



# Oracle データベースを保護します

## SnapCenter Software 4.5

NetApp  
September 29, 2025

# 目次

Oracle データベースを保護します	1
SnapCenter Plug-in for Oracle Database の概要を参照してください	1
Plug-in for Oracle Database の機能	1
Plug-in for Oracle Database の特長	1
Plug-in for Oracle Database でサポートされるストレージタイプ	3
Plug-in for Oracle に必要な最小 ONTAP 権限	4
SnapCenter Plug-in for Oracle Database をインストールします	8
SnapCenter Plug-in for Oracle Database のインストールワークフロー	8
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	8
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	17
SnapCenter Plug-in Loader サービスを設定します	24
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	28
プラグインの CA 証明書を有効にします	30
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	31
SnapCenter Plug-in for VMware vSphere をインストール	37
CA 証明書を導入する	37
CRL ファイルを設定します	37
Oracle データベースの保護を準備する	37
Oracle データベースをバックアップする	39
バックアップのワークフロー	39
Oracle データベースのバックアップ戦略を定義する	40
Oracle データベースをバックアップに使用できるかどうかを確認します	48
Oracle データベースのバックアップポリシーの作成	49
Oracle データベースのリソースグループを作成してポリシーを適用します	54
Oracle データベースをバックアップするための要件	56
Oracle リソースのバックアップ	57
Oracle データベースのリソースグループをバックアップする	60
UNIX コマンドを使用して Oracle データベースをバックアップします	61
Oracle データベースのバックアップ処理を監視する	62
Oracle データベースのバックアップ処理をキャンセルします	63
Topology ページで、Oracle データベースのバックアップとクローンを表示します	64
データベースバックアップのマウントとアンマウント	66
データベースバックアップをマウント	66
データベースバックアップをアンマウント	68
Oracle データベースのリストアとリカバリを行う	68
リストアワークフロー	68
Oracle データベースのリストアとリカバリの戦略を定義する	68
Oracle データベースをリストアするための要件	73

Oracle データベースをリストアします	74
ポイントインタイムリカバリを使用した表領域のリストアとリカバリ	79
ポイントインタイムリカバリを使用して、プラグイン可能なデータベースをリストアおよびリカバリ します	80
UNIX コマンドを使用して Oracle データベースをリストアおよびリカバリする	83
Oracle データベースのリストア処理を監視する	83
Oracle データベースのリストア処理をキャンセルします	84
Oracle データベースのクローニング	85
クローニングワークフロー	85
Oracle データベースのクローニング戦略を定義する	85
Oracle データベースをクローニングするための要件	87
Oracle データベースバックアップをクローニングする	89
プラグイン可能なデータベースをクローニングします	97
UNIX コマンドを使用して Oracle データベースバックアップをクローニングする	101
Oracle データベースクローンをスプリットします	102
プラグイン可能なデータベースのスプリットクローン	103
Oracle データベースのクローニング処理を監視する	104
クローンをリフレッシュします	105
プラグイン可能なデータベースのクローンを削除します	106

# Oracle データベースを保護します

## SnapCenter Plug-in for Oracle Database の概要を参照してください

### Plug-in for Oracle Database の機能

SnapCenter Plug-in for Oracle Database は、Oracle データベースに対応したデータ保護管理を提供する、NetApp SnapCenter ソフトウェアのホスト側コンポーネントです。

Plug-in for Oracle Database によって、Oracle Recovery Manager (RMAN)、検証、マウント、アンマウント、リストア、SnapCenter 環境での Oracle データベースのリカバリとクローニング Plug-in for Oracle Database は、すべてのデータ保護処理を実行するために SnapCenter Plug-in for UNIX をインストールします。

Plug-in for Oracle Database では、SAP アプリケーションを実行している Oracle データベースのバックアップを管理することができます。ただし、SAP BR \* Tools との統合はサポートされません。

- データファイル、制御ファイル、およびアーカイブログファイルをバックアップします。  
バックアップはコンテナデータベース (CDB) レベルでのみサポートされます。
- データベース、CDB、および Pluggable Database (PDB) のリストアとリカバリを行います。  
PDB の不完全リカバリはサポートされていません。
- ある時点までの本番環境データベースのクローンを作成します。  
クローニングは CDB レベルでのみサポートされます。
- バックアップをただちに検証します。
- リカバリ処理のためにデータバックアップとログバックアップのマウントとアンマウントを行います。
- バックアップ処理と検証処理をスケジュールします。
- すべての処理を監視します。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。

### Plug-in for Oracle Database の特長

Plug-in for Oracle Database は、Linux または AIX ホスト上で Oracle データベースと統合されるほか、ストレージシステム上でネットアップのテクノロジーと統合されます。

- 統一されたグラフィカルユーザインターフェイス

SnapCenter のインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。SnapCenter のインターフェイスから、すべてのプラグインで、バックアップ、リストア、リカバリ、クローニングの各処理を一貫した方法で実行できるほか、ダッシュボードビューで概要を把握したり、ロールベースアクセス制御 (RBAC) を設定したり、ジョブを監視したりすることができます。

- 中央管理の自動化

バックアップ処理とクローニング処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenter から E メールアラートを送信するように設定して、環境をプロアクティブに監視することもできます。

- 無停止の NetApp Snapshot コピーテクノロジー

SnapCenter では、 Plug-in for Oracle Database および Plug-in for UNIX でネットアップの Snapshot コピーテクノロジーを使用してデータベースがバックアップされます。Snapshot コピーはストレージスペースを最小限しか消費しません。

Plug-in for Oracle Database には、次のようなメリットもあります。

- バックアップ、リストア、クローニング、マウント、アンマウント、 検証ワークフローなどがあります
- ホストで設定されている Oracle データベースの自動検出
- Oracle Recovery Manager (RMAN) を使用したカタログ化とカタログ化解除がサポートされます。
- セキュリティが RBAC でサポートされ、ロール委譲が一元化されます

また、許可された SnapCenter ユーザにアプリケーションレベルの権限を付与するようにクレデンシャルを設定することもできます。

- NetApp FlexClone テクノロジーを使用して、本番環境のデータベースのスペース効率に優れたポイントインタイムコピーを作成し、テストまたはデータの抽出を行います

クローンを作成するストレージシステムに FlexClone ライセンスが必要です。

- SAN 環境および ASM 環境でバックアップを作成する際に、ONTAP の整合グループ (CG) 機能がサポートされます
- 自動化された無停止のバックアップ検証
- 複数のデータベースホストで同時に複数のバックアップを実行できます

1 回の処理で、1 つのホストのデータベースが同じボリュームを共有する場合に複数の Snapshot コピーが統合されます。

- 物理インフラと仮想インフラがサポートされます
- NFS、iSCSI、ファイバチャネル (FC)、RDM、NFS および VMFS 経由の VMDK、NFS、SAN、RDM、および VMDK 経由の ASM がサポートされます
- ONTAP の選択的 LUN マップ (SLM) 機能がサポートされます

デフォルトで有効になる SLM 機能は、最適パスを持たない LUN を定期的に検出して修正します。SLM を設定するには、`/var/opt/snapcenter/scu/etc.` にある `scu.properties` ファイル内のパラメータを変更します

- この機能を無効にするには、`ENABLE_LUNPATH_MONITORING` の値を `false` に設定します。
- LUN パスが自動的に修正される頻度を指定するには、`LUNPATH_MONITORING_INTERVAL` に値 (時間単位) を割り当てます。SLM の詳細については、を参照してください "『[ONTAP 9 SAN アドミニストレーションガイド](#)』"。

## Plug-in for Oracle Database でサポートされるストレージタイプ

SnapCenter は、物理マシンと仮想マシンの両方でさまざまなストレージタイプをサポートしています。SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX をインストールする前に、ストレージタイプがサポートされているかどうかを確認する必要があります。

SnapCenter では、Linux および AIX のストレージプロビジョニングはサポートされていません。

### Linux でサポートされているストレージタイプ

次の表に、Linux でサポートされるストレージタイプを示します。

マシン	ストレージタイプ
物理サーバ	<ul style="list-style-type: none"><li>• FC 接続 LUN</li><li>• iSCSI で接続された LUN</li><li>• NFS-connected ボリューム</li></ul>
VMware ESXi	<ul style="list-style-type: none"><li>• FC または iSCSI ESXi HBA によって接続された RDM LUN は、ホストに存在するすべてのホストバスアダプタを SnapCenter がスキャンするため、完了までに時間がかかることがあります。  /opt/NetApp/SnapCenter /spl/plugins/SCU/scucore /modules/SCU/ConfigU/Config_ にある * LinuxConfig.pm * ファイルを編集して、 * scsi_hosts_optimized_rescan * パラメーターの値を 1 に設定し、 ha_driver_names にリストされている HBA のみを再スキャンすることができます。</li><li>• iSCSI イニシエータによってゲストシステムに直接接続された iSCSI LUN</li><li>• VMFS データストアまたは NFS データストア上の VMDK</li><li>• ゲストシステムに直接接続された NFS ボリューム</li></ul>

### AIX でサポートされているストレージタイプ

次の表に、AIX でサポートされるストレージタイプを示します。

マシン	ストレージタイプ
物理サーバ	<ul style="list-style-type: none"> <li>• FC 接続 LUN と iSCSI 接続 LUN :</li> </ul> <p>SAN 環境では、ASM、LVM、および SAN のファイルシステムがサポートされます。</p> <div style="display: flex; align-items: center; margin: 10px 0;"> <div style="text-align: center; margin-right: 10px;">  </div> <div> <p>AIX およびファイルシステムでの NFS はサポートされていません。</p> </div> </div> <ul style="list-style-type: none"> <li>• 拡張ジャーナルファイルシステム (JFS2)</li> </ul> <p>SAN ファイルシステムおよび LVM レイアウトでのインラインロギングをサポートします。</p>

。 ["NetApp Interoperability Matrix Tool で確認できます"](#) サポートされているバージョンに関する最新情報が含まれています。

### Plug-in for Oracle に必要な最小 ONTAP 権限

必要な最小 ONTAP 権限は、データ保護に使用する SnapCenter プラグインによって異なります。

フルアクセスコマンド： <b>ONTAP 8.2_x_and later</b> に必要な最小権限
<ul style="list-style-type: none"> <li>• event generate-autosupport-log を指定します</li> </ul>
<ul style="list-style-type: none"> <li>• ジョブ履歴の表示</li> <li>• ジョブが停止しました</li> </ul>

フルアクセスコマンド： **ONTAP 8.2\_x\_and later** に必要な最小権限

- LUN
- lun attribute show
- lun create をクリックします
- lun delete
- LUN ジオメトリ
- LUN igroup add
- lun igroup create を追加します
- lun igroup delete
- LUN igroup の名前を変更します
- lun igroup show を参照してください
- LUN マッピングの追加 - レポートノード
- LUN マッピングが作成されます
- LUN マッピングが削除されます
- LUN マッピングの削除 - レポートノード
- lun mapping show
- lun modify を追加します
- LUN のボリューム内移動
- LUN はオフラインです
- LUN はオンラインです
- LUN の永続的予約はクリアします
- LUN のサイズ変更
- LUN シリアル
- lun show をクリックします

フルアクセスコマンド： **ONTAP 8.2\_x\_and later** に必要な最小権限

- SnapMirror ポリシー追加ルール
- snapmirror policy modify-rule
- snapmirror policy remove-rule」を実行します
- snapmirror policy show の略
- SnapMirror リストア
- snapmirror show の略
- snapmirror show -history の略
- SnapMirror の更新
- SnapMirror の update-ls-set
- snapmirror list-destinations

- バージョン

フルアクセスコマンド： **ONTAP 8.2\_x\_and later** に必要な最小権限

- volume clone create を実行します
- volume clone show を実行します
- ボリュームクローンスプリット開始
- ボリュームクローンスプリットは停止します
- volume create を実行します
- ボリュームを削除します
- volume file clone create を実行します
- volume file show-disk-usage
- ボリュームはオフラインです
- ボリュームはオンラインです
- volume modify を使用します
- volume qtree create を実行します
- volume qtree delete
- volume qtree modify の略
- volume qtree show の略
- ボリュームの制限
- volume show のコマンドです
- volume snapshot create を実行します
- ボリューム Snapshot の削除
- volume snapshot modify の実行
- ボリューム Snapshot の名前が変更されます
- ボリューム Snapshot リストア
- ボリューム Snapshot の restore-file
- volume snapshot show の実行
- ボリュームのアンマウント

- Vserver
- SVM CIFS です
- vserver cifs shadowcopy show
- vserver show のコマンドです

- Network Interface の略
- network interface show の略

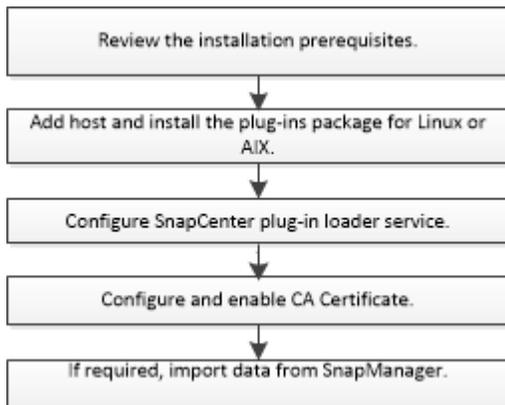
フルアクセスコマンド： **ONTAP 8.2\_x\_and later** に必要な最小権限

- MetroCluster のショーをご覧ください

## 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、プロセスが有効な root ユーザとして実行されます。

- 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。
- Linux または AIX ホストに Java 1.8.x、64 ビットをインストールしておく必要があります。

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。

## 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	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux の場合</li><li>• Oracle Linux の場合</li></ul> <p> 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。</p> <ul style="list-style-type: none"><li>• SUSE Linux Enterprise Server（SLES）</li></ul>
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	2 GB <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。</p>

項目	要件
必要なソフトウェアパッケージ	<p>Java 1.8.x (64 ビット) の Oracle Java と OpenJDK のバージョン</p> <p>Java を最新バージョンにアップグレードした場合は、<code>/var/opt/snapcenter/etc/sp/etc/spl.properties</code> にある <code>JAVA_HOME</code> 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。</p>

サポートされているバージョンの最新情報については、を参照してください "[NetApp Interoperability Matrix Tool](#) で確認できます"。

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。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` 1.8.7 以降。
- `root` 以外のユーザが Oracle インストールグループに含まれていることを確認します。
- `/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 / sudo 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 SCCMD = sha224:checksum_value== /home/
SUDO_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
SUDO_USER/.sc_netapp/Linux_Prechecks.sh
SUDO_USER ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
Defaults: SUDO_USER env_keep=JAVA_HOME
Defaults: SUDO_USER !visiblepw
Defaults: SUDO_USER !requiretty

```

\_sudo\_user\_ は、作成した root 以外のユーザの名前です。

チェックサム値は、\_C : \ProgramData\NetApp\SnapCenter \Package Repository\_ にある \* ORACLE\_checksum.txt \* ファイルから取得できます。

カスタムの場所を指定した場合、場所は \_custom\_path \NetApp\SnapCenter \Package Repository\_ になります。



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。

\* ベストプラクティス：セキュリティ上の理由から、インストールまたはアップグレードのたびに sudo エントリを削除することを推奨します。

## 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 6.1 以降
ホスト上の SnapCenter プラグインの最小 RAM	4 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	1 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) 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、を参照してください "[NetApp Interoperability Matrix Tool](#) で確認できます”。

**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。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 1.8.7 以降。
- root 以外のユーザが Oracle インストールグループに含まれていることを確認します。
- /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。

```
Cmdn_Alias SCCMD = 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
Cmdn_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
AIX_USER ALL=(ALL) NOPASSWD:SETENV: SCCMD, PRECHECKCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

\_aix\_user\_ は、作成した root 以外のユーザの名前です。

チェックサム値は、\_C : \ProgramData\NetApp\SnapCenter \Package Repository\_ にある \* ORACLE\_checksum.txt \* ファイルから取得できます。

カスタムの場所を指定した場合、場所は \_custom\_path \NetApp\SnapCenter \Package Repository\_ になります。



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。

\* ベストプラクティス：セキュリティ上の理由から、インストールまたはアップグレードのたびに sudo エントリを削除することを推奨します。

## 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。

フィールド	手順
ユーザ名 / パスワード	<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</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>◦ NETBIOS_USERNAME_</li> <li>◦ _ドメイン FQDN\ユーザ名_</li> </ul> <li>ローカル管理者（ワークグループのみ）</li> <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せん。Username フィールドの有効な形式は、<i>username</i> です</p>
認証モード	<p>使用する認証モードを選択します。</p> <p>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。</p>
sudo 権限を使用する	<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>

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

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。

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	<p>ホストタイプとして「* Linux *」または「* AIX *」を選択します。</p> <p>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。</p> <p>SnapCenter</p>
ホスト名	<p>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。</p> <p>SnapCenter は、DNS の適切な設定によって異なります。そのため、FQDN を入力することを推奨します。</p> <p>次のいずれかの IP アドレスまたは FQDN を入力できます。</p> <ul style="list-style-type: none"> <li>• スタンドアロンホスト</li> <li>• Oracle Real Application Clusters（RAC）環境内の任意のノード</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  ノード VIP や SCAN IP はサポートされていません </div> <p>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。</p>
クレデンシャル	<p>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。</p> <p>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>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。</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  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。 </div>

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	<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。</p> <p>デフォルトのポート番号は 8145 です。SnapCenter サーバがカスタムポートにインストールされている場合は、そのポート番号がデフォルトポートとして表示されます。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  プラグインを手動でインストールし、カスタムポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理は失敗します。 </div>
インストールパス	<p>デフォルトパスは、 <code>_/opt/NetApp/snapcenter_</code> です。</p> <p>必要に応じて、パスをカスタマイズできます。</p>
Oracle RAC のすべてのホストを追加します	<p>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。</p> <p>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。</p>
インストール前のチェックをスキップします	<p>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。</p>

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。

- 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。

- 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。

- 終了後 \*

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。

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 \*

- PowerShell を起動します。
- 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。
- `_ 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。

- 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"](#)。

## Plug-in Package for Linux を対話的にインストールする

Linux ホスト上では、SnapCenter Plug-ins Package for Linux を対話的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 環境変数に、ウィザードを起動する Linux ホストの IP アドレスとポート番号を指定する必要があります。
  - 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 \Package Repository\_ 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. プラグインをインストールするホストにインストールファイルをコピーします。
3. コマンドプロンプトから、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、「./SnapCenter\_linux\_host\_plugin.bin -l swing」を実行します
4. ウィザードの指示に従って、プラグインパッケージをインストールします。
5. [完了] をクリックしてインストールを完了します。

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またはコンソールモードでインストールします

SnapCenter Plug-ins Package for Linux は、コンソールモードまたはコマンドラインインターフェイス（CLI）を使用して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. 使用するインストールモードに応じて、次のいずれかの手順を実行します。

インストールモード	手順
コンソールモード	<ol style="list-style-type: none"><li>a. を実行します  SnapCenter_linux_host_plugin.bin – l console</li><li>b. 画面の指示に従ってインストールを完了します。</li></ol>



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。

### 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操作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、次の手順に従います。
    - 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。

## 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。  指定可能な値は、INFO、DEBUG、TRACE、ERROR、FATAL、警告を表示します。
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 に設定されません。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せん。

パラメータ名	説明
SPL ポート	<p>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。</p> <p>デフォルト値がない場合は、値を追加できます。</p> <p> 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。</p>
SNAPCENTER_server_host が必要です	<p>SnapCenter サーバの IP アドレスまたはホスト名を表示します。</p>
SPL キーストアパス	<p>キーストアファイルの絶対パスを表示します。</p>
SNAPCENTER_SERVER_PORT	<p>SnapCenter サーバが稼働しているポート番号を表示します。</p>
logs_MAX_COUNT	<p>SnapCenter Plug-in Loader ログファイルのうち、<code>_/custom_location/snapcenter /spl/logs_folder</code> に保持されているファイルの数を表示します。</p> <p>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。</p> <p> <code>spl.properties</code> 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。</p>
JAVA_HOME にアクセスします	<p>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。</p> <p>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。</p>
LOG_MAX_SIZE	<p>ジョブログファイルの最大サイズを表示します。</p> <p>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。</p>
retain_logs_of_last_days	<p>ログを保持する日数が表示されます。</p>

パラメータ名	説明
enable_certificate_validationを実行します	<p>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。</p> <p>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。</p>

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。

- root ユーザとして SnapCenter Plug-in Loader サービスを開始します。

```
`/custom_location/NetApp/snapcenter/spl/bin/spl start`  
** SnapCenter Plug-in Loader サービスを停止します。
```

```
`/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。

```
`/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。
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl status`  
** SnapCenter Plug-in Loader サービスで変更を探します。
```

