



Oracleデータベースのバックアップ SnapCenter software

NetApp
November 06, 2025

目次

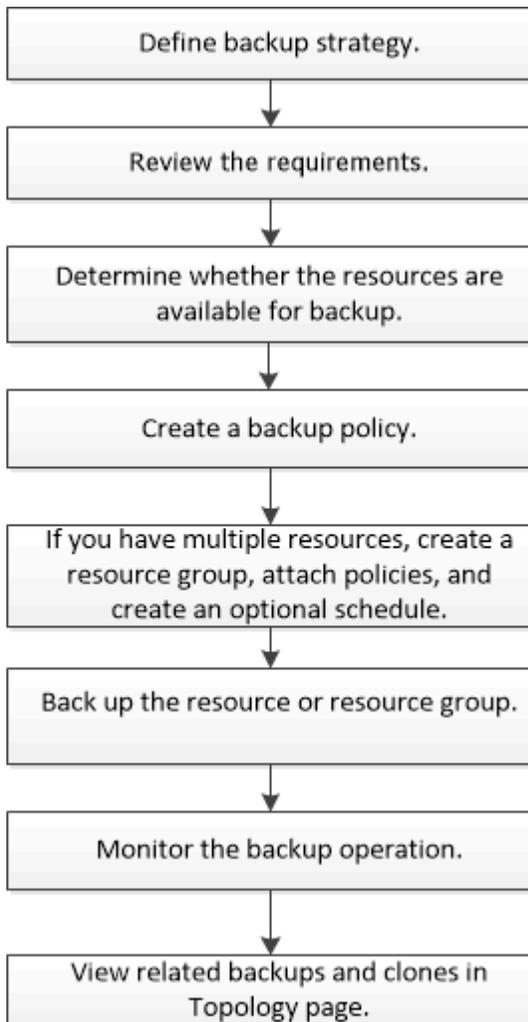
Oracleデータベースのバックアップ	1
バックアップ手順の概要	1
バックアップ構成情報	2
バックアップ対象としてサポートされるOracleデータベース構成	2
Oracleデータベースでサポートされるバックアップ タイプ	3
SnapCenterのOracleデータベース検出方法	3
RACセットアップにおける優先ノード	5
Oracle Recovery Managerを使用してバックアップをカタログ化する方法	6
バックアップ固有のプリスクリプトとポストスクリプト用に事前定義された環境変数	7
バックアップ保持オプション	13
バックアップ スケジュール	13
バックアップの命名規則	14
Oracleデータベースのバックアップの要件	14
バックアップに使用できるOracleデータベースの検出	15
ステップ1: SnapCenterがデータベース以外のエントリを検出しないようにする	15
ステップ2: リソースの発見	16
Oracleデータベースのバックアップ ポリシーの作成	17
Oracleデータベースのリソース グループの作成とポリシーの適用	23
リソース グループを作成し、ASA r2 システム上の Oracle リソースの二次保護を有効にします。	26
Oracleリソースのバックアップ	28
Oracleデータベースのリソース グループのバックアップ	31
Oracleデータベースのバックアップの監視	32
Oracleデータベースのバックアップ処理の監視	32
[Activity]ペインでデータ保護処理を監視	33
その他のバックアップ処理	33
UNIXコマンドを使用したOracleデータベースのバックアップ	33
Oracleデータベースのバックアップ処理のキャンセル	34
[Topology]ページでのOracleデータベースのバックアップとクローンの表示	35

Oracleデータベースのバックアップ

バックアップ手順の概要

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。バックアップ手順には、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、データベース上で複数の操作が実行されないように、Oracle データベース ホストの `/var/opt/snapcenter/sco/lock` ディレクトリに操作ロック 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完了したものの警告が表示された場合は、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ない場合、最終的にはキャンセルされる可能性があります。そのような場合は、次の手順を実行して、処理ロック 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、`/var/opt/snapcenter/sco/lock` に移動します。
2. 操作ロックを削除します。`rm -rf .sm_lock_dbssid.`

バックアップ構成情報

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 Standalone
- Oracle Real Application Clusters (RAC)
- Oracle Standalone Legacy
- Oracle Standalone Container Database (CDB)
- Oracle Data Guardスタンバイ

Data Guardスタンバイ データベースで作成できるのは、オフライン マウント バックアップのみです。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、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 データベースで作成できるのは、オンライン バックアップのみです。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場合は、管理されたリカバリ プロセス (MRP) が事前に停止し、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)

- ASM スタンドアロンおよび仮想マシン ディスク (VMDK) 上の ASM RAC

Oracleデータベースでサポートされているすべてのリストア方式の中で、VMDK上のASM RACデータベースで実行できるのはConnect and Copyリストアだけです。

- ASM スタンドアロンおよび Raw デバイス マッピング (RDM) 上の ASM RAC + ASMLib の有無にかかわらず、ASM 上の Oracle データベースでバックアップ、復元、およびクローン操作を実行できます。
- Oracle ASMフィルタ ドライバ (ASMFD)

PDB移行および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バージョンの最新情報については、"[NetApp Interoperability Matrix Tool](#)"。

Oracleデータベースでサポートされるバックアップ 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）
- データベース全体（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）

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であると、バックアップ処理は失敗します。

- 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は、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のOracleデータベース検出方法

リソースは、SnapCenterによって管理されるホスト上の Oracle データベースです。使用できる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。

