PostgreSQLリソースのバックアップ

SnapCenter software

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/snapcenter/protect-postgresql/back-up-postgresql-resources.html on January 09, 2026. Always check docs.netapp.com for the latest.

目次

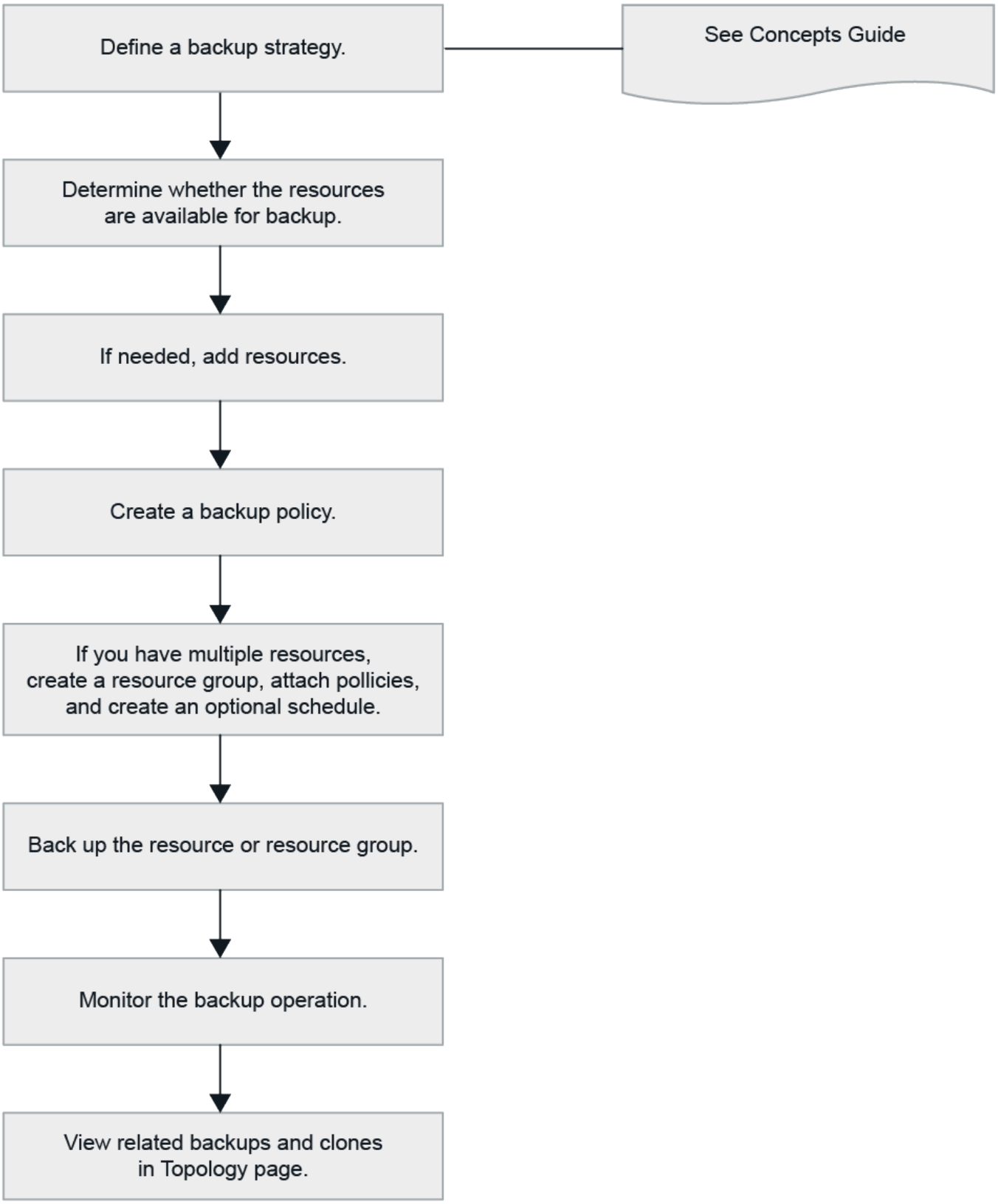
PostgreSQLリソースのバックアップ . . . 1
PostgreSQLリソースのバックアップ . . . 1
クラスタの自動検出 . . . 3
プラグインホストに手動でリソースを追加する . . . 3
PostgreSQLのバックアップポリシーの作成 . . . 5
リソースグループを作成してポリシーを適用 . . . 8
ASA R2システムで、リソースグループを作成し、PostgreSQLリソースのセカンダリ保護を有効にする . . . 12
PostgreSQL用の
PowerShellコマンドレットを使用して、ストレージシステム接続とクレデンシャルを作成する . . . 14
PostgreSQLのバックアップ . . . 16
リソースグループのバックアップ . . . 22
PostgreSQLバックアップ処理の監視 . . . 23
[Activity]ペインで、PostgreSQLクラスタのデータ保護処理を監視します。 . . . 24
PostgreSQLのバックアップ処理をキャンセルする . . . 24
[Topology]ページでPostgreSQLのバックアップとクローンを表示 . . . 25

