



SnapCenter Plug-in for MySQLのインストールの準備

SnapCenter software

NetApp
January 09, 2026

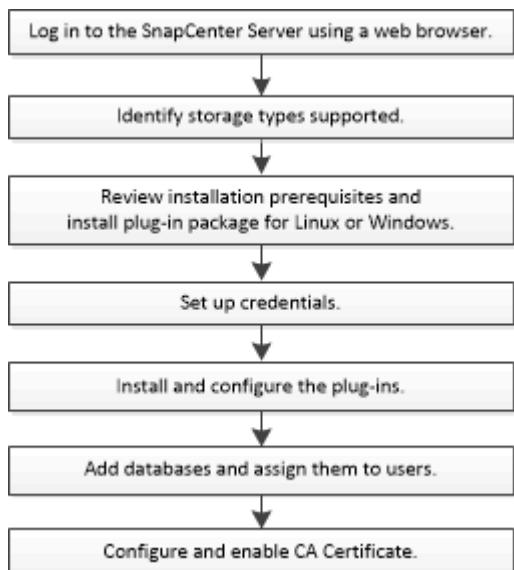
目次

SnapCenter Plug-in for MySQLのインストールの準備	1
SnapCenter Plug-in for MySQL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 MySQLをインストールするための前提条件	1
Windowsホスト	2
Linuxホスト	2
補助コマンド	2
Linuxホストのroot以外のユーザに対するsudo Privilegesの設定	3
SnapCenter Plug-ins Package for Windowsをインストールするホストの要件	5
SnapCenter Plug-ins Package for Linuxをインストールするホストの要件	5
SnapCenter Plug-in for MySQLのクレデンシャルを設定	6
SnapCenter Plug-in for MySQLのインストール	9
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	9
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	12
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 MySQLをインストールする	12
Plug-in for MySQLのインストールステータスの監視	13
CA証明書の設定	14
CA証明書CSRファイルの生成	14
CA証明書のインポート	15
CA証明書サムプリントの取得	16
WindowsホストプラグインサービスでのCA証明書の設定	16
LinuxホストでのSnapCenter MySQLプラグインサービス用のCA証明書の設定	17
Windowsホスト上のSnapCenter MySQLプラグインサービス用のCA証明書の設定	19
プラグインに対してCA証明書を有効にする	22

SnapCenter Plug-in for MySQLのインストールの準備

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

MySQLデータベースを保護する場合は、SnapCenter Plug-in for MySQL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 MySQL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 MySQLは、WindowsとLinuxの両方の環境で使用できます。

- Java 11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 Windows および Linux ホストではサポートされていません。

- Windowsの場合、Plug-in CreatorサービスはWindowsユーザ「LocalSystem」を使用して実行する必要があります。これは、Plug-in for MySQL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 Plug-in for Microsoft Windowsは、WindowsホストへのMySQLプラグインと一緒にデフォルトで導入されます。
- SnapCenterサーバがPlug-in for MySQL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。
- MySQL 5.7の場合は、MySQLの設定ファイル（my.cnfまたはmysql-server.cnf）にbinlogを指定する必要があります。

あります。

- MySQL 8.0より前のバージョンをご利用の場合は、MySQLXプラグインを手動でインストールして有効化する必要があります。MySQL 8.0以降では、MySQLXプラグインはデフォルトでインストールされ、有効化されています。

Windowsホスト

- ローカル管理者Privilegesを持つドメインユーザと、リモートホストに対するローカルログイン権限が必要です。
- Plug-in for MySQLをWindowsホストにインストールすると、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 11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をダウンロード"](#)

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 11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をダウンロード"](#)

- LinuxホストでMySQLデータベースを実行している場合は、Plug-in for MySQLのインストール時に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 MySQLで補足コマンドを実行するには、_allowed_commands.config_fileに追加する必要があります。

- Windowsホストのデフォルトの場所：C:\Program NetApp SnapCenter SnapCenter Plug-in Creator\etc\allowed_commands.config
- Linuxホストのデフォルトの場所：/opt/linux/scc/etc/allowed_commands.config NetApp SnapCenter