次のセクションでは、さまざまなタイプとバージョンのOracleデータベースを検出するためにSnapCenterが使用するプロセスについて説明します。

Oracle バージョン 11g から 12cR1 の場合

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ファイルにデータベー

ス エントリが含まれている必要があります。

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。

ASM

ASM インスタンス エントリが `/etc/oratab` ファイルに含まれている必要があります。

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。データベースは、`nomount`、`mount`、または `open` のいずれかの状態である必要があります。`/etc/oratab` ファイルにデータベース エントリが含まれている必要があります。

データベースがすでに検出され、バックアップがデータベースに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名前変更または削除とマークされます。

データベースを再配置した場合は、次の手順を実行する必要があります。

1. フェイルオーバーされた RAC ノードの `/etc/oratab` ファイルに、再配置されたデータベースのエントリを手動で追加します。
2. リソースを手動で更新します。
3. リソース ページから RAC One Node データベースを選択し、「データベース設定」をクリックします。
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。
5. SnapCenter の処理を実行します。
6. 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ときに、以前のノードの `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します。

Oracle バージョン 12cR2 から 18c、19c、または 21c の場合

RAC データベース

RAC データベースは `srvctl config` コマンドを使用して検出されます。`/etc/oratab` ファイルにデータベース エントリが含まれている必要があります。

スタンドアロン

スタンドアロン データベースは、`/etc/oratab` ファイルのエントリと `srvctl config` コマンドの出力に基づいて検出されます。

ASM

ASM インスタンス エントリが `/etc/oratab` ファイルに含まれている必要はありません。

RAC One Node

RAC One Node データベースは、`srvctl config` コマンドのみを使用して検出されます。データベースは、`nomount`、`mount`、または `open` のいずれかの状態である必要があります。データベースがすでに検出され、バックアップがデータベースに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名前変更または削除とマークされます。

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。リソースを手動で更新します。。リソース ページから RAC One Node データベースを選択し、「データベース設定」をクリックします。。デ

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。SnapCenterの処理を実行します。



/etc/oratab ファイルに Oracle 12cR2 および 18c データベース 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、データベースは検出されませんが、データベースは到達不能になり、ステータスはオフラインになります。

RACセットアップにおける優先ノード

Oracle Real Application Clusters (RAC) セットアップでは、SnapCenterがバックアップ操作を実行するために使用す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つまたは複数指定できます。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。

例

RACデータベースcdbracに3つのインスタンスがあり、cdbrac1はnode1に、cdbrac2はnode2に、cdbrac3はnode3に置かれているとします。

node1とnode2のインスタンスが優先ノードとして設定され、node2に第1優先順位、node1に第2優先順位が指定されています。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がバックアップできる状態にない場合（ホストでプラグイン エージェントが実行されていない、ホスト上のデータベース インスタンスが指定したタイプのバックアップを行うのに必要な状態にない、Flex ASM構成のnode2上のデータベース インスタンスがローカルASMインスタンスによって処理されていない、などの複数の原因が考えられます）、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セットアップ

Flex ASMセットアップでは、カーディナリティが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リストされません。Flex ASMクラスタ ノードのロールに変更があった場合は、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、あとから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なってい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。

外部カタログ データベース

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 インターフェイス (GUI) から[Database Settings]ウィザードを使用して外部カタログのクレデンシャルとTransparent Network Substrate (TNS) 名を指定することにより、そのデータベースを設定できます。外部カタログ データベースはCLIから設定することもできます。その場合は、Configure-SmOracleDatabaseコマンドを、-OracleRmanCatalogCredentialNameオプションおよび-OracleRmanCatalogTnsNameオプションとともに実行します。

RMANコマンド

SnapCenter GUIで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。バックアップの遅延カタログ作成を実行するには、`Catalog-SmBackupWithOracleRMAN`指示。

バックアップをカタログ化した後、`Get-SmBackupDetails`カタログ化されたデータファイルのタグ、制御ファイルのカタログパス、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するコマンド。

命名形式

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に、バックアップに対してSC_HASHCODEofDISKGROUP_DBSID_BACKUPIDという命名形式が使用されます。一方、ディスク グループ名が16文字未満である場合は、バックアップに対してDISKGROUPNAME_DBSID_BACKUPIDという命名形式が使用されます。これはSnapCenter 2.0で使用される形式と同じです。

HASHCODEofDISKGROUPは自動生成される2~10桁の番号で、各ASMディスク グループに固有です。

クロスチェック処理

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

データ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、制御ファイルの情報を更新できます。クロスチェックを有効にするには、Set-SmConfigSettingsコマンドを実行し、ENABLE_CROSSCHECKパラメータにTRUEを割り当てます。デフォルト値はFALSEです。

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings  
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

カタログ情報の削除

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。

処理時間が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や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。

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType  
Plugin -PluginCode SCO-ConfigSettings  
"KEY=ORACLE_PLUGIN_RMAN_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は、Get-Help command_nameを実行して確認できます。または、"[SnapCenterソフトウェア コマンド リファレンス ガイド](#)"。

バックアップ固有のプリスクリプトとポストスクリプト用に事前定義された環境変数

SnapCenterでは、バックアップ ポリシーの作成時にプリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。この機能は、VMDKを除くすべてのOracle設定でサポートされます。

SnapCenterにより、シェル スクリプトが実行される環境で直接アクセスできるパラメータの値が事前に定義されます。スクリプトの実行時に、これらのパラメータの値を手動で指定する必要はありません。

