Creating a profile for your database

SnapManager Oracle

NetApp
February 05, 2021

Table of Contents

Creating a profile for your database 1

Creating a profile for your database

You must create a profile for your database to perform any operation on that database. The profile contains information about the database and can reference only one database; however, a database can be referenced by multiple profiles. A backup that is created using one profile cannot be accessed from a different profile, even if both profiles are associated with the same database.

You must ensure that target database details are included in the /etc/oratab file.

These steps show how to create a profile for your database using the SnapManager UI. You can also use the CLI if you prefer.

For information about how to create profiles using the CLI, see the *SnapManager for Oracle Administration Guide for UNIX*.

1. From the Repositories tree, right-click the repository or the host and select **Create Profile**.
2. On the Profile Configuration Information page, enter the custom name and password for the profile.
3. On the Database Configuration Information page, enter the following information:

In this field…	Do this…
Database Name	Enter the name of the database you want to backup.
Database SID	Enter the secure ID (SID) of the database. The database name and the database SID can be the same.
Host	Enter the IP address of the host where the target database resides. You can also specify the host name if the host name is specified in the Domain Name System (DNS).
Host Account	Enter the Oracle user name of the target database. The default value for the user is oracle.
Host Group	Enter the Oracle user group name. The default value is dba. +

4. On the Database Connection Information page, select one of the following:

Choose this…	If you want to…
Use O/S Authentication	Use the credentials maintained by the operating system to authenticate users who access the database.

Choose this…	If you want to…
Use Database Authentication	Allow Oracle to authenticate an administrative user using password file authentication. Enter the appropriate database connection information. • In the **SYSDBA Privileged User Name** field, enter the name of the database administrator with administrative privileges. • In the **Password** field, enter the password of the database administrator. • In the **Port** field, enter the port number used to connect to the host where the database resides. The default value is .
Use ASM Instance Authentication	Allow Automatic Storage Management (ASM) database instance to authenticate an administrative user. Enter the appropriate ASM instance authentication information. • In the **SYSDBA/SYSASM Privileged User Name** field, enter the user name of the ASM instance administrator with administrative privileges. • In the **Password** field, enter password of the administrator.

Note: You can select the ASM authentication mode only if you have an ASM instance on the database host.

5. On the RMAN Configuration Information page, select one of the following:

Choose this…	If…
Do not use RMAN	You are not using RMAN to manage backup and restore operations.
Use RMAN via the control file	You are managing the RMAN repository using control files.
Use RMAN via Recovery Catalog	You are managing the RMAN repository using recovery catalog database. Enter the user name who has access to recovery catalog database, password, and the Oracle net service name of the database that manages the Transparent Network Substrate (TNS) connection. +

6. On the Snapshot Naming Information page, select the variables to specify a naming format for the Snapshot copy.

   You must include the smid variable in the naming format. The smid variable creates a unique Snapshot identifier.

7. On the Policy Settings page, perform the following:
   a. Enter the retention count and duration for each retention class.
   b. From the **Protection Policy** drop-down list, select the Protection Manager policy.
   c. If you want to back up archive logs separately, select the **Backup Archivelogs Separately** checkbox, specify the retention, and select the protection policy.

      You can select a policy which is different from the policy associated for datafiles. For example, if you have selected one of the Protection Manager policy for datafiles, you can select a different Protection Manager policy for archive logs.

8. On the Configure Notification Settings page, specify the email notification settings.
9. On the History Configuration Information page, select one of the options to maintain the history of SnapManager operations.
10. On the Perform Profile Create Operation page, verify the information and click **Create**.
11. Click **Finish** to close the wizard.

    If the operation fails, click **Operation Details** to view what caused the operation to fail.

Related information

SnapManager 3.4 for Oracle Administration Guide for UNIX