プラグインホストで追加コマンドを許可するには、エディタでopen_allowed_commands.config_fileを指定します。各コマンドは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。完全修飾パス名を指定し、パス名にスペースが含まれている場合は引用符 ("") で囲みます。

例：

コマンド：mountコマンド：umountコマンド：「C:\Program Files\SnapCreator NetApp Commands\sdcli.exe」コマンド：myscript.bat

_allowed_commands.config_fileが存在しない場合、コマンドまたはスクリプトの実行はブロックされ、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`_allowed_commands.config_`に存在しない場合、コマンドまたはスクリプトの実行はブロックされ、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。

Linuxホストのroot以外のユーザに対するsudo Privilegesの設定

SnapCenterでは、root以外のユーザがSnapCenter Plug-ins Package for Linuxをインストールしてプラグインプロセスを開始できます。プラグインプロセスをroot以外の有効なユーザとして実行します。複数のパスにアクセスできるようにroot以外のユーザにsudo Privilegesを設定する必要があります。

- ・必要なもの *
- ・sudoバージョン1.8.7以降
- ・umaskが0027の場合は、Javaフォルダとその中のすべてのファイルのアクセス許可が555であることを確認します。そうしないと、プラグインのインストールが失敗することがあります。
- ・root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- ・`/etc/ssh/sshd_config_file`を編集して、メッセージ認証コードアルゴリズム MACs HMAC-sha2-256 および MACs HMAC-sha2-512を設定します。

構成ファイルの更新後にsshdサービスを再起動します。

例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

- ・このタスクについて *

次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。

- /home/linux_user/.sc_netapp / snapcenter_linux_host_plugin.bin
- /custom_location /NetApp/snapcenter/spl/installation/plugins/uninstall
- /custom_location /NetApp/snapcenter/spl/bin/spl
- 手順 *

1. SnapCenter Plug-ins Package for LinuxをインストールするLinuxホストにログインします。
2. 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。