バックアップ ポリシーの作成でサポートされる事前定義された環境変数

- **SC_JOB_ID** は操作のジョブ ID を指定します。

例：256

- **SC_ORACLE_SID** はデータベースのシステム識別子を指定します。

複数のデータベースが処理対象となる場合、パラメータにはパイプで区切られたデータベース名が含まれます。

このパラメータはアプリケーション ボリュームに対して設定されます。

例: NFSB32|NFSB31

- **SC_HOST** はデータベースのホスト名を指定します。

RACの場合、ホスト名はバックアップが実行されるホストの名前です。

このパラメータはアプリケーション ボリュームに対して設定されます。

例：scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** は、データベースのオペレーティング システムの所有者を指定します。

データは <db1>@<osuser1>|<db2>@<osuser2> の形式になります。

例: NFSB31@oracle|NFSB32@oracle

- **SC_OS_GROUP** は、データベースのオペレーティング システム グループを指定します。

データは <db1>@<osgroup1>|<db2>@<osgroup2> の形式になります。

例: NFSB31@install|NFSB32@oinstall

- **SC_BACKUP_TYPE** は、バックアップの種類（オンラインフル、オンラインデータ、オンラインログ、オフラインシャットダウン、オフラインマウント）を指定します。

例:

- 完全バックアップの場合: ONLINEFULL
- データのみのバックアップ: ONLINEDATA
- ログのみのバックアップの場合: ONLINELOG

- **SC_BACKUP_NAME** はバックアップの名前を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1|AV@RG2_scspr2417819002_07-20-2021_12.16.48.9267

- **SC_BACKUP_ID** はバックアップ ID を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例: DATA@203|LOG@205|AV@207

- **SC_ORACLE_HOME** は、Oracle ホーム ディレクトリのパスを指定します。

例: NFSB32@/ora01/app/oracle/product/18.1.0/db_1|NFSB31@/ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_RETENTION** は、ポリシーで定義された保持期間を指定します。

例:

- 完全バックアップの場合: 毎時|DATA@DAYS:3|LOG@COUNT:4
- オンデマンドデータのみバックアップの場合: Ondemand|DATA@COUNT:2
- オンデマンドログのみバックアップの場合: Ondemand|LOG@COUNT:2

- **SC_RESOURCE_GROUP_NAME** はリソース グループの名前を指定します。

例: RG1

- **SC_BACKUP_POLICY_NAME** は、バックアップ ポリシーの名前を指定します。

例: backup_policy

- **SC_AV_NAME** はアプリケーション ボリュームの名前を指定します。

例: AV1|AV2

- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** は、データ ファイル ディレクトリのボリュームへの SVM のストレージ マッピングを指定します。LUNおよびqtreeの親ボリュームの名前になります。

データは <db1>@<SVM1:volume1>|<db2>@<SVM2:volume2> としてフォーマットされます。

例:

- 同じリソース グループ内の 2 つのデータベースの場合:
NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
- データ ファイルが複数のボリュームに分散している単一のデータベースの場合
: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS

- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** は、ログ ファイル ディレクトリのボリュームへの SVM のストレージ マッピングを指定します。LUNおよびqtreeの親ボリュームの名前になります。

例:

- 単一のデータベース インスタンスの場合: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
- 複数のデータベースインスタンスの場合:
NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO

- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** は、ストレージ システム名とボリューム名を含むスナップショットのリストを指定します。

例:

- 単一のデータベース インスタンスの場合
: buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 複数のデータベースインスタンスの場合:
NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

• **SC_PRIMARY_SNAPSHOT_NAMES** は、バックアップ中に作成されたプライマリスナップショットの名前を指定します。

例:

- 単一データベースインスタンスの場合: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0、RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 複数のデータベースインスタンスの場合: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 2つのボリュームを含む整合グループSnapshotの場合: cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_3_8_58_350

• **SC_PRIMARY_MOUNT_POINTS** は、バックアップの一部であるマウント ポイントの詳細を指定します。

詳細には、バックアップ対象のファイルの直接の親ではなく、ボリュームがマウントされているディレクトリが含まれます。ASM構成の場合は、ディスク グループの名前です。

データは <db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2> の形式になります。

例:

- 単一データベースインスタンスの場合: /mnt/nfsdb3_data、/mnt/nfsdb3_log、/mnt/nfsdb3_data1
- 複数のデータベースインスタンスの場合: NFSB31@/mnt/nfsdb31_data、/mnt/nfsdb31_log、/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data、/mnt/nfsdb32_log、/mnt/nfsdb32_data1
- ASMの場合: +DATA2DG、+LOG2DG

• **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** は、各マウント ポイントのバックアップ中に作成されたスナップショットの名前を指定します。

例:

- 単一データベースインスタンスの場合: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data、RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log
- 複数のデータベースインスタンスの場合: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_07-21-

2021_02.28.26.3973_0:/mnt/nfsb31_data, RG2_scspr2417819002_07-21-
2021_02.28.26.3973_1:/mnt/nfsb32_log

- **SC_ARCHIVELOGS_LOCATIONS** は、アーカイブ ログ ディレクトリの場所を指定します。

アーカイブ ログ ファイルの直接の親ディレクトリの名前になります。アーカイブ ログが複数の場所に配置されている場合は、すべての場所がキャプチャされます。これにはFRAのシナリオも含まれます。ディレクトリにソフトリンクが使用されている場合は、同じものが設定されます。

例:

- NFS上の単一データベースの場合: /mnt/nfsdb2_log
- NFS 上の複数のデータベースと、2つの異なる場所に配置されている NFSB31 データベース アーカイブ ログの場合: NFSB31@/mnt/nfsdb31_log1、/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log
- ASMの場合: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15

