



SnapCenter Plug-in for SAP HANA Databaseのインストールの準備

SnapCenter Software 5.0

NetApp
July 18, 2024

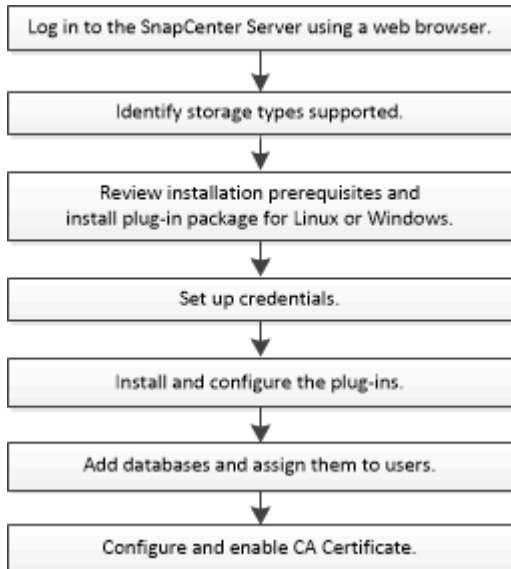
目次

| | |
|--|----|
| SnapCenter Plug-in for SAP HANA Databaseのインストールの準備 | 1 |
| SnapCenter Plug-in for SAP HANA Databaseのインストールワークフロー | 1 |
| ホストを追加して SnapCenter Plug-in for SAP HANA Database 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 | 3 |
| SnapCenter Plug-ins Package for Linuxをインストールするホストの要件 | 4 |
| SnapCenter Plug-in for SAP HANA Databaseのクレデンシャルを設定する | 5 |
| Windows Server 2012以降でのgMSAの設定 | 8 |
| SnapCenter Plug-in for SAP HANA Databasesのインストール | 9 |
| CA証明書の設定 | 15 |

SnapCenter Plug-in for SAP HANA Databaseのインストールの準備

SnapCenter Plug-in for SAP HANA Databaseのインストールワークフロー

SAP HANA データベースを保護する場合は、SnapCenter Plug-in for SAP HANA Database をインストールしてセットアップする必要があります。



ホストを追加して SnapCenter Plug-in for SAP HANA Database 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。SnapCenter Plug-in for SAP HANA Database は、Windows と Linux のどちらの環境でも使用できます。

- Java 1.8 (64ビット) をホストにインストールしておく必要があります。



IBM Javaはサポートされていません。

- SAP HANA データベースの対話型端末 (HDBSQL クライアント) をホストにインストールしておく必要があります。
- Windows の場合は、「LocalSystem」 Windows ユーザを使用してプラグインの Creator Service が実行されている必要があります。これは、Plug-in for SAP HANA Database がドメイン管理者としてインストールされている場合のデフォルトの動作です。
- Windowsの場合は、ユーザストアキーをシステムユーザとして作成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。

す。SnapCenter Plug-in for Microsoft Windows は、Windows ホストに SAP HANA プラグインを使用してデフォルトで導入されます。

- Linuxホストの場合、HDBのセキュアなユーザストアキーにはHDBSQL OSユーザとしてアクセスします。
- SnapCenter サーバが、Plug-in for SAP HANA Database ホストの 8145 ポートまたはカスタムポートにアクセスできる必要があります。

Windowsホスト

- リモートホストに対するローカルログイン権限を持つローカル管理者権限を持つドメインユーザが必要です。
- Plug-in for SAP HANA Database を Windows ホストにインストールする際に、SnapCenter Plug-in for Microsoft Windows が自動的にインストールされます。
- rootユーザまたはroot以外のユーザに対して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。
- Java 1.8 (64ビット) をWindowsホストにインストールしておく必要があります。

["すべてのオペレーティングシステム用のJavaダウンロード"](#)

["NetApp Interoperability Matrix Tool"](#)

Linuxホスト

- rootユーザまたはroot以外のユーザに対して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。
- Java 1.8 (64ビット) をLinuxホストにインストールしておく必要があります。

["すべてのオペレーティングシステム用のJavaダウンロード"](#)

["NetApp Interoperability Matrix Tool"](#)

- Linux ホストで実行されている SAP HANA データベースを Plug-in for SAP HANA Database のインストール時にインストールすると、SnapCenter Plug-in for UNIX 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、デフォルトのシェルとして `* bash *` が必要です。

補助コマンド

SnapCenter Plug-in for SAP HANAで補足コマンドを実行するには、ファイルにそのコマンドを含める必要があります `allowed_commands.config`。

`allowed_commands.config` ファイルは、SnapCenter Plug-in for SAP HANAディレクトリの「etc」サブディレクトリにあります。

Windowsホスト

デフォルト： `C:\Program Files\NetApp\SnapCenter\HANA\etc\allowed_commands.config`

カスタムパス：

`<Custom_Directory>\NetApp\SnapCenter\HANA\etc\allowed_commands.config` Windowsホスト：

