



# **SnapCenter Plug-in for**

## **MySQLのインストール準備**

### **SnapCenter software**

NetApp  
November 06, 2025

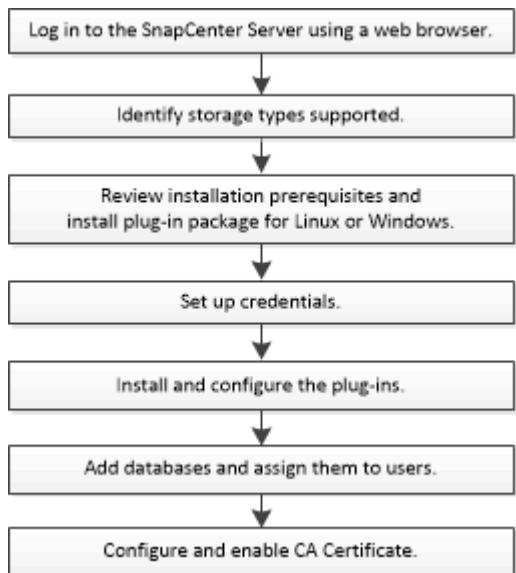
# 目次

SnapCenter Plug-in for MySQLのインストール準備	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以外のユーザへのsudo権限の設定	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のクレデンシャルの設定	6
SnapCenter Plug-in for MySQLのインストール	9
ホストの追加とリモート ホストへのプラグイン パッケージのインストール	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-ins 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たLinuxホストへのSnapCenter Plug-in for MySQLのインストール	12
Plug-in for MySQLのインストール ステータスの監視	14
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証明書の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 Plug-insサービスのCA証明書の設定	17
WindowsホストでのSnapCenter MySQLプラグイン サービスのCA証明書の設定	19
プラグインのCA証明書の有効化	22

# SnapCenter Plug-in for MySQLのインストール準備

## 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どちらの環境でも使用できます。

- 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、プラグイン クリエーター サービスは、"LocalSystem` Windows ユーザー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際、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。WindowsホストにMySQLプラグインをインストールすると、SnapCenter Plug-in for Microsoft Windowsもデフォルトで導入されます。
- SnapCenter Server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。

## Windowsホスト

- ローカル管理者権限があり、リモート ホストに対してローカル ログインのアクセス許可があるドメイン ユーザが必要です。
- 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"](#)

["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 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"](#)

["NetApp Interoperability Matrix Tool"](#)

- 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** を使用する必要があります。

## 補助コマンド

SnapCenter プラグイン for MySQL で補足コマンドを実行するには、そのコマンドを *allowed\_commands.config* ファイルに含める必要があります。

- Windows ホスト上のデフォルトの場所: C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed\_commands.config
- Linux ホスト上のデフォルトの場所: /opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config

プラグイン ホストで補足コマンドを許可するには、エディターで *allowed\_commands.config* ファイルを開きます。各コマンドを別々の行に入力します。コマンドでは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 ("") で囲んでください。

例えば：

コマンド: mount コマンド: umount コマンド: "C:\Program Files\ NetApp\ SnapCreator commands\sdcli.exe" コマンド: myscript.bat

*allowed\_commands.config* ファイルが存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワ

ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host.」

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、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host.」



すべてのコマンドを許可するには、ワイルドカード エントリ (\*) を使用しないでください。

## Linuxホストのroot以外のユーザへのsudo権限の設定

SnapCenter、非ルート ユーザーが Linux 用のSnapCenterプラグイン パッケージをインストールし、プラグインプロセスを開始できます。プラグイン プロセスは有効なroot以外のユーザとして実行されます。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。

### 必要なもの

- sudoバージョン1.8.7以降
- umask が 0027 の場合、java フォルダーとその中のすべてのファイルに 555 の権限が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可能性があります。
- 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* ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

この構成ファイルを更新したら、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/Config  
_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 をセットアップしている場合は、他の許可されたコマンドとともに、/etc/sudoers ファイルに次の行を追加する必要があります: '/<crs\_home>/bin/olsnodes'

*crs\_home* の値は、/etc/oracle/olr.loc ファイルから取得できます。

*LINUX\_USER* は、作成した非 root ユーザーの名前です。

*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\_ SnapCenter Server が Linux ホストに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際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、ホスト システムのスペースとサイジングに関する基本的な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、 <a href="#">"NetApp Interoperability Matrix Tool"</a> 。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要な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、ログ 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は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	<ul style="list-style-type: none"><li>ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル</li><li>PowerShell Core 7.4.2</li></ul> 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、 <a href="#">"NetApp Interoperability Matrix Tool"</a> 。