```
`/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
<AliasNameForCertificateToBeImported> -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 "<OriginalAliasName>" -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。

- 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。

## 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を示します ["NetApp Interoperability Matrix Tool で確認できます"](#)。

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。

<b>SnapManager for Oracle</b> および <b>SnapManager for SAP</b> から入手できます	を <b>SnapCenter</b> 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。

<b>SnapManager for Oracle</b> および <b>SnapManager for SAP</b> から入手できます	を <b>SnapCenter</b> に移動します
データベース	<p>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。</p> <p>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。</p>



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。

<b>SnapManager for Oracle</b> および <b>SnapManager for SAP</b> のパラメータと値	<b>SnapCenter</b> のパラメータと値	注：
バックアップの範囲 <ul style="list-style-type: none"> <li>• フル</li> <li>• データ</li> <li>• ログ</li> </ul>	バックアップの範囲 <ul style="list-style-type: none"> <li>• フル</li> <li>• データ</li> <li>• ログ</li> </ul>	
バックアップモード <ul style="list-style-type: none"> <li>• 自動</li> <li>• オンライン</li> <li>• オフラインです</li> </ul>	バックアップタイプ <ul style="list-style-type: none"> <li>• オンライン</li> <li>• オフラインシャットダウン</li> </ul>	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 <ul style="list-style-type: none"> <li>• 日</li> <li>• カウント</li> </ul>	保持 <ul style="list-style-type: none"> <li>• 日</li> <li>• カウント</li> </ul>	<p>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</p> <p>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。</p>

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 <ul style="list-style-type: none"> <li>• すべて</li> <li>• システム変更番号（SCN）</li> <li>• 日付</li> <li>• 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</li> </ul>	スケジュールのプルーニング <ul style="list-style-type: none"> <li>• すべて</li> <li>• 指定した時間および日数より前に作成されたログです</li> </ul>	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 <ul style="list-style-type: none"> <li>• 成功した処理のためにのみ送信される E メールです</li> <li>• 処理に失敗した場合にのみ送信される E メールです</li> <li>• 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</li> </ul>	通知 <ul style="list-style-type: none"> <li>• 常に</li> <li>• 失敗した場合</li> <li>• 警告</li> <li>• エラー</li> </ul>	E メール通知はインポートされません。  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。

1. インポートツールを実行する SnapManager ユーザーに、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。
2. 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-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 クレデンシャル・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。

3. `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利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的に停止されます。



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。

## SnapCenter Plug-in for VMware vSphere をインストール

データベースが仮想マシン（VM）に格納されている場合や VM とデータストアを保護する場合は、SnapCenter Plug-in for VMware vSphere 仮想アプライアンスを導入する必要があります。

導入の詳細については、を参照してください ["導入の概要"](#)。

### CA 証明書を導入する

SnapCenter Plug-in for VMware vSphere で CA 証明書を設定するには、を参照してください ["SSL 証明書を作成またはインポートします"](#)。

### CRL ファイルを設定します

SnapCenter Plug-in for VMware vSphere 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。VMware vSphere 用 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/config/crl_` です。

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。

## Oracle データベースの保護を準備する

バックアップ、クローニング、リストアなどのデータ保護処理を実行する場合は、事前に戦略を定義し、環境をセットアップする必要があります。また、SnapVault サーバで SnapMirror テクノロジーと SnapCenter テクノロジーを使用するように設定することもできます。

SnapVault テクノロジーと SnapMirror テクノロジーを活用するには、ストレージデバイス上のソースボリューム

とデスティネーションボリューム間のデータ保護関係を設定して初期化する必要があります。これらのタスクを実行するには、NetAppSystem Manager を使用するか、ストレージコンソールのコマンドラインを使用します。

Plug-in for Oracle Database を使用する前に、SnapCenter 管理者が SnapCenter Server のインストールと設定を行い、前提条件となるタスクを実行する必要があります。

- SnapCenter サーバをインストールして設定します。"詳細はこちら。"
- ストレージシステム接続を追加して SnapCenter 環境を設定します。"詳細はこちら。"



SnapCenter では、異なるクラスタにある同じ名前の SVM は複数サポートされません。SVM 登録またはクラスタ登録を使用して SnapCenter に登録する SVM は、それぞれ一意である必要があります。

- 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。"詳細はこちら。"
- ホストを追加し、プラグインをインストールし、リソースを検出します。
- VMware RDM LUN または VMDK に存在する Oracle データベースを SnapCenter Server で保護する場合は、SnapCenter Plug-in for VMware vSphere を導入して、SnapCenter にプラグインを登録する必要があります。
- Linux または AIX ホストに Java をインストールします。

を参照してください "[Linux ホストの要件](#)" または "[AIX ホストの要件](#)" を参照してください。

- アプリケーションファイアウォールのタイムアウト値は 3 時間以上に設定する必要があります。
- NFS 環境で Oracle データベースを使用している場合は、マウント、クローニング、検証、リストアの各処理を実行できるように、プライマリストレージまたはセカンダリストレージ用に少なくとも 1 つの NFS データ LIF を設定しておく必要があります。
- データパス（LIF）が複数ある場合、または dNFS 構成を使用している場合は、データベースホストで SnapCenter CLI を使用して次の作業を実行できます。
  - デフォルトでは、データベースホストのすべての IP アドレスが、クローンボリュームの Storage Virtual Machine（SVM）の NFS ストレージエクスポートポリシーに追加されます。特定の IP アドレスを使用する場合、または IP アドレスのサブセットに制限する場合は、Set-PreferredHostIPsInStorageExportPolicy CLI を実行します。
  - SVM に複数のデータパス（LIF）がある場合は、NFS クローンボリュームをマウントするための適切なデータパス（LIF）が SnapCenter によって選択されます。ただし、特定のデータパス（LIF）を指定する場合は、Set-SvmPreferredDataPath CLI を実行する必要があります。詳細については、コマンドリファレンスガイドを参照してください。
- SAN 環境で Oracle データベースを使用している場合は、次のガイドに記載された推奨事項に従って SAN 環境が設定されていることを確認してください。
  - "[Linux Unified Host Utilities の推奨されるホスト設定](#)"
  - "『[Using Linux Hosts with ONTAP storage](#)』を参照してください"
  - "[AIX Host Utilities の影響を受けるホスト設定](#)"
- Oracle Linux または RHEL 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管理（LVM）をインストールします。

- SnapManager for Oracle を使用していて、SnapCenter Plug-in for Oracle Database に移行する場合は、sccli コマンド sc-migrate を使用して、プロファイルを SnapCenter のポリシーおよびリソースグループに移行できます。
- バックアップレプリケーションが必要である場合は、ONTAP で SnapMirror と SnapVault を設定します

SnapCenter 4.1.1 ユーザの場合、SnapCenter Plug-in for VMware vSphere 4.1.1 のドキュメントには、仮想化されたデータベースとファイルシステムの保護に関する情報が記載されています。SnapCenter 4.2.x ユーザの場合、NetApp Data Broker 1.0 および 1.0.1 のドキュメントでは、Linux ベースの NetApp Data Broker 仮想アプライアンス（オープン仮想アプライアンス形式）が提供する SnapCenter Plug-in for VMware vSphere を使用して、仮想化されたデータベースとファイルシステムを保護する方法について説明しています。SnapCenter 4.3.x を使用する場合は、Linux ベースの SnapCenter Plug-in for VMware vSphere 仮想アプライアンス（オープン仮想アプライアンス形式）を使用して仮想化されたデータベースとファイルシステムを保護する方法について、SnapCenter Plug-in for VMware vSphere 4.3 のドキュメントを参照してください。

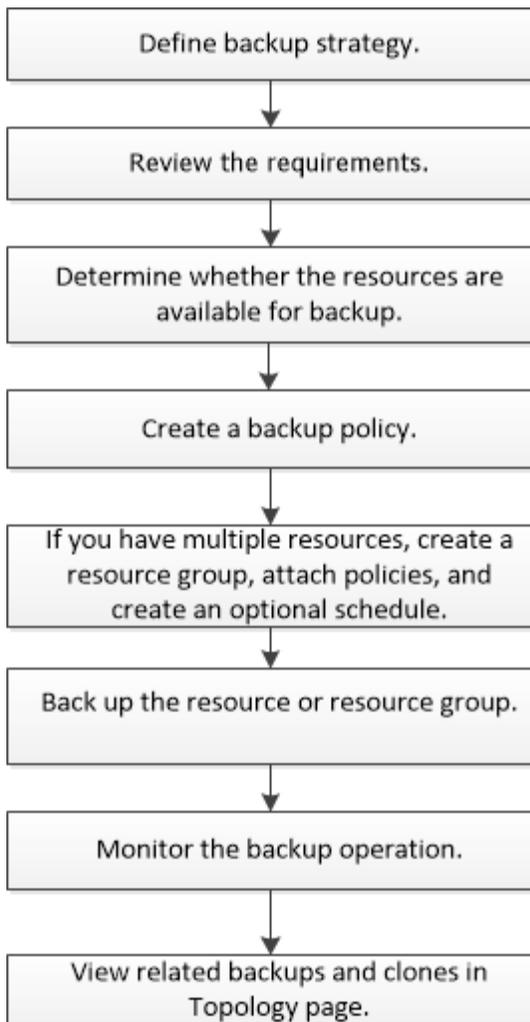
- 詳細はこちら \*
- ["Interoperability Matrix Tool で確認してください"](#)
- ["SnapCenter Plug-in for VMware vSphere のドキュメント"](#)
- ["RHEL 7 以降の非マルチパス環境でデータ保護処理が失敗する"](#)

## Oracle データベースをバックアップする

### バックアップのワークフロー

リソース（データベース）またはリソースグループのバックアップを作成することができます。バックアップのワークフローには、計画、バックアップするリソースの特定、バックアップポリシーの作成、リソースグループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



Oracle データベースのバックアップを作成する際に、データベースで複数の処理が実行されないようにするために、Oracle データベースホスト上に運用ロックファイル（.SM\_LOCK\_dbsid）を作成します。このファイルは、\_ORACLE\_HOME/dbs\_directory に作成されます。処理ロックファイルは、データベースのバックアップが完了すると自動的に削除されます。

ただし、前回のバックアップが警告付きで完了していた場合、処理ロックファイルが削除されず、次のバックアップ処理が待機キューに登録される可能性があります。\*.SM\_LOCK\_dbsid \* ファイルが削除されていない場合、このファイルは最終的にはキャンセルされる可能性があります。このような場合は、次の手順に従って操作ロックファイルを手動で削除する必要があります。

1. コマンドプロンプトから、\_ORACLE\_HOME/dbs に移動します。
2. 操作ロックを削除します：`rm -rf .SM_lock_dbsid.`

## Oracle データベースのバックアップ戦略を定義する

バックアップジョブを作成する前にバックアップ戦略を定義しておくことで、データベースの正常なリストアやクローニングに必要なバックアップを確実に作成できます。バックアップ戦略の大部分は、サービスレベルアグリーメント（SLA）、目標復旧時間（RTO）、および目標復旧時点（RPO）によって決まります。

SLA では、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処するために必要なサ

ービスレベルを定義します。RTO は、サービスの停止からビジネスプロセスの復旧までに必要となる時間です。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA、RTO、および RPO は、データ保護戦略に関与します。

バックアップ対象としてサポートされる **Oracle** データベース構成

SnapCenter では、各種の Oracle データベース構成のバックアップがサポートされます。

- Oracle スタンドアロン構成
- Oracle Real Application Clusters ( RAC )
- Oracle スタンドアロンレガシーです
- Oracle スタンドアロンコンテナデータベース ( CDB )
- Oracle Data Guard スタンバイ

Data Guard スタンバイデータベースのオフラインマウントバックアップだけを作成できます。オフラインシャットダウンバックアップ、アーカイブログのみのバックアップ、およびフルバックアップはサポートされていません。

- Oracle Active Data Guard スタンバイ

Active Data Guard スタンバイデータベースのオンラインバックアップだけを作成できます。アーカイブログのみのバックアップとフルバックアップはサポートされていません。



Data Guard スタンバイデータベースまたは Active Data Guard スタンバイデータベースのバックアップを作成する前に、管理されたリカバリプロセス ( MRP ) が停止し、バックアップが作成されたあとに MRP が開始されます。

- Automatic Storage Management ( ASM ; 自動ストレージ管理)
  - 仮想マシンディスク ( VMDK ) 上の ASM スタンドアロンおよび ASM RAC



Oracle データベースでサポートされるどのリストア方式でも、VMDK 上で実行できるのは ASM RAC データベースの Connect and Copy リストアだけです。

- raw デバイスマッピング ( RDM ) 上の ASM スタンドアロンおよび ASM RAC では、ASM 上の Oracle データベースに対して、ASMLib の有無に関係なく、バックアップ、リストア、クローニングの各処理を実行できます。
- Oracle ASM フィルタドライバ ( ASMFD )



PDB 移行処理と PDB クローニング処理はサポートされていません。

- Oracle Flex ASM

サポートされている Oracle の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"。

## Oracle データベースでサポートされるバックアップのタイプ

バックアップタイプでは、作成するバックアップのタイプを指定します。SnapCenter では、Oracle データベースに対してオンラインバックアップタイプとオフラインバックアップタイプがサポートされます。

### オンラインバックアップ

データベースがオンライン状態のときに作成されるバックアップを、オンラインバックアップと呼びます。ホットバックアップとも呼ばれるオンラインバックアップでは、データベースをシャットダウンすることなくバックアップを作成できます。

オンラインバックアップでは、次のファイルのバックアップを作成できます。

- データファイルと制御ファイルのみ
- アーカイブログファイルのみ（この場合はデータベースがバックアップモードになりません）
- データファイル、制御ファイル、アーカイブログファイルを含むフルデータベース

### オフラインバックアップ

データベースがマウント済み状態またはシャットダウン状態のときに作成されるバックアップを、オフラインバックアップと呼びます。オフラインバックアップはコールドバックアップとも呼ばれます。オフラインバックアップにはデータファイルと制御ファイルのみを含めることができます。オフラインマウントバックアップまたはオフラインシャットダウンバックアップのいずれかを作成できます。

- オフラインマウントバックアップを作成する場合は、データベースがマウント済み状態であることを確認する必要があります。

データベースがそれ以外の状態の場合は、バックアップ処理が失敗します。

- オフラインシャットダウンバックアップを作成する場合、データベースはどの状態でもかまいません。

データベースは、バックアップを作成するために必要な状態に変更されます。バックアップが作成されると、データベースは元の状態に戻ります。

## SnapCenter による Oracle データベースの検出方法

「リソース」とは、SnapCenter で管理されているホスト上の Oracle データベースのことです。使用可能なデータベースを検出したあとに、それらの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できます。SnapCenter がさまざまなタイプやバージョンの Oracle データベースを検出するプロセスについて理解しておく必要があります。

Oracle バージョン 11__ ~ 12_c_R1	Oracle バージョン 12_c_R2 から 18_c_c__
*RAC データベース *: RAC データベースは /etc/oratab エントリに基づいてのみ検出されます。  /etc/oratab ファイル内にデータベース・エントリが必要です。	*RAC データベース *: srvctl config コマンドを使用して RAC データベースが検出されます。

Oracle バージョン 11__ ~ 12_c_R1	Oracle バージョン 12_c_R2 から 18_c_c__
<ul style="list-style-type: none"> <li>• スタンドアロン * : スタンドアロン・データベースは、 /etc/oratab エントリに基づいてのみ検出されます。</li> </ul> <p>/etc/oratab ファイル内にデータベース・エントリが必要です。</p>	<ul style="list-style-type: none"> <li>• Standalone * : /etc/oratab ファイル内のエントリおよび srvctl config コマンドの出力に基づいて、スタンドアロンデータベースが検出されません。</li> </ul>
<p><b>ASM:</b> ASM インスタンス・エントリは、 /etc/oratab ファイル内に存在する必要があります。</p>	<p><b>ASM:</b> ASM インスタンス・エントリは、 /etc/oratab ファイル内に存在する必要はありません。</p>
<ul style="list-style-type: none"> <li>• RAC One Node * : RAC One Node データベースは、 /etc/oratab エントリに基づいてのみ検出されます。</li> </ul> <p>データベースは、 <i>nomount</i>、 <i>mount</i>、 または <i>_open_state</i> のいずれかである必要があります。 /etc/oratab ファイル内にデータベース・エントリが必要です。</p> <p>データベースがすでに検出され、バックアップが関連付けられている場合、 RAC One Node データベースのステータスは「Renamed」または「deleted」とマークされます。</p> <p>データベースを再配置する場合は、次の手順を実行する必要があります。</p> <ol style="list-style-type: none"> <li>1. フェイルオーバーが発生した RAC ノードの /etc/oratab ファイルに、再配置されたデータベース・エントリを手動で追加します。</li> <li>2. リソースを手動で更新する。</li> <li>3. リソースページから RAC One Node データベースを選択し、 * Database Settings * (データベース設定) をクリックします。</li> <li>4. データベースを設定して、データベースを現在ホストしている RAC ノードに優先クラスタノードを設定します。</li> <li>5. SnapCenter 処理を実行します。</li> </ol> <div style="border-left: 1px solid black; padding-left: 10px; margin-top: 20px;"> <p> あるノードから別のノードにデータベースを再配置した場合、および以前のノード内の oratab エントリが削除されていない場合は、同じデータベースが 2 回表示されないように、 oratab エントリを手動で削除する必要があります。</p> </div>	<ul style="list-style-type: none"> <li>• RAC One Node * : srvctl config コマンドのみを使用して、 RAC One Node データベースを検出します。</li> </ul> <p>データベースは、 <i>nomount</i>、 <i>mount</i>、 または <i>_open_state</i> のいずれかである必要があります。データベースがすでに検出され、バックアップが関連付けられている場合、 RAC One Node データベースのステータスは「Renamed」または「deleted」とマークされます。</p> <p>データベースを再配置する場合は、次の手順を実行する必要があります。</p> <ol style="list-style-type: none"> <li>1. リソースを手動で更新する。</li> <li>2. リソースページから RAC One Node データベースを選択し、 <b>Database Settings</b> をクリックします。</li> <li>3. データベースを設定して、データベースを現在ホストしている RAC ノードに優先クラスタノードを設定します。</li> <li>4. SnapCenter 処理を実行します。</li> </ol>



/etc/oratab ファイル内に Oracle 12\_c\_R2 および 18\_c\_database のエントリがあり、同じデータベースが `srvctl config` コマンドで登録されている場合、SnapCenter は重複するデータベースエントリを削除します。古いデータベースエントリがある場合は、データベースは検出されますが、データベースにアクセスできず、ステータスはオフラインになります。

## RAC セットアップで優先ノードを指定します

Oracle Real Application Clusters ( RAC ) セットアップでは、バックアップ処理が実行される優先ノードを指定できます。優先ノードを指定しない場合は、SnapCenter によって自動的に優先ノードが割り当てられ、そのノードにバックアップが作成されます。

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、これらの優先ノードで優先順位に従ってトリガされます。

例：RAC データベース `cdbrac` に 3 つのインスタンスがあります。 `cdbrac1 on node1`、 `cdbrac2 on node2`、および `cdbrac3 on node3`。 `node1` インスタンスと `node2` インスタンスが優先ノードとして設定され、 `node2` に最初の優先順位、 `node1` に 2 番目の優先順位が指定されます。バックアップ処理を実行すると、まず第 1 優先ノードである `node2` で処理が試行されます。 `node2` がバックアップの状態になっていない場合は、プラグインエージェントがホストで実行されていないなどの複数の理由で、ホスト上のデータベースインスタンスが指定したバックアップタイプに必要な状態になっていない可能性があります。または、FlexASM 構成内の `node2` 上のデータベースインスタンスがローカル ASM インスタンスで提供されていない場合は、 `node1` で処理が試行されます。 `node3` は、優先ノードのリストに含まれていないため、バックアップには使用されません。

Flex ASM 設定では、カード濃度が RAC クラスタ内のノード数より少ない場合、リーフノードは優先ノードとして表示されません。Flex ASM クラスタノードのロールに変更がある場合は、優先ノードが更新されるように、手動で検出する必要があります。

### 必要なデータベースの状態

バックアップを正常に完了するには、優先ノード上の RAC データベースインスタンスが必要な状態であることが必要です。

- オンラインバックアップを作成する場合は、設定された優先ノードの RAC データベースインスタンスの 1 つがオープン状態であることが必要です。
- オフラインマウントバックアップを作成する場合は、設定された優先ノードの RAC データベースインスタンスの 1 つがマウント状態であり、かつ他の優先ノードを含むその他すべてのインスタンスがマウント状態またはそれより低いレベルの状態であることが必要です。
- オフラインシャットダウンバックアップを作成する場合は、RAC データベースインスタンスはどの状態でもかまいませんが、優先ノードを指定する必要があります。