Linuxホスト

デフォルト： /opt/NetApp/snapcenter/scc/etc/allowed_commands.config

カスタムパス： <Custom Directory>/NetApp/snapcenter/scc/etc/allowed_commands.config

プラグインホストで追加のコマンドを許可するには、エディタでファイルを開きます allowed_commands.config。各コマンドを別々の行に入力します。大文字と小文字は区別されません。例えば、

コマンド:mount

コマンド：umount

完全修飾パス名を指定してください。パス名にスペースが含まれている場合は、パス名を引用符 (") で囲みます。例えば、

コマンド："C:\Program Files\NetApp\SnapCreator commands\sdcli.exe"

コマンド：myscript.bat

ファイルが存在しない場合は allowed_commands.config、コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"

コマンドまたはスクリプトがに存在しないと、`allowed_commands.config` コマンドまたはスクリプトの実行がブロックされ、次のエラーでワークフローが失敗します。

"[/mnt/mount-a]の実行は許可されていません。プラグインホストのファイル%sにコマンドを追加して許可します。"



ワイルドカードエントリ (*) を使用してすべてのコマンドを許可しないでください。

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 |

| 項目 | 要件 |
|---------------------------------------|---|
| 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 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <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。</p> </div> |
| 必要なソフトウェアパッケージ | <ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2以降 • Windows Management Framework (WMF) 4.0以降 • PowerShell 4.0以降 <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 "NetApp Interoperability Matrix Tool" ください。</p> <p>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。"</p> |

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

SnapCenter Plug-ins Package for Linux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とサイジングの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 | <ul style="list-style-type: none"> • Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) <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 "NetApp Interoperability Matrix Tool" ください。</p> |
| ホスト上のSnapCenterプラグイン用の最小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とログの最小スペース | 2 GB <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <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、最近実行した処理の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.x (64ビット) Oracle Javaおよび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/spl/etc/spl.propertiesにあるJAVA_HOMEオプションが、正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。</p> <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 "NetApp Interoperability Matrix Tool" ください。</p> |

SnapCenter Plug-in for SAP HANA Database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。

タスクの内容

- Linuxホスト

Linuxホストにプラグインをインストールするには、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は、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo権限を持つroot以外のユーザに対して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、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し、ユーザ名に完全な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。

Credential

Provide information for the Credential you want to add

Credential Name

Username ⓘ

Password

Authentication

Use sudo privileges ⓘ

Cancel OK

4. [クレデンシャル] 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 | 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。 |

| フィールド | 操作 |
|-----------|--|
| 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"> 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 <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"> NETBIOS_USERNAME_ _ドメイン FQDN\ ユーザ名_ <ul style="list-style-type: none"> ローカル管理者（ワークグループのみ） <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> <p>パスワードに二重引用符 (") またはバックティク (') 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。</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 | <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> <p> Linuxユーザのみに適用されます。</p> |

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 -Effectivelmmediant
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` で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。

SnapCenter Plug-in for SAP HANA Databasesのインストール

ホストを追加してリモートホストにプラグインパッケージをインストールする

SnapCenterの[ホストを追加]ページを使用してホストを追加し、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。プラグインはリモートホストに自動的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、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する場合は、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。

- 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する必要があります。
- ホストの管理については、管理に関するドキュメントを参照してください。
- 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 SAP HANA 用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"


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。
- SAP HANA システムレプリケーションでプライマリシステムとセカンダリシステムの両方のリソースを検出する場合は、root ユーザまたは sudo ユーザを使用してプライマリシステムとセカンダリシステムの両方を追加することを推奨します。

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]*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>ホストのタイプを選択します。</p> <ul style="list-style-type: none"> • ウィンドウ • Linux <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Plug-in for SAP HANA はHDBSQLクライアントホストにインストールされます。このホストはWindowsシステムでもLinuxシステムでもかまいません。</p> </div> |
| ホスト名 | <p>通信ホスト名を入力します。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、FQDNを入力することを推奨します。</p> <p>HDBSQLクライアントとHDBUserStoreをこのホストに設定する必要があります。</p> |

| フィールド | 操作 |
|---------|---|
| クレデンシャル | <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。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>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、クレデンシャルの詳細を確認できます。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  クレデンシャルの認証モードは、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。 </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。

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。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 style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  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。 </div> |
| インストールパス | <p>Plug-in for SAP HANAはHDBSQLクライアントホストにインストールされます。このホストはWindowsシステムでもLinuxシステムでもかまいません。</p> <ul style="list-style-type: none"> • 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。必要に応じて、パスをカスタマイズできます。 • Linux 用 SnapCenter Plug-ins パッケージのデフォルトパスは /opt/NetApp/SnapCenter です。必要に応じて、パスをカスタマイズできます。 |
| インストール前チェックをスキップ | <p>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。</p> |

| フィールド | 操作 |
|--|---|
| 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 | <p>Windowsホストで、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domainName\accountName\$の形式で指定してください。</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せん。</p> |