## 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、ホスト システムのスペースとサイジングに関する基本的な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"> <li>Red Hat Enterprise Linux</li> <li>SUSE Linux Enterprise Server (SLES)</li> </ul> <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、 "<a href="#">NetApp Interoperability Matrix Tool</a>"。</p>
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	<p>2 GB</p> <p></p> <p>十分なディスク スペースを割り当て、ログ 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は、最近実行した処理のログが作成されません。</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>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に関する最新情報については、 "<a href="#">NetApp Interoperability Matrix Tool</a>"。</p>

## SnapCenter Plug-in for MySQLのクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの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使用するクレデンシャルと、データベースやWindowsファイルシステムでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

### タスク概要

- 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権限があるroot以外のユーザに対して設定します。

**ベスト プラクティス:** ホストをデプロイしてプラグインをインストールした後でも Linux の認証情報を作成できますが、ベスト プラクティスとしては、SVM を追加した後、ホストをデプロイしてプラグインをインストールする前に認証情報を作成します。

- 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する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、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\*をクリックします。
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	操作
資格情報名	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"> <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。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"> <li>NetBIOS\ユーザー名</li> <li>ドメインFQDN\ユーザー名</li> </ul> <ul style="list-style-type: none"> <li>ローカル管理者（ワークグループの場合のみ）</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。ユーザー名フィールドの有効な形式は次のとおりです: <i>UserName</i></p> <p>パスワードには二重引用符 ("") やバッククオート (`) を使用しないでください。未満記号 (&lt;) と感嘆符 (!) を組み合わせて使用したりしないでください。たとえば、less than&lt;!10 、less than10&lt;!、バックティック`12 などです。</p>
パスワード	認証に使用するパスワードを入力します。
Authentication Mode	使用する認証モードを選択します。
Use sudo privileges	<p>非 root ユーザーの資格情報を作成する場合は、[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ユーザのみに該当します。</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]ページでユーザやユーザ 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

## ホストの追加とリモート ホストへのプラグイン パッケージのインストール

SnapCenterの[Add Host]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、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、ホストごとに実行できます。

### 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
- この処理は、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実行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際、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 サービスが実行中であ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。

### タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Server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、[ホスト] をクリックします。
2. 上部の\*管理対象ホスト\*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"><li>• Windows</li><li>• Linux</li></ul> <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が機能するためには、DNSが適切に設定されている必要があります。そのため、FQDNを入力することを推奨します。
Credentials	<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;"> <span style="font-size: 2em; margin-right: 10px;">i</span> <p>クレデンシャルの認証モードは、[Add Host] 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。</p> </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 Server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;"> <span style="font-size: 2em; margin-right: 10px;">i</span> <p>プラグインを手動でインストールしてカスタム 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、処理が失敗します。</p> </div>

フィールド	操作
Installation Path	<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"> <li>Windows 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは C:\Program Files\ NetApp\ SnapCenterです。必要に応じて、パスをカスタマイズできます。</li> <li>Linux 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは /opt/ NetApp/snapcenter です。必要に応じて、パスをカスタマイズできます。</li> </ul>
Skip preinstall checks	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オンにします。
クラスター内のすべてのホストを追加する	該当なし
Use group Managed Service Account (gMSA) to run the plug-in services	該当なし

#### 7. \*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、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\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のセットアップで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、[確認して送信] 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。



前述の手順で同じホストがSnapCenterに追加され、フィンガープリントが確認された場合でも、フィンガープリントの検証は必須です。

#### 9. インストールの進捗状況を監視します。

- Windows プラグインの場合、インストールおよびアップグレード ログは次の場所にあります:

C:\Windows\ SnapCenter plugin\Install<JOBID>\\_

- Linux プラグインの場合、インストール ログは次の場所にあります:

/var/opt/snapcenter/logs/SnapCenter\_Linux\_Host\_Plug-in\_Install<JOBID>.log\_、アップグレード ログ  
は次の場所にあります: /var/opt/snapcenter/logs/SnapCenter\_Linux\_Host\_Plug-  
in\_Upgrade<JOBID>.log\_

#### 終了後の操作

SnapCenter 6.0バージョンにアップグレードすると、既存のPerlベースのPlug-in for MySQLはリモート 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-ins Package for Linux / Windowsのインストール

