SnapCenter Plug-in for Oracle Database をインストールします

SnapCenter Software 6.0

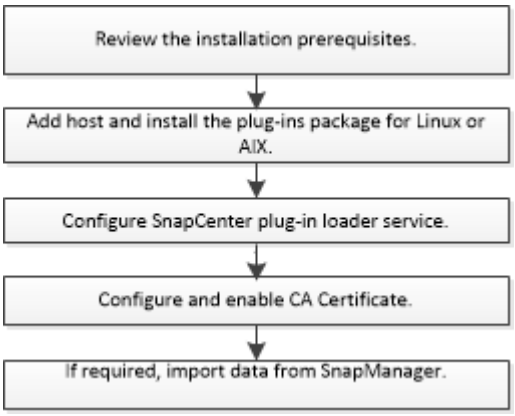
NetApp
September 17, 2024

目次

SnapCenter Plug-in for Oracle Database をインストールします

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

Oracle データベースを保護する場合は、 SnapCenter Plug-in for Oracle 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 Plug-in Package for Linux または AIX 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。

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

  SnapCenter Plug-in for Oracle Database は、 root 以外のユーザがインストールできます。ただし、プラグインプロセスをインストールして開始できるように root 以外のユーザに sudo 権限を設定する必要があります。プラグインをインストールすると、有効なroot以外のユーザとしてプロセスが実行されるようになります。

- AIX ホストに SnapCenter Plug-ins Package for AIX をインストールする場合は、ディレクトリレベルのシンボリックリンクを手動で解決しておく必要があります。

  SnapCenter Plug-ins Package for AIX は、ファイルレベルのシンボリックリンクを自動的に解決しますが、 JAVA_HOME の絶対パスを取得するためのディレクトリレベルのシンボリックリンクは解決しません。

- インストールユーザ用に、認証モードを Linux または AIX に設定してクレデンシャルを作成します。
- Java 11をLinuxホストまたはAIXホストにインストールしておく必要があります。

> Linuxホストに Java 11の認定エディションのみがインストールされていることを確認します。

Java のダウンロード方法については、次を参照してください。

- "すべてのオペレーティングシステム用の Java のダウンロード"
- "IBM Java for AIX の場合"

- Linux または AIX ホストで Oracle データベースを実行している場合は、 SnapCenter Plug-in for Oracle Database と SnapCenter Plug-in for UNIX の両方をインストールする必要があります。

> Plug-in for Oracle Database では、 SAP を対象とした Oracle データベースの管理も可能です。ただし、 SAP BR * Tools との統合はサポートされません。

- Oracle データベース 11.2.0.3 以降を使用している場合は、 13366202 Oracle パッチをインストールする必要があります。

> /etc/fstab ファイル内の UUID マッピングは SnapCenter でサポートされません。

- 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。

Linux ホストの要件

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

項目	要件
オペレーティングシステム	• Red Hat Enterprise Linux の場合 • Oracle Linux の場合 > Oracle Linux または Red Hat Enterprise Linux 6.6 または 7.0 オペレーティングシステムの LVM で Oracle データベースを使用している場合は、最新バージョンの論理ボリュームマネージャ（ LVM ）をインストールする必要があります。 • SUSE Linux Enterprise Server （ SLES ）
ホスト上の SnapCenter プラグインの最小 RAM	2 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 11 Oracle JavaおよびOpenJDK LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。 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 "NetApp Interoperability Matrix Tool で確認できます"ください。

Linux ホストの **root** 以外のユーザに **sudo** 権限を設定する

SnapCenter 2.0 以降のリリースでは、 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。
- 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/installing/plugins/uninstall
- /custom_location/NetApp/snapcenter /spl/bin/spl になります
- 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 !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 _ SnapCenterサーバーが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ための参照としてのみ使用してください。

AIX ホストの要件

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

SnapCenter Plug-ins Package for AIX に含まれている SnapCenter Plug-in for UNIX では、同時ボリュームグループはサポートされていません。

項目	要件
オペレーティングシステム	AIX 7.1以降
ホスト上の SnapCenter プラグインの最小 RAM	4 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	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。

項目	要件
必要なソフトウェアパッケージ	Java 11 IBM Java 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 "NetApp Interoperability Matrix Tool で確認できます"ください。

AIX ホストの **root** 以外のユーザに **sudo** 権限を設定します

SnapCenter 4.4 以降では、 root 以外のユーザが SnapCenter Plug-ins Package for AIX 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。
- /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/*aix_user*//.sc_netapp /snapcenter aix_host_plugin.bsx
- /custom_location/NetApp/snapcenter /spl/installing/plugins/uninstall
- /custom_location/NetApp/snapcenter /spl/bin/spl になります

- 手順 *

1. SnapCenter Plug-ins Package for AIX をインストールする AIX 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 HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_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
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_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。