- **SC_REDO_LOGS_LOCATIONS** は、REDO ログ ディレクトリの場所を指定します。

Redoログ ファイルの直接の親ディレクトリの名前になります。ディレクトリにソフトリンクが使用されている場合は、同じものが設定されます。

例:

- NFS上の単一データベースの場合: /mnt/nfsdb2_data/newdb1
- NFS上の複数のデータベースの場合:
NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
- ASMの場合: +LOG2DG/ASMDB2/ONLINELOG

- **SC_CONTROL_FILES_LOCATIONS** は制御ファイル ディレクトリの場所を指定します。

制御ファイルの直接の親ディレクトリの名前になります。ディレクトリにソフトリンクが使用されている場合は、同じものが設定されます。

例:

- NFS上の単一データベースの場合: /mnt/nfsdb2_data/fra/newdb1、/mnt/nfsdb2_data/newdb1
- NFS 上の複数のデータベースの場合:
NFSB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/fra/newdb32,/mnt/nfsdb32_data/newdb32
- ASMの場合: +LOG2DG/ASMDB2/CONTROLFILE

- **SC_DATA_FILES_LOCATIONS** は、データ ファイル ディレクトリの場所を指定します。

データ ファイルの直接の親ディレクトリの名前になります。ディレクトリにソフトリンクが使用されている場合は、同じものが設定されます。

例:

- NFS上の単一データベースの場合: /mnt/nfsdb3_data1、/mnt/nfsdb3_data/NEWDB3/datafile
- NFS 上の複数のデータベースの場合:
NFSB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32_data1,/

mnt/nfsdb32_data/NEWDB32/datafile

◦ ASMの場合: +DATA2DG/ASMDB2/DATAFILE、+DATA2DG/ASMDB2/TEMPFILE

- **SC_SNAPSHOT_LABEL** はセカンダリ ラベルの名前を指定します。

例: 時間別、日別、週別、月別、またはカスタム ラベル。

サポートされている区切り文字

- **:** は SVM 名とボリューム名を区切るために使用されます

例: buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- **@** は、データとデータベース名を区別し、値とキーを区別するために使用されます。

例:

- NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- NFSB31@oracle|NFSB32@oracle

- **|** は、2つの異なるデータベース間でデータを分離するため、および SC_BACKUP_ID、SC_BACKUP_RETENTION、および SC_BACKUP_NAME パラメータの2つの異なるエンティティ間でデータを分離するために使用されます。

例:

- DATA@203|LOG@205
- Hourly|DATA@DAYS:3|LOG@COUNT:4
- DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- **/** は、SC_PRIMARY_SNAPSHOT_NAMES および SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG パラメータのボリューム名とそのスナップショットを区別するために使用されます。

例: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- **,** は同じ DB の変数セットを区切るために使用されます。

例: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

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、または保持するバックアップ コピーの数（ONTAPでは最大255個のコピー）を指定することができます。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、スケジュール タイプに一致する保持ラベルを持つ保持された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 タイプが変更されると、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。

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、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。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とRPOはデータ保護戦略に関わる要件です。

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。データベースを頻繁にバックアップするほど、SnapCenterが復元時に使用するトランザクション ログが少なくなり、復元操作が高速化されます。

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頻度）は、一部のプラグインではスケジュール タイプと呼ばれ、ポリシー構成の一部です。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。頻度を選択しなかった場合は、オンデマンドのみのポリシーが作成されます。設定 >

ポリシー をクリックすると、ポリシーにアクセスできます。

- 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 グループ設定の一部です。たとえば、週次バックアップのポリシーが構成されたリソース グループがある場合は、毎週木曜日の午後 10 時にバックアップするようにスケジュールを構成できます。リソース > リソース グループ をクリックすると、リソース グループのスケジュールにアクセスできます。

バックアップの命名規則

Snapshot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名にタイムスタンプが追加されるので、コピーが作成されたタイミングを特定できます。

Snapshot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、[スナップショット コピーにカスタム名形式を使用する] 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スナップショット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名にタイムスタンプのサフィックスが追加されます。

Oracleデータベースのバックアップの要件

Oracleデータベースをバックアップする前に、前提条件が満たされ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関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror 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しているすべてのデー

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。

- 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を持つデータベースが「MOUNT」または「OPEN」のいずれかの状態であることを確認する必要があります。
- 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。
- バックアップ対象のデータベースが大きい場合 (サイズが TB 単位)、 SnapCenter Server ホストの `C:\Program Files\NetApp\SMCore\SMCoreServiceHost.exe.config` ファイルで `RESTTimeout` の値を 86400000 ミリ秒に増やす必要があります。

値を変更する場合は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てください。

バックアップに使用できるOracleデータベースの検出

リソースとなるのは、ホスト上でSnapCenterによって管理されているOracleデータベースです。使用できる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。

開始する前に

- SnapCenter Server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) にある場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。

詳細については、以下を参照してください。 ["SnapCenter Plug-in for VMware vSphereの導入"](#)。

- データベースが VMDK ファイル システム上に存在する場合は、vCenter にログインし、**VM** オプション > 詳細 > 構成の編集 に移動して、VM の `disk.enableUUID` の値を `true` に設定する必要があります。
- さまざまなタイプとバージョンのOracleデータベースを検出するためにSnapCenterが実行するプロセスを確認しておく必要があります。