## Oracle Recovery Manager を使用してバックアップをカタログ化する方法

Oracle Recovery Manager ( RMAN ) で Oracle データベースのバックアップをカタログ化することにより、Oracle RMAN リポジトリにバックアップ情報を保存できます。

カタログ化されたバックアップは、あとでブロックレベルのリストア処理や表領域のポイントインタイムリカバリ処理に使用できます。カタログ化されたバックアップが不要となった場合は、カタログ情報を削除できます。

カタログ化するためには、データベースの状態が少なくともマウント済み状態であることが必要です。カタログ化を実行できるのは、データバックアップ、アーカイブログバックアップ、およびフルバックアップです。

複数のデータベースを含むリソースグループのバックアップに対してカタログ化を有効にすると、データベースごとにカタログ化が実行されます。Oracle RAC データベースの場合は、データベースが少なくともマウント済み状態にある優先ノードでカタログ化が実行されます。



RAC データベースのバックアップをカタログ化する場合は、そのデータベースに対して他のジョブが実行されていないことを確認します。別のジョブが実行されている場合は、カタログ化処理がキューに登録されずに失敗します。

デフォルトでは、ターゲットデータベースの制御ファイルがカタログ化に使用されます。外部カタログデータベースを追加する場合は、SnapCenter グラフィカルユーザーインターフェース（GUI）のデータベース設定ウィザードを使用して、外部カタログの資格情報と透過ネットワーク印刷材（TNS）名を指定して構成できます。CLI から外部カタログデータベースを設定するには、Configure-SmOracleDatabase コマンドで -OracleRmanCatalogCredentialName オプションおよび -OracleRmanCatalogTnsName オプションを実行します。

SnapCenter GUI から Oracle バックアップポリシーを作成する際にカタログ化オプションを有効にした場合は、バックアップ処理の一環として Oracle RMAN を使用してバックアップがカタログ化されます。バックアップのカタログ化は、Catalog-SmBackupWithOracleRMAN コマンドを実行して遅延させることもできます。バックアップをカタログ化したら、Get-SmBackupDetails コマンドを実行して、カタログ化されたデータファイルのタグ、制御ファイルカタログのパス、カタログ化されたアーカイブログの場所などのカタログ化されたバックアップ情報を取得できます。

SnapCenter 3.0 では、ASM ディスクグループ名が 16 文字以上である場合、バックアップに使用される命名形式は SC\_HASHCODEofDISKGROUP\_DBSID\_backupid です。ただし、ディスク・グループ名が 16 文字未満の場合、バックアップに使用される命名形式は DISKGROUPNAME\_DBSID\_backupid です。これは、SnapCenter 2.0 で使用される形式と同じです。



HASHCODEofDISKGROUP は、各 ASM ディスクグループに固有の自動生成番号（2～10桁）です。

バックアップに関する RMAN リポジトリ情報が古くなってバックアップのリポジトリレコードがその物理ステータスと一致しなくなった場合は、クロスチェックを実行してリポジトリ情報を更新できます。たとえば、ユーザがオペレーティングシステムコマンドでディスクからアーカイブログを削除した場合、実際にはディスクにログがないにもかかわらず、制御ファイルにはディスクにログがあることが示されます。クロスチェック処理では、制御ファイルを情報で更新できます。クロスチェックをイネーブルにするには、Set-SmConfigSettings コマンドを実行して、enable\_croschck パラメータに値 true を割り当てます。デフォルト値は FALSE です。

```
'scli Set-SmConfigSettings - ConfigSettingsTypePlugin - PluginCodeSCO-ConfigSettings"  
key=enable_CROSCHECK、 value=true"
```

カタログ情報を削除するには、Uncatalog-SmBackupWithOracleRMAN コマンドを実行します。SnapCenter GUI ではカタログ情報を削除できません。ただし、バックアップを削除するとき、またはカタログ化されたバックアップに関連する保持設定とリソースグループを削除するときに、カタログ化されたバックアップの情報も削除されます。



SnapCenter ホストを強制的に削除する場合は、そのホストに関連するカタログ化されたバックアップの情報が削除されません。ホストを強制的に削除する場合は、事前にそのホストに関連するすべてのカタログ化されたバックアップの情報を削除しておく必要があります。

ORACLE\_PLUGIN\_RMAN\_CATALOG\_TIMEOUT パラメータに指定されたタイムアウト値を超えたためにカタログ化とカタログ解除が失敗した場合は、次のコマンドを実行して、パラメータの値を変更する必要があります。

ます。

```
`/opt/NetApp/snapcenter /spl/bin/sccli Set-SmConfigSettings - 構成設定タイププラグイン - プラグインコード  
sc-ConfigSettings" key=oracle_plugin_rman_catala_catalog_timeout、 value=user_defined_value"
```

パラメータの値を変更したら、次のコマンドを実行して SnapCenter Plug-in Loader (SPL) サービスを再起動します。

```
`/opt/NetApp/SnapCenter /spl/bin/spl restart
```

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 コマンド `_name` を実行して取得できます。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リファレンスガイド](#)"。

## バックアップスケジュール

バックアップ頻度 (スケジュールタイプ) はポリシーで指定され、バックアップスケジュールはリソースグループの設定で指定されます。バックアップの頻度またはスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率とデータの重要性です。使用頻度の高いリソースは 1 時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは 1 日に 1 回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービスレベルアグリーメント (SLA)、目標復旧時点 (RPO) などがあります。

SLA は、想定されるサービスのレベルを定義し、サービスの可用性やパフォーマンスなど、サービス関連の多くの問題に対処します。RPO は、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA と RPO は、データ保護戦略に関与します。

使用頻度の高いリソースであっても、フルバックアップは 1 日に 1~2 回で十分です。たとえば、定期的なトランザクションログバックアップを実行すれば、必要なバックアップが作成されます。データベースをバックアップする回数が多いほど、リストア時に SnapCenter が使用する必要のあるトランザクションログの数が少なくなります。これにより、リストア処理の時間を短縮できます。

バックアップスケジュールには、次の 2 つの要素があります。

- バックアップ頻度

バックアップ頻度 (バックアップを実行する間隔) は、ポリシー設定の一部であり、一部のプラグインでは `_schedule type` と呼ばれます。ポリシーでは、バックアップ頻度として、毎時、毎日、毎週、または毎月を選択できます。頻度を選択しない場合は、オンデマンドのみのポリシーが作成されます。ポリシーにアクセスするには、`* Settings * > * Policies *` をクリックします。

- バックアップスケジュール

バックアップスケジュール (バックアップが実行される日時) は、リソースグループの設定の一部です。たとえば、リソースグループのポリシーで週に 1 回のバックアップが設定されている場合は、毎週木曜日の午後 10 時にバックアップが実行されるようにスケジュールを設定できます。リソースグループのスケジュールにアクセスするには、`* リソース * > * リソースグループ *` をクリックします。

## バックアップの命名規則

Snapshot コピーのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則では Snapshot コピー名にタイムスタンプが追加されるため、コピーが作成されたタイミングを特定できます。

Snapshot コピーでは、次のデフォルトの命名規則が使用されます。

「resourcegroupname\_hostname\_timestamp」

バックアップリソースグループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- `_dts1_` は リソースグループ名です。
- `mach1x88` はホスト名です。
- `03-12-2015_23.17.26` は日付とタイムスタンプです。

または、「\* Snapshot コピーにカスタム名形式を使用」を選択して、リソースまたはリソースグループを保護しながら Snapshot コピー名の形式を指定することもできます。たとえば、`customtext_resourcegroup_policy_hostname` や `resourcegroup_hostname` などの形式です。デフォルトでは、Snapshot コピー名にタイムスタンプのサフィックスが追加されます。

#### バックアップ保持オプション

バックアップコピーを保持する日数を選択するか、保持するバックアップコピーの数を指定できます。指定できる最大数は ONTAP で 255 個です。たとえば、組織の必要に応じて、10 日分のバックアップコピーや 130 個のバックアップコピーを保持できます。

ポリシーを作成する際に、バックアップタイプおよびスケジュールタイプの保持オプションを指定できます。

SnapMirror レプリケーションを設定すると、デスティネーションボリュームに保持ポリシーがミラーリングされます。

SnapCenter は、保持されているバックアップの保持ラベルがスケジュールタイプと一致する場合には、バックアップを削除します。リソースまたはリソースグループに対してスケジュールタイプが変更された場合、古いスケジュールタイプラベルのバックアップがシステムに残ることがあります。



バックアップコピーを長期にわたって保持する場合は、SnapVault バックアップを使用する必要があります。

プライマリストレージボリュームまたはセカンダリストレージボリュームを使用してバックアップコピーを検証する

プライマリストレージボリュームまたは SnapMirror または SnapVault セカンダリストレージボリュームでバックアップコピーを検証することができます。セカンダリストレージボリュームを使用して検証を実行すると、プライマリストレージボリュームの負荷が軽減されます。

プライマリストレージボリュームまたはセカンダリストレージボリュームにあるバックアップを検証すると、すべてのプライマリ Snapshot コピーとセカンダリ Snapshot コピーが検証済みとマークされます。

SnapMirror および SnapVault セカンダリストレージボリューム上のバックアップコピーを検証するには、SnapRestore ライセンスが必要です。

## Oracle データベースをバックアップに使用できるかどうかを確認します

リソースとは、SnapCenter で管理されているホスト上の Oracle データベースのことです。使用可能なデータベースを検出したあとに、それらの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できます。

- 必要なもの \*
- SnapCenter サーバのインストール、ホストの追加、ストレージシステム接続の作成、クレデンシャルの追加などのタスクを完了しておく必要があります。
- データベースが仮想マシンディスク（VMDK）または raw デバイスマッピング（RDM）上にある場合は、SnapCenter Plug-in for VMware vSphere を導入し、SnapCenter にプラグインを登録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 "[SnapCenter Plug-in for VMware vSphere を導入](#)"。

- データベースが VMDK ファイルシステムにある場合は、vCenter にログインして \* VM オプション \* > \* Advanced \* > \* Edit configuration \* に移動し、VM の DISK.enableUUID\_true の値を設定しておく必要があります。
- SnapCenter データベースのさまざまなタイプやバージョンを検出するための、Oracle のプロセスを確認しておく必要があります。
- このタスクについて \*

プラグインをインストールすると、その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。

データベースが検出されるためには、データベースが少なくともマウント済み状態であることが必要です。Oracle Real Application Clusters（RAC）環境で、検出が実行されるホスト内の RAC データベースインスタンスが検出されるためには、データベースインスタンスが少なくともマウント済み状態であることが必要です。リソースグループには、正常に検出されたデータベースのみを追加できます。

ホスト上で Oracle データベースを削除した場合、SnapCenter サーバは認識しないため、削除されたデータベースのリストが表示されます。SnapCenter リソースのリストを更新するには、リソースを手動で更新する必要があります。

- 手順 \*
- 1. 左側のナビゲーションペインで、\* 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。

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。次に、をクリックします  アイコンをクリックして、フィルタペインを閉じます。

3. [リソースの更新] をクリックします。

RAC One Node シナリオでは、データベースが現在ホストされているノード上の RAC データベースとして検出されます。

- 結果 \*

データベースは、データベースタイプ、ホストまたはクラスタ名、関連するリソースグループとポリシー、ステータスなどの情報とともに表示されます。

- データベースがネットアップ以外のストレージシステム上にある場合、ユーザインターフェイスの総合的なステータス列にはバックアップに使用できないメッセージが表示されます。

ネットアップ以外のストレージシステム上のデータベースには、データ保護処理を実行できません。

- データベースがネットアップストレージシステム上にあり、保護されていない場合は、ユーザインターフェイスの総合的なステータス列に Not protected というメッセージが表示されます。
- データベースがネットアップストレージシステム上にあり、保護されている場合、ユーザインターフェイスの総合的なステータス列には、バックアップに使用可能なメッセージが表示されます。



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。

## Oracle データベースのバックアップポリシーの作成

SnapCenter を使用して Oracle データベースリソースをバックアップする前に、バックアップ対象のリソースまたはリソースグループのバックアップポリシーを作成する必要があります。バックアップポリシーとは、バックアップを管理、スケジューリング、および保持する方法を定めた一連のルールです。レプリケーション、スクリプト、バックアップタイプの設定を指定することもできます。ポリシーを作成することで、別のリソースやリソースグループでポリシーを再利用して時間を節約することができます。

- 必要なもの \*
- バックアップ戦略を定義しておく必要があります。
- SnapCenter のインストール、ホストの追加、データベースの検出、ストレージシステム接続の作成などのタスクを実行して、データ保護の準備をしておく必要があります。
- Snapshot コピーをミラーセカンダリストレージまたはバックアップセカンダリストレージにレプリケートするユーザには、SnapCenter 管理者がユーザに対してソースとデスティネーションの両方のボリューム用に SVM 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、[\* ポリシー \*] をクリックします。
3. ドロップダウン・リストから「\* Oracle Database \*」を選択します。
4. [新規作成 (New)] をクリックする。
5. [名前] ページで、ポリシー名と概要を入力します。
6. [Backup Type] ページで、次の手順を実行します。

- オンライン・バックアップ \* を作成する場合は、\* オンライン・バックアップ \* を選択します。

バックアップの対象として、すべてのデータファイル、制御ファイル、アーカイブログファイル、データファイルと制御ファイル、またはアーカイブログファイルのみを指定する必要があります。

ます。

- オフライン・バックアップ\* を作成する場合は、\* オフライン・バックアップ\* を選択し、次のいずれかのオプションを選択します。
  - データベースがマウント状態のときにオフラインバックアップを作成する場合は、\* Mount\* を選択します。
  - データベースをシャットダウン状態に変更してオフラインシャットダウンバックアップを作成する場合は、\* Shutdown\* を選択します。

Pluggable Database (PDB) がある場合、バックアップ作成前に PDB の状態を保存するには、「\* PDB の状態を保存」を選択する必要があります。これにより、バックアップ作成後に PDB を元の状態に戻すことができます。

- オンデマンド\*、\* 毎時\*、\* 毎日\*、\* 毎週\*、または\* 毎月\* を選択して、スケジュールの頻度を指定します。



リソースグループを作成する際に、バックアップ処理のスケジュール（開始日と終了日）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソースグループを作成できますが、各ポリシーに異なるバックアップスケジュールを割り当てることもできます。



午前 2 時にスケジュールを設定した場合、夏時間（DST）中はスケジュールはトリガーされません。

- Oracle Recovery Manager (RMAN) を使用してバックアップをカタログ化する場合は、[\* Catalog backup with Oracle Recovery Manager (RMAN) \*] を選択します。

一度に 1 つのバックアップのカタログ化を実行するには、GUI を使用するか、SnapCenter CLI コマンド Catalog-SmBackupWithOracleRMAN を使用します。



RAC データベースのバックアップをカタログ化する場合は、そのデータベースに対して他のジョブが実行されていないことを確認します。別のジョブが実行されている場合は、カタログ化処理がキューに登録されずに失敗します。

- バックアップ後にアーカイブ・ログのプルーニングを行う場合は、バックアップ後にアーカイブ・ログをプルーニング\* を選択します。



データベースで設定されていないアーカイブ・ログ・デスティネーションからのアーカイブ・ログの削除は、スキップされます。



Oracle Standard Edition を使用している場合は、アーカイブログのバックアップ中に log\_archive\_dest パラメータと log\_archive\_duplex\_dest パラメータを使用できません。

- アーカイブログを削除できるのは、アーカイブログファイルをバックアップの一部として選択した場合だけです。



削除処理を正常に行うには、RAC 環境のすべてのノードがすべてのアーカイブログの場所にアクセスできることを確認する必要があります。

状況	作業
すべてのアーカイブログを削除します	[Delete all archive logs*] を選択します。
古いアーカイブログを削除します	「* 次より古いアーカイブログを削除」を選択し、削除するアーカイブログの経過時間を日数と時間数で指定します。
すべてのデスティネーションからアーカイブログを削除します	すべての保存先からアーカイブ・ログを削除する*を選択します。
バックアップの一部であるログデスティネーションからアーカイブログを削除します	[* バックアップの一部である保存先からアーカイブ・ログを削除する*]を選択します。

Prune archive logs after backup

**Prune log retention setting**

Delete all archive logs

Delete archive logs older than

**Prune log destination setting**

Delete archive logs from all the destinations

+  Delete archive logs from the destinations which are part of backup

7. [保持] ページで 'バックアップ・タイプ' の保持設定と [バックアップ・タイプ] ページで選択したスケジュール・タイプを指定します

状況	作業
----	----

<p>一定数の Snapshot コピーを保持します</p>	<p>保持する Snapshot コピーの総数 * を選択し、保持する Snapshot コピーの数を指定します。</p> <p>Snapshot コピーの数が指定した数を超えると、古いものから順に Snapshot コピーが削除されます。</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> 最大保持数は、ONTAP 9.4 以降のリソースでは 1018、ONTAP 9.3 以前のリソースでは 254 です。保持期間を基盤となる ONTAP バージョンの値よりも大きい値に設定すると、バックアップが失敗します。</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> SnapVault レプリケーションを有効にする場合は、保持数を 2 以上に設定する必要があります。保持数を 1 に設定すると、新しい Snapshot コピーがターゲットにレプリケートされるまで最初の Snapshot コピーが SnapVault 関係の参照 Snapshot コピーになるため、保持処理が失敗することがあります。</p> </div>
<p>Snapshot コピーを特定の日数だけ保持します</p>	<p>「* Snapshot コピーを保持する期間」を選択し、Snapshot コピーを削除するまで保持する日数を指定します。</p>



アーカイブログバックアップを保持できるのは、アーカイブログファイルをバックアップの一部として選択した場合だけです。

## 8. Replication (レプリケーション) ページで、レプリケーション設定を指定します。

フィールド	手順
<p>ローカル Snapshot コピーの作成後に SnapMirror を更新します</p>	<p>別のボリュームにバックアップセットのミラーコピーを作成する場合 ( SnapMirror レプリケーション) は、このフィールドを選択します。</p>
<p>ローカル Snapshot コピーの作成後に SnapVault を更新します</p>	<p>ディスクツーディスクのバックアップレプリケーション ( SnapVault バックアップ) を実行する場合は、このオプションを選択します。</p>

フィールド	手順
セカンダリポリシーのラベル	<p>Snapshot ラベルを選択します。</p> <p>選択した Snapshot コピーラベルに応じて、ONTAP はラベルに一致するセカンダリ Snapshot コピー保持ポリシーを適用します。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> ローカル Snapshot コピーの作成後に「* SnapMirror を更新」を選択した場合は、必要に応じてセカンダリポリシーラベルを指定できません。ただし、ローカル Snapshot コピーの作成後に「* Update SnapVault」を選択した場合は、セカンダリポリシーラベルを指定する必要があります。</p> </div>
エラー再試行回数	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。



セカンダリストレージでの Snapshot コピーの最大数に達しないように、ONTAP でセカンダリストレージの SnapMirror 保持ポリシーを設定する必要があります。

9. スクリプトページで、バックアップ処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

プリスクリプトとポストスクリプトは、`/var/opt/snapcenter /spl/scripts_or` に保存するか、このパス内の任意のフォルダに保存する必要があります。デフォルトでは、`/var/opt/snapcenter /spl/scripts_path` が読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は 60 秒です。

10. [Verification] ページで、次の手順を実行します。
  - a. 検証処理を実行するバックアップスケジュールを選択します。
  - b. 検証スクリプトのコマンドセクションで、検証処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

プリスクリプトとポストスクリプトは、`/var/opt/snapcenter /spl/scripts_or` に保存するか、このパス内の任意のフォルダに保存する必要があります。デフォルトでは、`/var/opt/snapcenter /spl/scripts_path` が読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は 60 秒です。

1. 概要を確認し、[完了] をクリックします。

## Oracle データベースのリソースグループを作成してポリシーを適用します

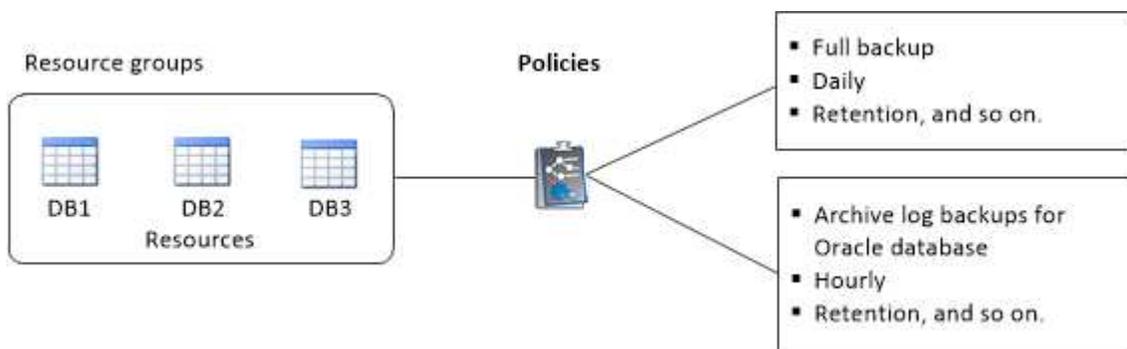
リソースグループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。リソースグループを使用すると、特定のアプリケーションに関連付けられているすべてのデータを同時にバックアップできます。

