クラウドネイティブのOracleデータベースをバックアップ

BlueXP backup and recovery

NetApp
April 18, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/bluexp-backup-recovery/task-quick-start-oracle.html on April 18, 2024. Always check docs.netapp.com for the latest.

目次

クラウドネイティブのOracleデータベースをバックアップ 1
クイックスタート 1
ONTAP のFSXを設定します 2
Cloud Volumes ONTAP を設定します 3
Azure NetApp Files を設定します 3
SnapCenter Plug-in for Oracleをインストールし、データベースホストを追加します 4
クラウドネイティブのOracleデータベースをバックアップ 11

クラウドネイティブのOracleデータベースをバックアップ

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。

1 構成がサポートされていることを確認します

- オペレーティングシステム
  - RHEL 7.5以降および8.x
  - OL 7.5以降および8.x
  - SLES 15 SP4
- ネットアップのクラウドストレージ：
  - NetApp ONTAP 対応の Amazon FSX
  - Cloud Volumes ONTAP
  - Azure NetApp Files の特長
- ストレージレイアウト：
  - NFS v3およびv4.1（dNFSを含む）
  - ASMを使用するiSCSI（ASMFD、ASMLib、ASMUdev）

> Azure NetApp Files はSAN環境をサポートしていません。

- データベースレイアウト：Oracle StandardおよびOracle Enterprise Standalone（従来型およびマルチテナントCDBおよびPDB）
- データベースのバージョン：19cと21c

2 **BlueXP**にサインアップします

BlueXPにはWebベースのコンソールからアクセスできます。BlueXPの利用を開始するには、まず既存のNetApp Support Site クレデンシャルを使用するか、ネットアップクラウドログインアカウントを作成して登録します。詳細については、を参照してください "BlueXPにサインアップします"。

3 **BlueXP**にログインします

BlueXPに登録すると、Webベースのコンソールからログインできます。詳細については、を参照してください "BlueXPにログインします"。

4 **BlueXP**アカウントを管理します

ユーザー、サービスアカウント、ワークスペース、コネクタを管理することで、アカウントを管理できます。詳細については、を参照してください "BlueXPアカウントを管理します"。

ONTAP のFSXを設定します

BlueXPを使用してFSx for ONTAP 作業環境を作成し、ボリュームや追加のデータサービスを追加、管理する必要があります。また、AWSでコネクタを作成して、パブリッククラウド環境内のリソースとプロセスをBlueXPで管理できるようにする必要があります。

ONTAP 作業環境用のFSXを作成します

データベースがホストされているFSx for ONTAP 作業環境を作成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 "Amazon FSX for ONTAP の利用を開始しましょう" および "Amazon FSX for ONTAP 作業環境の作成と管理"。

FSx for ONTAP 作業環境は、BlueXPまたはAWSを使用して作成できます。AWSを使用してを作成した場合は、BlueXPのONTAP システム用FSXを検出する必要があります。

コネクタを作成します

アカウント管理者はAWSでコネクタを作成し、BlueXPでパブリッククラウド環境内のリソースとプロセスを管理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 "BlueXPからAWSでコネクタを作成する"。

- FSx for ONTAP の作業環境とデータベースの管理には、同じコネクタを使用する必要があります。
- FSx for ONTAP の作業環境とデータベースが同じ仮想プライベートクラウド（VPC）内にある場合は、コネクタを同じVPCに導入できます。
- FSx for ONTAPの作業環境とデータベースが異なるVPCにある場合：
  - FSx for ONTAP でNAS（NFS）ワークロードが設定されている場合は、どちらかのVPCにコネクタを作成できます。
  - SANワークロードのみが設定されていて、NAS（NFS）ワークロードを使用する予定がない場合は、FSx for ONTAP システムが作成されたVPCにコネクタを作成する必要があります。

> NAS（NFS）ワークロードを使用する場合は、データベースVPCとAmazon VPC間のトランジットゲートウェイが必要です。フローティングIPアドレスであるNFS IPアドレスには、転送ゲートウェイ経由でのみ別のVPCからアクセスできます。VPCをピアリングしてフローティングIPアドレスにアクセスすることはできません。

コネクタを作成したら、**[**ストレージ**]**>* Canvas **>** My Working Environments **>**[Add Working Environment]*をクリックし、プロンプトに従って作業環境を追加します。
コネクタからOracleデータベースホストおよびFSx作業環境への接続が確立されていることを確認します。コネクタは、FSx作業環境のクラスタ管理IPアドレスに接続できる必要があります。