PostgreSQLリソースのバックアップ

PostgreSQLリソースのバックアップ

リソース（クラスタ）またはリソースグループのバックアップを作成できます。バックアップのワークフローには、計画、バックアップするクラスタの特定、バックアップポリシーの管理、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。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html["SnapCenter ソフトウェアコマンドレットリファレンスガイド"^]です。

クラスタの自動検出

リソースとは、SnapCenterで管理されるLinuxホスト上のPostgreSQLクラスタです。使用可能なPostgreSQLクラスタを検出したら、リソ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セットアップなどのタスクを完了しておく必要があります。
- SnapCenter Plug-in for PostgreSQLでは、RDM / VMDK仮想環境にあるリソースの自動検出はサポートされていません。

タスクの内容

- プラグインをインストールすると、そのLinuxホスト上のすべてのクラスタが自動的に検出されて[リソース]ページに表示されます。
- 自動検出されるのはクラスタのみです。

自動検出されたリソースを変更または削除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*[リソース]*をクリックし、リストからPlug-in for PostgreSQLを選択します。
2. [Resources]ページで、[View]リストからリソースタイプを選択します。
3. （オプション）*をクリックし、ホスト名を選択します。

   次に、**をクリックしてフィルタペインを閉じることができます。

4. [* リソースの更新 *] をクリックして、ホストで使用可能なリソースを検出します。

   リソースは、リソースタイプ、ホスト名、関連するリソースグループ、バックアップタイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

   - クラスタがNetAppストレージに配置されていて保護されていない場合は、[全体のステータス]列に「保護されていません」と表示されます。
   - クラスタがNetAppストレージシステム上にあり保護されている場合、バックアップ処理が実行されていないと、[全体のステータス]列に[バックアップが実行されていません]と表示されます。それ以外の場合は、前回のバックアップステータスに基づいて、「 Backup failed 」または「 Backup succeeded 」に変わります。

SnapCenterの外部でクラスタの名前を変更した場合は、リソースを更新する必要があります。

プラグインホストに手動でリソースを追加する

自動検出はWindowsホストではサポートされていません。PostgreSQLクラスタリソースを手動で追加する必要があります。

開始する前に

- 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セットアップなどのタスクを完了しておく必要があります。

タスクの内容

自動検出は、次の構成ではサポートされません。

- RDMとVMDKのレイアウト

手順

1. 左側のナビゲーションペインで、ドロップダウンリストからSnapCenter Plug-in for PostgreSQLを選択し、*[リソース]*をクリックします。
2. [Resources]ページで、*[Add PostgreSQL resources]*をクリックします。
3. [Provide Resource Details]ページで、次の操作を実行します。

フィールド	操作
名前	クラスタ名を指定します。
ホスト名	ホスト名を入力します。
タイプ	クラスタを選択します。
インスタンス	クラスタの親であるインスタンスの名前を指定します。
クレデンシャル	クレデンシャルを選択するか、クレデンシャルの情報を追加します。 これはオプションです。

