SnapCenter Plug-in for SAP HANA Database をインストールする準備をします

SnapCenter Software 4.8

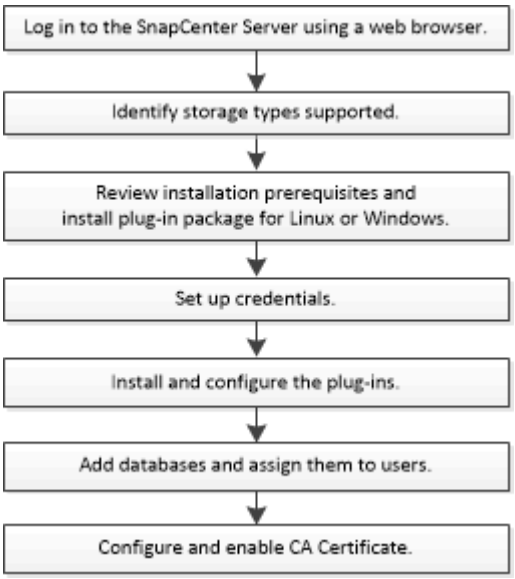
NetApp
January 18, 2024

目次

SnapCenter Plug-in for SAP HANA Database をインストールする準備をします

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。

- 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。

  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 SYSTEM 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 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 ホストの場合は、 HDB Secure User Store キーに 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

- 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。
- 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。
- Windows 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。

  "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"

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。

  "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"

- 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。

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"。

項目	要件
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 4.7.2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、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

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、ホストシステムの基本的なスペース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	• Red Hat Enterprise Linux の場合 • SUSE Linux Enterprise Server （ SLES ） 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

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 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	Java 1.8.x （ 64 ビット）の Oracle Java と OpenJDK のバージョン 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。 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 Plug-in for SAP HANA Database 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。

- このタスクについて *
- 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

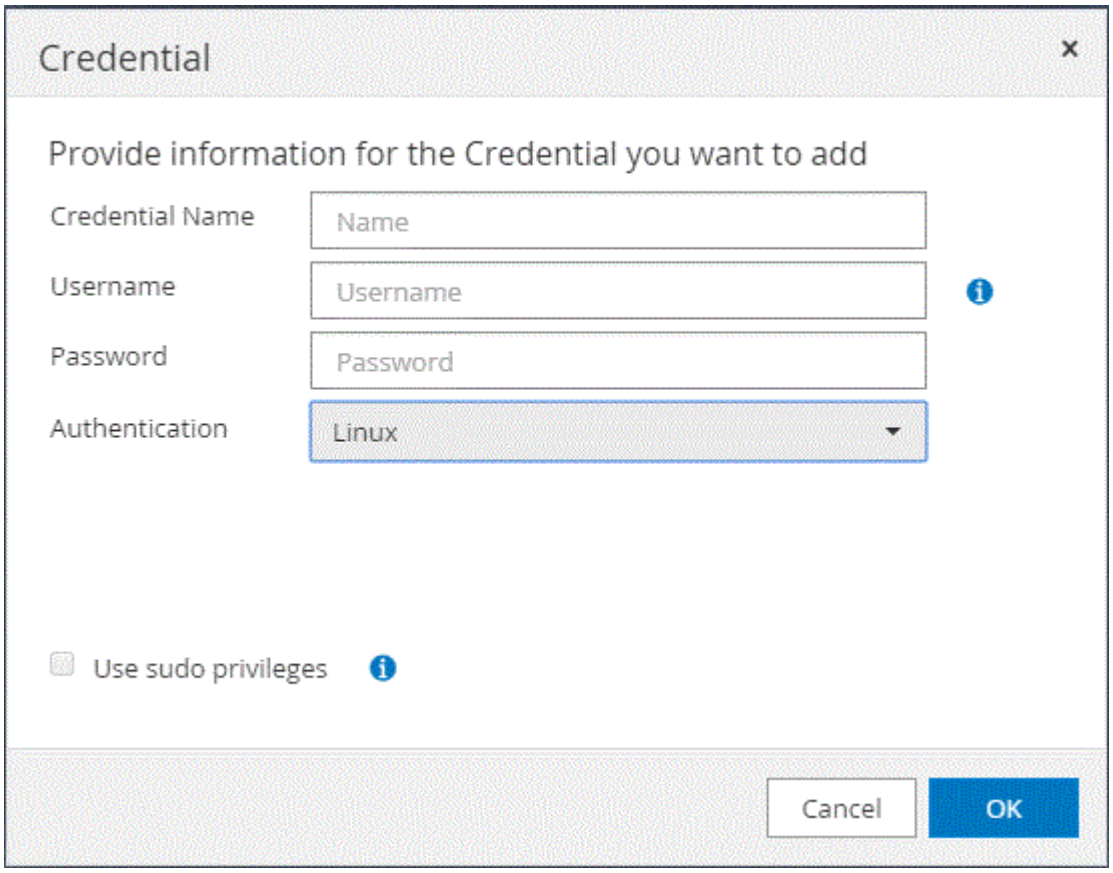
プラグインのインストール前に Windows クレデンシャルをセットアップする必要があります。

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。

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	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 _ • 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。
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	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。 Linux ユーザのみに該当します。

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,…>
. . を実行します `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。

      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>`

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。

SnapCenter Plug-in for SAP HANA Databases 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

ホストの追加ページを使用 SnapCenter 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、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。
- 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。

- 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。
- 管理マニュアルには、ホストの管理に関する情報が記載されています。
- 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 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"

- 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。
- 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には、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（ 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	ホストのタイプを選択します。 • Windows の場合 • Linux の場合 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。
ホスト名	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。 HDBSQL クライアントと HDBUserStore をこのホスト上に設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名を選択するか、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。 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。 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。

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。
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	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。 • 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。

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	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。 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する] 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。

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。

1. 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 *

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。

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 Plug-in for SAP HANA Database** をインストールします

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。

- 必要なもの *
- HDBSQL クライアントが配置された各 Linux ホストに Plug-in for SAP HANA Database を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 で確認できます"

- 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、 Windows ホストに SnapCenter がインストールされている必要があります。
- 手順 *

1. Linux インストールファイル（ snapcenter _ linux_host_plugin.bin ）の SnapCenter Plug-ins パッケージを C ： \ProgramData\NetApp\SnapCenter \Package リポジトリから、 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
```

1. 次のコマンドを入力して、 =<installation directory>/NetApp/snapcenter /cscc /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。
2. 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 のインストールのステータスを監視します

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、証明書を調達する前に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、および*.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 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>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_
certhash=$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 ホストで SnapCenter SAP HANA 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を管理し、CA証明書を設定し、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、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ために、SnapCenterカスタムプラグインサービスを使用して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。

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が格納されているフォルダ（/opt/NetApp/snapcenter/scc/etc）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 -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 -keystore keystore.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 -keystore keystore.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 SAP HANA 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を管理し、CA証明書を設定し、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、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ために、SnapCenterカスタムプラグインサービスを使用して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。

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keystore_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_が格納さ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. 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。

著作権に関する情報

商標に関する情報