- **>** Canvas **>** My Working Environments **>**[作業環境の追加]*をクリックして、作業環境を追加します。

  コネクタからデータベースホストおよびFSx for ONTAP 作業環境への接続が確立されていることを確認します。コネクタは、FSx for ONTAP 作業環境のクラスタ管理IPアドレスに接続する必要があります。

- コネクター（Connector）>コネクターを管理（Manage Connectors）*をクリックし、コネクター名を選択して、コネクターIDをコピーします。

Cloud Volumes ONTAP を設定します

BlueXPを使用してCloud Volumes ONTAP 作業環境を作成し、ボリュームや追加のデータサービスを追加および管理する必要があります。また、BlueXPでパブリッククラウド環境内のリソースとプロセスを管理できるように、クラウド環境用のコネクタを作成する必要もあります。

Cloud Volumes ONTAP 作業環境を作成します

既存のCloud Volumes ONTAP システムを検出し、BlueXPに追加できます。詳細については、を参照してください "既存のCloud Volumes ONTAP システムをBlueXPに追加する"。

コネクタを作成します

クラウド環境向けCloud Volumes ONTAP の導入は、いくつかの手順で開始できます。詳細については、次のいずれかを参照してください。

- "AWS での Cloud Volumes ONTAP のクイックスタート"
- "Azure での Cloud Volumes ONTAP のクイックスタート"
- "Google Cloud の Cloud Volumes ONTAP のクイックスタート"

Cloud Volumes ONTAP 作業環境とデータベースの両方を管理するには、同じコネクタを使用する必要があります。

- Cloud Volumes ONTAP の作業環境とデータベースが同じVirtual Private Cloud（VPC；仮想プライベートクラウド）またはVNetにある場合は、コネクタを同じVPCまたはVNetに導入できます。
- Cloud Volumes ONTAP 作業環境があり、データベースが異なるVPCまたはVNetにある場合は、VPCまたはVNetがピアリングされていることを確認します。

Azure NetApp Files を設定します

BlueXPを使用してAzure NetApp Files 作業環境を作成し、ボリュームや追加のデータサービスを追加および管理する必要があります。Azureでコネクタを作成して、パブリッククラウド環境内のリソースとプロセスをBlueXPで管理できるようにすることも必要です。

Azure NetApp Files 作業環境を作成します

データベースがホストされているAzure NetApp Files 作業環境を作成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 "Azure NetApp Files の詳細をご覧ください" および "Azure NetApp Files 作業環境を作成します"。

コネクタを作成します

BlueXPのアカウント管理者は、Azureにコネクタを導入して、パブリッククラウド環境内のリソースとプロセスをBlueXPで管理できるように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 "BlueXPからAzureにコネクタを作成します"。

- コネクタからデータベースホストへの接続が確立されていることを確認します。
- Azure NetApp Files の作業環境とデータベースが同じ仮想ネットワーク（VNet）にある場合は、コネクタを同じVNetに導入できます。
- Azure NetApp Files 作業環境とデータベースが異なるVNetにあり、Azure NetApp Files でNAS（NFS）ワークロードが設定されている場合は、どちらかのVNetにコネクタを作成できます。

コネクタを作成したら、**[**ストレージ**]**>* Canvas **>**[マイ作業環境]**>**[作業環境の追加]*をクリックして作業環境を追加します。

SnapCenter Plug-in for Oracleをインストールし、データベースホストを追加します

SnapCenter Plug-in for Oracleを各Oracleデータベースホストにインストールし、データベースホストを追加し、ホスト上のデータベースを検出して、ポリシーを割り当ててバックアップを作成する必要があります。

- データベースホストでSSHが有効になっている場合は、次のいずれかの方法でプラグインをインストールできます。
  - UIからSSHオプションを使用してプラグインをインストールし、ホストを追加します。 詳細はこちら。。
  - スクリプトを使用してプラグインをインストールし、手動オプションを使用してUIからホストを追加します。 詳細はこちら。。
- SSHが無効になっている場合は、プラグインを手動でインストールし、UIからmanualオプションを使用してホストを追加します。 詳細はこちら。。