4. [ストレージフットプリントの入力]ページで、ストレージタイプを選択して1つ以上のボリューム、LUN、およびqtreeを選択し、*[保存]*をクリックします。

   オプション：*アイコンをクリックすると、他のストレージシステムからボリューム、LUN、およびqtreeを追加できます + 。

5. オプション：[Resource Settings]ページで、Windowsホスト上のリソースにPostgreSQLプラグインのカスタムのキーと値のペアを入力します。
6. 概要を確認し、 [完了] をクリックします。

   クラスタは、ホスト名、関連付けられているリソースグループとポリシー、全体的なステータスなどの情報とともに表示されます。

リソースへのアクセスをユーザに許可する場合は、ユーザにリソースを割り当てる必要があります。これにより、ユーザは自分に割り当てられているアセットに対して権限のある操作を実行できます。

"ユーザまたはグループを追加してロールとアセットを割り当てる"

終了後

- クラスタを追加したら、PostgreSQLクラスタの詳細を変更できます。
- SnapCenter 5.0から移行されたリソース（表領域とクラスタ）は、SnapCenter 6.0ではPostgreSQLクラスタタイプとしてタグ付けされます。
- SnapCenter 5.0以前から移行された手動で追加したリソースを変更する場合は、カスタムキーと値のペアの*[リソースの設定]*ページで次の手順を実行します。
  - 「* Name *」フィールドに「port」という用語を指定します。
  - 「* value *」フィールドにポート番号を指定します。

PostgreSQLのバックアップポリシーの作成

SnapCenterを使用してPostgreSQL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は、バックアップを管理、スケジュール、および保持する方法を規定する一連のルールです。

開始する前に

- バックアップ戦略を定義しておく必要があります。

  詳細については、PostgreSQLクラスタのデータ保護戦略の定義に関する情報を参照してください。

- データ保護の準備として、SnapCenter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セットアップ、リソースの追加などのタスクを実行しておく必要があります。
- Snapshot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の両方に対応する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。

  また、レプリケーション、スクリプト、およびアプリケーションの設定をポリシーで指定することもできます。これらのオプションを使用することで、別のリソースグループにポリシーを再利用して時間を節約できます。

タスクの内容

- SnapLock
  - [バックアップコピーを特定の日数だけ保持する]オプションを選択した場合は、SnapLockの保持期間を指定した保持日数以下にする必要があります。
  - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されなくなります。その結果、ポリシーで指定された数よりも多くのSnapshotが保持される可能性があります。
  - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、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. [新規作成（ New ）] をクリックする。
4. [Name]ページで、ポリシーの名前と詳細を入力します。
5. [Policy type]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. [* カスタム・バックアップ設定 *] セクションで、キー値形式でプラグインに渡す必要がある特定のバックアップ設定を指定します。

      プラグインに渡すキー値は複数指定できます。
6. [Backup and Replication]ページで、次の操作を実行します。
   a. 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、終了日、頻度）を指定できます。これにより、ポリシーとバックアップ頻度が同じである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ている場合、夏時間（DST）中はスケジュールはトリガーされません。

   a. [Snapshot settings]セクションで、*[Backup Type]*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	作業
一定数のSnapshotを保持	[保持するコピー数]*を選択し、保持するSnapshotの数を指定します。 Snapshotの数が指定した数を超えると、最も古いコピーから順にSnapshotが削除されます。 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可能性があります。 最大保持値は 1018 です。保持期間がONTAPバージョンでサポートされている値よりも高い値に設定されている場合、バックアップは失敗します。

状況	作業
Snapshotを特定の日数だけ保持	[コピーを保持する期間]*を選択し、Snapshotを削除するまでの日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、日、月、または年を指定します。 SnapLock保持期間は100年未満にする必要があります。

7. 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. [Select secondary replication options]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一方または両方を選択します。