ステップ1: SnapCenterがデータベース以外のエントリを検出しないようにする

oratabファイルに追加されたデータベース以外のエントリがSnapCenterで検出されないようにすることができます。

手順

1. Oracle 用プラグインをインストールした後、root ユーザーはディレクトリ `/var/opt/snapcenter/sco/etc/` の下に **sc_oratab.config** ファイルを作成する必要があります。

Oracleバイナリの所有者とグループに書き込み権限を付与して、将来ファイルを管理できるようにします。

2. データベース管理者は、**sc_oratab.config** ファイルにデータベース以外のエントリを追加する必要があります。

`/etc/oratab` ファイル内の非データベース エントリに対して定義されているのと同じ形式を維持することをお勧めします。または、ユーザーは非データベース エンティティ文字列を追加するだけでもかまいません。

ん。



この文字列では大文字と小文字が区別されます。先頭に#が付いているテキストはコメントとして扱われます。コメントは非データベース名の後ろに追加できます。

```
For example:
-----
# Sample entries
# Each line can have only one non-database name
# These are non-database name
oratar # Added by the admin group -1
#Added by the script team
NEWSPT
DBAGNT:/ora01/app/oracle/product/agent:N
-----
```

3. リソースを検出します。

sc_oratab.config に追加されたデータベース以外のエントリは、リソース ページに表示されません。



SnapCenterプラグインをアップグレードする前に、sc_oratab.configファイルのバックアップを作成することを常に推奨します。

ステップ2: リソースの発見

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検出されて[Resources]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。正常に検出されたデータベースのみをリソース グループに追加できます。

ホスト上のOracleデータベースを削除した場合、SnapCenter Serverはそのことを認識せず、削除されたデータベースをリストに表示します。SnapCenterリソース 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。

クリック  [フィルターアイコン] 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ーします。次に、imagfilter_icon.gif[filter icon]_icon.png[] アイコンをクリックして、フィルター パネルを閉じることができます。

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で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。



SnapCenterの外部でデータベースの名前が変更された場合は、リソースを更新する必要があります。

- データベースがNetApp以外のストレージ システムにある場合は、ユーザ インターフェイスの[Overall Status]列に「Not available for backup」というメッセージが表示されます。

NetApp以外のストレージにあるデータベースには、データ保護処理を実行できません。

- データベースがNetAppストレージ システムにあって保護されていない場合は、ユーザ インターフェイスの[Overall Status]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NetAppストレージ システムにあって保護されている場合は、ユーザ インターフェイスの[Overall Status]列に「Available for backup」というメッセージが表示されます。



Oracleデータベース認証が有効になっている場合は、リソース ビューに赤い南京錠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、または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、バックアップをどのように管理し、スケジューリングし、保持するかを定める一連のルールです。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たい場合に時間を節約できます。

始める前に

- 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。
- root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプト ディレクトリとポストスクリプト ディレクトリに手動で割り当てる必要があります。
- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、["SnapMirrorアクティブ同期のオブジェクト数の制限"](#)。

タスク概要

[Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。

+ スナップショットのロック期間を指定すると、保持期間が終了するまでスナップショットが削除されなくなります。その結果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。

+ ONTAP 9.12.1 以下のバージョンでは、リストアの一環としてSnapLock Vault スナップショットから作成されたクローンには、SnapLock Vault の有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップ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、[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* をクリックします。
5. 「名前」 ページで、ポリシー名と詳細を入力します。
6. ポリシー タイプ ページで、次の手順を実行します。

a. ストレージタイプを選択します。

b. ポリシーの範囲を選択:

- *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。

データファイル、制御ファイル、アーカイブ ログ ファイルすべて、データファイルと制御ファイルのみ、アーカイブ ログ ファイルのみのいずれをバックアップするかを指定する必要があります。

- 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された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、[マウント] 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、「シャットダウン」を選択します。

プラグブル データベース (PDB) があり、バックアップを作成する前に PDB の状態を保存する場合は、「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。

- c. 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、「**Oracle Recovery Manager (RMAN)** を使用したバックアップのカタログ化」を選択します。

GUIまたはSnapCenter CLIコマンドCatalog-SmBackupWithOracleRMANを使用して、一度に1つのバックアップのカタログ化を遅らせて実行できます。



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。

d. バックアップ後にアーカイブ ログを削除する場合は、[バックアップ後にアーカイブ ログを削除する]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す。

- 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ためには、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	操作
すべてのアーカイブ ログを削除	*すべてのアーカイブ ログを削除*を選択します。
古いアーカイブ ログを削除	次の期間より古いアーカイブ ログを削除する を選択し、削除するアーカイブ ログの保存期間を日数と時間で指定します。
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	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	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. スナップショットとレプリケーション ページで、次の手順を実行します。

- a. オンデマンド、時間別、日次、週次、または*月次*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実行されません。

- a. データ スナップショットの保持設定セクションで、バックアップ タイプ ページで選択したバックアップ タイプとスケジュール タイプの保持設定を指定します。

状況	操作
特定の数のSnapshotを保持	<p>*保持するコピー*を選択し、保持するスナップショットの数を指定します。</p> <p>Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。</p> <div style="display: flex; flex-direction: column; gap: 10px;"> <div style="display: flex; align-items: center;"> <p>最大保持値は 1018 です。保持数を、使用しているONTAPバージョンがサポートする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="display: flex; align-items: center;"> <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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。</p> </div> </div>
Snapshotを特定の日数だけ保持	<p>*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。</p>
スナップショットコピーのロック期間	<p>スナップショット コピーのロック期間 を選択し、期間を日数、月数、または年数で指定します。</p> <p>SnapLock保持期間は100年未満にする必要があります。</p>

- b. アーカイブ ログ スナップショットの保持設定セクションで、バックアップ タイプ ページで選択したバックアップ タイプとスケジュール タイプの保持設定を指定します。