前提条件

ホストを追加する前に、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。

- 作業環境とコネクタを作成しておきます。
- コネクタがOracleデータベースホストに接続されていることを確認します。

  接続問題 を解決する方法については、を参照してください "BlueXP Connectorホストからアプリケーションデータベースホストへの接続を検証できませんでした"。

  コネクタが失われた場合、または新しいコネクタを作成した場合は、コネクタを既存のアプリケーションリソースに関連付ける必要があります。コネクタを更新する手順については、を参照してください "コネクタの詳細を更新します"。

- BlueXPユーザーに「アカウント管理者」の役割があることを確認します。

- データ保護処理用に、アプリケーションホストにroot以外の（sudo）アカウントが存在することを確認します。
- Java 11（64ビット）のOracle JavaまたはOpenJDKが各Oracleデータベースホストにインストールされていて、JAVA_HOME変数が適切に設定されていることを確認します。
- SSHベースのインストールを実行する場合は、コネクタでSSHポートへの通信が有効になっていることを確認します（デフォルト：22）。
- データ保護処理が機能するように、コネクタがプラグインポート（デフォルト：8145）との通信が有効になっていることを確認します。
- 最新バージョンのプラグインがインストールされていることを確認します。プラグインをアップグレードするには、を参照してください SnapCenter Plug-in for Oracle Databaseをアップグレードします。

SSHオプションを使用してUIからホストを追加します

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。

   ホストをすでに追加していて、別のホストを追加する場合は、**[**アプリケーション**]**>*[データベースの管理]*[追加]*をクリックし、手順5に進みます。

2. [アプリケーションの検出]をクリックします。
3. クラウドネイティブ*を選択し、*次へ*をクリックします。

   このアカウントのすべてのユーザに対してスケジュールされたデータ保護処理を実行するために、<accountid> SnapCenter System_Roleが割り当てられたサービスアカウント（*SnapCenter -account -system*）が作成されます。
   スケジュールされたバックアップ処理の実行には、サービスアカウント（_SnapCenter -account -<accountid> _）を使用します。サービスアカウントは絶対に削除しないでください。
   サービスアカウントを表示するには、**[**アカウント**]**>*[アカウントの管理]*[メンバー]*をクリックします。

4. アプリケーションタイプとして[Oracle]を選択します。
5. [Host details]ページで、次の手順を実行します。

   a. SSHを使用して*を選択します。
   b. プラグインをインストールするホストのFQDNまたはIPアドレスを指定します。

      コネクタがFQDNまたはIPアドレスを使用してデータベースホストと通信できることを確認します。

   c. プラグインパッケージのホストへのコピーに使用するroot以外のユーザ（sudo）を指定します。

      rootユーザはサポートされません。

   d. SSHとプラグインポートを指定します。

      デフォルトのSSHポートは22で、プラグインポートは8145です。

   プラグインをインストールしたら、アプリケーションホスト上のSSHポートを閉じることができます。SSHポートはデータ保護処理には必要ありません。

a. コネクタを選択します。

b. （オプション）コネクタとホストの間でキーレス認証が有効になっていない場合は、ホストとの通信に使用するSSH秘密鍵を指定する必要があります。

> SSH秘密鍵はアプリケーション内のどこにも保存されず、他の操作にも使用されません。

c. 「 * 次へ * 」をクリックします。

6. [Configuration]ページで、次の手順を実行します。

   a. Oracleデータベースを実行しているLinuxマシンにログインして、Oracleデータベースホストでの**SnapCenter**ユーザのsudoアクセスを設定します。

   b. BlueXP UIに表示されたテキストをコピーします。

   c. Linuxマシンで_/etc/sudoers.d/snapcenter_fileを作成し、コピーしたテキストを貼り付けます。

   d. BlueXP UIで、チェックボックスを選択し、*[次へ]*をクリックします。

7. 詳細を確認し、*[アプリケーションの検出]*をクリックします。

   - プラグインをインストールすると、検出処理が開始されます。
   - 検出処理が完了すると、ホスト上のすべてのデータベースが表示されます。データベースでOS認証が無効になっている場合は、*[設定]*をクリックしてデータベース認証を有効にします。詳細については、を参照してください Oracleデータベースのクレデンシャルを設定する。
   - すべてのホストを表示するには、[設定]をクリックし、[ホスト]を選択します。
   - [*設定]をクリックし、[*ポリシー]を選択して、組み込みポリシーを表示します。組み込みのポリシーを確認し、要件に合わせて編集するか、新しいポリシーを作成します。