_aix_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 _ SnapCenterサーバーが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ための参照としてのみ使用してください。

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Linux または AIX ホストにプラグインパッケージをインストールするため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 *

このクレデンシャルは、 root ユーザに対して作成されるほか、プラグインプロセスをインストールして開始する sudo 権限がある root 以外のユーザに対しても作成されます。

詳細については、を参照してください Linux ホストの root 以外のユーザに sudo 権限を設定する または AIX ホストの root 以外のユーザに sudo 権限を設定します

* 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で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。

- 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、クレデンシャル情報を入力します。

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。
ユーザ名 / パスワード	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 SnapCenter プラグインをインストールするシステムのドメイン管理者を指定します。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
認証モード	使用する認証モードを選択します。 プラグインホストのオペレーティングシステムに応じて、 Linux または AIX のいずれかを選択します。

フィールド	手順
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。

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、「 * 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。

Oracle データベースのクレデンシャルを設定します

Oracle データベースに対してデータ保護処理を実行するために使用するクレデンシャルを設定する必要があります。

- このタスクについて *

Oracle データベースでサポートされているさまざまな認証方式を確認しておく必要があります。詳細については、を参照してください"クレデンシャルの認証方式を指定します"。

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、ユーザ名に少なくともリソースグループとバックアップ権限が必要です。

Oracle データベース認証を有効にしている場合、リソースビューに赤い鍵のアイコンが表示されます。データベースを保護できるようにデータベースのクレデンシャルを設定するか、データベースをリソースグループに追加してデータ保護処理を実行する必要があります。

> クレデンシャルの作成時に誤った詳細を指定すると、エラーメッセージが表示されます。[キャンセル] をクリックしてから、もう一度実行してください。

- 手順 *

1. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、 [* 表示] リストから [* データベース *] を選択します。
3. をクリックします をクリックし、ホスト名とデータベースタイプを選択してリソースをフィルタリングします。

   をクリックします をクリックしてフィルタペインを閉じます。
4. データベースを選択し、 * データベース設定 * > * データベースの設定 * をクリックします。
5. [データベース設定の設定] セクションの [既存の資格情報を使用する *] ドロップダウンリストから、Oracle データベースでデータ保護ジョブを実行するために使用する資格情報を選択します。

   > Oracle ユーザには sysdba 権限が必要です。

   をクリックしてクレデンシャルを作成することもできます 。

6. ASM 設定の設定セクションの既存の認証情報を使用ドロップダウンリストから、 ASM インスタンスでデータ保護ジョブを実行するために使用する認証情報を選択します。

   ASM ユーザには SYSASM 権限が必要です。

   をクリックしてクレデンシャルを作成することもできます ＋。

7. [RMAN カタログ設定の構成] セクションの [既存のクレデンシャルを使用する *] ドロップダウンリストから、 Oracle Recovery Manager （ RMAN ）カタログデータベースでデータ保護ジョブを実行するために使用するクレデンシャルを選択します。

   をクリックしてクレデンシャルを作成することもできます ＋。

   TNSNAME フィールドに、 SnapCenter サーバーがデータベースとの通信に使用する透過ネットワーク印刷材 (TNS) ファイル名を入力します。

8. [* Preferred RAC Nodes] フィールドで、バックアップに優先する Real Application Cluster （ RAC ）ノードを指定します。

   優先ノードには、 RAC データベースインスタンスが存在するクラスタノードを 1 つまたはすべて指定できます。バックアップ処理は、指定したノードでのみ、指定した順序で実行されます。

   RAC One Node では、優先ノードにリストされるノードは 1 つだけで、この優先ノードはデータベースが現在ホストされているノードです。

   RAC One Node データベースのフェイルオーバーまたは再配置後に、 SnapCenter リソースページでリソースを更新すると、データベースが以前にホストされていた優先 RAC ノード * リストからホストが削除されます。データベースを再配置する RAC ノードは *RAC ノード * に表示され、手動で優先 RAC ノードとして設定する必要があります。

詳細については、を参照してください "RAC セットアップで優先ノードを指定します"。

1. [OK] をクリックします。

GUI を使用して、 Linux または AIX 用のホストを追加し、 Plug-ins Package をインストールします

ホストの追加ページを使用してホストを追加し、 SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をインストールできます。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。

- このタスクについて *

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。クラスタ（ Oracle RAC ）にプラグインをインストールする場合は、クラスタのすべてのノードにプラグインがインストールされている必要があります。Oracle RAC One Node の場合、このプラグインはアクティブノードとパッシブノードの両方にインストールする必要があります。

