Backing up and verifying your databases

SnapManager Oracle

NetApp
February 12, 2024

Table of Contents

Backing up and verifying your databases

After installing SnapManager, you can create a basic backup of your database and verify that backup to ensure it does not contain any corrupt files.

Related information

SnapManager backup overview

Defining a backup strategy

Creating a profile for your database

Backing up your database

Verifying database backups

Scheduling recurring backups

SnapManager backup overview

SnapManager uses NetApp Snapshot technology to create backups of databases. You can use the DBVERIFY utility, or you can use SnapManager to verify the integrity of the backups.

SnapManager backs up a database by creating Snapshot copies of the volumes containing data files, control files, and archive log files. Together, these Snapshot copies comprise a backup set that SnapManager can use to restore a database.

Defining a backup strategy

Defining a backup strategy before creating your backups ensures that you have backups to successfully restore your databases. SnapManager provides flexible granular backup schedule to meet your Service Level Agreement (SLA).

For SnapManager best practices, see *TR 3761*.

What mode of SnapManager backup do you need?

SnapManager supports two modes of backups:

Backup mode	Description
Online backup	Creates a backup of the database when the database is in online state. This backup mode is also called a hot backup.

Backup mode	Description
Offline backup	Creates a backup of the database when the database is either in a mounted or shutdown state. This backup mode is also called a cold backup.

What type of SnapManager backup do you need?

SnapManager supports three types of backups:

Backup type	Description
Full backup	Creates a backup of the entire database, which includes all the datafiles, control files, and archive log files.
Partial backup	Creates a backup of selected datafiles, control files, tablespaces, and archive log files
Archive log-only backup	Creates a backup of only the archive log files.You must select **Backup Archivelogs Separately** while creating the profile.

What type of database profile do you need?

SnapManager creates backups based on whether the database profile separates the archive log backups from the data file backups.

Profile type	Description
A single database profile for combined backup of data files and archive logs	Allows you to create: • Full backup containing all the data files, archive log files, and control files • Partial backup containing selected data files, tablespaces, archive log files, and control files
Separate database profiles for archive log backups and data file backups	Allows you to create: • Combined backup with different labels for data file backup and archive log backup • Data-files-only backup of all the data files along with the control files • Partial data-files-only backup of selected data files or tablespaces along with the control files • Archive-logs-only backup

What naming conventions should be used for Snapshot copies?

Snapshot copies created by backups can follow a custom naming convention. Custom text or built-in variables such as the profile name, the database name, and the database SID provided by SnapManager can be used to create the naming convention. You can create the naming convention while creating the policy.

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

The Snapshot copy naming convention can be changed during or after the creation of a profile. The updated pattern applies only to Snapshot copies that have not yet been created; existing Snapshot copies retain the previous pattern.

How long do you want to retain backup copies on the primary storage system and the secondary storage system?

A backup retention policy specifies the number of successful backups to retain. You can specify the retention policy while creating the policy.

You can select hourly, daily, weekly, monthly, or unlimited as the retention class. For each retention class, you can specify the retention count and retention duration, either together or individually.

- Retention count determines the minimum number of backups of a particular retention class that should be retained.

  For example, if backup schedule is *daily* and retention count is *10*, then 10 daily backups are retained.

  > The maximum number of Snapshot copies that Data ONTAP allows you can retain is 255. After it reaches the maximum limit, by default the creation of new Snapshot copies fail. However, you can configure the rotation policy in Data ONTAP to delete older Snapshot copies.

- Retention duration determines the minimum number of days for which the backup should be retained.

  For example, if backup schedule is *daily* and retention duration is *10*, then 10 days of daily backups are retained.

If you set up SnapMirror replication, the retention policy is mirrored on the destination volume.

> For long-term retention of backup copies, you should use SnapVault.

Do you want to verify backup copies using the source volume or a destination volume?

If you use SnapMirror or SnapVault, you can verify backup copies using the Snapshot copy on the SnapMirror or SnapVault destination volume rather than the Snapshot copy on the primary storage system. Using a destination volume for verification reduces the load on the primary storage system.