手動オプションを使用して**UI**からホストを追加し、スクリプトを使用してプラグインをインストールします

Oracleホストのroot以外のユーザアカウントに対してSSHキーベースの認証を設定し、次の手順を実行してプラグインをインストールします。

作業を開始する前に

コネクタへのSSH接続が有効になっていることを確認します。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [アプリケーションの検出]をクリックします。
3. クラウドネイティブ*を選択し、*次へ*をクリックします。

   このアカウントのすべてのユーザに対してスケジュールされたデータ保護処理を実行するために、<accountid> SnapCenter System_Roleが割り当てられたサービスアカウント（*SnapCenter -account -system*）が作成されます。
   スケジュールされたバックアップ処理の実行には、サービスアカウント（_SnapCenter -account -<accountid> _）を使用します。サービスアカウントは絶対に削除しないでください。
   サービスアカウントを表示するには、**[**アカウント**]**>*[アカウントの管理]*[メンバー]*をクリックします。

4. アプリケーションタイプとして[Oracle]を選択します。
5. [Host details]ページで、次の手順を実行します。
   a. [* Manual*]を選択します。
   b. プラグインがインストールされているホストのFQDNまたはIPアドレスを指定します。

      コネクタがFQDNまたはIPアドレスを使用してデータベースホストと通信できることを確認します。

   c. プラグインポートを指定します。

      デフォルトポートは8145です。

   d. プラグインパッケージのホストへのコピーに使用するroot以外のユーザ（sudo）を指定します。
   e. コネクタを選択します。
   f. チェックボックスを選択して、プラグインがホストにインストールされていることを確認します。
   g. 「 * 次へ * 」をクリックします。
6. [Configuration]ページで、次の手順を実行します。
   a. Oracleデータベースを実行しているLinuxマシンにログインして、Oracleデータベースホストでの SnapCenterユーザのsudoアクセスを設定します。
   b. BlueXP UIに表示されたテキストをコピーします。
   c. Linuxマシンで_/etc/sudoers.d/snapcenter_fileを作成し、コピーしたテキストを貼り付けます。
   d. BlueXP UIで、チェックボックスを選択し、*[次へ]*をクリックします。
7. Connector VMにログインします。
8. コネクタに付属のスクリプトを使用してプラグインをインストールします。

   ```
   sudo /var/lib/docker/volumes/service-manager-
   2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
   --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
   --pluginport <plugin_port> --sshport <host_ssh_port>
   ```

   古いコネクタを使用している場合は、次のコマンドを実行してプラグインをインストールします。

   ```
   sudo
   /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
   in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
   --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
   ```

名前	説明	必須	デフォルト
plugin_hostの略	Oracleホストを指定します	はい。	-
host_user_nameを指定します	Oracleホストに対するSSH権限を持つSnapCenter ユーザを指定します	はい。	-

名前	説明	必須	デフォルト
host_ssh_keyを指定します	SnapCenter ユーザのSSHキーを指定します。このキーは、Oracleホストへの接続に使用されます	はい。	-
PLUGIN_PORT	プラグインで使用されるポートを指定します	いいえ	8145
host_ssh_portを指定します	OracleホストのSSHポートを指定します	いいえ	22

例：

- `sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`
- `sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`

9. BlueXP UIで詳細を確認し、*[アプリケーションの検出]*をクリックします。
   - 検出処理が完了すると、ホスト上のすべてのデータベースが表示されます。データベースでOS認証が無効になっている場合は、*[設定]*をクリックしてデータベース認証を有効にします。詳細については、を参照してください Oracleデータベースのクレデンシャルを設定する。
   - すべてのホストを表示するには、[設定]をクリックし、[ホスト]を選択します。
   - [*設定]をクリックし、[*ポリシー]を選択して、組み込みポリシーを表示します。組み込みのポリシーを確認し、要件に合わせて編集するか、新しいポリシーを作成します。

手動オプションを使用して**UI**からホストを追加し、プラグインを手動でインストールします

OracleデータベースホストでSSHキーベースの認証が有効になっていない場合は、次の手動手順を実行してプラグインをインストールし、manualオプションを使用してUIからホストを追加する必要があります。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [アプリケーションの検出]をクリックします。
3. クラウドネイティブ*を選択し、*次へ*をクリックします。