- このタスクについて \*

Oracle DBVERIFY ユーティリティを使用してバックアップを検証するには、ASM ディスクグループ上にファイルがあるデータベースが「mount」または「open」状態であることを確認する必要があります。

リソースグループに 1 つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義する必要があります。

次の図は、データベースのリソース、リソースグループ、およびポリシーの関係を示しています。



- 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、[\* 新しいリソースグループ \*] をクリックします。
3. [名前] ページで、次の操作を実行します。

フィールド	手順
名前	リソースグループの名前を入力します。   リソースグループ名は 250 文字以内にする必要があります。
タグ	リソースグループを検索するときに役立つラベルを入力します。  たとえば、複数のリソースグループに HR をタグとして追加すると、あとから HR タグに関連付けられたすべてのリソースグループを検索できます。

フィールド	手順
Snapshot コピーには、カスタムの名前形式を使用します	Snapshot コピー名にカスタムの名前形式を使用する場合は、このチェックボックスをオンにして名前形式を入力します。  たとえば 'customText_resource group_policy_hostname や resource group_hostname などですデフォルトでは、Snapshot コピー名の後ろにタイムスタンプが追加されます。
バックアップからアーカイブログデステーションを除外します	バックアップの対象から外すアーカイブログファイルのデステーションを指定します。

4. Resources ページで、\* Host \* ドロップダウン・リストから Oracle データベース・ホスト名を選択します。



リソースが Available Resources セクションに表示されるのは、リソースが正常に検出された場合のみです。最近リソースを追加した場合は、リソースリストを更新しないと、使用可能なリソースのリストにリソースが表示されません。

5. [使用可能なリソース ( Available Resources ) ] セクションからリソースを選択し、[ 選択したリソース ( Selected Resources ) ] セクションに移動する。



1つのリソースグループ内の Linux ホストと AIX ホストの両方からデータベースを追加することができます。

6. [Policies] ページで、次の手順を実行します。

- a. ドロップダウンリストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。

[ 選択したポリシーのスケジュールを設定 ] セクションに、選択したポリシーが一覧表示されます。

- b. \* をクリックします  \* スケジュールを設定するポリシーの [ スケジュールの設定 ] 列。

- c. [Add schedules for policy\_name] ウィンドウで、スケジュールを設定し、[OK] をクリックします。

ここで、\_policy\_name\_ は 選択したポリシーの名前です。

設定されたスケジュールは、[ 適用されたスケジュール ] 列に一覧表示されます。

サードパーティ製バックアップスケジュールが SnapCenter バックアップスケジュールと重複している場合、それらのバックアップスケジュールはサポートされません。

7. [Verification] ページで、次の手順を実行します。
  - a. Load locators \* (ロケータのロード) をクリックして、SnapMirror または SnapVault ポリ्यूームをロードし、セカンダリ・ストレージ上で検証を実行します。
  - b. \* をクリックします  \* Configure Schedules (スケジュールの設定) 列で、ポリシーのすべてのスケジュールタイプの検証スケジュールを設定します。
  - c. Add Verification Schedules\_policy\_name\_dialog box で、次の処理を実行します。

状況	手順
バックアップ後に検証を実行します	[Run verification after backup] を選択します。
検証をスケジュールします	[Run scheduled verification] を選択し、ドロップダウン・リストからスケジュール・タイプを選択します。

- d. セカンダリ・ストレージ・システムのバックアップを検証するには、セカンダリ・サイトで \* Verify on secondary location \* を選択します。
- e. [OK] をクリックします。

設定した検証スケジュールは、Applied Schedules 列にリスト表示されます。

8. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および Eメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、[ジョブレポートの添付 (Attach Job Report)] を選択します。



Eメール通知を利用する場合は、GUI または PowerShell コマンド Set-SmtpServer を使用して、SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、[完了] をクリックします。

## Oracle データベースをバックアップするための要件

Oracle データベースをバックアップする前に、前提条件を満たしていることを確認する必要があります。

- ポリシーを適用したリソースグループを作成しておく必要があります。
- セカンダリストレージとの SnapMirror 関係があるリソースをバックアップする場合、ストレージユーザに割り当てられた ONTAP ロールには「'SnapMirro all」権限を含める必要があります。ただし、「vsadmin」ロールを使用している場合、「'SnapMirro all」権限は必要ありません。
- バックアップ処理で使用されるアグリゲートを、データベースが使用する Storage Virtual Machine (SVM) に割り当てておく必要があります。
- データベースでセカンダリ保護が有効になっている場合は、そのデータベースに属するすべてのデータボリュームとアーカイブログボリュームが保護されていることを確認しておく必要があります。

- ASM ディスク・グループ上にファイルがあるデータベースが 'Oracle DBVERIFY ユーティリティを使用してバックアップを検証するには' マウント状態またはオープン状態であることを確認しておく必要があります
- ボリュームマウントポイントの長さが 240 文字を超えないことを確認しておく必要があります。
- バックアップするデータベースが大容量（TB 単位）の場合は、SnapCenter サーバホストで RESTTimeout の値を 86400000~in\_C : \Program Files\NetApp\SMCore \SMCoreServiceHost.exe.config\_file に増やしてください。

値を変更するときに実行中のジョブがないことを確認し、値を増やしたあとに SnapCenter SMCore サービスを再起動します。

## Oracle リソースのバックアップ

どのリソースグループにも含まれていないリソースは、のリソースページからバックアップすることができます。

- 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。

次に、\* をクリックします  \* をクリックすると、フィルタペインが閉じます。

4. バックアップするデータベースを選択します。

Database - Protect（データベース - 保護）ページが表示されます。

5. リソースページで、次の操作を実行します。

フィールド	手順
Snapshot コピーには、カスタムの名前形式を使用します	Snapshot コピー名にカスタムの名前形式を使用する場合は、このチェックボックスをオンにして名前形式を入力します。  たとえば 'customText_policy_hostname や resource_hostname などですデフォルトでは、Snapshot コピー名の後ろにタイムスタンプが追加されます。
バックアップからアーカイブログデスティネーションを除外します	バックアップの対象から外すアーカイブログファイルのデスティネーションを指定します。

6. [Policies] ページで、次の手順を実行します。

- a. ドロップダウンリストから 1 つ以上のポリシーを選択します。



また、\* をクリックしてポリシーを作成することもできます  \*

[ 選択したポリシーのスケジュールを設定 ] セクションに、選択したポリシーが一覧表示されます。

- b.  をクリックします  スケジュールを設定するポリシーの Configure Schedules (スケジュールの設定) 列。
- c. [Add schedules for policy\_name] ウィンドウで、スケジュールを設定し、[OK] をクリックします。

\_policy\_name\_ は、選択したポリシーの名前です。

設定されたスケジュールは、[ 適用されたスケジュール ] 列に一覧表示されます。

7. [Verification] ページで、次の手順を実行します。

- a. Load locators \* (ロケータのロード) をクリックして、SnapMirror または SnapVault ボリュームをロードし、セカンダリ・ストレージ上で検証を実行します。
- b.  をクリックします  Configure Schedules (スケジュールの設定) 列で、ポリシーのすべてのスケジュールタイプの検証スケジュールを設定します。
- c. Add Verification Schedules\_policy\_name\_dialog box で、次の処理を実行します。

状況	手順
バックアップ後に検証を実行します	[Run verification after backup] を選択します。
検証をスケジュールします	[Run scheduled verification] を選択し、ドロップダウン・リストからスケジュール・タイプを選択します。  <div style="border: 1px solid gray; padding: 5px; display: inline-block;">  Flex ASM 設定では、カードの数が RAC クラスタ内のノード数より少ない場合、リーフノードで検証操作を実行できません。 </div>

- d. セカンダリストレージ上のバックアップを検証するには、セカンダリストレージ上で \* Verify on secondary location \* を選択します。
- e. [OK] をクリックします。

設定した検証スケジュールは、Applied Schedules 列にリスト表示されます。

8. [ 通知 ] ページの [ 電子メールの設定 \* ] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および E メール の件名を指定する必要があります。リソ

ース上で実行されたバックアップ処理のレポートを添付する場合は、[ジョブレポートの添付]を選択します。



E メール通知を利用する場合は、GUI または PowerShell コマンド `Set-SmtpServer` を使用して、SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、[完了]をクリックします。

データベーストポロジのページが表示されます。

2. [今すぐバックアップ]をクリックします。

3. [バックアップ] ページで、次の手順を実行します。

- a. リソースに複数のポリシーを適用している場合は、「\* Policy \*」ドロップダウン・リストから、バックアップに使用するポリシーを選択します。

オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

- b. [バックアップ]をクリックします。

4. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

• 終了後 \*

- AIX のセットアップでは 'lkdev コマンドを使用してロックし 'rendev コマンドを使用して' バックアップされたデータベースが存在するディスクの名前を変更できません

デバイスのロックまたは名前変更は、そのバックアップを使用してリストアしても、リストア処理には影響しません。

- データベースクエリの実行時間がタイムアウト値を超えたためにバックアップ処理が失敗した場合は、`Set-SmConfigSettings` コマンドレットを実行して `ORACLE_SQL_QUERY_TIMEOUT` パラメータと `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` パラメータの値を変更します。

パラメータの値を変更したら、次のコマンド '`/opt/NetApp/snapcenter /spl/bin/spl restart`' を実行して、SnapCenter Plug-in Loader (SPL) サービスを再起動します

- ファイルにアクセスできず、検証プロセス中にマウントポイントを使用できないと、エラーコード `DBV-00100 specified file` が表示されて処理が失敗することがあります。sco.properties の `verification_delay` パラメータと `verification_retry_count` パラメータの値を変更する必要があります。

パラメータの値を変更したら、次のコマンド '`/opt/NetApp/snapcenter /spl/bin/spl restart`' を実行して、SnapCenter Plug-in Loader (SPL) サービスを再起動します

- MetroCluster 構成では、フェイルオーバー後に SnapCenter が保護関係を検出できない場合があります。
- VMDK 上のアプリケーションデータおよび SnapCenter Plug-in for VMware vSphere の Java ヒープサイズが不足している場合、バックアップが失敗することがあります。

Java のヒープサイズを増やすには、スクリプトファイル `/opt/NetApp/init_scripts/scvservice_.` を探します。このスクリプトでは、「do\_start method」コマンドは SnapCenter VMware プラグインサービスを起動します。このコマンドを次のように更新します：「`java -jar -Xmx8192M-Xms4096M`」

- 詳細はこちら \*
- "MetroCluster のフェイルオーバー後に SnapMirror 関係または SnapVault 関係を検出できません"
- "SnapCenter 処理では、Oracle RAC One Node データベースがスキップされます"
- "Oracle 12c ASM データベースの状態を変更できませんでした"
- "AIX システムでのバックアップ、リストア、クローニングの各処理のパラメータをカスタマイズできません"

## Oracle データベースのリソースグループをバックアップする

リソースグループは、ホストまたはクラスタ上のリソースの集まりです。リソースグループのバックアップ処理は、リソースグループに定義されているすべてのリソースを対象に実行されます。

リソースグループは、リソースページからオンデマンドでバックアップできます。リソースグループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

### • 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 [\* リソースグループ \*] を選択します。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、\* をクリックします。▼\* をクリックし、タグを選択します。次に、\* をクリックします。▼\* をクリックすると、フィルタペインが閉じます。

3. [リソースグループ] ページで、バックアップするリソースグループを選択し、[今すぐバックアップ \*] をクリックします。



2つのデータベースが統合されたリソースグループがある場合に、一方のデータベースのデータファイルがネットアップ以外のストレージにあると、もう一方のデータベースがネットアップストレージにあっても、バックアップ処理は中止されます。

4. [バックアップ] ページで、次の手順を実行します。
  - a. 複数のポリシーをリソースグループに関連付けている場合は、「\* Policy \*」ドロップダウンリストから、バックアップに使用するポリシーを選択します。

オンデマンドバックアップ用に選択したポリシーがバックアップスケジュールに関連付けられている場合は、スケジュールタイプに指定した保持設定に基づいてオンデマンドバックアップが保持されます。

- b. [バックアップ] をクリックします。

5. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

### • 終了後 \*

- AIX のセットアップでは 'lkdev コマンドを使用してロックし 'rendev コマンドを使用して' バックアップされたデータベースが存在するディスクの名前を変更できます

デバイスのロックまたは名前変更は、そのバックアップを使用してリストアしても、リストア処理には影響しません。

- データベースクエリの実行時間がタイムアウト値を超えたためにバックアップ処理が失敗した場合は、`Set-SmConfigSettings` コマンドレットを実行して `ORACLE_SQL_QUERY_TIMEOUT` パラメータと `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` パラメータの値を変更します。

パラメータの値を変更したら、次のコマンド '`/opt/NetApp/snapcenter /spl/bin/spl restart`' を実行して、SnapCenter Plug-in Loader (SPL) サービスを再起動します

- ファイルにアクセスできず、検証プロセス中にマウントポイントを使用できないと、エラーコード `DBV-00100 specified file` が表示されて処理が失敗することがあります。 `sco.properties` の `verification_delay` パラメータと `verification_retry_count` パラメータの値を変更する必要があります。

パラメータの値を変更したら、次のコマンド '`/opt/NetApp/snapcenter /spl/bin/spl restart`' を実行して、SnapCenter Plug-in Loader (SPL) サービスを再起動します

## UNIX コマンドを使用して Oracle データベースをバックアップします

バックアップのワークフローには、計画、バックアップするリソースの特定、バックアップポリシーの作成、リソースグループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

- 必要なもの \*
- ストレージシステム接続を追加し、 `SmStorageConnection_or_Add-SmCredential_` のコマンドを使用してクレデンシャルを作成しておく必要があります。
- `Command_Open-SmConnection_` を使用して SnapCenter サーバとの接続セッションを確立しておく必要があります。

SnapCenter アカウントでのログインセッションは 1 つしか確立できず、トークンはユーザのホームディレクトリに保存されます。



接続セッションは 24 時間のみ有効です。ただし、`TokenNeverExpires` オプションを使用して期限切れにならないトークンを作成し、セッションを常に有効にすることができます。

- このタスクについて \*

次のコマンドを実行して、SnapCenter サーバとの接続の確立、Oracle データベースインスタンスの検出、ポリシーとリソースグループの追加、バックアップの作成と検証を行います。

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、`Get-Help_command_name_` を実行して取得できます。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リファレンスガイド](#)"。

- 手順 \*
- 1. 指定されたユーザ用に SnapCenter サーバとの接続セッションを開始します： `Open-SmConnection`
- 2. ホストリソースの検出処理を実行します： `Get-SmResources`
- 3. Real Application Cluster (RAC) データベースのバックアップ処理に使用する Oracle データベースのクレデンシャルと優先ノードを設定します： `Configure - SmOracleDatabase`

4. バックアップポリシーを作成します。 *Add-SmPolicy*
5. セカンダリ（ SnapVault または SnapMirror ）ストレージの場所に関する情報を取得します： *get -SmSecondaryDetails*

このコマンドは、指定したリソースのプライマリストレージからセカンダリストレージへのマッピングの詳細を取得します。バックアップリソースグループを作成する際に、このマッピングの詳細を使用してセカンダリの検証を設定できます。

6. リソースグループを SnapCenter に追加します： *Add-SmResourceGroup*
7. バックアップを作成する： *New-SmBackup*

WaitForCompletion オプションを使用してジョブをポーリングすることができます。このオプションを指定した場合は、バックアップジョブが完了するまでコマンドが引き続きサーバをポーリングします。

8. SnapCenter からログを取得します： *Get-SmLogs*

## Oracle データベースのバックアップ処理を監視する

SnapCenterJobs ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、処理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、操作の対応する状態を示します。

-  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
-  キャンセルされました
- 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、次の手順を実行します。
    - a. をクリックします  バックアップ処理だけが表示されるようにリストをフィルタリングします。
    - b. 開始日と終了日を指定します。
    - c. [\* タイプ] ドロップダウン・リストから、 [\*Backup] を選択します。
    - d. [Status](ステータス \*) ドロップダウンから、バックアップステータスを選択します。
    - e. [適用 (Apply)] をクリックして、正常に完了した操作を表示する。

4. バックアップジョブを選択し、 [ \* 詳細 \* ] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスがと表示されます  で、ジョブの詳細をクリックすると、バックアップ処理の子タスクの一部がまだ実行中であるか、警告の兆候がマークされていることがわかります。

5. [ \* ジョブの詳細 \* ] ページで、 [ \* ログの表示 \* ] をクリックします。

**View logs** ボタンをクリックすると、選択した操作の詳細なログが表示されます。

**[Activity]** ペインでデータ保護操作を監視します

[ アクティビティ ( Activity ) ] パネルには、最近実行された 5 つの操作が表示されまた、操作が開始された日時と操作のステータスも表示されます。

[Activity (アクティビティ)] ペインには、バックアップ、リストア、クローン、およびスケジュールされたバックアップ処理に関する情報が表示されます。Plug-in for SQL Server または Plug-in for Exchange Server を使用している場合は、再シード処理に関する情報もアクティビティペインに表示されます。

• 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. をクリックします  をクリックして、最近の 5 つの操作を表示します。

いずれかの処理をクリックすると、その処理の詳細がジョブの詳細ページに表示されます。

## Oracle データベースのバックアップ処理をキャンセルします

実行中、キューに登録済み、または応答しないバックアップ処理をキャンセルできません。

バックアップ処理をキャンセルするには、SnapCenter 管理者またはジョブ所有者としてログインする必要があります。

• このタスクについて \*

バックアップ処理をキャンセルすると、SnapCenter サーバは処理を停止し、作成されたバックアップが SnapCenter サーバに登録されていない場合は、ストレージからすべての Snapshot コピーを削除します。バックアップがすでに SnapCenter サーバに登録されている場合、キャンセル後も、作成済みの Snapshot コピーはロールバックされません。

- キャンセルできるのは、キューに登録されたか実行中のログ処理またはフルバックアップ処理のみです。
- 検証の開始後に処理をキャンセルすることはできません。

検証前に処理をキャンセルした場合、処理はキャンセルされ、検証処理は実行されません。

- カタログ処理の開始後にバックアップ処理をキャンセルすることはできません。
- バックアップ処理は、Monitor (モニタ) ページまたは Activity (アクティビティ) ペインからキャンセ

ルできます。

- SnapCenter GUI に加え、CLI コマンドを使用して処理をキャンセルすることもできます。
- キャンセルできない操作に対しては、[ジョブのキャンセル] ボタンが無効になっています。
- ロールの作成中に 'このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できるようにする \* を選択した場合は 'そのロールを使用している間に '他のメンバーのキューに入っているバックアップ操作をキャンセルできます
- ステップ \*

次のいずれかを実行します。

方法	アクション
監視ページ	<ol style="list-style-type: none"><li>1. 左側のナビゲーションペインで、 * Monitor * &gt; * Jobs * をクリックします。</li><li>2. 操作を選択し、 * ジョブのキャンセル * をクリックします。</li></ol>
アクティビティペイン	<ol style="list-style-type: none"><li>1. バックアップジョブを開始したら、をクリックします  をクリックして、最近の 5 つの操作を表示します。</li><li>2. 処理を選択します。</li><li>3. [ジョブの詳細] ページで、 [* ジョブのキャンセル*] をクリックします。</li></ol>

- 結果 \*

処理がキャンセルされ、リソースが元の状態に戻ります。

キャンセル中または実行中の状態でキャンセルした処理が応答しない場合は、 `Cancel-SmJobID<int> -Force` を実行してバックアップ処理を強制的に停止する必要があります。

## Topology ページで、 Oracle データベースのバックアップとクローンを表示します

リソースのバックアップまたはクローニングを準備する際に、プライマリストレージとセカンダリストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

- このタスクについて \*

トポロジページでは、選択したリソースまたはリソースグループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を確認し、対象を選択してデータ保護処理を実行できます。

[コピーの管理] ビューの次のアイコンを確認して、プライマリストレージまたはセカンダリストレージ (ミラーコピーまたはバックアップコピー) でバックアップとクローンが使用可能かどうかを判断できます。

-



には、プライマリストレージ上にあるバックアップとクローンの数が表示されます。



には、SnapMirror テクノロジーを使用してセカンダリストレージにミラーリングされたバックアップとクローンの数が表示されます。



には、SnapVault テクノロジーを使用してセカンダリストレージにレプリケートされたバックアップとクローンの数が表示されます。

表示されるバックアップの数には、セカンダリストレージから削除されたバックアップも含まれます。たとえば、4つのバックアップだけを保持するポリシーを使用して6つのバックアップを作成した場合、バックアップの数は6と表示されます。



mirror-vault タイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数にはバージョンに依存しないバックアップは含まれません。

#### • 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 \*] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューでリソースを選択します。

リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. 概要カードを確認して、プライマリストレージとセカンダリストレージにあるバックアップとクローンの数をサマリで確認します。

サマリカードセクションには、バックアップとクローンの合計数とログバックアップの合計数が表示されます。

「\* Refresh \*」 ボタンをクリックすると、ストレージの照会が開始され、正確な数が表示されます。

5. [コピーの管理] ビューで、プライマリストレージまたはセカンダリストレージから \* バックアップ \* または \* クローン \* をクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、マウント、アンマウント、名前変更を実行します。カタログ化、カタログ化解除、および削除の各処理。



セカンダリストレージ上のバックアップは、名前変更または削除できません。

- ログバックアップを選択した場合は、名前変更、マウント、アンマウント、カタログ化解除、および DELETE 処理が含まれます。

- Oracle Recovery Manager (RMAN) を使用してバックアップをカタログ化した場合、そのカタログ化されたバックアップの名前は変更できません。

7. クローンを削除する場合は、表でクローンを選択し、をクリックします .