7. [Submit (送信)] をクリックします。

[Skip prechecks]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ホストが満たしているかどうかを検証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、.NETのバージョン、場所 (Windowsプラグインの場合)、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、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、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。

8. 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。

クラスタセットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。



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。

9. 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た複数のリモートホストへのSnapCenter Plug-in Package for Linux / Windowsのインストール

PowerShellコマンドレットInstall-SmHostPackageを使用すると、複数のホストにSnapCenter Plug-in Package for Linux / Windowsを同時にインストールできます。

開始する前に

プラグインパッケージ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、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](#)"。

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。

4. 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 Plug-in for SAP HANA Databaseをインストールする

SnapCenter ユーザインターフェイス（UI）を使用して、SnapCenter Plug-in for SAP HANA Database をインストールする必要があります。環境で 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、コマンドラインインターフェイス（CLI）を使用して、Plug-in for SAP HANA Database 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。

開始する前に

- Plug-in for SAP HANA Databaseは、HDBSQLクライアントが配置されている各Linuxホストにインストールする必要があります。
- SnapCenter Plug-in for SAP HANA Database をインストールする Linux ホストは、依存するソフトウェア、データベース、オペレーティングシステムの要件を満たしている必要があります。

サポートされる構成の最新情報については、Interoperability Matrix Tool（IMT）を参照してください。

["NetApp Interoperability Matrix Tool"](#)

- SnapCenter Plug-in for SAP HANA Database は、SnapCenter Plug-ins Package for Linux の一部です。SnapCenter Plug-ins Package for Linuxをインストールする前に、SnapCenterをWindowsホストにインストールしておく必要があります。

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Plug-in for SAP HANA Database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 -DSERVER_IP=server_name_or_ip_address  
-DSERVER_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. 次のコマンドを入力して、=<installation directory>/NetApp/snapcenter /csc /etc/SC_SMS_Services.properties ファイルを編集し、plugins/enabled=hana : 3.0 パラメータを追加します。

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






コマンドで使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](#)"。

Plug-in for SAP HANA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
-  完了済み
-  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： \ocalmachine\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"
```

Linuxホスト上のSnapCenter SAP HANAプラグインサービスのCA証明書の設定

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キーストアのパスワードと使用中のCA署名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ます。



カスタムプラグインキーストアのパスワードと、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を同じにする必要があります。

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

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
keytool -list -v -keystore keystore.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ます。



ルートCA証明書のあとに中間CA証明書を追加する必要があります。

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

カスタムプラグインの信頼ストアにCA署名キーペア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/opt/NetApp/snapcenter/scc/etcが格納されているフォルダに移動します。
2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

```
keytool -list -v -keystore keystore.jks
```

6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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ファイルの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SCC_CERTIFICATE_ALIASキーに対して更新します。

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

SnapCenterカスタムプラグインの証明書失効リスト（CRL）を設定する

タスクの内容

- 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で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/scc/etc/crl」です。

手順

1. crl_pathキーに対して、agent.propertiesファイルのデフォルトディレクトリを変更および更新できます。

このディレクトリには、複数のCRLファイルを配置できます。受信証明書は、各CRLに対して検証されません。

Windowsホスト上のSnapCenter SAP HANAプラグインサービス用のCA証明書の設定

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キーストアのパスワードと使用中のCA署名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。

4. パスワードを変更したら、サービスを再起動します。



カスタムプラグインキーストアのパスワードと、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を同じにする必要があります。

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

ルート証明書または中間証明書は、カスタムプラグインの信頼ストアに秘密鍵なしで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. 「*keystore.jks*」ファイルを探します。
3. キーストアに追加された証明書を一覧表示します。

```
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ます。



ルートCA証明書のあとに中間CA証明書を追加する必要があります。

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

カスタムプラグインの信頼ストアにCA署名キーペア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. *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一覧表示します。

```
keytool -list -v キーストア .JKS
```

4. 秘密鍵と公開鍵の両方が設定された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一覧表示します。

```
keytool -list -v キーストア .JKS
```

6. 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キーストアに含まれていることを確認します。
7. CA証明書に追加し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ファイルのキー `keystore_pass` の値です。

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

8. 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 `SCC_CERTIFICATE_ALIAS` キーに対して更新します。
9. カスタムプラグインの信頼ストアにCA署名キーペアを設定したら、サービスを再起動します。

SnapCenterカスタムプラグインの証明書失効リスト (CRL) を設定する

タスクの内容

- 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で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せん。
2. このディレクトリには、複数のCRLファイルを配置できます。

受信証明書は、各CRLに対して検証されます。

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 © 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。