Oracle RACにプラグインをインストールする場合は、パスワードベースの認証のみがサポートされます。SSHキーベースの認証はサポートされていません。

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があるロールが割り当てられている必要があります。

> 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（ 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	ホストタイプとして「 * Linux * 」または「 * AIX * 」を選択します。 ホストが追加され、 Plug-in for Oracle Database と Plug-in for UNIX がホストにインストールされていない場合はインストールされます。 SnapCenter
ホスト名	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。 次のいずれかの IP アドレスまたは FQDN を入力できます。 • スタンドアロンホスト • Oracle Real Application Clusters （ RAC ）環境内の任意のノード ノード VIP や SCAN IP はサポートされていません SnapCenter を使用してホストを追加する際、ホストがサブドメインの一部である場合は、 FQDN を指定する必要があります。

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	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。
Oracle RAC のすべてのホストを追加します	Oracle RAC のすべてのクラスタノードを追加するには、このチェックボックスを選択します。 Flex ASM セットアップでは、ハブノードとリーフノードのどちらであるかに関係なく、すべてのノードが追加されます。

フィールド	手順
オプションのプレインストールチェックを省略します	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。

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。

   ファイアウォールの拒否ルールで指定されているプラグインポートのファイアウォールステータスは、事前確認スクリプトで検証されません。

   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\Virtual \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. 指紋を確認し、 * 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。

   SnapCenter は ECDSA アルゴリズムをサポートしていません。

   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 / log_ にあります。

- 結果 *

ホスト上のすべてのデータベースが自動的に検出され、リソースページに表示されます。何も表示されない場合は、 * リソースを更新 * をクリックします。

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. [* 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。

Linux または AIX 用のプラグインパッケージをインストールする別の方法

コマンドレットまたはCLIを使用して、LinuxまたはAIX用のPlug-ins Packageを手動でインストールすることもできます。

プラグインを手動でインストールする前に、_ C：\ProgramData\NetApp\SnapCenter \Package Repository_にあるキー* snapcenter public_key.pub と snapcenter _ linux_host_plugin.bin .sig *を使用して、バイナリパッケージの署名を検証する必要があります。

> プラグインをインストールするホストに* OpenSSL 1.0.2G*がインストールされていることを確認します。

次のコマンドを実行して、バイナリパッケージの署名を検証します。

- Linuxホストの場合： `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- AIXホストの場合： `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bsx.sig snapcenter_linux_host_plugin.bsx`

コマンドレットを使用して複数のリモートホストにインストールします

Linux 用 SnapCenter Plug-ins Package または SnapCenter Plug-ins Package for AIX を複数のホストにインストールするには、 _ Install -SmHostPackage_PowerShell コマンドレットを使用する必要があります。

- 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 にログインする必要があります。

- 手順 *

1. PowerShell を起動します。
2. SnapCenter サーバホストで、 _Open-SmConnection_cmdlet 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_cmdlet と、必要なパラメータを使用して、 Linux または SnapCenter Plug-in Package for AIX をインストール SnapCenter 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。

   > ファイアウォールの拒否ルールで指定されているプラグインポートのファイアウォールステータスは、事前確認スクリプトで検証されません。

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"。

クラスタホストにをインストールします

クラスタホストの両方のノードに、 SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をインストールする必要があります。

クラスタホストの各ノードには 2 つの IP があります。IP の 1 つが各ノードのパブリック IP で、 2 つ目の IP が両方のノードで共有されるクラスタ IP になります。

- 手順 *

1. クラスタホストの両方のノードに、 SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をインストールします。
2. SNAPCENTER_server_host 、 SPL_PORT 、 SNAPCENTER_server_port 、および SPL_enabled_plugins パラメータの正しい値が、 /var/opt/snapcenter /spl/etc/_ にある spl.properties ファイルで指定されていることを確認します。

   spl.properties で SPL_enabled_plugins が指定されていない場合は、 SPL_enabled_plugins を追加して値 sco 、 SCU を割り当てることができます。

3. SnapCenter サーバホストで、 _Open-SmConnection_cmdlet 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。

4. 各ノードで、 _Set-PreferredHostIPsInStorageExportPolicy_sccli コマンドおよび必要なパラメータを使用して、ノードの優先 IP を設定します。
5. SnapCenter サーバホストで、クラスタ IP のエントリと、対応する DNS 名を _C ： \Windows\System32\drivers\etc\hosts_に 追加します。
6. ホスト名に対応するクラスタ IP を指定して、 _Add-SmHost_cmdlet を使用して SnapCenter サーバにノードを追加します。

ノード 1 で Oracle データベースを検出し（クラスタ IP がノード 1 でホストされていることが前提）、データベースのバックアップを作成します。フェイルオーバーが発生した場合は、ノード 1 に作成されたバックアップを使用して、ノード 2 のデータベースをリストアできます。ノード 1 に作成したバックアップを使用して、ノード 2 にクローンを作成することもできます。