SnapmirrorStatusUpdateWaitTime に割り当てられた値がより小さい場合、データボリュームとログボリュームが正常に保護されても、ミラーとバックアップのバックアップコピーはトポロジページに表示されません。SnapmirrorStatusUpdateWaitTime に割り当てられた値は、\_Set-SmConfigSettings\_PowerShell コマンドレットを使用して増やす必要があります。

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、Get-Help\_command\_name\_ を実行して取得できます。

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リファレンスガイド](#)" または "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。

## データベースバックアップのマウントとアンマウント

バックアップ内のファイルにアクセスする必要がある場合は、1つまたは複数のデータベースバックアップおよびログのみのバックアップをマウントできます。バックアップは、バックアップが作成されたホストにも、同じタイプの Oracle およびホスト構成を使用するリモートホストにもマウントできます。バックアップを手動でマウントした場合は、処理の完了後にバックアップを手動でアンマウントする必要があります。任意のインスタンスで、データベースのバックアップを任意のホストにマウントできます。処理を実行する際には、バックアップを1つだけマウントできます。



Flex ASM 設定では、カードの数が RAC クラスタ内のノード数より少ない場合、リーフノードでマウント操作を実行できません。

### データベースバックアップをマウント

バックアップ内のファイルにアクセスする場合は、データベースバックアップを手動でマウントする必要があります。

- 必要なもの \*
- NFS 環境に Automatic Storage Management (ASM) データベースインスタンスがあり、ASM バックアップをマウントする場合は、ASM\_diskstring パラメータで定義されている既存のパスに ASM ディスクパス /var/opt/snapcenter /scors/backup\_\*/\*\*/\* を追加しておく必要があります。
- NFS 環境に ASM データベースインスタンスがあり、リカバリ操作の一環として ASM ログバックアップをマウントする場合は、ASM\_diskstring パラメータで定義されている既存のパスに ASM ディスクパス /var/opt/snapcenter /scu/clones/\*\_\* を追加しておく必要があります。
- ASM\_diskstring パラメータで、ASMFD または configure\_ORCL : \*\_ を使用する場合は、\_AFD : \*\_ を設定します。



asm\_diskstring パラメータの編集方法については、を参照してください "[asm\\_diskstring にディスクパスを追加する方法](#)"。

- バックアップのマウント時にソースデータベースホストと異なる ASM ポートを使用する場合は、ASM

のクレデンシャルと ASM ポートを設定する必要があります。

- 代替ホストにマウントする場合は、代替ホストが次の要件を満たしていることを確認する必要があります。
  - UID と GID が元のホストと同じである
  - Oracle のバージョンが元のホストと同じである
  - OS のディストリビューションとバージョンが元のホストと同じである
- iSCSIプロトコルとFCプロトコルが混在するigroupを使用して、LUNがAIXホストにマッピングされていないことを確認してください。詳細については、を参照してください "[LUNのデバイスを検出できませんというエラーが表示されて処理に失敗します](#)".

• 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 \*] または [\* リソースグループ \*] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューでデータベースを選択します。

データベーストポロジのページが表示されます。

4. Manage Copies (コピーの管理) ビューから、プライマリまたはセカンダリ (ミラーまたはレプリケートされた) ストレージシステムから \* Backups (バックアップ) \* を選択します。

5. 表からバックアップを選択し、をクリックします 。

6. バックアップのマウントページで、バックアップをマウントするホストを \* から選択し、バックアップをマウントするホストを \* ドロップダウン・リストから選択します。

mount path `/var/opt/snapcenter /scx/backup_mount/backup_name/database-name_name _` が表示されます。

ASM データベースのバックアップをマウントする場合は、マウントパス + `diskgroupname_SID_backupid` が表示されます。

1. [マウント] をクリックします。

• 終了後 \*

- マウントされたバックアップに関する情報を取得するには、次のコマンドを実行します。

```
./sccli get-SmBackup - BackupName backup_name -ListMountInfo
```

- ASM データベースをマウントした場合、マウントされたバックアップに関する情報を取得するには、次のコマンドを実行します。

```
./sccli get-smbbackup-BackupNamediskgroupname_SID_backupid-listmountinfo
```

- バックアップ ID を取得するには、次のコマンドを実行します。

```
./sccli get-Smbbackup - BackupNamebackup_name
```

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、`Get-Help_command_name_` を実行して取得できます。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リファレンスガイド](#)"。

## データベースバックアップをアンマウント

マウントされたデータベースバックアップ上のファイルにアクセスする必要がなくなった場合は、そのバックアップを手動でアンマウントできます。

### • 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 \*] または [\* リソースグループ \*] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューでデータベースを選択します。

データベースストポロジのページが表示されます。

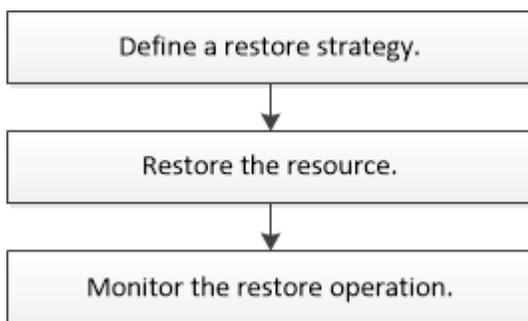
4. マウントされているバックアップを選択し、をクリックします 。
5. [OK] をクリックします。

## Oracle データベースのリストアとリカバリを行う

### リストアワークフロー

リストアワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

次のワークフローは、リストア処理の実行順序を示しています。



### Oracle データベースのリストアとリカバリの戦略を定義する

データベースのリストアとリカバリを行う前に戦略を定義しておくこと、リストア処理とリカバリ処理を正常に実行できるようになります。

## リストア処理とリカバリ処理でサポートされるバックアップのタイプ

SnapCenter では、各種の Oracle データベースバックアップのリストアとリカバリがサポートされます。

- オンラインデータバックアップ
- オフラインシャットダウンデータバックアップ
- オフラインマウントデータバックアップ
- フルバックアップ
- Data Guard スタンバイデータベースのオフラインマウントバックアップ
- Active Data Guard スタンバイデータベースの、データのためのオンラインバックアップ



Active Data Guard スタンバイデータベースのリカバリは実行できません。

- Real Application Clusters ( RAC ) 構成でのオンラインデータバックアップ、オンラインフルバックアップ、オフラインマウントバックアップ、オフラインシャットダウンバックアップ
- Automatic Storage Management ( ASM ) 構成でのオンラインデータバックアップ、オンラインフルバックアップ、オフラインマウントバックアップ、オフラインシャットダウンバックアップ

## Oracle データベースでサポートされるリストア方式のタイプ

SnapCenter では、Oracle データベースに対して Connect and Copy リストアと In Place リストアがサポートされます。SnapCenter は、リストア処理中に、データを失うことなくリストアに使用するファイルシステムに適したリストア方式を決定します。



SnapCenter はボリュームベースの SnapRestore をサポートしていません。

### Connect and Copy リストア

データベースレイアウトがバックアップと異なる場合や、バックアップ作成後に新しいファイルがある場合は、Connect and Copy リストアが実行されます。Connect and Copy リストア方式では、次のタスクが実行されます。

- 手順 \*
  1. ボリュームは Snapshot コピーからクローニングされ、ファイルシステムスタックは、クローニングされた LUN またはボリュームを使用してホスト上に構築されます。
  2. クローニングされたファイルシステムから元のファイルシステムにファイルがコピーされます。
  3. クローニングされたファイルシステムがホストからアンマウントされ、クローニングされたボリュームが ONTAP から削除されます。



Flex ASM 設定 (カードの数が RAC クラスタ内のノード数より少ない場合) または VMDK または RDM 上の ASM RAC データベースでは、Connect and Copy リストア方式のみがサポートされます。

In Place リストアを強制的に有効にした場合でも、次のシナリオでは SnapCenter によって Connect and Copy リストアが実行されます。

- 8.3 より前のバージョンの Data ONTAP でセカンダリストレージシステムからリストアする
- データベースインスタンスが設定されていない Oracle RAC セットアップのノードに存在する ASM ディスクグループをリストアする場合
- Oracle RAC セットアップで、いずれかのピアノードで ASM インスタンスまたはクラスタインスタンスが実行されていない場合、またはピアノードが停止している場合
- 制御ファイルのみをリストア
- ASM ディスクグループに存在する表領域の一部をリストアします
- ディスクグループは、データファイル、SP ファイル、パスワードファイルの間で共有されます
- RAC 環境のリモートノードに SnapCenter Plug-in Loader (SPL) サービスがインストールされていないか実行されていない場合
- Oracle RAC に新しいノードが追加され、SnapCenter サーバは新しく追加されたノードを認識しません

#### In Place リストアを実行します

データベースレイアウトがバックアップとほぼ同じであり、かつストレージとデータベーススタックで設定変更が行われていない場合は、In Place リストアが実行されて、ファイルまたは LUN のリストアが ONTAP 上で実行されます。SnapCenter では、In Place リストア方式の一環として Single File SnapRestore (SFSR) のみがサポートされます。



Data ONTAP 8.3 以降では、セカンダリサイトからの In Place リストアがサポートされます。

データベースで In Place リストアを実行する場合は、ASM ディスクグループにデータファイルだけがあることを確認してください。ASM ディスクグループまたはデータベースの物理構造に変更を加えた場合は、バックアップを作成する必要があります。In Place リストアを実行すると、ディスクグループにバックアップ時と同じ数のデータファイルが格納されます。

ディスクグループまたはマウントポイントが次の基準に一致する場合は、In Place リストアが自動的に適用されます。

- バックアップ後に新しいデータファイルが追加されていない (外部ファイルチェック)
- バックアップ後に ASM ディスクまたは LUN の追加、削除、または再作成が行われていない (ASM ディスクグループの構造変更チェック)
- LVM ディスクグループに対して LUN の追加、削除、または再作成が行われていない (LVM ディスクグループの構造変更チェック)



In Place リストアを強制的に有効にすることもできます。有効にするには、GUI、SnapCenter CLI、または PowerShell コマンドレットを使用して、外部ファイルチェックおよび LVM ディスクグループの構造変更チェックを無効にします。

#### ASM RAC で In Place リストアを実行します

SnapCenter では、リストアを実行するノードがプライマリノードと呼ばれ、ASM ディスクグループがある RAC 上のその他すべてのノードがピアノードと呼ばれます。SnapCenter は、ストレージリストア処理を実行する前に、ASM ディスクグループがマウント状態にあるすべてのノードで、ディスクマウントする ASM ディスクグループの状態を変更します。ストレージのリストアが完了すると、SnapCenter はリストア処理前と同じ状態で ASM ディスクグループの状態を変更します。

SAN 環境では、ストレージリストア処理の前に、SnapCenter がすべてのピアノードからデバイスを削除し、LUN のマッピング解除処理を実行します。ストレージリストア処理が完了すると、SnapCenter は LUN マップ処理を実行し、すべてのピアノードでデバイスを構築します。SAN 環境の LUN 上に Oracle RAC ASM レイアウトが存在する場合は、SnapCenter のリストア中に、ASM ディスクグループが存在する RAC クラスタのすべてのノードで LUN のマッピング解除、LUN のリストア、および LUN のマッピングが実行されます。リストア前に RAC ノードのすべてのイニシエータが LUN に使用されていなかった場合でも、SnapCenter をリストアすると、すべての RAC ノードのすべてのイニシエータを含む新しい igroup が作成されます。

- ピアノードでリストア前の処理中にエラーが発生した場合は、リストア前の処理が成功したピアノードで SnapCenter が自動的に ASM ディスクグループの状態をリストア実行前の状態にロールバックします。プライマリノードおよび処理が失敗したピアノードでは、ロールバックはサポートされていません。新たなリストアを実行する前に、ピアノードの問題を手動で修正し、プライマリノード上の ASM ディスクグループをマウント状態に戻す必要があります。
- リストア処理中にエラーが発生した場合は、リストア処理が失敗し、ロールバックは実行されません。新たなリストアを実行する前に、ストレージリストア問題を手動で修正し、プライマリノード上の ASM ディスクグループをマウント状態に戻す必要があります。
- いずれかのピアノードでリストア後の処理中にエラーが発生した場合、SnapCenter は他のピアノードでリストア処理を続行します。ピアノードでリストア後の問題を手動で修正する必要があります。

### Oracle データベースでサポートされるリストア処理のタイプ

SnapCenter では、Oracle データベースに対してさまざまなタイプのリストア処理を実行できます。

データベースをリストアする前に、バックアップが検証されて、実際のデータベースファイルと比較して足りないファイルがないかが確認されます。

#### フルリストア

- データファイルのみをリストアします
- 制御ファイルのみをリストアします
- データファイルと制御ファイルをリストアします
- Data Guard スタンバイデータベースと Active Data Guard スタンバイデータベースにあるデータファイル、制御ファイル、および REDO ログファイルをリストアします

#### 部分リストア

- 選択した表領域のみをリストアします
- 選択した Pluggable Database (PDB) のみをリストア
- 1 つの PDB の選択した表領域のみをリストアします

### Oracle データベースでサポートされるリカバリ処理のタイプ

SnapCenter では、Oracle データベースに対してさまざまなタイプのリカバリ処理を実行できます。

- 最後のトランザクションまで (すべてのログ) のデータベース
- 特定の System Change Number (SCN) までのデータベース
- 特定の日時までのデータベース

リカバリの日時はデータベースホストのタイムゾーンに基づいて指定する必要があります。

SnapCenter には 'Oracle データベースのリカバリ・オプションはありません



スタンバイとしてのデータベースロールで作成されたバックアップを使用してリストアを実行した場合、Plug-in for Oracle Database ではリカバリがサポートされません。物理スタンバイデータベースは、常に手動でリカバリする必要があります。

## Oracle データベースのリストアとリカバリに関する制限事項

リストア処理とリカバリ処理を実行する前に、制限事項を確認しておく必要があります。

11.2.0.4 から 12.1.0.1 までの Oracle のいずれかのバージョンを使用している場合、\_renamedg\_command の実行時にリストア処理がハング状態になります。この問題を修正するには、Oracle パッチ 19544733 を適用します。

次のリストア処理とリカバリ処理はサポートされていません。

- ルートコンテナデータベース（CDB）の表領域のリストアとリカバリ
- 一時表領域および PDB に関連付けられた一時表領域のリストア
- 複数の PDB から同時に行う表領域のリストアとリカバリ
- ログバックアップのリストア
- 別の場所へのバックアップのリストア
- Data Guard スタンバイデータベースまたは Active Data Guard スタンバイデータベース以外の構成での redo ログファイルのリストア
- SPFILE およびパスワード・ファイルのリストア
- 同じホスト上の既存のデータベース名を使用して再作成され、SnapCenter で管理されていて、有効なバックアップがあるデータベースに対してリストア処理を実行すると、DBID が異なる場合でも、新しく作成されたデータベースファイルが上書きされます。

これを回避するには、次のいずれかの操作を実行します。

- データベースを再作成したら、SnapCenter リソースを検出します
- 再作成したデータベースのバックアップを作成します

## 表領域のポイントインタイムリカバリに関する制限事項

- SYSTEM、SYSAUX、UNDO の PITR（ポイント・イン・タイム・リカバリ）はサポートされていません
- 表領域の PITR は、他のタイプのリストアと同時に実行できません
- テーブルスペースの名前を変更したあと、名前を変更する前に名前を特定の時点にリカバリする場合は、以前の表領域名を指定する必要があります
- 1 つの表領域内の表に対する制約が別の表領域に含まれている場合は、両方の表領域をリカバリする必要があります
- テーブルとそのインデックスが異なるテーブルスペースに格納されている場合は、PITR を実行する前に

インデックスを削除する必要があります

- PITR を使用して、現在のデフォルトテーブルスペースを回復することはできません
- PITR を使用して、次のオブジェクトを含む表領域を回復することはできません。
  - 基になるオブジェクト（実体化ビュー (Materialized View) など）または含まれるオブジェクト（パーティション化されたテーブルなど）を含むオブジェクトは '基になるオブジェクトまたは含まれるオブジェクトがすべてリカバリ・セットに含まれている場合を除きます

また、分割されたテーブルのパーティションが異なるテーブルスペースに格納されている場合は、PITR を実行する前にテーブルを削除するか、すべてのパーティションを同じテーブルスペースに移動してから PITR を実行する必要があります。

- セグメントを元に戻すかロールバックします
- Oracle 8 では、複数の受信者と互換性のある拡張キューを使用でき
- SYS ユーザが所有するオブジェクト

これらのタイプのオブジェクトの例としては、PL/SQL、Java クラス、呼び出しプログラム、ビュー、同義語、ユーザー、特権、寸法、ディレクトリ、およびシーケンス。

## Oracle データベースをリストアするためのソースとデスティネーション

プライマリストレージまたはセカンダリストレージにあるバックアップコピーから Oracle データベースをリストアすることができます。データベースは、同じデータベースインスタンスの同じ場所にのみリストアできます。ただし、Real Application Cluster (RAC) セットアップでは、データベースを他のノードにリストアできます。

### リストア処理のソース

プライマリストレージまたはセカンダリストレージ上のバックアップからデータベースをリストアすることができます。複数ミラー構成でセカンダリストレージ上のバックアップからリストアする場合は、セカンダリストレージミラーをソースとして選択できます。

### リストア処理のデスティネーション

データベースは、同じデータベースインスタンスの同じ場所にのみリストアできます。

RAC セットアップでは、クラスタ内の任意のノードから RAC データベースをリストアできます。

## Oracle データベースをリストアするための要件

Oracle データベースをリストアする前に、前提条件を満たしていることを確認する必要があります。

- リストアとリカバリの戦略を定義しておく必要があります。
- ユーザが Snapshot コピーをミラーまたはバックアップにレプリケートする場合は、ソースボリュームとデスティネーションボリューム両方の Storage Virtual Machine (SVM) を SnapCenter 管理者がユーザに割り当てておく必要があります。
- バックアップの一環としてアーカイブログが削除される場合は、必要なアーカイブログのバックアップを手動でマウントしておく必要があります。

- 仮想マシンディスク（VMDK）上にある Oracle データベースをリストアする場合は、クローン VMDK を割り当てるための必要な数の空きスロットがゲストマシンにあることを確認してください。
- データベースでセカンダリ保護が有効になっている場合は、そのデータベースに属するすべてのデータボリュームとアーカイブログボリュームが保護されていることを確認する必要があります。
- 制御ファイルまたはフルデータベースのリストアを実行するには、RAC One Node データベースが「nomount」状態であることを確認する必要があります。
- NFS 環境に ASM データベースインスタンスがある場合は、ASM ディスクパス /var/opt/snapcenter /cu/clones/\*/\*\_ を asm\_diskstring パラメータで定義された既存のパスに追加して、リカバリ操作の一環として ASM ログバックアップを正常にマウントする必要があります。
- ASM\_diskstring パラメータで、ASMFD または configure\_ORCL : \*\_ を使用する場合は、\_AFD : \*\_ を設定します。



asm\_diskstring パラメータの編集方法については、を参照してください "[asm\\_diskstring にディスクパスを追加する方法](#)"

- OS 認証を無効にし、Oracle データベースの Oracle データベース認証を有効にしている場合は、\_\$\_ORACLE\_HOME/network/admin\_for ASM データベースで使用可能な \* listener.ora \* ファイルに静的リスナーを設定し、そのデータベースのデータファイルと制御ファイルをリストアする必要があります。
- データベースサイズがテラバイト（TB）単位の場合は、Set-SmConfigSettings コマンドを実行して、SCORestoreTimeout パラメータの値を増やす必要があります。
- vCenter に必要なすべてのライセンスがインストールされ、最新の状態であることを確認する必要があります。

