destalias  
"simple_alias" -keystore keystore.jks
```

・ agent.properties ファイルの CA 証明書からエイリアス名を設定します。

この値をキー SCC\_CERTIFICATE\_ALIAS に更新します。

8. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

## SnapCenter Custom Plug-ins の証明書失効リスト（CRL）を設定します

### • このタスクについて \*

- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
  - SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、「`/opt/netapp/snapcenter /sscc /etc/crl`」です。
  - 手順 \*
1. `agent.properties` ファイルのデフォルトディレクトリを、キー `crl_path` に対して変更および更新できます。

このディレクトリに複数の CRL ファイルを配置できます。着信証明書は各 CRL に対して検証されます。

## Windows ホストで SnapCenter Custom Plug-ins サービスの CA 証明書を設定します

カスタムプラグインキーストアとその証明書のパスワードの管理、CA 証明書の設定、カスタムプラグインの信頼ストアへのルート証明書または中間証明書の設定、SnapCenter Custom Plug-ins の信頼ストアを使用したカスタムプラグインの信頼ストアへの CA 署名キーペアの設定、インストールされたデジタル証明書のアクティブ化が必要です。

カスタムプラグインは、`_C : \Program Files\NetApp\SnapManager\Snapcenter Plug-in Creator\etc_both`にある `file_keystore.JKS_` を信頼ストアおよびキーストアとして使用します。

カスタムプラグインのキーストアのパスワード、および使用中の **CA** 署名済みキーペアのエイリアスを管理します

- 手順 \*
1. カスタムプラグインキーストアのデフォルトパスワードは、カスタムプラグインエージェントのプロパティファイルから取得できます。

`key_keystore.pass_` に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.JKS
```



Windows のコマンドプロンプトで「`keytool`」コマンドが認識されない場合は、`keytool` コマンドを完全なパスに置き換えます。

```
C : \Program Files\Java<JDK_version>\bin\keytool .exe "-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、キーストアに使用されているパスワードと同じパスワードに変更します。

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.JKS
```

`agent.properties` ファイル内のキー `keystore.pass` に対しても同じキーを更新します。

1. パスワードを変更したら、サービスを再起動してください。



カスタムプラグインキーストアのパスワード、および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が同じである必要があります。

ルート証明書または中間証明書をカスタムプラグインの信頼ストアに設定します

カスタムプラグインの信頼ストアの秘密鍵を使用せずにルート証明書または中間証明書を設定する必要があります。

• 手順 \*

1. カスタムプラグインの keystore\_C : \Program Files\NetApp\Virtual \SnapCenter \Snapcenter Plug-in Creator\etc\備え ているフォルダに移動します
2. ファイル 'keystore.jks' を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .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 myRootCA -file/root/USERTrustRSA_Root.cer -keystore  
keystore.JKS
```

5. カスタムプラグインの信頼ストア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てください。



ルート CA 証明書、中間 CA 証明書の順に追加する必要があります。

**CA 署名キーペア**をカスタムプラグインの信頼ストアに設定します

CA 署名キーペアをカスタムプラグインの信頼ストアに設定する必要があります。

• 手順 \*

1. カスタムプラグインの keystore\_C : \Program Files\NetApp\Virtual \SnapCenter \Snapcenter Plug-in Creator\etc\備え ているフォルダに移動します
2. file\_keystore.JKS\_</Z1> を探します。
3. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .JKS
```

4. 秘密鍵と公開鍵の両方を含む CA 証明書を追加します。

```
keytool -importkeystore -srckeystore.root/ snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.JKS -deststoretype JKS
```

5. キーストアに追加された証明書を表示します。

```
keytool -list -v キーストア .JKS
```

6. キーストアに、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含まれていることを確認します。
7. CA 証明書用に追加され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。

デフォルトのカスタムプラグインキーストアパスワードは、agent.properties ファイル内のキー keystore.pass の値です。

```
keytool -keypasswd -alias "alias_name_in_ca_cert" -keystore keystore.JKS_
```

1. agent.properties ファイルの CA 証明書からエイリアス名を設定します。

この値をキー SCC\_CERTIFICATE\_ALIAS に更新します。

2. CA 署名済みキーペアをカスタムプラグインの信頼ストアに設定したら、サービスを再起動します。

## SnapCenter Custom Plug-ins の証明書失効リスト（CRL）を設定します

- このタスクについて \*
- 関連する CA 証明書の最新の CRL ファイルをダウンロードするには、を参照してください ["SnapCenter CA 証明書の証明書失効リストファイルを更新する方法"](#)。
- SnapCenter カスタムプラグインは、事前に設定されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter カスタムプラグインの CRL ファイルのデフォルトディレクトリは、'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl' です。
- 手順 \*
- 1. agent.properties ファイルのデフォルトディレクトリを、キー crl\_path に対して変更および更新できます。
- 2. このディレクトリに複数の CRL ファイルを配置できます。

着信証明書は各 CRL に対して検証されます。

## 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。





コマンドレットで利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。

## 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。