   このアカウントのすべてのユーザに対してスケジュールされたデータ保護処理を実行するために、<accountid> SnapCenter System_Roleが割り当てられたサービスアカウント（*SnapCenter -account -system*）が作成されます。
   スケジュールされたバックアップ処理の実行には、サービスアカウント（_SnapCenter -account -<accountid> _）を使用します。サービスアカウントは絶対に削除しないでください。

サービスアカウントを表示するには、**[**アカウント**]**>*[アカウントの管理]*[メンバー]*をクリックします。

4. アプリケーションタイプとして[Oracle]を選択します。
5. [ホストの詳細]ページで、次の手順を実行します。
   a. [* Manual*]を選択します。
   b. プラグインがインストールされているホストのFQDNまたはIPアドレスを指定します。

      FQDNまたはIPアドレスを使用して、コネクタがデータベースホストと通信できることを確認します。

   c. プラグインポートを指定します。

      デフォルトポートは8145です。

   d. プラグインパッケージのホストへのコピーに使用するsudo非root（sudo）ユーザを指定します。
   e. コネクタを選択します。
   f. チェックボックスを選択して、プラグインがホストにインストールされていることを確認します。
   g. 「 * 次へ * 」をクリックします。
6. [Configuration]ページで、次の手順を実行します。
   a. Oracleデータベースを実行しているLinuxマシンにログインして、OracleデータベースホストでSnapCenterユーザのsudoアクセスを設定します。
   b. BlueXP UIに表示されたテキストをコピーします。
   c. Linuxマシンで_/etc/sudoers.d/snapcenter_fileを作成し、コピーしたテキストを貼り付けます。
   d. BlueXP UIで、チェックボックスを選択し、*[次へ]*をクリックします。
7. Connector VMにログインします。
8. SnapCenter Linuxホストプラグインバイナリをダウンロードします。
   ```
   sudo docker exec -it cloudmanager_scs_cloud curl -X GET
   'http://127.0.0.1/deploy/downloadLinuxPlugin'
   ```

   プラグインのバイナリは次の場所にあります。*cd /var/lib/docker/volumes/service-manager [1]-2_cloudmanager_SCS_cloud_volume/_data/$*（*sudo docker ps | grep -Po" cloudmanager_SCS_cloud*：。？***"|sed -e 's/***$//"| cut-f2-d"*：*"*）*/sc-linux-host-plugin*

9. scpまたはその他の別の方法を使用して、上記のパスから各<non root user (sudo)> データベースホストの_/ home/oracle/.sc_netapp_pathに_snapcenter_linux_host_plugin_sc.bin_をコピーします。
10. root以外の（sudo）アカウントを使用してOracleデータベースホストにログインします。
11. ディレクトリを_/ home/home /<non root user> /.sc_netapp/_に変更し、次のコマンドを実行してバイナリの実行権限を有効にします。
    ```
    chmod +x snapcenter_linux_host_plugin_scs.bin
    ```
12. OracleプラグインをSudo SnapCenter ユーザとしてインストールします。
    ```
    ./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
    ```
13. コネクタVMのcopy_certificate.pem_from_certificate/client/certificate/*path <base_mount_path>*をプラグインホストの/var/opt/snapcenter/spl/etc/にコピーします。

14. _/var/opt/snapcenter/spl/etcに移動し、keytoolコマンドを実行してcertificate.pemをインポートします。
```
keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks
-deststorepass snapcenter -noprompt
```
15. SPLを再起動します。 `systemctl restart spl`
16. コネクタから次のコマンドを実行して、コネクタからプラグインに到達できることを確認します。
```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
plug-in host>:<plug-in port>/PluginService/Version --cert
/config/client/certificate/certificate.pem --key
/config/client/certificate/key.pem
```
17. BlueXP UIで詳細を確認し、*[アプリケーションの検出]*をクリックします。
    - 検出処理が完了すると、ホスト上のすべてのデータベースが表示されます。データベースでOS認証が無効になっている場合は、*[設定]*をクリックしてデータベース認証を有効にします。詳細については、を参照してください Oracleデータベースのクレデンシャルを設定する。
    - すべてのホストを表示するには、[設定]をクリックし、[ホスト]を選択します。
    - [*設定]をクリックし、[*ポリシー]を選択して、組み込みポリシーを表示します。組み込みのポリシーを確認し、要件に合わせて編集するか、新しいポリシーを作成します。