状況	操作
特定の数のSnapshotを保持	<p>*保持するコピー*を選択し、保持するスナップショットの数を指定します。</p> <p>Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> 最大保持値は 1018 です。保持数を、使用しているONTAPバージョンがサポートする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> <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がターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。</p> </div>
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
スナップショットコピーのロック期間	<p>スナップショット コピーのロック期間 を選択し、期間を日数、月数、または年数で指定します。</p> <p>SnapLock保持期間は100年未満にする必要があります。</p>

c. ポリシーラベルを選択します。



リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

8. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの1つまたは両方を選択します。



セカンダリ スナップショット コピーのロック期間 を有効にするには、セカンダリ レプリケーション オプションを選択する必要があります。

フィールド	操作
Update SnapMirror after creating a local Snapshot	<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>このオプションは、SnapMirrorアクティブ同期に対して有効にする必要があります。</p> <p>セカンダリレプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。</p> <p>トポロジページの更新ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLockの有効期限が更新されます。</p>
Update SnapVault after creating a local Snapshot	<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> <p>SnapLockがSnapLock Vaultと呼ばれるONTAPのセカンダリにのみ設定されている場合、[トポロジ]ページの[更新]ボタンをクリックすると、ONTAPから取得されたセカンダリのロック期間が更新されます。</p> <p>SnapLock Vaultの詳細については、"バックアップデスティネーションのSnapshotコピーのWORM状態へのコミット"</p> <p>見る"[Topology]ページでのOracleデータベースのバックアップとクローンの表示"。</p>
Error retry count	<p>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。</p>



セカンダリストレージでSnapshotの上限に達しないように、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。

- [Script]ページで、バックアップ処理の前またはあと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。

プレスクリプトとポストスクリプトは、`/var/opt/snapcenter/spl/scripts` またはこのパス内の任意のフォルダーに保存する必要があります。デフォルトでは、`/var/opt/snapcenter/spl/scripts` パスが設定されます。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。

SnapCenter、事前スクリプトと事後スクリプトを実行するときに、事前定義された環境変数を使用できま

す。"詳細情報"

10. [Verification]ページで、次の手順を実行します。

- 検証処理の実行対象となるバックアップ スケジュールを選択します。
- [Verification script commands]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引数とパスを入力します。

プレスクリプトとポストスクリプトは、`/var/opt/snapcenter/spl/scripts` またはこのパス内の任意のフォルダーに保存する必要があります。デフォルトでは、`/var/opt/snapcenter/spl/scripts` パスが設定されます。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。

11. 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 グループの作成とポリシーの適用

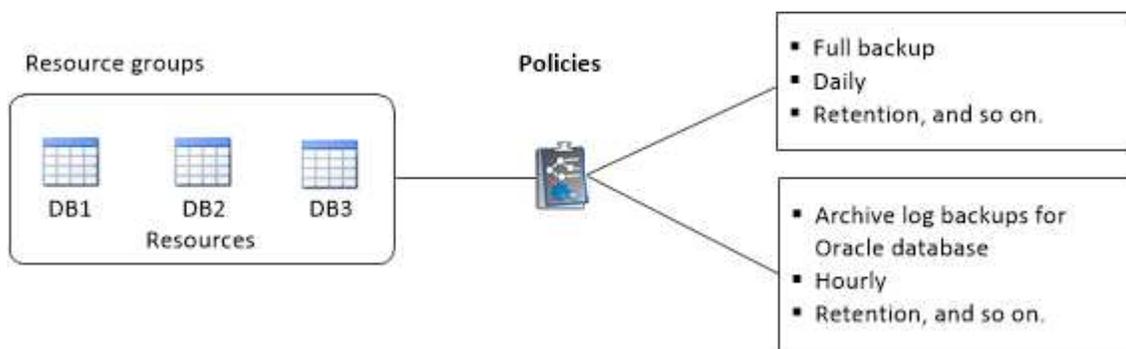
リソース グループはコンテナであり、バックアップして保護するリソースをここに追加します。リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。

タスク概要

- 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 グループにファイルが格納されているデータベースが「MOUNT」または「OPEN」状態である必要があります。

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します。

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



- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotのロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期を使用するリソースを含む既存のリソース グループにSnapMirrorアクティブ同期を使用しない新しいデータベースを追加することはできません。
- SnapMirrorアクティブ同期のフェイルオーバー モードである既存のリソース グループに新しいデータバ

ースを追加することはできません。リソースを追加できるのは、通常の状態またはフェイルバック状態のリソース グループのみです。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、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. [Name] ページで、次の操作を実行します。
 - a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上の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。

- c. Snapshot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`などの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. 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。



必要に応じて、プレフィックスも含めて、Oracleで設定されたものとまったく同じデスティネーションを使用してください。

4. [リソース] ページで、[ホスト] 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。



[Available Resources] セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources] のリストには表示されません。

5. [Available Resources] セクションでリソースを選択し、[Selected Resources] セクションに移動します。



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できません。

6. アプリケーション設定ページで、バックアップ オプションを選択します。

7. [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。

[Configure schedules for selected policies] セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[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。

設定したスケジュールが[Applied Schedules]列にリストされます。

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

8. [Verification]ページで、次の手順を実行します。

- a. 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で検証を実行します。
- b. クリック  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構成するには、[スケジュールの構成] 列で をクリックします。
- c. [Add Verification Schedules *policy_name*]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証] 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が、[Applied Schedules]列にリストされます。

9. 通知ページの 電子メール設定 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」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のSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