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
$LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl,
/opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
$LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
$LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: $LINUX_USER env_keep += "IATEMPDIR"
Defaults: $LINUX_USER env_keep += "JAVA_HOME"
Defaults: $LINUX_USER !visiblepw
Defaults: $LINUX_USER !requiretty
```



RACセットアップを実行している場合は、他の許可されているコマンドとともに、/etc/sudoersファイルに次のように追加します。'/RAC/bin/olsnodes'<crs_home>

_crs_home_fileの値は、/etc/oracle/olr.loc_fileから取得できます。

_linux_user_は、作成したroot以外のユーザの名前です。

_checksum_value_は、次の場所にある* sc_unix_plugins_checksum.txt *ファイルから取得できます。

- _C : \ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt (SnapCenter ServerがWindowsホストにインストールされている場合)。
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ LinuxホストにSnapCenterサーバがインストールされている場合。

この例は、独自のデータを作成するための参照としてのみ使用してください。

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に関する最新情報については、 "NetApp Interoperability Matrix Tool" 。
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
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	5GB  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	<ul style="list-style-type: none">ASP.NET Core Runtime 8.0.12（およびそれ以降のすべての8.0.xパッチ）Hosting BundlePowerShell Core 7.4.2 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。"

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に関する最新情報については、 "NetApp Interoperability Matrix Tool"。</p>
ホスト上のSnapCenterプラグイン用の最小RAM	1GB
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	<p>2GB</p> <p></p> <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>
必要なソフトウェアパッケージ	<p>Java 11 Oracle JavaおよびOpenJDK</p> <p>を最新バージョンにアップグレードした場合は、/var/opt/java/spl/etc/spl.propertiesにあるJAVA_HOMEオプションが正しいSnapCenter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>

SnapCenter Plug-in for MySQLのクレデンシャルを設定

SnapCenterでは、クレデンシャルを使用してSnapCenter処理のユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースまたは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クレデンシャルをそれぞれ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 Privilegesがある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。
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 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。</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。

SnapCenter Plug-in for MySQL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。ホストを追加して、個々のホスト用のプラグインパッケージをインストールできます。

開始する前に

- SnapCenter ServerホストのオペレーティングシステムがWindows 2019で、プラグインホストのオペレーティングシステムがWindows 2022の場合は、次の手順を実行する必要があります。
 - Windows Server 2019 (OSビルド17763.5936) 以降にアップグレードする
 - Windows Server 2022 (OSビルド20348.2402) 以降にアップグレードする
- 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。
- 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。

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。

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 <p> Plug-in for MySQLをMySQLデータベースサーバにインストールする必要があります。</p>

フィールド	操作
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が適切に設定されているかどうか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。
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="display: flex; align-items: center;"> 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。

REST APIを使用してPlug-in for MySQLをインストールする場合は、バージョンを3.0として渡す必要があります。例：mysql : 3.0

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="display: flex; align-items: center;"> 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>

フィールド	操作
インストールパス	<p>Plug-in for MySQLはMySQL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	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。
クラスタ内すべてのホストを追加	該当なし。
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	該当なし。

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 に関する場合は、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する場合は、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。

- Windows プラグインの場合、インストールログとアップグレードログは _C:\Windows\SnapCenter <JOBID> にあります。
- Linux プラグインの場合、インストールログは _/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install_Install_Linux.log <JOBID> にあり、アップグレードログは _/var/opt/snapcenter/logs/SnapCenter <JOBID>.log_ にあります。

終了後

SnapCenter 6.0 にアップグレードする場合は、既存の Perl ベースの Plug-in for MySQL がリモート プラグイン サーバからアンインストールされます。

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に対するローカル管理者権限を持つドメイン ユーザとして SnapCenter にログインしておく必要があります。

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 MySQL 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 MySQL Database をインストールする必要があります。ご使用の環境で SnapCenter UI からの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、コンソール モードまたはサイレント モードで Plug-in for MySQL Database をインストールできます。

開始する前に

- Plug-in for MySQL Database は、MySQL インスタンスを保護する必要がある各 Linux ホストにインストールする必要があります。

- SnapCenter Plug-in for MySQL 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、および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。

その "Interoperability Matrix Tool (IMT)" サポートされている構成に関する最新情報が含まれています。

- SnapCenter Plug-in for MySQL Databaseは、SnapCenter Plug-ins Package for Linuxに含まれています。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 MySQL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. /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties ファイルを編集し、plugins_enabled=mysql : 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 MySQL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きます。
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ビ化するには、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ホストでのSnapCenter MySQLプラグインサービス用のCA証明書の設定

インストールされたデジタル証明書をアクティビ化するには、SnapCenter プラグインサービスを使用して、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 証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、*/opt/NetApp/snapcenter/scc/etc* にあるファイル「keystore.jks」を使用します。

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する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

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。



プラグインキーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは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プラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグインキーストアが格納されているフォルダー (/opt/NetApp/snapcenter/scc/etc) 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  
.  
ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、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。

CA署名キーペアをプラグイン信頼ストアに設定する

CA署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグインキーストア /opt/NetApp/snapcenter/scc/etc が含まれるフォルダーに移動します。
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  
. 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. CA署名キーペアをプラグイントラストストアに設定した後、サービスを再起動します。

プラグインの証明書失効リスト (CRL) を構成する

タスクの内容

- SnapCenter プラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- SnapCenter 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す。

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

インストールされたデジタル証明書をアクティビ化するには、SnapCenter プラグインサービスを使用して、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 証明書を構成し、プラグイントラストストアにルート証明書または中間証明書を構成し、プラグイントラストストアに CA 署名キーペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc にあるファイル keystore.jks を使用します。

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する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

`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。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは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プラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_` 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. ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、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。

CA署名キーペアをプラグイン信頼ストアに設定する

CA署名キーペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_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. CA署名キーペアをプラグイントラストストアに設定した後、サービスを再起動します。

SnapCenterプラグインの証明書失効リスト(CRL)を構成する

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プラグインは、事前に構成されたディレクトリ内のCRLファイルを検索します。
- SnapCenter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 © 2026 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隨時、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 5225.227-19（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。