> 他の SnapCenter 処理の実行中にフェイルオーバーが発生すると、古いボリューム、ディレクトリ、およびロックファイルが存在します。

Linux用のPlug-ins Packageをサイレントモードでインストールします

コマンドラインインターフェイス（CLI）を使用して、SnapCenter Plug-ins Package for Linuxをサイレントモードで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ための前提条件を確認しておく必要があります。
- DISPLAY 環境変数が設定されていないことを確認する必要があります。

  DISPLAY 環境変数が設定されている場合は、 UNSET DISPLAY を実行してから、プラグインを手動でインストールする必要があります。

- このタスクについて *

コンソールモードでのインストール中に必要なインストール情報を指定する必要がありますが、サイレントモードでのインストールでは、インストール情報を指定する必要はありません。

- 手順 *

1. SnapCenter Plug-ins Package for Linux を SnapCenter Server のインストール場所からダウンロードします。

   デフォルトのインストールパスは、 _C ： \ProgramData\NetApp\SnapCenter \PackageRepository_です 。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ダウンロードしたディレクトリに移動します。
3. を実行します

   `../SnapCenter _Linux_host_plugin.bin -i サイレント -dport=8145 - DSERVER_IP=SnapCenter _Server_FQDN -DSERVER_HTTPS_PORT=SnapCenter _ Server_Port- DUSER_INSTALL_DIR=/opt/custom_path

4. /var/opt/snapcenter /spl/etc/__ にある spl.properties ファイルを編集して、 spl_enabled_plugins/SCO 、 SCU を追加し、 SnapCenter Plug-in Loader サービスを再起動します。

プラグインパッケージのインストールでは、 SnapCenter サーバではなく、ホストにプラグインが登録されます。SnapCenter GUI または PowerShell コマンドレットを使用してホストを追加し、 SnapCenter サーバにプラグインを登録します。ホストの追加中に、クレデンシャルとして [None] を選択します。ホストを追加すると、インストールしたプラグインが自動的に検出されます。

AIX 用プラグインパッケージをサイレントモードでインストールします

コマンドラインインターフェイス（ CLI ）を使用して、 SnapCenter Plug-ins Package for AIX をサイレントモードで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ための前提条件を確認しておく必要があります。
- DISPLAY 環境変数が設定されていないことを確認する必要があります。

  DISPLAY 環境変数が設定されている場合は、 UNSET DISPLAY を実行してから、プラグインを手動でインストールする必要があります。

- 手順 *

  1. SnapCenter Server のインストール場所から、 SnapCenter Plug-ins Package for AIX をダウンロードします。

     デフォルトのインストールパスは、 _C ： \ProgramData\NetApp\SnapCenter \PackageRepository_です 。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ダウンロードしたディレクトリに移動します。
  3. を実行します

     `./snapcenter aix_host_plugin.bsx -i silent-dport=8145 - DSERVER_IP=SnapCenter _Server_FQDN -DSERVER_HTTPS_PORT=SnapCenter _Server_Port-DUSER_INSTALL_DIR=/opt/custom_path-DISKALL_LOG_LOG_NAME=SnapCenter _AIX_FILE_INSTAN_INSTAN_INSTAN_MANUALL_INSTALLATUE_FEATURE_FILE=SnapCenter _ インストール手動 MDULE=SnapCenter _ インストール _ インストール _ インストール _ インストール _ インストール _ インストール _ インストール _ インストール _ インストール _ インストール _ インストール _ インストール _ インストール _ オプション =SnapCenter _ インストール _ インストール _ インストール _ インストール _ ホスト名 = SnapCenter _ インストール _

  4. /var/opt/snapcenter /spl/etc/__ にある spl.properties ファイルを編集して、 spl_enabled_plugins/SCO 、 SCU を追加し、 SnapCenter Plug-in Loader サービスを再起動します。

プラグインパッケージのインストールでは、 SnapCenter サーバではなく、ホストにプラグインが登録されます。SnapCenter GUI または PowerShell コマンドレットを使用してホストを追加し、 SnapCenter サーバにプラグインを登録します。ホストの追加中に、クレデンシャルとして [None] を選択します。ホストを追加すると、インストールしたプラグインが自動的に検出されます。

SnapCenter Plug-in Loader サービスを設定します

SnapCenter Plug-in Loader サービスは、 Linux または AIX 用のプラグインパッケージを

ロードして、 SnapCenter サーバーと通信します。SnapCenter Plug-in Loader サービスは、 Linux 用の SnapCenter Plug-ins Package または AIX 用 SnapCenter Plug-ins Package をインストールするとインストールされます。

- このタスクについて *

SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をインストールすると、SnapCenter Plug-in Loader サービスが自動的に開始されます。SnapCenter Plug-in Loader サービスが自動的に開始されない場合は、次のことを行う必要があります。