ライセンスがインストールされていない場合、または最新の状態でない場合は、警告メッセージが表示されます。警告を無視して続行すると、RDM からのリストアが失敗します。

- iSCSI プロトコルと FC プロトコルが混在する igroup を使用して、LUN が AIX ホストにマッピングされていないことを確認してください。詳細については、を参照してください "[LUN のデバイスを検出できませんというエラーが表示されて処理に失敗します](#)"。

## Oracle データベースをリストアします

データ損失が発生した場合は、SnapCenter を使用して 1 つ以上のバックアップからアクティブファイルシステムにデータをリストアし、そのあとにデータベースをリカバリできます。

- このタスクについて \*

リカバリは、設定したアーカイブログの場所にあるアーカイブログを使用して実行します。リカバリに必要なアーカイブログが設定済みの場所がない場合は、ログを含む Snapshot コピーをマウントし、外部アーカイブログとしてパスを指定する必要があります。

ASM データベースを ASMLib から ASMFD に移行する場合、ASMLib で作成されたバックアップは、データベースのリストアには使用できません。ASMFD 構成にバックアップを作成し、これらのバックアップを使用してリストアする必要があります。同様に、ASM データベースを ASMFD から ASMLib に移行する場合は、リストアする ASMLib 構成にバックアップを作成する必要があります。

データベースをリストアすると、データベースで複数の処理が実行されないように、Oracle データベースホ

スト上に \$ORACLE\_HOME/dbs ディレクトリ内に処理ロックファイル (.SM\_lock\_dbsid) が作成されます。処理ロックファイルは、データベースのリストアが完了すると自動的に削除されます。



SPFILE およびパスワード・ファイルのリストアはサポートされていません。

• 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\*] または [\* リソースグループ\*] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューでデータベースを選択します。

データベーストポロジのページが表示されます。

4. Manage Copies (コピーの管理) ビューから、プライマリまたはセカンダリ (ミラーまたはレプリケートされた) ストレージシステムから \* Backups (バックアップ) \* を選択します。
5. 表からバックアップを選択し、\* をクリックします  \*
6. Restore Scope ページで、次のタスクを実行します。

- a. Real Application Clusters (RAC) 環境でデータベースのバックアップを選択した場合は、RAC ノードを選択します。
- b. ミラーデータまたはバックアップデータを選択した場合：
  - ミラーまたはボルトにログバックアップがない場合、何も選択されず、ロケータは空です。
  - ミラーまたはバックアップにログバックアップが存在する場合は、最新のログバックアップが選択され、対応するロケータが表示されます。



選択したログバックアップがミラーとバックアップの場所の両方に存在する場合、両方のロケータが表示されます。

- c. 次の操作を実行します。

リストアの対象	手順
データベースのすべてのデータファイル	「* すべてのデータファイル*」を選択します。  データベースのデータファイルのみがリストアされます。制御ファイル、アーカイブログ、または REDO ログファイルはリストアされません。
表領域	[* 表領域*] を選択します。  リストアする表領域を指定できます。

リストアの対象	手順
制御ファイル	<p data-bbox="902 159 1349 191">「* 制御ファイル *」を選択します。</p> <div data-bbox="922 415 976 472" style="border: 1px solid black; border-radius: 50%; width: 33px; height: 33px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> <span data-bbox="927 422 971 466" style="font-size: 24px; font-weight: bold;">i</span> </div> <p data-bbox="1036 239 1430 646">制御ファイルをリストアするときは、ディレクトリ構造が存在するか、または正しいユーザおよびグループの所有権を持つディレクトリ構造が作成されていることを確認してください（存在する場合）。これにより、リストアプロセスによってファイルがターゲットの場所にコピーされるようになります。ディレクトリが存在しない場合、リストアジョブは失敗します。</p>
REDO ログファイル	<p data-bbox="894 716 1357 747">[再実行ログファイル]を選択します。</p> <p data-bbox="894 785 1468 884">このオプションは、Data Guard スタンバイデータベースまたは Active Data Guard スタンバイデータベースに対してのみ使用できます。</p> <div data-bbox="922 1003 976 1060" style="border: 1px solid black; border-radius: 50%; width: 33px; height: 33px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> <span data-bbox="927 1010 971 1054" style="font-size: 24px; font-weight: bold;">i</span> </div> <p data-bbox="1036 936 1430 1136">REDO ログファイルは、Data Guard 以外のデータベースにはバックアップされません。Data Guard 以外のデータベースの場合、リカバリはアーカイブログを使用して実行されます。</p>
Pluggable Database (PDB)	<p data-bbox="894 1203 1468 1268">Pluggable Database * を選択し、リストアする PDB を指定します。</p>
Pluggable Database (PDB) の表領域	<p data-bbox="894 1325 1484 1423">Pluggable Database (PDB) tablespaces * を選択し、リストアする PDB とその PDB の表領域を指定します。</p> <p data-bbox="894 1461 1468 1526">このオプションは、リストア対象に PDB を選択した場合にのみ選択できます。</p>

- d. リストアとリカバリに必要な場合は、「\* データベースの状態を変更」を選択して、データベースの状態をリストアとリカバリ処理の実行に必要な状態に変更します。

データベースの状態は、高いレベルから順に、オープン、マウント済み、開始、シャットダウンがあります。リストア処理を実行するために、データベースの状態を高いレベルから低いレベルに変更する必要がある場合は、このチェックボックスをオンにします。リストア処理を実行するために、データベースの状態を低いレベルから高いレベルに変更する必要がある場合は、このチェックボックスをオンにしなくても自動的に状態が変更されます。

データベースが OPEN 状態で、リストアのためにデータベースが MOUNTED 状態である必要がある

場合、データベースの状態はこのチェックボックスをオンにした場合にのみ変更されます。

- a. バックアップ後に新しいデータファイルが追加された場合や、LUN が LVM ディスクグループに追加、削除、再作成された場合にインプレースリストアを実行するには、\* Force in place restore \* を選択します。

7. Recovery Scope ページで、次のアクションを実行します。

状況	手順
最後のトランザクションまでリカバリする場合	[ * すべてのログ * ] を選択します。
特定の System Change Number ( SCN ) までリカバリする場合	[ * Until SCN ( System Change Number ) ] を選択します。
特定の日時までリカバリする必要がある	[ * 日付と時刻 * ] を選択します。  データベースホストのタイムゾーンの日付と時刻を指定する必要があります。
リカバリが不要である場合	「 * リカバリなし * 」を選択します。
外部アーカイブログの場所を指定する	外部アーカイブログの場所を指定する * を選択し、外部アーカイブログファイルの場所を指定します。  バックアップの一環としてアーカイブログが削除される場合に、必要なアーカイブログのバックアップを手動でマウントしたときは、リカバリのために、マウントしたバックアップのパスを外部アーカイブログの場所として指定する必要があります。  <ul style="list-style-type: none"><li>• "ONTAPによるOracleデータ保護"</li><li>• "ORA-00308 エラーで処理が失敗します"</li></ul>

アーカイブログボリュームが保護されておらず、データボリュームが保護されている場合は、セカンダリバックアップからリカバリを伴うリストアを実行できません。リストアするには、「 \* リカバリなし \* 」を選択する必要があります。

オープンデータベースオプションを選択して RAC データベースをリカバリする場合は、リカバリ処理が開始された RAC インスタンスのみがオープン状態に戻ります。



Data Guard スタンバイデータベースおよび Active Data Guard スタンバイデータベースでは、リカバリがサポートされません。

8. PreOps ページで、リストア処理の前に実行するプリスクリプトのパスと引数を入力します。

プリスクリプトは、\_ /var/opt/snapcenter /spl/scripts\_path またはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、 /var/opt/snapcenter /spl/scripts\_path が読み込まれます。スク

リプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は 60 秒です。

## 9. PostOps ページで、次の手順を実行します。

- a. リストア処理のあとに実行するポストスクリプトのパスと引数を入力します。

ポストスクリプトは、`_ /var/opt/snapcenter /spl/scripts_or` のいずれか、このパス内の任意のフォルダに保存する必要があります。デフォルトでは、`/var/opt/snapcenter /spl/scripts_path` が読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

- b. リカバリ後にデータベースを開く場合は、チェックボックスを選択します。

リカバリ後にデータベースを開くように指定した場合は、制御ファイル付きまたは制御ファイルなしのコンテナデータベース（CDB）をリストアしたあと、または CDB 制御ファイルのみをリストアしたあとに CDB のみが開き、CDB 内の Pluggable Database（PDB）は開きません。

RAC セットアップでは、リカバリに使用される RAC インスタンスのみがリカバリ後に開きます。



制御ファイル付きのユーザ表領域、制御ファイル付きまたは制御ファイルなしのシステム表領域、あるいは制御ファイル付きまたは制御ファイルなしの PDB をリストアすると、リストア処理に関連する PDB の状態のみが元の状態に変更されます。リストアに使用されなかった他の PDB の状態は保存されていないため、元の状態に変更されません。リストアに使用されなかった PDB の状態は、手動で変更する必要があります。

## 10. [通知] ページの [電子メールの設定\*] ドロップダウンリストから、電子メール通知を送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および Eメールの件名を指定する必要があります。実行したリストア処理のレポートを添付する場合は、[ジョブレポートの添付]を選択する必要があります。



Eメール通知を利用する場合は、GUI または PowerShell コマンド `Set-SmtpServer` を使用して、SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、[完了] をクリックします。

2. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

- 詳細はこちら \*
- "SnapCenter 処理では、Oracle RAC One Node データベースがスキップされます"
- "セカンダリの SnapMirror または SnapVault の場所からリストアできませんでした"
- "孤立したインカネーションのバックアップからのリストアに失敗しました"
- "AIX システムでのバックアップ、リストア、クローニングの各処理のパラメータをカスタマイズできません"

## ポイントインタイムリカバリを使用した表領域のリストアとリカバリ

データベース内の他の表領域に影響を与えずに、破損または削除された表領域のサブセットをリストアできます。SnapCenter では、RMAN を使用して表領域のポイントインタイムリカバリ（PITR）を実行します。

- 必要なもの \*

表領域の PITR を実行するために必要なバックアップは、カタログ化されてマウントされている必要があります。

- このタスクについて \*

PITR 操作中に、RMAN は指定された補助宛先に補助インスタンスを作成します。補助デスティネーションは、マウントポイントまたは ASM ディスクグループです。マウント先に十分なスペースがある場合は、専用のマウントポイントではなく、マウントされた場所の 1 つを再利用できます。

ソースデータベースに表領域がリストアされるように、日時または SCN を指定する必要があります。

ASM、NFS、および SAN 環境上の複数の表領域を選択してリストアできます。たとえば、TS2 および TS3 の表領域が NFS 上にあり、TS4 が SAN 上にある場合は、1 回の PITR 処理ですべての表領域をリストアできます。



RAC セットアップでは、RAC の任意のノードから表領域の PITR を実行できます。

- 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 \*] または [\* リソースグループ \*] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューで、タイプがシングルインスタンス（マルチテナント）のデータベースを選択します。

データベーストポロジのページが表示されます。

4. Manage Copies（コピーの管理）ビューから、プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージシステムから \* Backups（バックアップ）\* を選択します。

バックアップがカタログ化されていない場合は、バックアップを選択し、\* Catalog \* をクリックします。

5. カタログ化されたバックアップを選択し、\* をクリックします  \*

6. Restore Scope ページで、次のタスクを実行します。
  - a. Real Application Clusters（RAC）環境でデータベースのバックアップを選択した場合は、RAC ノードを選択します。
  - b. [\* 表領域 \*] を選択し、リストアする表領域を指定します。



SYSAUX 'システム' および UNDO の各テーブルスペースでは 'PITR' を実行できません

- c. リストアとリカバリに必要な場合は、「\* データベースの状態を変更」を選択して、データベースの状態をリストアとリカバリ処理の実行に必要な状態に変更します。

7. Recovery Scope ページで、次のいずれかを実行します。

- 特定の System Change Number (SCN) までリカバリする場合は、「\* Until SCN \*」を選択し、SCN と補助のデスティネーションを指定します。
- 特定の日にリカバリする場合は、[\* 日付と時刻 \* (\* Date and Time \*)] を選択して、日時と補助的な保存先を指定します。SCN または日付と時刻を指定すると、SnapCenter には、PITR の実行に必要なバックアップのうち、カタログ化されておらず、マウントされていないバックアップが表示されます。

8. PreOps ページで、リストア処理の前に実行するプリスクリプトのパスと引数を入力します。

プリスクリプトは、/var/opt/snapcenter /spl/scripts パスまたはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、/var/opt/snapcenter /spl/scripts パスが読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は 60 秒です。

1. PostOps ページで、次の手順を実行します。
  - a. リストア処理のあとに実行するポストスクリプトのパスと引数を入力します。
  - b. リカバリ後にデータベースを開く場合は、チェックボックスを選択します。
2. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メール通知を送信するシナリオを選択します。
3. 概要を確認し、[完了] をクリックします。
4. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

ポイントインタイムリカバリを使用して、プラグイン可能なデータベースをリストアおよびリカバリします

コンテナデータベース (CDB) 内の他の PDB に影響を与えることなく、破損または破棄された Pluggable Database (PDB) をリストアおよびリカバリできます。SnapCenter は、RMAN を使用して PDB のポイントインタイムリカバリ (PITR) を実行します。

- 必要なもの \*

PDB の PITR を実行するために必要なバックアップは、カタログ化してマウントする必要があります。



RAC セットアップでは、RAC セットアップのすべてのノードの PDB を手動で閉じます (状態を mounted に変更します)。

- このタスクについて \*

PITR 操作中に、RMAN は指定された補助宛先に補助インスタンスを作成します。補助デスティネーションは、マウントポイントまたは ASM ディスクグループです。マウント先に十分なスペースがある場合は、専用のマウントポイントではなく、マウントされた場所の 1 つを再利用できます。

PDB の PITR を実行するには、日時または SCN を指定する必要があります。RMAN は、データファイルを含む読み取り / 書き込み、読み取り専用、またはドロップされた PDB をリカバリできます。

リストアとリカバリが可能なのは次の場合だけです。

- 一度に 1 つの PDB
- PDB 内の 1 つの表領域
- 同じ PDB の複数の表領域



RAC セットアップでは、RAC の任意のノードから表領域の PITR を実行できます。

• 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 \*] または [\* リソースグループ \*] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューで、タイプがシングルインスタンス (マルチテナント) のデータベースを選択します。

データベーストポロジのページが表示されます。

4. Manage Copies (コピーの管理) ビューから、プライマリまたはセカンダリ (ミラーまたはレプリケートされた) ストレージシステムから \* Backups (バックアップ) \* を選択します。

バックアップがカタログ化されていない場合は、バックアップを選択し、\* Catalog \* をクリックします。

5. カタログ化されたバックアップを選択し、\* をクリックします  \*

6. Restore Scope ページで、次のタスクを実行します。
  - a. Real Application Clusters (RAC) 環境でデータベースのバックアップを選択した場合は、RAC ノードを選択します。
  - b. PDB 内の PDB または表領域をリストアするかどうかに応じて、次のいずれかの操作を実行します。

状況	手順
----	----

PDB をリストアします	<p>i. Pluggable Database ( PDB ) * を選択します。</p> <p>ii. リストアする PDB を指定します。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  PDB\$SEED データベースで PITR を実行することはできません。 </div>
PDB のリストア表領域	<p>i. Pluggable Database ( PDB ) tablespaces * を選択します。</p> <p>ii. PDB を指定します。</p> <p>iii. リストアする表領域を 1 つまたは複数指定します。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  SYSAUX ' システム ' および UNDO の各テーブルスペースでは 'PITR を実行できません </div>

- c. リストアとリカバリに必要な場合は、「\* データベースの状態を変更」を選択して、データベースの状態をリストアとリカバリ処理の実行に必要な状態に変更します。

7. Recovery Scope ページで、次のいずれかを実行します。

- 特定の System Change Number ( SCN ) までリカバリする場合は、「\* Until SCN \*」を選択し、SCN と補助のデスティネーションを指定します。
- 特定の日にリカバリする場合は、[\* 日付と時刻 \* ( \* Date and Time \* ) ] を選択して、日時と補助的な保存先を指定します。SCN または日付と時刻を指定すると、SnapCenter には、PITR の実行に必要なバックアップのうち、カタログ化されておらず、マウントされていないバックアップが表示されます。

8. PreOps ページで、リストア処理の前に実行するプリスクリプトのパスと引数を入力します。

プリスクリプトは、`/var/opt/snapcenter /spl/scripts` パスまたはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、`/var/opt/snapcenter /spl/scripts` パスが読み込まれます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は 60 秒です。

1. PostOps ページで、次の手順を実行します。

- a. リストア処理のあとに実行するポストスクリプトのパスと引数を入力します。
- b. リカバリ後にデータベースを開く場合は、チェックボックスを選択します。

RAC セットアップでは、データベースがリカバリされたノードでのみ PDB が開きます。RAC セットアップの他のすべてのノードで、リカバリされた PDB を手動で開く必要があります。

2. [通知] ページの [電子メールの設定 \*] ドロップダウンリストから、電子メール通知を送信するシナリオを選択します。
3. 概要を確認し、[完了] をクリックします。
4. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

## UNIX コマンドを使用して Oracle データベースをリストアおよびリカバリする

リストアとリカバリのワークフローには、計画、リストア処理とリカバリ処理の実行、および処理の監視が含まれます。

- このタスクについて \*

次のコマンドを実行して、SnapCenter サーバとの接続を確立し、バックアップをリストしてその情報を取得し、バックアップをリストアする必要があります。

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、`Get-Help_command_name_` を実行して取得できます。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リファレンスガイド](#)"。

- 手順 \*

1. 指定されたユーザ用に SnapCenter サーバとの接続セッションを開始します： `Open-SmConnection`
2. リストアするバックアップに関する情報を取得します： `Get-SmBackup`
3. 指定したバックアップに関する詳細情報を取得します： `Get-SmBackupDetails`

このコマンドは、指定されたバックアップ ID に一致する指定されたリソースのバックアップに関する詳細情報を取得します。情報には、データベース名、バージョン、ホーム、開始 SCN と終了 SCN、表領域、Pluggable Database とその表領域などがあります。

4. バックアップからデータをリストアする： `Restore-SmBackup`

## Oracle データベースのリストア処理を監視する

Jobs ページを使用して、SnapCenter の各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理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 \*

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

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
-  キャンセルされました
- 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、次の手順を実行します。
  - a. をクリックします  リストをフィルタリングして、リストア処理のみを表示します。
  - b. 開始日と終了日を指定します。
  - c. [\* タイプ] ドロップダウン・リストから、 [リストア \*] を選択します。
  - d. [\* Status \*] ドロップダウン・リストから、リストア・ステータスを選択します。
  - e. [適用 (Apply) ] をクリックして、正常に完了した操作を表示する。
4. リストアジョブを選択し、 \* Details \* 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。

**View logs** ボタンをクリックすると、選択した操作の詳細なログが表示されます。



ボリュームベースのリストア処理の完了後、バックアップメタデータは SnapCenter リポジトリから削除されますが、バックアップカタログのエントリが SAP HANA のカタログに残ります。リストアジョブのステータスが表示されます  では、ジョブの詳細をクリックして、いくつかの子タスクの警告サインを表示する必要があります。警告をクリックし、表示されたバックアップカタログのエントリを削除します。

## Oracle データベースのリストア処理をキャンセルします

キューに格納されているリストアジョブをキャンセルできます。

リストア処理をキャンセルするには、SnapCenter 管理者またはジョブ所有者としてログインする必要があります。

- このタスクについて \*
- キューに登録されたリストア処理は、Monitor ページまたは Activity ペインからキャンセルできます。
- 実行中のリストア処理はキャンセルできません。
- SnapCenter GUI、PowerShell コマンドレット、または CLI コマンドを使用して、キューに登録されたリストア処理をキャンセルできます。
- キャンセルできないリストア処理の場合、[ジョブのキャンセル] ボタンは使用できません。
- ロールの作成中に [ユーザー \ グループ] ページで [このロールのすべてのメンバーが他のメンバーオブジェクトを表示して操作できる] を選択した場合は、そのロールを使用している間に、他のメンバーのキューに登録されているリストア操作をキャンセルできます。
- ステップ \*