Install-SmHostPackage PowerShellコマンドレットを使用すると、複数のホストにSnapCenter Plug-ins 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 Server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関する情報は、*Get-Help command\_name* を実行すると取得できます。あるいは、"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、-skipcheck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たLinuxホストへのSnapCenter Plug-in for MySQLのインストール

SnapCenter Plug-in for MySQL Database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。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環境では、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Linuxホストごと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、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に関する最新の情報については、Interoperability Matrix Tool (IMT) を参照してください。

#### "NetApp Interoperability Matrix Tool"

- SnapCenter Plug-in for 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 Server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 プロンプトから、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 は SMCore HTTPS 通信ポートを指定します。
- -DSERVER\_IP は、SnapCenter Server の IP アドレスを指定します。
- -DSERVER\_HTTPS\_PORT は、SnapCenter Server の HTTPS ポートを指定します。
- -DUSER\_INSTALL\_DIR は、Linux 用のSnapCenterプラグイン パッケージ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. /<インストール ディレクトリ>/ 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 Server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関する情報は、*Get-Help command\_name* を実行すると取得できます。あるいは、"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

[Jobs]ページを使用して、SnapCenterプラグインパッケージのインストールの進捗状況を監視できます。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。

### タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録

### 手順

- 左側のナビゲーションペインで、[モニター]をクリックします。
- \*モニター\*ページで、\*ジョブ\*をクリックします。
- ジョブページで、プラグインのインストール操作のみがリスト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。
  - \*フィルター\*をクリックします。
  - オプション：開始日と終了日を指定します。
  - [タイプ]ドロップダウンメニューから、[プラグインのインストール]を選択します。
  - [Status]ドロップダウンメニューから、インストールのステータスを選択します。
  - \*適用\*をクリックします。
- 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。
- \*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、生成したCSRを使用して認証局 (CA) から取得した証明書をインポートできます。証明書には秘密キー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証明書のRSAキーの長さは最低3072ビットである必要があります。

CSRを生成するための情報については、["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は、CA 証明書 CSR ファイルの生成をスキップできます。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）と、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。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。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 Server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] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] 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 コンピューター > 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] > [インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*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、[次へ] 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。



インポートする証明書は秘密キーと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 です)。

7. 「個人用」 フォルダに対して手順5を繰り返します。

## CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための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て、「拇印」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、拇印が「a9 09 50 2d d8 2a e4 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」になります。

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 -Path 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 Serverと、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、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore Port>
```

例えば：

```
> 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"
```

例えば：

```
> $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 Plug-insサービスの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キー
エンtries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* ファイルのキー KEYSTORE\_PASS も同様に更新します。

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含まれるフォルダーに移動します: /opt/NetApp/snapcenter/scc/etc。
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の一覧を表示します。

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

4. ルート証明書か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証明書を追加してから、中間CA証明書を追加する必要があります。

## プラグイン信頼ストアにCA署名キーペアを構成する

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の一覧を表示します。

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

4. 秘密キーと公開キー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の一覧を表示します。

```
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

認めます。

## 7. CA証明書に追加した秘密キーのパスワードを、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、スペースや特殊文字（「*」、「」）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

タスク概要

- 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. キーCRL\_PATH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、更新できます。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

## WindowsホストでのSnapCenter MySQLプラグイン サービスの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。

これはキー \_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
```



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キー 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 "証明書内のエイリアス名" -keystore keystore.jks
```

*agent.properties* ファイルのキー KEYSTORE\_PASS も同様に更新します。

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の一覧を表示します。

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

4. ルート証明書か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証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアにCA署名キーペアを構成する

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. ファイル *keystore.jks* を見つけます。
3. キーストアに追加された証明書の一覧を表示します。

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

4. 秘密キーと公開キー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の一覧を表示します。

```
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キーのパスワードを、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 "CA証明書のエイリアス名" -keystore keystore.jks
```

8. *agent.properties* ファイル内の 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

タスク概要

- 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、["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. キー CRL\_PATH に対して、*agent.properties* ファイル内のデフォルトディレクトリを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ファイルを格納できます。

受信する証明書については、それぞれのCRLに対して検証が行われます。

## プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインで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

- 実行 `Set-SmCertificateSettings` コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで使用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"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、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] 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。

終了後の操作

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Server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いないか、プラグイン ホストに割り当てられていないことを示します。
- \* \* は CA 証明書が正常に検証されたことを示します。
- \* \* は、CA 証明書を検証できなかったことを示します。
- \* \* は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

## 著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、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。