- プラグインが動作しているディレクトリが削除されていないことを確認してください
- Java 仮想マシンに割り当てられているメモリ容量を増やします

spl.properties ファイルは、 */custom_location/NetApp/snapcenter /spl/etc/* にあり、次のパラメータを含みます。これらのパラメータにはデフォルト値が割り当てられています。

パラメータ名	説明
LOG_LEVEL の値	サポートされるログレベルを表示します。 指定できる値は、trace、debug、info、warn、error、致命的だ
SPL プロトコル	SnapCenter Plug-in Loader でサポートされているプロトコルを表示します。 HTTPS プロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。
SNAPCENTER_server_protocol 」を参照してください	SnapCenter サーバでサポートされているプロトコルを表示します。 HTTPS プロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。
ske_JAVAHOME_update を実行します	デフォルトでは、 SPL サービスは Java パスを検出し、 JAVA_HOME パラメータを更新します。 したがって、デフォルト値は FALSE に設定されます。デフォルトの動作を無効にして Java パスを手動で修正する場合は、 true に設定します。
SPL キーストアパス	キーストアファイルのパスワードを表示します。 この値は、パスワードを変更する場合や新しいキーストアファイルを作成する場合にのみ変更できます。

パラメータ名	説明
SPL ポート	SnapCenter Plug-in Loader サービスが実行されているポート番号を表示します。 デフォルト値がない場合は、値を追加できます。 プラグインのインストール後は値を変更しないでください。
SNAPCENTER_server_host が必要です	SnapCenter サーバの IP アドレスまたはホスト名を表示します。
SPL キーストアパス	キーストアファイルの絶対パスを表示します。
SNAPCENTER_SERVER_PORT	SnapCenter サーバが稼働しているポート番号を表示します。
logs_MAX_COUNT	SnapCenter Plug-in Loader ログファイルのうち、_/custom_location/snapcenter /spl/logs_folder に保持されているファイルの数を表示します。 デフォルト値は 5000 に設定されています。指定した値よりも多い数のファイルがある場合は、変更後の最新の 5000 個のファイルが保持されます。ファイル数のチェックは、 SnapCenter Plug-in Loader サービスが開始されたときから 24 時間ごとに自動的に行われます。 spl.properties ファイルを手動で削除すると、保持されるファイル数は 9999 に設定されます。
JAVA_HOME にアクセスします	SPL サービスの開始に使用される JAVA_HOME の絶対ディレクトリパスを表示します。 このパスは、インストール時および SPL の開始時に決定されます。
LOG_MAX_SIZE	ジョブログファイルの最大サイズを表示します。 最大サイズに達すると、ログファイルが圧縮され、そのジョブの新しいファイルにログが書き込まれます。
retain_logs_of _last_days	ログを保持する日数が表示されます。

パラメータ名	説明
enable_certificate_validationを実行します	ホストでCA証明書の検証が有効になっている場合はtrueと表示されます。 このパラメータを有効または無効にするには、spl.propertiesを編集するか、SnapCenter GUIまたはコマンドレットを使用します。

これらのパラメータのいずれかがデフォルト値に割り当てられていない場合、または値を割り当てたり変更したりする場合は、 spl.properties ファイルを変更します。また、 spl.properties ファイルを確認して編集し、パラメータに割り当てられている値に関連する問題のトラブルシューティングを行うこともできます。spl.properties ファイルを変更したら、 SnapCenter Plug-in Loader サービスを再起動する必要があります。

- 手順 *
  1. 必要に応じて、次のいずれかの操作を実行します。
     - SnapCenter Plug-in Loaderサービスを開始します。
       - rootユーザとして、次のコマンドを実行します。
         `/custom_location/NetApp/snapcenter/spl/bin/spl start`
       - root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
     - SnapCenter Plug-in Loader サービスを停止します。
       - rootユーザとして、次のコマンドを実行します。
         `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
       - root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

       stop コマンドに -force オプションを指定すると、 SnapCenter Plug-in Loader サービスを強制的に停止できます。ただし、既存の処理が終了するため、実行する前に十分に注意する必要があります。

     - SnapCenter Plug-in Loader サービスを再起動します。
       - rootユーザとして、次のコマンドを実行します。
         `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
       - root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - SnapCenter Plug-in Loader サービスのステータスを確認します。
       - rootユーザとして、次のコマンドを実行します。
         `/custom_location/NetApp/snapcenter/spl/bin/spl status`
       - root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
     - SnapCenter Plug-in Loader サービスで変更を探します。

- rootユーザとして、次のコマンドを実行します。
  `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- root以外のユーザとして、次のコマンドを実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Linux ホストに SnapCenter Plug-in Loader （ SPL ）サービスを使用して CA 証明書を設定します