フィールド	操作
• ローカル Snapshot コピー作成後に SnapMirror を更新 *	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。 ONTAPの保護関係のタイプがミラーとバックアップの場合、このオプションのみを選択すると、プライマリで作成されたSnapshotはデスティネーションに転送されませんが、デスティネーションのリストに表示されます。このSnapshotをリストア処理の対象としてデスティネーションで選択すると、「Secondary Location is not available for the selected vaulted/mirrored backup」というエラーメッセージが表示されます。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。 [Topology]ページの[Refresh]*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のSnapLock有効期限が更新されます。 を参照して "[TopologyページでPostgreSQLリソースに関連するバックアップとクローンを表示"]

フィールド	操作
• ローカル Snapshot コピー作成後に SnapVault を更新 *	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。 セカンダリレプリケーションでは、SnapLockの有効期限によってプライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]*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のSnapLock有効期限が更新されます。 SnapLockがONTAPのセカンダリ（SnapLock Vault）にのみ設定されている場合、[Topology]ページの*[Refresh]*ボタンをクリックすると、ONTAPから取得したセカンダリのロック期間が更新されます。 SnapLock Vaultの詳細については、「SnapVaultデスティネーションでSnapshotをWORM状態にコミットする」を参照してください。 を参照して "[Topologyページで PostgreSQLリソースに関連するバックアップとクローンを表示"]
• 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のSnapshot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. 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てポリシーを適用

リソースグループはコンテナであり、バックアップおよび保護するリソースを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。リソースグループはすべてのデータ保護ジョブに必要です。また、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。

タスクの内容

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンにSnapLock Vaultの有効期限が継承されます。SnapLockの有効期限が過ぎた時点で、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、 * 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	操作
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あとで検索する際に役立つラベルを1つ以上入力します。 たとえば、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。
Snapshotコピーにカスタムの名前形式を使用する	このチェックボックスをオンにして、Snapshot名に使用するカスタムの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名にタイムスタンプが追加されます。

4. Resources ページで、 * Host * ドロップダウン・リストからホスト名を選択し、 * Resource Type * ドロップダウン・リストからリソース・タイプを選択します。

   これは、画面上の情報をフィルタリングするのに役立ちます。

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、右矢印をクリックして [選択したリソース（ * Selected Resources ）] セクションに移動します。
6. [アプリケーションの設定] ページで、次の操作を行います。

   a. [*Backups] の矢印をクリックして、追加のバックアップ・オプションを設定します。

      整合グループのバックアップを有効にし、次のタスクを実行します。

フィールド	操作
整合グループのSnapshot処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。 Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。

フィールド	操作
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

+

a. [Scripts]*の矢印をクリックし、休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドを入力します。障害発生時に終了する前に実行するPREコマンドを入力することもできます。

b. [カスタム構成 *] の矢印をクリックし、このリソースを使用するすべてのデータ保護操作に必要なカスタムキーと値のペアを入力します。

パラメータ	設定	説明
archive_log_enable	（Y/N）	アーカイブログ管理でアーカイブログを削除できます。
アーカイブログの保持	日数	アーカイブログを保持する日数を指定します。 この設定は NTAP_SNAPSHOT_RETENTIONS 以上である必要があります。
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブログが格納されているディレクトリのパスを指定します。

パラメータ	設定	説明
ARCHIVE_LOG_EXT	ファイル拡張子	アーカイブ ログ ファイルの拡張子を指定します。 たとえば、アーカイブ ログが log_backup_0_1.log の場合、ファイル拡張子として .log を指定します。
archive_log_recursive_SE arch	（Y/N）	サブディレクトリ内のアーカイブログを管理できます。 アーカイブログがサブディレクトリにある場合は、このパラメータを使用してください。

カスタムのキーと値のペアは、PostgreSQL Linuxプラグインシステムでサポートされ、一元化されたWindowsプラグインとして登録されたPostgreSQLクラスタではサポートされません。

c. Snapshotコピーツール*の矢印をクリックして、スナップショットを作成するツールを選択します。

状況	作業
SnapCenterを使用してPlug-in for Windowsを使用し、スナップショットを作成する前にファイルシステムを整合性のある状態にします。Linuxリソースの場合、このオプションは適用されません。	ファイルシステムの整合性を維持した状態で SnapCenter を選択します。
SnapCenter：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで SnapCenter * を選択します。
Snapshotコピーを作成するためにホストで実行するコマンドを入力します。	[その他]*を選択し、ホストで実行するSnapshotを作成するコマンドを入力します。