10. 概要を確認し、[完了] をクリックします。

リソース グループを作成し、ASA r2 システム上の Oracle リソースの二次保護を有効にします。

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、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. [Name] ページで、次の操作を実行します。
 - a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上の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。

- c. Snapshot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`などの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. 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。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたのと同じ宛先を使用する必要があります。

4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。



[Available Resources]セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
6. アプリケーション設定ページで、バックアップ オプションを選択します。
7. [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  をクリックしてポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[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。

設定したスケジュールが[Applied Schedules]列にリストされます。

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

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」 ページが表示されるので、次の手順を実行する必要があります。
 - a. レプリケーション ポリシーのタイプを選択します。



同期レプリケーション ポリシーはサポートされていません。

- b. 使用する整合性グループのサフィックスを指定します。
- c. [宛先クラスター] および [宛先 SVM] ドロップダウンから、使用するピア クラスターと SVM を選択します。



クラスターと SVM のピアリングはSnapCenterではサポートされていません。クラスターと SVM のピアリングを実行するには、System Manager またはONTAP CLI を使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification]ページで、次の手順を実行します。
 - a. ロケーターのロード 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

ストレージで検証を実行します。

- b. クリック  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構成するには、[スケジュールの構成] 列で をクリックします。
- c. [Add Verification Schedules policy_name]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証] 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が、[Applied Schedules]列にリストされます。

2. 通知ページの 電子メール設定 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」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のSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

Oracleリソースのバックアップ

どのリソース グループにもまだ含まれていないリソースは、[Resources]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 を選択し、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 、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します。

そのあとに  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]ページが表示されます。

5. [Resources]ページで、次の手順を実行します。

- a. Snapshot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。

例えば、`customtext_policy_hostname``または ``resource_hostname`。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- b. 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。

クリックするとポリシーを作成できます 。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. クリック  必要なポリシーのスケジュールを構成するには、[スケジュールの構成] 列をクリックします。

- c. 「ポリシー_`policy_name`のスケジュールを追加」ウィンドウでスケジュールを設定し、OK。

`policy_name` は、選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

7. [Verification]ページで、次の手順を実行します。

- a. 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を検証します。

- b. クリック  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構成するには、[スケジュールの構成] 列で をクリックします。 + 「検証スケジュールの追加 `policy_name`」ダイアログ ボックスで、次の手順を実行できます。

- c. *バックアップ後に検証を実行*を選択します。

- d. *スケジュールされた検証を実行する*を選択し、ドロップダウン リストからスケジュールの種類を選択します。



Flex ASMセットアップでは、カーディナリティがRACクラスタ内のノード数より少ない場合、リーフ ノードで検証処理を実行できません。

- e. 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 ロケーションで検証] を選択します。

- f. [OK]をクリックします。

設定した検証スケジュールが、[Applied Schedules]列にリストされます。

8. 通知ページで、*電子メール設定*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。

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。リソースに対して実行されたバックアップ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」を選択します。



電子メール通知の場合は、GUIまたはPowerShellコマンドを使用してSMTPサーバーの詳細を指定する必要があります。Set-SmSmtplibServer。

9. 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。

10. *今すぐバックアップ* をクリックします。

11. [Backup] 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た場合は、バックアップに使用するポリシーを[Policy] ドロップダウン リストから選択します。

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、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ* をクリックします。

12. モニター > ジョブ をクリックして、操作の進行状況を監視します。

終了後の操作

- AIX セットアップでは、`lkdev` ロックするコマンドと `rendev` バックアップされたデータベースが保存されていたディスクの名前を変更するコマンド。

そのバックアップを使用してリストアを実行する際、デバイスのロックおよび名前変更がリストア処理に影響することはありません。

- 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操作が失敗した場合は、以下のコマンドを実行してORACLE_SQL_QUERY_TIMEOUTおよびORACLE_PLUGIN_SQL_QUERY_TIMEOUTパラメータの値を変更する必要があります。`Set-SmConfigSettings` コマンドレット:

パラメータの値を変更した後、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`

- 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場合、処理が失敗し、エラー コード DBV-00100 Specified FILE が表示されることがあります。`sco.properties` の VERIFICATION_DELAY および 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後、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`

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

Java 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` を見つけま

す。その脚本では、`do_start method`` コマンドは、SnapCenter VMware プラグイン サービスを開始します。このコマンドを次のように更新します。 ``Java -jar -Xmx8192M -Xms4096M。`

詳細情報の参照

- "MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"
- "Oracle RAC One NodeデータベースはSnapCenter操作の実行ではスキップされます"
- "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、復元、クローン操作のカスタマイズ可能なパラメータ" (ログインが必要です)

Oracleデータベースのリソース グループのバックアップ

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。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に対して実行されます。

リソース グループは、[Resources] 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バックアップが作成されます。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、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。
3. 検索ボックスにリソースグループ名を入力するか、 をクリックして、タグを選択します。

 をクリックし  でフィルタ ペインを閉じます。

4. [Resource Group] ページで、バックアップするリソース グループを選択します。



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がNetApp以外のストレージにあると、もう一方のデータベースがNetApp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。

5. [Backup] ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーが関連付けられている場合は、[ポリシー] ドロップダウン リストから使用するバックアップ 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、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*を選択します。
6. モニター > ジョブ を選択して進行状況を監視します。

終了後の操作

- AIXセットアップでは、``lkdev`` ロックするコマンドと ``rendev`` バックアップされたデータベースが保存されていたディスクの名前を変更するコマンド。