SPL 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、ルート証明書または中間証明書を SPL の信頼ストアに設定し、 CA 署名キーペアを SPL の信頼ストアと SnapCenter Plug-in Loader サービスを使用して設定して、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。

> SPL は、ファイル 'keystore.jkS' を使用します。このファイルは、 '/var/opt/snapcenter /spl/etc にあり、どちらもトラストストアおよびキーストアとして使用されます。

SPL キーストアのパスワードと使用中の CA 署名済みキーペアのエイリアスを管理します

- 手順 *

1. SPL プロパティファイルから SPL 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 'PL_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>" -keystore keystore.jks
   ```

   spl.properties ファイル内のキー SPL の _keystore.pass に対しても同じ内容を更新します。

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。

> SPL 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 SPL の信頼ストアに設定します

SPL の信頼ストアへ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. SPL キーストアが格納されているフォルダ（ /var/opt/snapcenter /spl/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
. ルート証明書または中間証明書を追加します。
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath>
-keystore keystore.jks
. SPL
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、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 SPL の信頼ストアに設定します

CA 署名鍵ペアを SPL 信頼ストアに設定する必要があります。

- 手順 *
  1. SPL のキーストア /var/opt/snapcenter /spl/ などを含む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
. 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 <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. 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
. 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。
. 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 SPL キーストアパスワードは、 spl.properties ファイル内のキー SPL の keystore.pass

の値です。

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>"
-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 "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. spl.properties ファイルにあるキーストアからエイリアス名を設定します。
```

この値をキー SPL の certificate_alias に更新します。

4. CA 署名済みキーペアを SPL 信頼ストアに設定したら、サービスを再起動します。

SPL の証明書失効リスト（ CRL ）を設定します

SPL 用に CRL を設定する必要があります

- このタスクについて *
- SPL 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。
- SPL の CRL ファイルのデフォルトディレクトリは、 _var/opt/snapcenter /spl/etc/crl_です 。
- 手順 *
  1. spl.properties ファイル内のデフォルトディレクトリを、キー SPL_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。

作業を開始する前に

- 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. 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。

完了後

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。

SnapManager for Oracle および SnapManager for SAP から SnapCenter にデータをインポートします

SnapManager for Oracle および SnapManager for SAP から SnapCenter にデータをインポートすると、以前のバージョンのデータを引き続き使用することができます。

コマンドラインインターフェイス（ Linux ホストの CLI ）からインポートツールを実行して、 SnapManager for Oracle および SnapManager for SAP から SnapCenter にデータをインポートできます。

インポートツールを使用すると、 SnapCenter にポリシーとリソースグループが作成されます。SnapCenter で作成されるポリシーとリソースグループは、 SnapManager for Oracle および SnapManager for SAP のプロファイルとそれらのプロファイルを使用して実行される処理に対応しています。SnapCenter インポートツールでは、 SnapManager for Oracle および SnapManager for SAP のリポジトリデータベースとインポートするデータベースが処理されます。

- プロファイル、スケジュール、およびプロファイルを使用して実行される処理がすべて取得されます。
- 一意の処理ごと、およびプロファイルに関連付けられているスケジュールごとに、 SnapCenter バックアップポリシーを作成します。
- ターゲットデータベースごとにリソースグループを作成します。

インポートツールは、 /opt/NetApp/SnapCenter /spl/bin_ にある sc-migrate スクリプトを実行することによって実行できます。インポートするデータベースホストに Linux 用の SnapCenter Plug-ins パッケージをインストールすると、 sc-migrate スクリプトが */opt/NetApp/snapcenter / spl/bin* にコピーされます。

データのインポートは、 SnapCenter のグラフィカルユーザインターフェイス（ GUI ）ではサポートされていません。

SnapCenter では、 Data ONTAP 7-Mode はサポートされていません。7-Mode Transition Tool を使用して、Data ONTAP 7-Mode を実行するシステムに格納されているデータと構成を ONTAP システムに移行できます。

データのインポートがサポートされる構成

SnapManager 3.4.x for Oracle および SnapManager 3.4.x for SAP から SnapCenter にデータをインポートする前に、 SnapCenter Plug-in for Oracle Database でサポートされる構成を確認しておく必要があります。

SnapCenter Plug-in for Oracle Databaseでサポートされる構成については、を参照して "NetApp Interoperability Matrix Tool で確認できます"ください。