Oracleデータベースのクレデンシャルを設定する

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

手順

1. データベースでOS認証が無効になっている場合は、*[設定]*をクリックしてデータベース認証を変更します。
2. ユーザ名、パスワード、およびポートの詳細を指定します。

   データベースがASMにある場合は、ASMも設定する必要があります。

   Oracleユーザにはsysdba権限が必要で、ASMユーザにはSYSASM権限が必要です。

3. [**Configure**] をクリックします。

SnapCenter Plug-in for Oracle Databaseをアップグレードします

最新の新機能や機能拡張を利用するには、SnapCenter Plug-in for Oracleをアップグレードする必要があります。BlueXP UIまたはコマンドラインを使用してアップグレードできます。

作業を開始する前に

- ホストで実行中の処理がないことを確認します。

手順

1. **>**[アプリケーション]**>**[ホスト]*をクリックします。
2. いずれかのホストでプラグインアップグレードを利用できるかどうかを[Overall Status]列で確認します。
3. UIまたはコマンドラインを使用してプラグインをアップグレードします。

UIを使用してアップグレードする	コマンドラインを使用してアップグレードします

a. をクリックします ••• ホストに対応し、*[プラグインのアップグレード]*をクリックします。
b. [Configuration]ページで、次の手順を実行します。
i. Oracleデータベースを実行しているLinuxマシンにログインして、Oracleデータベースホストで SnapCenterユーザのsudoアクセスを設定します。
ii. BlueXP UIに表示されたテキストをコピーします。
iii. Linuxマシンで_/etc/sudoers.d/snapcenter_fileを編集し、コピーしたテキストを貼り付けます。
iv. BlueXP UIで、チェックボックスを選択し、*[アップグレード]*をクリックします。
	a. コネクタVMにログインします。
	b. 次のスクリプトを実行します。
	`sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`
	
	古いコネクタを使用している場合は、次のコマンドを実行してプラグインをアップグレードします。
	`sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`

クラウドネイティブのOracleデータベースをバックアップ

組み込みのポリシーまたは作成したポリシーを割り当てて、スケジュールされたバックアップまたはオンデマンドバックアップを作成できます。

ポリシーの作成時にカタログ化を有効にした場合は、Oracle Recovery Manager（RMAN）を使用してOracleデータベースバックアップをカタログ化することもできます。（RMAN）のカタログ化は、Azure NetApp Files上のデータベースでのみサポートされます。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。

Oracleデータベースを保護するポリシーを作成します

組み込みのポリシーを編集しない場合は、ポリシーを作成できます。

- 手順 *

1. [アプリケーション]ページの[設定]ドロップダウンリストから、[ポリシー]を選択します。
2. ［ポリシーの作成］をクリックします。

3. ポリシー名を指定します。
4. （オプション）バックアップ名の形式を編集します。
5. スケジュールと保持の詳細を指定します。
6. スケジュールとして_daily_and_weekly_を 選択し、RMANカタログへの登録を有効にする場合は、*[Catalog backup with Oracle Recovery Manager（RMAN）]*を選択します。
7. （オプション）バックアップの成功後に実行するポストスクリプトのパスとタイムアウト値（Snapshotのセカンダリストレージへのコピーなど）を入力します。

   必要に応じて、引数を指定することもできます。

   ポストスクリプトは、_/var/opt/snapcenter/spl/scripts _というパスに保存する必要があります。

   POSTスクリプトは、一連の環境変数をサポートします。

環境変数	説明
SC_ORACLE_SID	OracleデータベースのSIDを指定します。
sc_hostの略	データベースのホスト名を指定します
SC_BACKUP_NAME	バックアップの名前を指定します。データバックアップ名とログバックアップ名は区切り文字で連結されます。
SC_BACKUP_POLICY_NAME	バックアップの作成に使用するポリシーの名前を指定します。
sc_primary_data_volume_full_pathを指定します	区切り文字として「、」を使用して連結されたデータボリュームパスを指定します。 Azure NetApp Filesボリュームの場合、情報はを使用して連結されます。 */subscriptions/｛subscription_id｝/resourceGroups/｛resource_group｝/providers/｛provider｝/netAppAccounts/｛anfaccount｝/capacityPools/｛capacity_pool｝/volumes/｛VolumeName｝*
sc_primary_archivelogs_volume_full_pathを指定します	区切り文字として「、」を使用して連結されたアーカイブログボリュームのパスを指定します。 Azure NetApp Filesの場合は、を使用して連結された情報 */subscriptions/｛subscription_id｝/resourceGroups/｛resource_group｝/providers/｛provider｝/netAppAccounts/｛anfaccount｝/capacityPools/｛capacity_pool｝/volumes/｛VolumeName｝*