次のいずれかを実行します。

方法	アクション
監視ページ	<ol style="list-style-type: none"> <li>1. 左側のナビゲーションペインで、 * Monitor * &gt; * Jobs * をクリックします。</li> <li>2. ジョブを選択し、 * ジョブのキャンセル * をクリックします。</li> </ol>
アクティビティペイン	<ol style="list-style-type: none"> <li>1. リストア処理を開始したら、をクリックします   をクリックして、最近の 5 つの操作を表示します。</li> <li>2. 処理を選択します。</li> <li>3. [ ジョブの詳細 ] ページで、 [ * ジョブのキャンセル * ] をクリックします。</li> </ol>

## Oracle データベースのクローニング

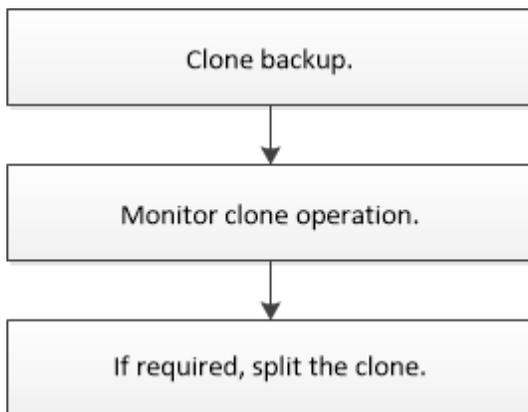
### クローニングワークフロー

クローニングワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

データベースをクローニングする理由には次のものがあります。

- アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のデータベースの構造およびコンテナツを使用してテストするため。
- データの抽出と操作を行うツールを使用してデータウェアハウスにデータを取り込むため。
- 誤って削除または変更されたデータをリカバリするため。

次のワークフローは、クローニング処理の実行順序を示しています。



### Oracle データベースのクローニング戦略を定義する

データベースをクローニングする前に戦略を定義しておくこと、クローニング処理を確実に成功させることができます。

## クローニングでサポートされるバックアップのタイプ

SnapCenter では、Oracle データベースの各種バックアップのクローニングがサポートされます。

- オンラインデータバックアップ
- オンラインフルバックアップ
- オフラインマウントバックアップ
- オフラインシャットダウンバックアップ
- Data Guard スタンバイデータベースおよび Active Data Guard スタンバイデータベースのバックアップ
- Real Application Clusters (RAC) 構成でのオンラインデータバックアップ、オンラインフルバックアップ、オフラインマウントバックアップ、オフラインシャットダウンバックアップ
- Automatic Storage Management (ASM) 構成でのオンラインデータバックアップ、オンラインフルバックアップ、オフラインマウントバックアップ、オフラインシャットダウンバックアップ



マルチパス構成ファイルで `user_friendly_name` オプションが `yes` に設定されていて、`udev` ルールファイルを使用して Oracle ASM ディスクに対してエイリアスまたはシンボリックリンクが定義されている場合、Oracle ASM 設定はサポートされません。



アーカイブログのバックアップのクローニングはサポートされていません。

## Oracle データベースでサポートされるクローニングのタイプ

Oracle データベース環境では、SnapCenter がデータベースバックアップのクローニングをサポートします。バックアップのクローニングは、プライマリストレージシステムおよびセカンダリストレージシステムから行うことができます。

SnapCenter サーバは、NetApp FlexClone テクノロジーを使用してバックアップをクローニングします。

クローンを更新するには、「Refresh-SmClone」コマンドを実行します。このコマンドは、データベースのバックアップを作成し、既存のクローンを削除し、同じ名前で作成します。



クローンの更新処理は、UNIX コマンドでのみ実行できます。

## Oracle データベースのクローンの命名規則

SnapCenter 3.0 以降では、ファイルシステムのクローンに、ASM ディスクグループのクローンとは異なる命名規則が使用されます。

- SAN または NFS ファイルシステムの命名規則は、`FileSystemNameofsourcedatabE_CLONESID` です。
- ASM ディスクグループの命名規則は、`SC_HASHCODEofDISKGROUP_CLONESID` です。

`HASHCODEofDISKGROUP` は、ASM ディスクグループごとに一意の自動生成番号（2～10桁）です。

## Oracle データベースのクローニングの制限

データベースをクローニングする前に、クローニング処理の制限事項を確認しておく必要があります。

- Oracle 11.2.0.4 ~ 12.1.0.1 のいずれかのバージョンを使用している場合、\_renamedg\_command の実行時にクローン操作がハング状態になります。この問題を修正するには、Oracle パッチ 19544733 を適用します。
- ホストに直接接続された LUN（Windows ホストで Microsoft iSCSI イニシエータを使用した場合など）から、同じ Windows ホストまたは別の Windows ホスト上の VMDK または RDM LUN に、あるいはその逆に、データベースをクローニングすることはできません。
- ボリュームマウントポイントのルートディレクトリを共有ディレクトリにすることはできません。
- クローンが含まれている LUN を新しいボリュームに移動した場合、そのクローンは削除できません。

## Oracle データベースをクローニングするための要件

Oracle データベースをクローニングする前に、前提条件を満たしていることを確認する必要があります。

- SnapCenter を使用してデータベースのバックアップを作成しておく必要があります。

クローニング処理が成功するためには、オンラインデータバックアップとログバックアップ、またはオフライン（マウントまたはシャットダウン）バックアップが正常に作成されている必要があります。

- 制御ファイルまたは REDO ログファイルのパスをカスタマイズする場合は、必要なファイルシステムまたは Automatic Storage Management（ASM）ディスクグループを事前にプロビジョニングしておく必要があります。

デフォルトでは、クローンデータベースの REDO ログおよび制御ファイルは、ASM ディスクグループ、またはクローンデータベースのデータファイル用に SnapCenter でプロビジョニングされたファイルシステムに作成されます。

- NFS 経由で ASM を使用している場合は、ASM\_diskstring パラメータで定義された既存のパスに /var/opt/snapcenter /scu/clones/\*/\*\_ を追加する必要があります。
- ASM\_diskstring パラメータで、ASMFD または configure\_ORCL : \* \_ を使用する場合は、\_AFD : \* \_ を設定します。

asm\_diskstring パラメータの編集方法については、を参照してください "[asm\\_diskstring にディスクパスを追加する方法](#)"。

- 代替ホストでクローニングを作成する場合、代替ホストは次の要件を満たす必要があります。
  - SnapCenter Plug-in for Oracle Database を代替ホストにインストールする必要があります。
  - クローンホストは、プライマリストレージまたはセカンダリストレージから LUN を検出できる必要があります。
    - プライマリストレージまたはセカンダリ（バックアップまたはミラー）ストレージから代替ホストにクローニングする場合は、セカンダリストレージと代替ホストの間に iSCSI セッションが確立されているか、FC 用に適切にゾーニングされていることを確認してください。
    - バックアップ・ストレージまたはミラー・ストレージから同じホストにクローニングする場合は、バックアップまたはミラー・ストレージとホストの間に iSCSI セッションが確立されているか、FC 用に適切にゾーニングされているかを確認してください。
    - 仮想環境でクローニングを行う場合は、プライマリストレージまたはセカンダリストレージと、代替ホストをホストする ESX サーバの間で iSCSI セッションが確立されていること、または FC 用に適切にゾーニングされていることを確認してください。 [+] 詳細については、を参照してください。

さい "Host Utilitiesのマニュアル"。

- ソースデータベースが ASM データベースの場合は、次の手順を実行します。
  - クローンを実行するホスト上で、ASM インスタンスが稼働している必要があります。
  - クローニングされたデータベースのアーカイブログファイルを専用の ASM ディスクグループに配置する場合は、クローン処理の前に ASM ディスクグループをプロビジョニングする必要があります。
  - データディスクグループの名前は設定できますが、クローンを実行するホスト上の他の ASM ディスクグループでは名前が使用されないようにしてください。

ASM ディスクグループにあるデータファイルは、SnapCenter のクローニングワークフローの一環としてプロビジョニングされます。

- データ LUN の保護タイプと、ミラー、バックアップ、ミラー - ヴォールトなどのログ LUN は、ログバックアップを使用して代替ホストへのクローニング中にセカンダリロケータを検出するために同じである必要があります。
- 12\_c\_c\_database のバックアップをクローニングするためのシード PDB 関連情報を取得するには、ソースデータベースのパラメータファイルで `exclude_seed_cdb_view` の値を `FALSE` に設定する必要があります。

シード PDB とは、CDB が PDB を作成する際に使用する、システム付属のテンプレートです。シード PDB の名前は `PDB$SEED` です。PDB\$SEED については、Oracle Doc ID 1940806.1 を参照してください。



この値は、12\_c\_database をバックアップする前に設定する必要があります。

- SnapCenter は 'autofs' サブシステムによって管理されるファイル・システムのバックアップをサポートします。データベースを複製する場合は 'データ・マウント・ポイント' が autofs マウント・ポイントのルートにないことを確認してください。これは 'プラグイン・ホストのルート・ユーザ' には 'autofs マウント・ポイントのルートの下にディレクトリを作成する権限がないためです'。

制御ログファイルと REDO ログファイルがデータマウントポイントにある場合は、制御ファイルのパスを変更し、それに従ってログファイルのパスをやり直す必要があります。



新しいクローン・マウント・ポイントを 'autofs' サブシステムに手動で登録できます。新しいクローンマウントポイントは自動的に登録されません。

- TDE（自動ログイン）を使用していて、同じホストまたは代替ホスト上にデータベースのクローンを作成する場合は、`/etc/oracle/ウォレット/$ORACLE_SID_` の下にあるウォレット（キーファイル）をソースデータベースからクローンデータベースにコピーする必要があります。
- Oracle Linux 7 以降または Red Hat Enterprise Linux（RHEL）7 以降の Storage Area Network（SAN；ストレージエリアネットワーク）環境でのクローニングを正常に実行するには、の値として、`/etc/lvm/lvmlvm/lvmmetad=0` を設定し、`lvm2-lvmetad` サービスを停止する必要があります。
- Oracle データベース 11.2.0.3 以降を使用していて、NID スクリプトを使用して補助インスタンスのデータベース ID を変更している場合は、13366202 Oracle パッチをインストールする必要があります。
- ボリュームをホストするアグリゲートが Storage Virtual Machine（SVM）に割り当てられたアグリゲートルISTに含まれていることを確認する必要があります。
- iSCSI プロトコルと FC プロトコルが混在する `igroup` を使用して、LUN が AIX ホストにマッピングされていないことを確認してください。詳細については、を参照してください **"LUNのデバイスを検出できません"**

いうエラーが表示されて処理に失敗します"。

## Oracle データベースバックアップをクローニングする

SnapCenter を使用して、データベースのバックアップを使用して Oracle データベースをクローニングすることができます。

### • このタスクについて \*

クローニング処理では、データベースデータファイルのコピーが作成され、新しいオンライン REDO ログファイルと制御ファイルが作成されます。指定したリカバリ・オプションに基づいて、データベースを指定した時刻までリカバリすることもできます。



Linux ホストで作成されたバックアップを AIX ホストにクローニングしようとする、クローニングが失敗します。その逆も同様です。

SnapCenter では、Oracle RAC データベースのバックアップからクローニングした場合にスタンドアロンデータベースが作成されます。SnapCenter では、Data Guard スタンバイデータベースおよび Active Data Guard スタンバイデータベースのバックアップからのクローニングをサポートしています。

クローニング中に、SnapCenter はリカバリ処理用にログバックアップをマウントします。リカバリ後、ログバックアップはアンマウントされます。これらのクローンはすべて、`/var/opt/snapcenter/scu/clones/`の下にマウントされます。NFS 経由で ASM を使用している場合は、`ASM_diskstring` パラメータで定義された既存のパスに `/var/opt/snapcenter/scu/clones/*/*_` を追加する必要があります。

SAN 環境で ASM データベースのバックアップをクローニングする際には、クローニングされるホストデバイスの `udev` ルールが `/etc/udev/rules.d/999-scu-netapp.rules_` に作成されます。クローニングされるホストデバイスに関連付けられた `udev` ルールは、クローンを削除すると削除されます。



Flex ASM 設定では、カードの数が RAC クラスタ内のノード数より少ない場合、リーフノードでクローン操作を実行できません。

### • 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\*] または [\*リソースグループ\*] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューでデータベースを選択します。

データベーストポロジのページが表示されます。

4. [コピーの管理] ビューで、バックアップを [ローカルコピー] (プライマリ)、[ミラーコピー] (セカンダリ)、または [バックアップコピー] (セカンダリ) から選択します。
5. 表からデータバックアップを選択し、\* をクリックします  \*
6. [名前] ページで、次のいずれかの操作を実行します。

状況	手順
データベース（CDB または CDB 以外）のクローンを作成します。	<p>a. クローンの SID を指定します。</p> <p>クローンの SID はデフォルトでは使用できず、SID の最大長は 8 文字です。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  クローンを作成するホストに、同じ SID を持つデータベースが存在しないようにします。 </div>
Pluggable Database（PDB）のクローニング	<p>a. <b>[PDB Clone]</b> を選択します。</p> <p>b. クローニングする PDB を指定します。</p> <p>c. クローニングされた PDB の名前を指定します。PDB をクローニングする詳細な手順については、<a href="#">を参照してください</a> <b>"プラグイン可能なデータベースをクローニングします"</b>。</p>

ミラーデータまたはバックアップデータを選択した場合：

- ミラーまたはボルトにログバックアップがない場合、何も選択されず、ロケータは空です。
- ミラーまたはバックアップにログバックアップが存在する場合は、最新のログバックアップが選択され、対応するロケータが表示されます。



選択したログバックアップがミラーとバックアップの場所の両方に存在する場合、両方のロケータが表示されます。

7. [場所] ページで、次の操作を実行します。

フィールド	手順
ホストをクローニングする	<p>ソースデータベースホストがデフォルトで入力されています。</p> <p>代替ホスト上にクローンを作成する場合は、ソース・データベース・ホストと同じバージョンの Oracle および OS を持つホストを選択します。</p>

フィールド	手順
データファイルの場所	<p>データファイルの場所がデフォルトで入力されています。</p> <p>SAN または NFS ファイルシステムの SnapCenter のデフォルトの命名規則は、FileSystemNameofsourcedatabE_CLONESID です。</p> <p>ASM ディスクグループの SnapCenter のデフォルトの命名規則は、SC_HASHCODEofDISKGROUP_CLONESID です。HASHCODEofDISKGROUP は、ASM ディスクグループごとに一意の自動生成番号（2～10桁）です。</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>ASM ディスクグループ名をカスタマイズする場合は、Oracle がサポートする最大長に名前の長さが準拠していることを確認してください。</p> </div> <p>別のパスを指定する場合は、クローンデータベースのデータファイルマウントポイントまたは ASM ディスクグループ名を入力する必要があります。データファイルパスをカスタマイズする場合は、制御ファイルと REDO ログファイルの ASM ディスクグループ名またはファイルシステムも、データファイルに使用されている名前か、既存の ASM ディスクグループまたはファイルシステムに変更する必要があります。</p>

フィールド	手順
制御ファイル	<p data-bbox="863 157 1487 226">制御ファイルのパスがデフォルトで入力されています。</p> <p data-bbox="863 262 1487 399">制御ファイルは、データファイルと同じ ASM ディスクグループまたはファイルシステムに配置されます。制御ファイルのパスを無効にする場合は、別の制御ファイルのパスを指定します。</p> <div data-bbox="896 451 1487 556"><p data-bbox="1015 451 1453 546">ファイルシステムまたは ASM ディスクグループがホストに存在する必要があります。</p></div> <p data-bbox="863 598 1487 766">デフォルトでは、制御ファイルの数はソースデータベースの数と同じになります。制御ファイルの数は変更できますが、データベースをクローニングするには少なくとも 1 つの制御ファイルが必要です。</p> <p data-bbox="863 808 1487 903">制御ファイルのパスを、ソースデータベースとは異なるファイルシステム（既存）にカスタマイズできます。</p>

フィールド	手順
REDO ログ	<p>redo ログファイルグループ、パス、およびサイズがデフォルトで入力されています。</p> <p>REDO ログは、クローンデータベースのデータファイルと同じ ASM ディスクグループまたはファイルシステムに配置されます。REDO ログファイルのパスを上書きする場合は、ソースデータベースとは別のファイルシステムに REDO ログファイルのパスをカスタマイズできます。</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  新しいファイルシステムまたは ASM ディスクグループがホストに存在する必要があります。 </div> <p>デフォルトでは、Redo ロググループの数、Redo ログファイルのサイズはソースデータベースのサイズと同じになります。次のパラメータを変更できます。</p> <ul style="list-style-type: none"> <li>• Redo ロググループの数</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  データベースをクローニングするには、少なくとも 2 つの REDO ロググループが必要です。 </div> <ul style="list-style-type: none"> <li>• 各グループの REDO ログファイルとそのパス</li> </ul> <p>REDO ログファイルのパスを、ソースデータベースとは別のファイルシステム（既存）にカスタマイズできます。</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  データベースをクローニングするには、Redo ロググループに少なくとも 1 つの REDO ログファイルが必要です。 </div> <ul style="list-style-type: none"> <li>• Redo ログファイルのサイズ</li> </ul>

8. [Credentials] ページで、次の操作を実行します。

フィールド	手順
sys ユーザのクレデンシャル名	<p>クローンデータベースのシステムユーザパスワードを定義するために使用するクレデンシャルを選択します。</p> <p>ターゲットホストの sqlnet.ora ファイルで SQLNET.authentication_services が none に設定されている場合は、SnapCenter GUI で Credential として *None を選択しないでください。</p>
ASM インスタンス資格情報名	<p>クローンホスト上の ASM インスタンスへの接続に対して OS 認証が有効な場合は、「*なし」を選択します。</p> <p>それ以外の場合は、「'sys'」ユーザまたはクローン・ホストに適用可能な「'ysasm'」権限を持つユーザで構成された Oracle ASM クレデンシャルを選択します。</p>

Oracle ホーム、ユーザ名、およびグループの詳細が、ソースデータベースから自動的に入力されます。この値は、クローンを作成するホストの Oracle 環境に基づいて変更できます。

9. PreOps ページで、次の手順を実行します。

- a. クローニング処理の前に実行するプリスクリプトのパスと引数を入力します。

プリスクリプトは、`_ /var/opt/snapcenter /spl/scripts_or` 内のいずれかのフォルダに保存する必要があります。デフォルトでは、`/var/opt/snapcenter /spl/scripts_path` が読み込まれます。このパス内の任意のフォルダにスクリプトを配置した場合は、スクリプトが配置されているフォルダまでの完全なパスを指定する必要があります。

- b. Database Parameter settings セクションで、データベースの初期化に使用される、すでに入力されているデータベースパラメータの値を変更します。

をクリックすると、パラメータを追加できます  \*

Oracle Standard Edition を使用していて、データベースがアーカイブログモードで実行されている場合、またはアーカイブ REDO ログからデータベースをリストアする場合は、パラメータを追加してパスを指定します。

- LOG\_ARCHIVE\_dest の略
- log\_archive\_duplex\_dest



Fast Recovery Area (FRA) は、すでに格納されているデータベースパラメータに定義されていません。関連パラメータを追加することで、FRA を構成できます。



LOG\_ARCHIVE のデフォルト値は \$ORACLE\_HOME/clone\_sid で、クローンデータベースのアーカイブログはこの場所に作成されます。log\_archive\_dest\_1 パラメータを削除した場合、アーカイブ・ログの場所は Oracle によって決定されます。log\_archive\_dest\_1 を編集して、アーカイブ・ログの新しい場所を定義できます。ただし、ファイル・システムまたはディスク・グループが、ホスト上に存在し、使用可能になっている必要があります。

a. [\*Reset] をクリックして、データベースパラメータのデフォルト設定を取得します。

1. PostOps ページで、\* Recover database \* および \* Until Cancel \* がデフォルトで選択されて、クローンデータベースのリカバリを実行します。

SnapCenter は、クローニング用に選択されたデータバックアップ後に、破損していない一連のアーカイブログを含む最新のログバックアップをマウントすることによってリカバリを実行します。セカンダリストレージでクローニングを実行するには、プライマリストレージでログとデータのバックアップを実行し、セカンダリストレージでログとデータのバックアップを実行する必要があります。

SnapCenter が適切なログ・バックアップを検出できない場合は、[データベースのリカバリ \*] および [キャンセルまで \*] オプションは選択されません。外部アーカイブログの場所を指定する：\* でログバックアップを使用できない場合は、外部アーカイブログの場所を指定します。\*複数のログの場所を指定できます。



フラッシュリカバリ領域（FRA）と Oracle Managed Files（OMF）をサポートするように設定されているソースデータベースをクローニングする場合は、リカバリのログデスティネーションも OMF ディレクトリ構造に従っている必要があります。

ソースデータベースが Data Guard スタンバイデータベースまたは Active Data Guard スタンバイデータベースの場合、PostOps ページは表示されません。Data Guard スタンバイデータベースまたは Active Data Guard スタンバイデータベースの場合、SnapCenter には SnapCenter GUI でリカバリのタイプを選択するオプションはありませんが、ログを適用せずに、Cancel リカバリタイプを使用してデータベースをリカバリします。