データが **SnapCenter** にインポートされます

プロファイル、スケジュール、およびプロファイルを使用して実行される処理をインポートできます。

SnapManager for Oracle および **SnapManager for SAP** から入手できます	を **SnapCenter** に移動します
処理とスケジュールが設定されていないプロファイル	ポリシーは、デフォルトのバックアップタイプを「 Online 」、バックアップスコープを「 Full 」に設定して作成されます。
1 つ以上の処理が設定されたプロファイル	プロファイルとそのプロファイルを使用して実行される処理の一意の組み合わせに基づいて複数のポリシーが作成されます。 SnapCenter で作成されるポリシーには、プロファイルおよび対応する処理から取得されたアーカイブ・ログの削除および保持の詳細が含まれます。
Oracle Recovery Manager （ RMAN ）の設定を含むプロファイル	Oracle Recovery Manager * オプションを有効にした場合、 * Catalog backup でポリシーが作成されます。 SnapManager で外部 RMAN のカタログ化を使用していた場合は、 SnapCenter で RMAN カタログの設定を行う必要があります。既存のクレデンシャルを選択するか、新しいクレデンシャルを作成できます。 SnapManager で制御ファイルを使用して RMAN を設定した場合は、 SnapCenter で RMAN を設定する必要はありません。
プロファイルに関連付けられたスケジュール	スケジュールに対してのみポリシーが作成されます。

SnapManager for Oracle および **SnapManager for SAP** から入手できます	を **SnapCenter** に移動します
データベース	インポートしたデータベースごとにリソースグループが作成されます。 Real Application Clusters （ RAC ）セットアップでは、インポート後にインポートツールを実行したノードが優先ノードになり、そのノードに対してリソースグループが作成されます。

プロファイルをインポートすると、バックアップポリシーと一緒に検証ポリシーが作成されます。

SnapManager for Oracle および SnapManager for SAP のプロファイル、スケジュール、およびプロファイルを使用して実行されるすべての処理を SnapCenter にインポートすると、異なるパラメータの値もインポートされます。

SnapManager for Oracle および **SnapManager for SAP** のパラメータと値	**SnapCenter** のパラメータと値	注：
バックアップの範囲 • フル • データ • ログ	バックアップの範囲 • フル • データ • ログ	
バックアップモード • 自動 • オンライン • オフラインです	バックアップタイプ • オンライン • オフラインシャットダウン	バックアップモードが自動の場合、インポートツールは処理の実行時にデータベースの状態を確認し、バックアップタイプをオンラインまたはオフラインシャットダウンに適切に設定します。
保持 • 日 • カウント	保持 • 日 • カウント	SnapManager for Oracle および SnapManager for SAP では ' 日数とカウントの両方を使用して保存期間を設定します SnapCenter には、days_or_Counts があります。したがって、 SnapManager for Oracle と SnapManager for SAP で個数よりも日数が優先されることから、日数に基づいて保持が設定されます。

SnapManager for Oracle および **SnapManager for SAP** のパラメータと値	**SnapCenter** のパラメータと値	注：
スケジュールのプルーニング • すべて • システム変更番号（ SCN ） • 日付 • 指定した時間、日、週、および月よりも前に作成されたログです	スケジュールのプルーニング • すべて • 指定した時間および日数より前に作成されたログです	SnapCenter は、 SCN 、日付、週、および月に基づくプルーニングをサポートしていません。
通知 • 成功した処理のためにのみ送信される E メールです • 処理に失敗した場合にのみ送信される E メールです • 処理の成功と失敗の両方について送信される E メールです	通知 • 常に • 失敗した場合 • 警告 • エラー	E メール通知はインポートされます。 ただし、 SnapCenter GUI を使用して SMTP サーバを手動で更新する必要があります。E メールの件名は、設定できるように空白になります。

SnapCenter にインポートされないデータ

インポートツールは、すべてのデータを SnapCenter にインポートするわけではありません。

次のものを SnapCenter にインポートすることはできません。

- バックアップメタデータ
- パーシャル・バックアップ
- raw デバイスマッピング（ RDM ）および Virtual Storage Console （ VSC ）関連のバックアップ
- SnapManager for Oracle および SnapManager for SAP のリポジトリで使用可能なロールとクレデンシャル
- 検証、リストア、クローニングの処理に関するデータ
- 処理の削除
- SnapManager for Oracle および SnapManager for SAP のプロファイルで指定されたレプリケーションの詳細

  インポートの完了後に、 SnapCenter で作成した対応するポリシーを手動で編集してレプリケーションの詳細を含める必要があります。

- カタログ化されたバックアップの情報

データをインポートする準備をします

SnapCenter へのデータのインポート処理を正常に実行するには、データをインポートする前に特定のタスクを実行する必要があります。

- 手順 *

1. インポートするデータベースを特定します。
2. SnapCenter を使用して、データベースホストを追加し、 SnapCenter Plug-ins Package for Linux をインストールします。
3. SnapCenter を使用して、ホスト上のデータベースで使用される Storage Virtual Machine （ SVM ）の接続を設定します。
4. 左側のナビゲーションペインで、 * リソース * をクリックし、リストから適切なプラグインを選択します。
5. リソースページで、インポートするデータベースが検出されて表示されていることを確認します。