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 + 。

ポリシーが[Configure schedules for selected policies]セクションに表示されます。

b. [スケジュールの設定]列で、設定するポリシーの**をクリックします + 。

c. [Add schedules for policy_name_] ダイアログボックスで、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、 [* Applied Schedules] 列に表示されます。

サードパーティの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はサポートされません。

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。SMTP サーバーは、 * Settings * > * Global Settings * で設定する必要があります。

9. 概要を確認し、 [完了] をクリックします。

ASA R2システムで、リソースグループを作成し、PostgreSQLリソースのセカンダリ保護を有効にする

リソースグループを作成して、ASA R2システム上のリソースを追加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ないでください。
- 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ないことを確認してください。

タスクの内容

- セカンダリ保護は、ログインしているユーザに「* SecondaryProtection *」機能が有効な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した場合、プライマリおよびセカンダリ整合グループの作成時にリソースグループがメンテナンスモードになります。プライマリとセカンダリの整合グループが作成されると、リソースグループはメンテナンスモードを終了します。
- SnapCenterでは、クローンリソースのセカンダリ保護はサポートされません。

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. [名前] 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文字以内にする必要があります。

   b. 後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、HRをタグとして複数のリソースグループに追加した場合、後でHRタグに関連付けられているすべてのリソースグループを検索できます。

c. このチェックボックスをオンにして、Snapshot名に使用するカスタムの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名にタイムスタンプが追加されます。

d. バックアップしない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ものとまったく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。

> 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。最近追加したリソースは、リソースリストを更新するまで使用可能なリソースのリストに表示されません。

5. [Available Resources]セクションからASA R2リソースを選択し、[Selected Resources]セクションに移動します。
6. [Application Settings]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。

[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. 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. [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。

サードパーティの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はサポートされません。

8. 選択したポリシーでセカンダリ保護が有効になっている場合は、[Secondary Protection]ページが表示され、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. 使用する整合グループサフィックスを指定します。

c. [デスティネーションクラスタ]と[デスティネーションSVM]のドロップダウンで、使用するピアクラスタとSVMを選択します。

クラスタと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[Secondary Protected Resources]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. 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. [Configure Schedules]列内をクリックし + て、ポリシーのすべてのスケジュールタイプに対して検証スケジュールを設定します。
   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	[Run verification after backup] を選択します。
検証のスケジュールを設定	[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。

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メール通知を使用する場合は、GUIまたはPowerShellコマンドSet-SmSmSmtpServer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。

PostgreSQL用のPowerShellコマンドレットを使用して、ストレージシステム接続とクレデンシャルを作成する

PowerShellコマンドレットを使用してPostgreSQLクラスタをバックアップ、リストア、またはクローニングするには、Storage Virtual Machine（SVM）接続とクレデンシャル

を作成する必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールに必要な権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

  ストレージシステム接続の追加中にホストプラグインのインストールを実行しないでください。ホストキャッシュが更新されず、SnapCenter GUIでクラスタのステータスが「Not available for backup」または「Not on NetApp storage」と表示されることがあります。

- ストレージシステム名は一意である必要があります。

  SnapCenter では、異なるクラスタに同じ名前のストレージシステムを複数配置することはサポートされていません。SnapCenter でサポートされるストレージシステムには、それぞれ一意の名前およびデータ LIF の IP アドレスを割り当てる必要があります。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell Core接続セッションを開始します。

```
PS C:\> Open-SmConnection
```

2. Add-SmStorageConnectionコマンドレットを使用して、ストレージシステムへの新しい接続を作成します。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Add-SmCredentialコマンドレットを使用して、新しいクレデンシャルを作成します。

   次に、Windowsクレデンシャルを使用してFinanceAdminという名前の新しいクレデンシャルを作成する例を示します。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. SnapCenterサーバにPostgreSQL通信ホストを追加します。