1. [作成（ Create ）] をクリックします。

RMANカタログリポジトリを設定します

リカバリカタログデータベースをRMANカタログリポジトリとして設定できます。リポジトリを設定しない場合、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RMANカタログ・リポジトリになります。

作業を開始する前に

ターゲット・データベースをRMANカタログ・データベースに手動で登録する必要があります。

手順

1. [アプリケーション]ページで、をクリックします ••• >*詳細を表示*。
2. [Database details]セクションで、をクリックします RMANカタログリポジトリを設定するには、次の手順を実行します。
3. RMANを使用してバックアップをカタログ化するためのクレデンシャルと、カタログリカバリデータベースのTransparent Network Substrate（TNS）名を指定します。
4. [**Configure**] をクリックします。

Oracleデータベースのバックアップを作成します

組み込みのポリシーを割り当てるか、ポリシーを作成してデータベースに割り当てることができます。ポリシーを割り当てると、ポリシーで定義されたスケジュールに従ってバックアップが作成されます。

> Amazon FSx for NetApp ONTAP またはCloud Volumes ONTAP でASMディスクグループを作成する場合は、ディスクグループ間に共通のボリュームが存在しないことを確認してください。各ディスクグループに専用のボリュームを配置する必要があります。

- 手順 *

1. [アプリケーション]ページで、データベースがポリシーを使用して保護されていない場合は、[ポリシーの割り当て]をクリックします。

   データベースが1つ以上のポリシーを使用して保護されている場合は、をクリックして複数のポリシーを割り当てることができます ••• >*ポリシーの割り当て*。

2. ポリシーを選択し、* assign *をクリックします。

   バックアップは、ポリシーで定義されたスケジュールに従って作成されます。ポリシーでRMANカタログを有効にしている場合は、ワークフローの最後のバックアップでカタログ化処理が別のジョブとして起動されます。カタログ化の進捗状況はジョブモニタで確認できます。カタログ化が成功すると、*[バックアップの詳細]*に各バックアップのカタログのステータスが表示されます。

   > スケジュールされたバックアップ処理の実行には、サービスアカウント（_SnapCenter -account-<account_id> _）を使用します。

Oracleデータベースのオンデマンドバックアップを作成する

ポリシーを割り当てたら、アプリケーションのオンデマンドバックアップを作成できます。

- 手順 *

  1. [アプリケーション]ページで、をクリックします ••• アプリケーションに対応して、*オンデマンドバックアップ*をクリックします。
  2. アプリケーションに複数のポリシーが割り当てられている場合は、ポリシーと保持階層を選択し、*[バックアップの作成]*をクリックします。

     ポリシーでRMANカタログを有効にしている場合は、ワークフローの最後のバックアップでカタログ化処理が別のジョブとして起動されます。カタログ化の進捗状況はジョブモニタで確認できます。カタログ化が成功すると、*[バックアップの詳細]*に各バックアップのカタログのステータスが表示されます。

制限

- では、FSXボリュームと重複する複数のASMディスクグループに存在するOracleデータベースの整合グループSnapshotはサポートされていません
- OracleデータベースがAmazon FSx for NetApp ONTAP またはCloud Volumes ONTAP 上にあり、ASM上に設定されている場合は、SVM名がFSxシステム全体で一意であることを確認してください。FSXシステム間でSVM名が同じ場合は、それらのSVM上にあるOracleデータベースのバックアップはサポートされません。
- 大規模なデータベース（250GB以上）をリストアしたあとに、同じデータベースでフルオンラインバックアップを実行すると、次のエラーメッセージが表示されて処理が失敗することがあります。

  ```
  failed with status code 500, error
  {\"error\":{\"code\":\"app_internal_error\",\"message\":\"Failed to create
  snapshot. Reason: Snapshot operation not allowed due to clones backed by
  snapshots. Try again after sometime.
  ```

  この問題 の修正方法については、以下を参照してください。 "Snapshotでバックアップされたクローンが原因で、Snapshot処理を実行できません"。

著作権に関する情報

Copyright © 2024 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。