   インポートツールを実行する場合は、データベースにアクセスできる必要があります。アクセスできないと、リソースグループの作成が失敗します。

   データベースにクレデンシャルが設定されている場合は、 SnapCenter で対応するクレデンシャルを作成し、そのクレデンシャルをデータベースに割り当ててから、データベースの検出を再度実行する必要があります。データベースが Automatic Storage Management （ ASM ）にある場合は、 ASM インスタンスのクレデンシャルを作成し、そのクレデンシャルをデータベースに割り当てる必要があります。

6. インポートツールを実行 SnapManager するユーザに、 SnapManager for Oracle または SnapManager for SAP ホストから Oracle for Oracle または SnapManager for SAP CLI コマンド（スケジュールを一時停止するコマンドなど）を実行するための十分な権限があることを確認します。
7. SnapManager for Oracle または SnapManager for SAP ホストで次のコマンドを実行して、スケジュールを一時停止します。

   a. SnapManager for Oracle ホストでスケジュールを一時停止する場合は、次のコマンドを実行します。

      - 'mo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name _FOR_repository_database
      - 「 mo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name _FOR_repository_database 」のように入力します
      - 'mo credential set -profile-name profile_name

      smo credential set コマンドは、ホストのプロファイルごとに実行する必要があります。

   b. SnapManager for SAP ホストでスケジュールを一時停止する場合は、次のコマンドを実行します。

      - 「 MSAP クレデンシャルセット - repository-dbname repository_database_name -host host_name -port port_number - login -username user_name _FOR_repository_database
      - 「 MSAP profile sync -repository -dbname repository_database_name -host host_name -port

port_number -login -username host_user_name _FOR_repository_database 」のように入力します

- 'MSSAP クリデンシャル・セット - プロファイル名 profile_name

> SMSAP のクレデンシャルセットコマンドは、ホストの各プロファイルに対して実行する必要があります。

1. hostname-f を実行するときに、データベースホストの Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）が表示されることを確認します

   FQDN が表示されない場合は、 /etc/hosts を変更してホストの FQDN を指定する必要があります。

データをインポートする

データベースホストからインポートツールを実行して、データをインポートできます。

- このタスクについて *

インポート後に作成される SnapCenter バックアップポリシーの名前の形式は、次のとおりです。

- 処理とスケジュールが設定されていないプロファイルに対して作成されたポリシーの場合、 sm_created 形式は「 sm_created 」です。

  プロファイルを使用して処理を実行しない場合は、対応するポリシーが作成され、デフォルトのバックアップタイプは online 、バックアップスコープは full になります。

- 1 つ以上の操作を持つプロファイルに対して作成されたポリシーには、SM_profileName_BACKUPMODE_BACKUPSCOPE_Migrated 形式があります。
- プロファイルに関連付けられたスケジュールに対して作成されたポリシーは、SM_profileName_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_Migrated 形式です。
- 手順 *

  1. インポートするデータベースホストにログインします。
  2. /opt/NetApp/SnapCenter /spl/bin_ にある sc-migrate スクリプトを実行して、インポートツールを実行します。
  3. SnapCenter サーバのユーザ名とパスワードを入力します。

     クレデンシャルの検証後、 SnapCenter との接続が確立されます。

  4. SnapManager for Oracle または SnapManager for SAP のリポジトリデータベースの詳細を入力します。

     リポジトリデータベースのホストで使用できるデータベースが表示されます。

  5. ターゲットデータベースの詳細を入力します。

     ホスト上のすべてのデータベースをインポートする場合は、「 all 」と入力します。

  6. 処理に失敗した場合のシステムログの生成や ASUP メッセージの送信を有効にする場合は、 _Add-SmStorageConnection_or_Set-SmStorageConnection_command を実行して有効にする必要がありま

す。

> インポート処理をキャンセルする場合は、インポートツールの実行中またはインポートの完了後に、インポート処理で作成された SnapCenter ポリシー、クレデンシャル、およびリソースグループを手動で削除する必要があります。

- 結果 *

プロファイル、スケジュール、およびプロファイルを使用して実行される処理に対応した SnapCenter バックアップポリシーが作成されます。各ターゲットデータベースのリソースグループも作成されます。

データのインポートが正常に完了すると、 SnapManager for Oracle および SnapManager for SAP で、インポートしたデータベースに関連付けられたスケジュールが一時停止されます。

> インポートの完了後は、 SnapCenter を使用してインポートしたデータベースまたはファイルシステムを管理する必要があります。

インポートツールを実行するたびに、 spl_migration_timestamp.log という名前の _/var/opt/snapcenter /spl/logs_directory にログが格納されます。このログを参照して、インポートエラーを確認し、トラブルシューティングを行うことができます。