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode PostgreSQL
```

5. パッケージとSnapCenter Plug-in for PostgreSQLをホストにインストールします。

   Linuxの場合：

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL
```

Windowsの場合：

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL -FilesystemCode scw -RunAsName FinanceAdmin
```

6. SQLLIBへのパスを設定します。

   Windowsの場合、PostgreSQLプラグインはSQLLIBフォルダのデフォルトパス「C：\Program Files\IBM\SQLLIB\bin」を使用します。

   デフォルトのパスを上書きする場合は、次のコマンドを使用します。

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
PostgreSQL -configSettings @{"PostgreSQL_SQLLIB_CMD" =
"<custom_path>\IBM\SQLLIB\BIN"}
```

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"。

PostgreSQL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、のページからバックアップすることができます。

開始する前に

- バックアップポリシー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。
- Snapshotコピーベースのバックアップ処理の場合は、すべてのテナントクラスタが有効でアクティブであることを確認してください。
- 休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドの場合は、該当するコマンドがプラグインホストのコマンドリストで次のパスから使用できるかどうかを確認する必要があります。
  - Windowsホストのデフォルトの場所：*C：\Program NetApp SnapCenter SnapCenter Plug-in Creator\etc\allowed_commands.config*
  - Linuxホストのデフォルトの場所：*/opt/linux/scc/etc/allowed_commands.config* NetApp SnapCenter

コマンドがコマンドリストに存在しない場合、処理は失敗します。

SnapCenter UI

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、リソースタイプに基づいて **View**] ドロップダウンリストからリソースをフィルタリングします。

   *を選択し、ホスト名とリソ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。その後、を選択してフィルタペインを閉じることができます 。

3. バックアップするリソースを選択します。
4. [Resource]ページで、*[Use custom name format for Snapshot copy]*を選択し、Snapshot名に使用するカスタムの名前形式を入力します。

   たとえば、 _customText_policy_hostname_or_resource_hostname_hostname_1 です。デフォルトでは、Snapshot名にタイムスタンプが追加されます。

5. [アプリケーションの設定] ページで、次の操作を行います。

   - [Backups]*矢印を選択して、追加のバックアップオプションを設定します。

     必要に応じて整合グループのバックアップを有効にし、次のタスクを実行します。

フィールド	操作
「整合グループSnapshot」処理が完了するまで待機する時間がある	Snapshot処理が完了するまでの待機時間を指定するには、* Urgent 、 Medium 、または Relaxed *を選択します。Urgent = 5秒、Medium = 7秒、Relaxed = 20秒。
WAFL同期を無効にする	WAFL整合ポイントを強制しない場合は、このオプションを選択します。