そのバックアップを使用してリストアを実行する際、デバイスのロックおよび名前変更がリストア処理に影響することはありません。

- 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操作が失敗した場合は、以下のコマンドを実行してORACLE_SQL_QUERY_TIMEOUTおよびORACLE_PLUGIN_SQL_QUERY_TIMEOUTパラメータの値を変更する必要があります。`Set-SmConfigSettings` コマンドレット:

パラメータの値を変更した後、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

- 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場合、処理が失敗し、エラー コードDBV-00100 Specified FILEが表示されることがあります。sco.properties の VERIFICATION_DELAY_ および 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後、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

Oracleデータベースのバックアップの監視

バックアップ処理とデータ保護処理の進捗状況を監視する方法について説明します。

Oracleデータベースのバックアップ処理の監視

SnapCenterの[Jobs]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、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

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

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。
 - a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。

- 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*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
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は  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 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処理を監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各処理に関する情報が表示されます。

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. クリック  アクティビティ ペインで、最新の 5 つの操作を表示します。

いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

その他のバックアップ処理

UNIXコマンドを使用したOracleデータベースのバックアップ

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

- `Add-SmStorageConnection` コマンドと `Add-SmCredential` コマンドを使用して、ストレージ システム接続を追加し、資格情報を作成しておく必要があります。
- `Open-SmConnection` コマンドを使用して、SnapCenter Server 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時間を過ぎると無効になります。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、セッションが無効にならないようにすることができます。

このタスクについて

次に示すコマンドを実行して、SnapCenter Server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関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンド リファレンス ガイド](#)"。

手順

1. 指定されたユーザーのSnapCenter Server との接続セッションを開始します: `Open-SmConnection`
2. ホスト リソース検出操作を実行します: `Get-SmResources`
3. Real Application Cluster (RAC) データベースのバックアップ操作に Oracle データベースの資格情報と優先ノードを構成します: `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`

このコマンドでは、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が取得されます。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. SnapCenterにリソース グループを追加します: `Add-SmResourceGroup`
7. バックアップを作成します: `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ない場合は、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のキャンセル

実行中のバックアップ処理、キューに登録されたバックアップ処理、応答しないバックアップ処理をキャンセルできます。

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 Serverにより処理が停止されます。作成されたバックアップがSnapCenter Serverに登録されていない場合、ストレージからすべてのSnapshotが削除されます。バックアップがすでにSnapCenter Serverに登録されている場合、キャンセルがトリガーされても、すでに作成されているSnapshotはロールバックされません。

- キャンセルできるのは、キューに登録されているか実行中のログ バックアップまたはフル バックアップの処理だけです。
- 検証の開始後は、処理をキャンセルできません。

検証前に処理をキャンセルすると、処理はキャンセルされ、検証処理は実行されません。

- カタログ処理が開始されたあと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]ページまたは[Activity]ペインでキャンセルできます。
- SnapCenter GUIからだけでなく、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の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [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のオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられた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
[Monitor]ページ	<ol style="list-style-type: none"> 1. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 2. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	<ol style="list-style-type: none"> 1. バックアップジョブを開始したら、 アクティビティ ペインで、最新の 5 つの操作を表示します。 2. 処理を選択します。 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。

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。

キャンセルした操作がキャンセル中または実行中の状態で応答しない場合は、Cancel-SmJob -JobID <int> -Force を実行して、バックアップ操作を強制的に停止する必要があります。

[Topology]ページでのOracleデータベースのバックアップとクローンの表示

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

[Topology]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参照し、対象を選択してデータ保護処理を実行できます。

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）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリストレージで使用可能なバックアップとクローンの数を表示します。
-  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ているバックアップとクローンの数を表示します。
-  SnapVaultテクノロジーを使用してセカンダリストレージに複製されたバックアップとクローンの数を表示します。

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、バックアップを4個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。



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。

SnapMirrorアクティブ同期 (当初はSnapMirror Business Continuity [SM-BC] としてリリース) としてセカンダリ関係がある場合は、次の追加アイコンが表示されます。

-  レプリカサイトが稼働しています。
-  レプリカサイトはダウンしています。
-  セカンダリミラーまたはボールド関係が再確立されていません。

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] 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[Topology]ページが表示されます。

4. [Summary Card]で、プライマリストレージとセカンダリストレージ上にあるバックアップとクローンの数の概要を確認します。

[Summary Card]セクションには、バックアップとクローンの総数およびログバックアップの総数が表示されます。

更新 ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

アプリケーション リソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

SnapMirrorアクティブ同期の場合、[更新] ボタンをクリックすると、プライマリ サイトとレプリカ サイトの両方に対してONTAPを照会してSnapCenterバックアップ インベントリが更新されます。週次スケジュールでも、SnapMirrorアクティブ同期関係を含むすべてのデータベースに対してこの処理が実行されます。

- SnapMirrorアクティブ同期とONTAP（バージョン9.14.1のみ）では、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップの関係については、フェイルオーバー後に手動で設定する必要があります。ONTAP 9.15.1以降は、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップが、自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。バックアップが作成された後にのみ、「更新」をクリックできます。

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、カタログ化、カタログ解除、削除の各処理を実行します。



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、名前の変更、マウント、マウント解除、カタログ、カタログ解除、および削除の操作のみを実行できます。
- 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に割り当てられている値が小さい場合は、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いても、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。Set-SmConfigSettings PowerShell コマンドレットを使用して、SnapmirrorStatusUpdateWaitTime に割り当てられた値を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関する情報は、Get-Help *command_name* を実行すると取得できます。

あるいは、"[SnapCenterソフトウェア コマンド 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](#)"。

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。