フィールド名	説明
キャンセルするまで	SnapCenter は、クローニング用に選択されたデータバックアップのあとに、アーカイブログの連続が解除された最新のログバックアップをマウントすることによってリカバリを実行します。クローンデータベースは、欠落または破損したログファイルまでリカバリされます。
日付と時刻	SnapCenter は、指定された日時までデータベースをリカバリします。指定できる形式は、mm/dd/yyyy hh:mm:ss です   時刻は 24 時間形式で指定できません。

フィールド名	説明
Until SCN (システム変更番号)	SnapCenter は、指定された System Change Number (SCN) までデータベースをリカバリします。
外部アーカイブログの場所を指定します	外部アーカイブログの場所を指定します。
新しい DBID を作成します	<p>デフォルトでは、*新しい DBID* を作成チェック・ボックスが選択され、ソース・データベースとは別の、クローン・データベースに一意の番号 (DBID) が生成されます。</p> <p>ソースデータベースの DBID をクローンデータベースに割り当てる場合は、このチェックボックスをオフにします。このシナリオでは、ソースデータベースがすでに登録されている外部の RMAN カタログにクローニングされたデータベースを登録する場合に、処理が失敗します。</p>
一時表領域用の tempfile を作成します	<p>クローニングされたデータベースのデフォルトの一時表領域に対して一時ファイルを作成する場合は、チェックボックスをオンにします。</p> <p>このチェックボックスをオフにすると、tempfile を使用せずにデータベースクローンが作成されず。</p>
クローン作成時に適用する SQL エントリを入力します	クローン作成時に適用する SQL エントリを追加します。
クローニング処理のあとに実行するスクリプトを入力します	<p>クローニング処理の実行後に実行するポストスクリプトのパスと引数を指定します。</p> <p>PostScript は /var/opt/snapcenter /spl/scripts_or に保存するか、このパス内の任意のフォルダに保存する必要があります。デフォルトでは、/var/opt/snapcenter /spl/scripts_path が読み込まれます。</p> <p>このパス内の任意のフォルダにスクリプトを配置した場合は、スクリプトが配置されているフォルダまでの完全なパスを指定する必要があります。</p>

1. [通知] ページの [電子メールの設定\*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および Eメールの件名を指定する必要があります。実行したクローン処理のレポートを添付する場合は、\*ジョブレポートの添付\*を選択します。



E メール通知を利用する場合は、GUI または PowerShell コマンド Set-SmtpServer を使用して、SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、[完了] をクリックします。



クローニング処理の一環としてリカバリを実行する場合は、リカバリが失敗してもクローンが作成され、警告が表示されます。このクローンに対して手動リカバリを実行することで、クローンデータベースの整合性を確保できます。

2. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

• 結果 \*

データベースをクローニングしたあとにリソースページを更新すると、クローンデータベースが、バックアップに使用できるリソースの1つとしてリストに追加されます。クローンデータベースは、標準バックアップワークフローを使用して他のデータベースと同様に保護することも、リソースグループ（新規作成または既存）に含めることもできます。クローニングされたデータベースは、さらにクローニング（クローンのクローニング）が可能です。

クローニング後は、クローンデータベースの名前を絶対に変更しないでください。



クローニング中にリカバリを実行しなかった場合は、不適切なリカバリが原因でクローンデータベースのバックアップが失敗し、手動によるリカバリが必要になることがあります。また、アーカイブログが格納されたデフォルトの場所がネットアップ以外のストレージにある場合や、ストレージシステムに SnapCenter が設定されていない場合も、ログバックアップが失敗することがあります。

AIX のセットアップでは、lkdev コマンドを使用して、クローニングされたデータベースが存在するディスクの名前をロックし、rendev コマンドを使用して変更できます。

デバイスをロックしたり名前を変更したりしても、クローンの削除処理には影響しません。SAN デバイス上に構築された AIX LVM レイアウトの場合、クローニングされた SAN デバイスではデバイスの名前変更はサポートされません。

- 詳細はこちら \*
- "リストアまたはクローニングが失敗して ORA-00308 エラーメッセージが表示されます"
- "クローンデータベースをリカバリできませんでした"
- "AIX システムでのバックアップ、リストア、クローニングの各処理のパラメータをカスタマイズできません"

## プラグイン可能なデータベースをクローニングします

プラグイン可能なデータベース（PDB）を、同じホストまたは代替ホスト上にある別のターゲット CDB にクローニングすることができます。クローニングした PDB を目的の SCN または日時にリカバリすることもできます。

• 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\*] または[\* リソースグループ\*] を選択します。
3. データベースの詳細ビューまたはリソースグループの詳細ビューで、タイプがシングルインスタンス (マルチテナント) のデータベースを選択します。

データベーストポロジのページが表示されます。

4. [コピーの管理] ビューで、バックアップを[ローカルコピー] (プライマリ)、[ミラーコピー] (セカンダリ)、または[バックアップコピー] (セカンダリ) から選択します。
5. 表からバックアップを選択し、\* をクリックします  \*
6. [名前] ページで、次の操作を実行します。
  - a. [PDB Clone] を選択します。
  - b. クローニングする PDB を指定します。



一度にクローニングできる PDB は 1 つだけです。

- c. クローン PDB の名前を指定します。

7. [場所] ページで、次の操作を実行します。

フィールド	手順
ホストをクローニングする	ソースデータベースホストがデフォルトで入力されています。  代替ホスト上にクローンを作成する場合は、ソース・データベース・ホストと同じバージョンの Oracle および OS を持つホストを選択します。
ターゲット CDB	クローニングされた PDB を含める CDB を選択します。  ターゲット CDB が実行されていることを確認します。
データベースの状態	PDB を読み取り / 書き込みモードで開く場合は、「* クローン PDB を読み取り / 書き込みモードで開く」チェックボックスをオンにします。

<p>データファイルの場所</p>	<p>データファイルの場所がデフォルトで入力されています。</p> <p>SAN または NFS ファイルシステムの SnapCenter のデフォルトの命名規則は、FileSystemNameofsourcedatabE_SCJOBID です。</p> <p>ASM ディスクグループの SnapCenter のデフォルトの命名規則は、SC_HASHCODEofDISKGROUP_SCJOBID です。HASHCODEofDISKGROUP は、ASM ディスクグループごとに一意の自動生成番号（2～10桁）です。</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p> ASM ディスクグループ名をカスタマイズする場合は、Oracle がサポートする最大長に名前の長さが準拠していることを確認してください。</p> </div> <p>別のパスを指定する場合は、クローンデータベースのデータファイルマウントポイントまたは ASM ディスクグループ名を入力する必要があります。</p>
-------------------	---

Oracle ホーム、ユーザ名、およびグループの詳細が、ソースデータベースから自動的に入力されます。この値は、クローンを作成するホストの Oracle 環境に基づいて変更できます。

8. PreOps ページで、次の手順を実行します。

- a. クローニング処理の前に実行するプリスクリプトのパスと引数を入力します。

プリスクリプトは `/var/opt/snapcenter /spl/scripts` またはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、`/var/opt/snapcenter /spl/scripts` パスが読み込まれます。このパス内の任意のフォルダにスクリプトを配置した場合は、スクリプトが配置されているフォルダまでの完全なパスを指定する必要があります。

- b. 補助 CDB クローンデータベースのパラメータ設定セクションで、データベースの初期化に使用される、すでにデータが格納されているデータベースパラメータの値を変更します。

9. [\*Reset] をクリックして、データベースパラメータのデフォルト設定を取得します。

10. PostOps ページで、\* Until Cancel \* がデフォルトで選択され、クローンデータベースのリカバリを実行します。

SnapCenter が適切なログ・バックアップを見つけられない場合は、\* Until Cancel \* オプションは選択されません。外部アーカイブログの場所を指定する：\* でログバックアップを使用できない場合は、外部アーカイブログの場所を指定します。\*複数のログの場所を指定できます。



フラッシュリカバリ領域（FRA）と Oracle Managed Files（OMF）をサポートするように設定されているソースデータベースをクローニングする場合は、リカバリのログデスティネーションも OMF ディレクトリ構造に従っている必要があります。

フィールド名	説明
キャンセルするまで	<p>SnapCenter は、クローニング用に選択されたデータバックアップのあとに、アーカイブログの連続が解除された最新のログバックアップをマウントすることによってリカバリを実行します。</p> <p>セカンダリストレージでクローンを実行するには、プライマリストレージでログとデータのバックアップを実行し、セカンダリストレージでログとデータのバックアップを実行する必要があります。クローンデータベースは、欠落または破損したログファイルまでリカバリされます。</p>
日付と時刻	<p>SnapCenter は、指定された日時までデータベースをリカバリします。</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>時刻は 24 時間形式で指定できません。</p> </div>
Until SCN (システム変更番号)	<p>SnapCenter は、指定された System Change Number (SCN) までデータベースをリカバリします。</p>
外部アーカイブログの場所を指定します	<p>外部アーカイブログの場所を指定します。</p>
新しい DBID を作成します	<p>デフォルトでは、補助クローンデータベースに対して新しい DBID * を作成チェック・ボックスは選択されません。</p> <p>補助クローンデータベースとソースデータベースを区別するために一意の番号 (DBID) を生成する場合は、このチェックボックスを選択します。</p>
一時表領域用の tempfile を作成します	<p>クローニングされたデータベースのデフォルトの一時表領域に対して一時ファイルを作成する場合は、チェックボックスをオンにします。</p> <p>このチェックボックスをオフにすると、tempfile を使用せずにデータベースクローンが作成されます。</p>
クローン作成時に適用する SQL エントリを入力します	<p>クローン作成時に適用する SQL エントリを追加します。</p>

フィールド名	説明
クローニング処理のあとに実行するスクリプトを入力します	<p>クローニング処理の実行後に実行するポストスクリプトのパスと引数を指定します。</p> <p>PostScript は /var/opt/snapcenter /spl/scripts_or に保存するか、このパス内の任意のフォルダに保存する必要があります。</p> <p>デフォルトでは、 /var/opt/snapcenter /spl/scripts_path が読み込まれます。このパス内の任意のフォルダにスクリプトを配置した場合は、スクリプトが配置されているフォルダまでの完全なパスを指定する必要があります。</p>

11. [通知] ページの [ 電子メールの設定 \*] ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者の E メールアドレス、および E メール の件名を指定する必要があります。実行したクローン処理のレポートを添付する場合は、\* ジョブレポートの添付 \* を選択します。



E メール通知を利用する場合は、GUI または PowerShell コマンド Set-SmtpServer を使用して、SMTP サーバの詳細を指定しておく必要があります。

1. 概要を確認し、[完了] をクリックします。
2. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

• 終了後 \*

クローニングされた PDB のバックアップを作成する場合は、クローン PDB のみをバックアップできないため、PDB がクローニングされたターゲット CDB をバックアップしてください。セカンダリ関係を使用してバックアップを作成する場合は、ターゲット CDB のセカンダリ関係を作成する必要があります。

RAC セットアップでは、クローニングされた PDB のストレージは、PDB クローンが実行されたノードにのみ接続されます。RAC の他のノードの PDB はマウント状態です。クローニングした PDB に他のノードからアクセスできるようにするには、その PDB を他のノードに手動で接続してください。

- 詳細はこちら \*
- "リストアまたはクローニングが失敗して ORA-00308 エラーメッセージが表示されます"
- "AIX システムでのバックアップ、リストア、クローニングの各処理のパラメータをカスタマイズできません"

## UNIX コマンドを使用して Oracle データベースバックアップをクローニングする

クローニングワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

- このタスクについて \*

次のコマンドを実行して、Oracle データベースのクローン仕様ファイルを作成し、クローニング処理を開始

する必要があります。

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、`Get-Help_command_name_` を実行して取得できます。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リファレンスガイド](#)"。

- 手順 \*

1. 指定したバックアップから Oracle データベースのクローン仕様を作成します：`New-SmOracleCloneSpecification`



セカンダリデータ保護ポリシーが Unified mirror-vault の場合は、`-IncludeSecondaryDetails` のみを指定します。`SecondaryStorageType` を指定する必要はありません。

このコマンドは、指定したソースデータベースとそのバックアップに対して、Oracle データベースのクローン仕様ファイルを自動的に作成します。作成するクローンデータベースに対して自動的に生成される値がこの仕様ファイルに取り込まれるようにするために、クローンデータベースの SID も指定する必要があります。



クローン仕様ファイルは、`/var/opt/snapcenter /sca/clone_specs__` に作成されます。

2. クローンリソースグループまたは既存のバックアップからクローン処理を開始する：`New-SmClone`

このコマンドによってクローニング処理が開始されます。クローニング処理では、Oracle クローン仕様ファイルのパスも指定する必要があります。リカバリオプション、クローニング処理が実行されるホスト、プリスクリプト、ポストスクリプト、およびその他の詳細を指定することもできます。

デフォルトでは、クローンデータベースのアーカイブログデスティネーションファイルには、`$ORACLE_HOME/clone_SID` が自動的に入力されます。

## Oracle データベースクローンをスプリットします

SnapCenter を使用して、クローニングされたリソースを親リソースからスプリットできます。スプリットされたクローンは、親リソースに依存しません。

- このタスクについて \*
- 中間のクローンに対してクローンスプリット処理を実行することはできません。

たとえば、データベースバックアップから clone1 を作成したあとで、Clone1 のバックアップを作成し、そのバックアップ（Clone2）をクローニングできます。Clone2 を作成すると、clone1 は中間クローンであり、clone1 でクローンスプリット処理を実行することはできません。ただし、Clone2 でクローンスプリット処理を実行することはできます。

Clone2 をスプリットしたあとは、clone1 が中間クローンではなくなるため、clone1 でクローンスプリット処理を実行できます。

- クローンをスプリットすると、クローンのバックアップコピーが削除されます。
- クローンスプリット処理の制限事項については、を参照してください "[ONTAP 9 論理ストレージ管理ガイド](#)"。

- ストレージシステム上のボリュームまたはアグリゲートがオンラインであることを確認します。
- 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. クローニングされたリソース（データベースや LUN など）を選択し、をクリックします 。
  4. スプリットするクローンの推定サイズとアグリゲートで使用可能なスペースを確認し、\* Start \* をクリックします。
  5. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

SMCore サービスが再起動され、クローンスプリット処理が実行されたデータベースがリソースページにクローンとして表示される場合、クローンスプリット処理が停止します。\_Stop-SmJob\_cmdlet を実行してクローンスプリット処理を停止し、クローンスプリット処理を再試行する必要があります。

クローンがスプリットされているかどうかを確認するためにポーリング時間を長くしたり、ポーリング時間を短縮したりする場合は、SMCoreServiceHost.exe.config ファイルの CloneSplitStatusCheckPollTime パラメータの値を変更して、クローンスプリット処理のステータスをポーリングする SMCore の時間間隔を設定できます。この値はミリ秒で、デフォルト値は 5 分です。

例：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```



バックアップ、リストア、またはその他のクローンスプリットの実行中は、クローンスプリットの開始処理が失敗します。クローンスプリット処理は、実行中の処理が完了してから再開してください。

## プラグイン可能なデータベースのスプリットクローン

SnapCenter を使用して、クローニングされた Pluggable Database (PDB) をスプリットできます。

- このタスクについて \*

PDB がクローニングされたターゲット CDB のバックアップを作成した場合は、PDB クローンをスプリットすると、クローン PDB を含むターゲット CDB のすべてのバックアップからもクローニングされた PDB が削除されます。



PDB クローンは、インベントリビューやリソースビューに表示されません。

- 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. リソースまたはリソースグループのビューからソースコンテナデータベース（CDB）を選択します。
3. [コピーの管理]ビューで'プライマリまたはセカンダリ（ミラーまたはレプリケートされた）ストレージ・システムから[クローン\*]を選択します
4. PDB クローン（targetCDB：PDBClone）を選択し、をクリックします 。
5. スプリットするクローンの推定サイズとアグリゲートで使用可能なスペースを確認し、\* Start \* をクリックします。
6. 操作の進行状況を監視するには、\* Monitor \* > \* Jobs \* をクリックします。

## Oracle データベースのクローニング処理を監視する

Jobs ページを使用して、SnapCenter のクローニング処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理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
-  キャンセルされました
- 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、次の手順を実行します。
  - a. をクリックします  をクリックして、クローニング処理のみが表示されるようにリストをフィルタリングします。
  - b. 開始日と終了日を指定します。
  - c. [Type](タイプ) ドロップダウンリストから '[\*Clone](クローン\*)' を選択します
  - d. [\* Status \*] ドロップダウン・リストから、クローンのステータスを選択します。
  - e. [適用 (Apply)] をクリックして、正常に完了した操作を表示する。
4. クローンジョブを選択し、\* Details \* 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。

## クローンをリフレッシュします

クローンを更新するには、*Refresh-SmClone* コマンドを実行します。このコマンドは、データベースのバックアップを作成し、既存のクローンを削除し、同じ名前でクローンを作成します。



PDB クローンは更新できません。

- 必要なもの \*
- スケジュールされたバックアップが有効になっていない状態で、オンラインフルバックアップまたはオフラインデータバックアップポリシーを作成します。
- バックアップエラーのみに関する E メール通知をポリシーで設定します。
- オンデマンドバックアップの保持数を適切に定義して、不要なバックアップがないことを確認します。
- 更新クローン処理で特定されるリソースグループには、オンラインフルバックアップまたはオフラインデータバックアップポリシーのみが関連付けられていることを確認します。
- データベースが 1 つだけのリソースグループを作成する。
- clone refresh コマンドに対して cron ジョブが作成される場合は、SnapCenter スケジュールおよび cron スケジュールがデータベースリソースグループに対して重複しないようにしてください。

clone refresh コマンド用に作成された cron ジョブの場合、24 時間ごとに Open-SmConnection を実行してください。

- クローンの SID がホストで一意であることを確認します。

複数の更新クローン処理で同じクローン仕様ファイルを使用する場合、または同じクローン SID を持つクローン仕様ファイルを使用する場合は、ホスト上で SID を持つ既存のクローンが削除され、そのクローンが作成されます。

- セカンダリ・バックアップを使用してクローンを作成するには 'バックアップ・ポリシーがセカンダリ保護で有効になっていること' およびクローン仕様ファイルが作成されていることを確認してください
  - プライマリクローン仕様ファイルを指定し、ポリシーでセカンダリ更新オプションを選択した場合、バックアップが作成され、セカンダリに更新が転送されます。ただし、クローンはプライマリバックアップから作成されます。
  - プライマリクローン仕様ファイルを指定し、ポリシーでセカンダリ更新オプションが選択されていない場合、プライマリ上にバックアップが作成され、プライマリからクローンが作成されます。
- 手順 \*
  1. 指定されたユーザ用に SnapCenter サーバとの接続セッションを開始します： *Open-SmConnection*
  2. 指定したバックアップから Oracle データベースのクローン仕様を作成します： *New-SmOracleCloneSpecification*



セカンダリデータ保護ポリシーが Unified mirror-vault の場合は、-IncludeSecondaryDetails のみを指定します。SecondaryStorageType を指定する必要はありません。

このコマンドは、指定したソースデータベースとそのバックアップに対して、Oracle データベースの

クローン仕様ファイルを自動的に作成します。作成するクローンデータベースに対して自動的に生成される値がこの仕様ファイルに取り込まれるようにするために、クローンデータベースの SID も指定する必要があります。



クローン仕様ファイルは、`/var/opt/snapcenter /sca/clone_specs__` に作成されます。

### 3. Run\_Refresh - SmClone\_。

"PL-SCO-20032: CanExecute 操作がエラーで失敗した場合 : PL-SCO-300331: Redo ログファイル +SC\_2959770772\_clmdb/clredolog/redo01\_01.log Exist" エラーメッセージが表示されたときに、操作が失敗した場合は、`-WaitToTriggerClone_` に高い値を指定してください。

UNIX コマンドの詳細については、を参照してください "[SnapCenter ソフトウェアコマンドリファレンスガイド](#)"。

## プラグイン可能なデータベースのクローンを削除します

不要になった Pluggable Database (PDB) のクローンは削除できます。

PDB がクローニングされたターゲット CDB のバックアップを作成した場合、PDB クローンを削除すると、クローン PDB もターゲット CDB のバックアップから削除されます。



PDB クローンは、インベントリビューやリソースビューに表示されません。

#### • 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. リソースまたはリソースグループのビューからソースコンテナデータベース (CDB) を選択します。
3. [コピーの管理] ビューで 'プライマリまたはセカンダリ (ミラーまたはレプリケートされた) ストレージ・システムから [クローン \*]' を選択します
4. PDB クローン (targetCDB : PDBClone) を選択し、をクリックします .
5. [OK] をクリックします。

## 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随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。