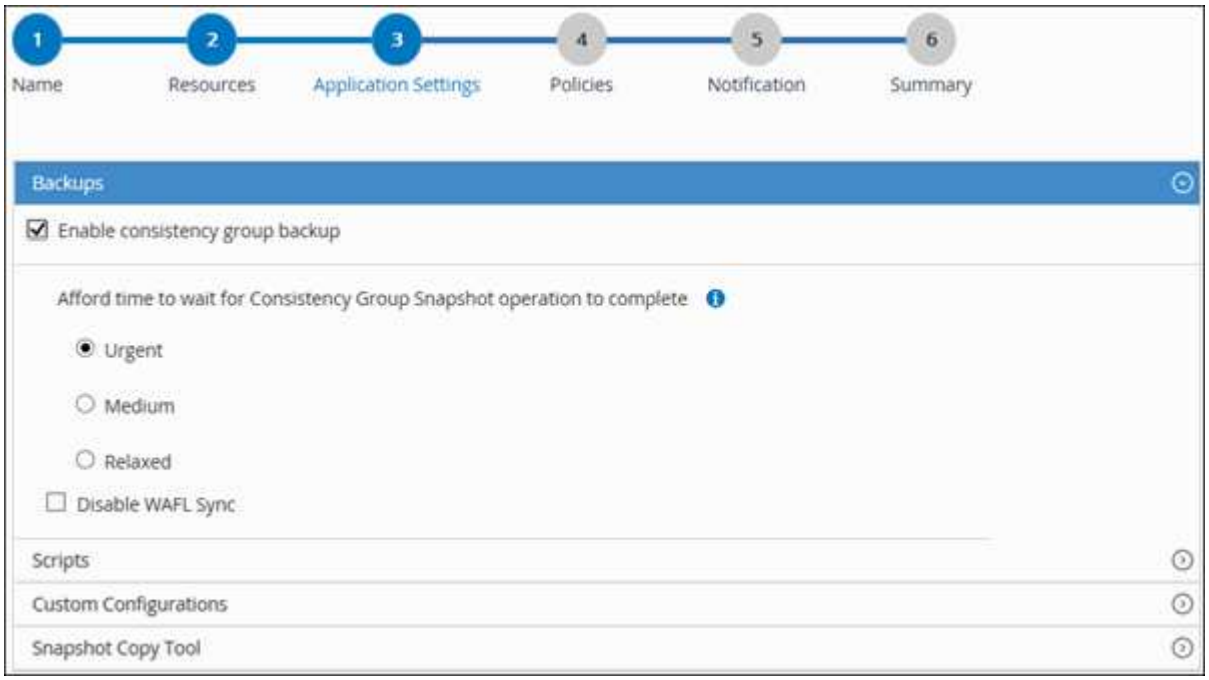
   - [Scripts]*の矢印を選択して、休止、Snapshot、および休止解除の処理のプリコマンドとポストコマンドを実行します。

     バックアップ処理を終了する前にPREコマンドを実行することもできます。プリスクリプトとポストスクリプトは SnapCenter サーバで実行されます。

   - [**Custom Configurations**]矢印を選択し、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。
   - Snapshotコピーツール*の矢印を選択して、Snapshotを作成するツールを選択します。

状況	作業
SnapCenter：ストレージレベルのSnapshotを作成	ファイルシステムの整合性なしで SnapCenter * を選択します。

状況	作業
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する	ファイルシステムの整合性を維持した状態でSnapCenter を選択します。
Snapshotを作成するコマンドを入力するには	[その他]*を選択し、コマンドを入力してSnapshotを作成します。



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。

   **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. 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]列で**を選択します + 。

   c. [Add schedules for policy_policy_name_]ダイアログボックスで、スケジュールを設定し、*[OK]*を選択します。

   _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. [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。SMTP は、 * Settings * > * Global Settings * でも設定する必要があります。

8. 概要を確認し、*[終了]*を選択します。

   リソーストポロジページが表示されます。

9. [今すぐバックアップ]*を選択します。
10. Backup （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た場合は、 [* 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にバックアップスケジュールが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に指定した保持設定に基づいて保持されます。

    b. 「 * Backup * 」を選択します。
11. 操作の進行状況を監視するには、 * Monitor * > * Jobs * をクリックします。
    - 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。

      詳細については、次を参照してください。 "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"

    - 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ヒープサイズが十分でないと、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_Command* によって、 *SnapCenter VMware* プラグインサービスが開始されます。このコマンドを次のように更新します。 *_java -jar -Xmx8192M -Xms4096M*

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定したユーザのSnapCenterサーバとの接続セッションを開始します。

   ```
   PS C:\> Open-SmConnection
   ```

   ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmResourcesコマンドレットを使用して、手動でリソースを追加します。

   次に、PostgreSQLインスタンスを追加する例を示します。

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Add-SmPolicyコマンドレットを使用して、バックアップポリシーを作成します。
4. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソースグループを追加します。
5. New-SmBackupコマンドレットを使用して、新しいバックアップジョブを開始します。

   この例は、リソースグループをバックアップする方法を示しています。

   ```
   C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-
   clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
   -Policy postgresql_policy1
   ```

   この例では、保護されたリソースをバックアップしています。

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
   -Policy postgresql_policy2
   ```

6. Get-smJobSummaryReportコマンドレットを使用して、ジョブのステータス（実行中、完了、失敗）を監視します。

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Get-SmBackupReportコマンドレットを使用して、リストアやクローニングの処理を実行するバックアップID、バックアップ名などのバックアップジョブの詳細を監視します。

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

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"。

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に対して実行されます。

開始する前に

- ポリシーを適用して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。

タスクの内容

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、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。

   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、を選択し、タグを選択します。その後、を選択してフィルタペインを閉じることができます 。

3. [Resource Groups]ページで、バックアップするリソースグループを選択し、*[Back up Now]*を選択します。
4. Backup （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にバックアップスケジュールが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に指定した保持設定に基づいて保持されます。

   b. 「 * Backup * 」を選択します。
5. 処理の進捗状況を監視するために、**[監視]**>*[ジョブ]*を選択します。

PostgreSQLバックアップ処理の監視

[SnapCenterJobs]ページを使用して、さまざまなバックアップ処理の進捗状況を監視できます。進捗状況を確認して、いつ完了したか、問題が発生していないかを確認できます。

タスクの内容

[Jobs]ページには次のアイコンが表示され、処理の状態が示されます。

- 実行中
- 完了しまし
- 失敗
- 完了（警告あり）または警告のため開始できませんでした
- キューに登録済み
- キャンセル済み

手順

1. 左側のナビゲーションペインで、 **Monitor** をクリックします。
2. [モニター] ページで、 [* ジョブ *] をクリックします。
3. Jobs （ジョブ）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、 **[*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は表示されますが ✔ 、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進行中であるか、警告サインが表示されていることがあります。

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

   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、PostgreSQLクラスタのデータ保護処理を監視します。

[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。

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. [Activity]ペインでをクリックすると、 ^ペインアイコン"] 最新の5つの処理が表示されます。

   いずれかの処理をクリックすると、*[ジョブの詳細]*ページに処理の詳細が表示されます。

PostgreSQLのバックアップ処理をキャンセルする

キューに登録されているバックアップ処理をキャンセルできます。

- 必要なもの *
- 操作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。
- バックアップ操作は、 **Monitor** ページまたは **Activity** ペインからキャンセルできます。
- 実行中のバックアップ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、バックアップ処理をキャンセルできます。
- 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

- 手順 *

  1. 次のいずれかを実行します。

アクセス元	アクション
監視ページ	a. 左側のナビゲーションペインで、 * Monitor * > * Jobs * をクリックします。 b. 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	a. バックアップ処理を開始したら、[Activity]ペインの**をクリックしペインアイコン"]て、最新の5つの処理を表示します。 b. 処理を選択します。 c. ［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。

処理がキャンセルされ、リソースが以前の状態に戻ります。

[Topology]ページでPostgreSQLのバックアップとクローンを表示

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ときに、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立つことがあります。

タスクの内容

プライマリストレージと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にあるバックアップとクローンの数が表示されます。
- SnapMirrorテクノロジ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。
- SnapVaultテクノロジ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、バックアップを4つだけ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。

[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可能なすべてのバックアップとクローンを確認できます。これらのバックアップとクローンの詳細を表示し、選択してデータ保護処理を実行できます。

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 *] 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. サマリー・カード * を確認して、プライマリ・ストレージとセカンダリ・ストレージで使用可能なバックアップとクローンの数を確認します。

   [サマリカード]セクションには、Snapshotコピーベースのバックアップとクローンの総数が表示されます。

   「 * 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。

   SnapLockが有効なバックアップが作成された場合、*[Refresh]*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は、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限も更新されます。

   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有効期限がONTAPから取得されます。

   オンデマンドバックアップのあと、*[リフレッシュ]*ボタンをクリックすると、バックアップまたはクローンの詳細がリフレッシュされます。

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、削除の各処理を実行します。

   セカンダリストレージにあるバックアップは、名前の変更や削除はできません。

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。
8. クローンをスプリットする場合は、テーブルでクローンを選択し、をクリックします 。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

ネットアップは、ここに記載されているすべての製品に対する変更を随時、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権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

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