Related information

NetApp Technical Report 3761: SnapManager for Oracle: Best Practices

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

Backing up your database

After creating a profile, you must back up your database. You can schedule recurring backups after the initial backup and verification.

These steps show how to create a backup of your database using the SnapManager user interface. You can also use the command-line interface (CLI) if you prefer.

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

1. From the Repositories tree, right-click the profile containing the database you want to back up, and select **Backup**.
2. In **Label**, enter a custom name for the backup.

   You must not include spaces or special characters in the name. If you do not specify a name, SnapManager automatically creates a backup label.

   From SnapManager 3.4, you can modify the backup label created automatically by SnapManager. You can edit the override.default.backup.pattern and new.default.backup.pattern configuration variables to create your own default backup label pattern.

3. Select **Allow startup or shutdown of database, if necessary** to modify the state of the database, if required.

   This option ensures that if the database is not in the required state to create a backup, SnapManager automatically brings the database to the desired state to complete the operation.

4. On the Database, Tablespaces or Datafiles to Backup page, perform the following:
   a. Select **Backup Datafiles** to back up either the full database, selected data files, or selected tablespaces.
   b. Select **Backup Archivelogs** to back up the archive log files separately.
   c. Select **Prune Archivelogs** if you want to delete the archive log files from the active file system that is already backed up.

      If Flash Recovery Area (FRA) is enabled for archive log files, then SnapManager fails to prune the archive log files.

   d. Select **Protect the backup** if you want to enable backup protection.

      This option is enabled only if the protection policy was selected while creating the profile.

   e. Select **Protect Now** if you want to protect the backup immediately to the secondary storage overriding Protection Manager's protection schedule.
   f. From the **Type** drop-down list, select the type of backup (offline or online) you want to create.

      If you select Auto, SnapManager creates a backup based on the current state of the database.

   g. From the **Retention Class** drop-down list, select the retention class.
   h. Select the **Verify backup using the Oracle DBVERIFY utility** check box if you want to ensure that the backed-up files are not corrupted.
5. On the Task Enabling page, specify whether you want to perform tasks before and after backup operations are completed.
6. On the Perform Backup Operation page, verify the information and click **Backup**.
7. Click **Finish** to close the wizard.

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

Verifying database backups

You can verify the backup of your database to ensure that the backed-up files are not corrupted.

If you did not select the **Verify backup using the Oracle DBVERIFY utility** check box while creating a backup, you must perform these steps manually to verify the backup. However, if you selected the check box, SnapManager automatically verifies the backup.

1. From the **Repositories** tree, select the profile.
2. Right-click the backup that you want to verify, and select **Verify**.
3. Click **Finish**.

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

In the **Repository** tree, right-click the backup, and then click **Properties** to view the results of the verify operation.

You can use backed-up files to perform restore operations. For information about how to perform restore operations using the SnapManager user interface (UI), see the *Online Help*. If you want to use the command-line interface (CLI) to perform restore operations, see the *SnapManager for Oracle Administration Guide for UNIX*.

Related information

SnapManager 3.4 for Oracle Administration Guide for UNIX

Scheduling recurring backups

You can schedule backup operations so that the backups are initiated automatically at regular intervals. SnapManager allows you to schedule backups on an hourly, daily, weekly, monthly, or one-time basis.

You can assign multiple backup schedules for a single database. However, when scheduling multiple backups for the same database, you must ensure that the backups are not scheduled at the same time.

These steps show how to create a backup schedule for your database using the SnapManager user interface (UI). You can also use the command-line interface (CLI) if you prefer. For information about how to schedule backups using the CLI, see the *SnapManager for Oracle Administration Guide for UNIX*.

1. From the Repositories tree, right-click the profile containing the database for which you want to create a backup schedule, and select **Schedule Backup**.
2. In **Label**, enter a custom name for the backup.

   You must not include spaces or special characters in the name. If you do not specify a name, SnapManager automatically creates a backup label.

   From SnapManager 3.4, you can modify the backup label created automatically by SnapManager. You can edit the override.default.backup.pattern and new.default.backup.patternconfiguration variables to create your own default backup label pattern.

3. Select **Allow startup or shutdown of database, if necessary** to modify the state of the database, if required.

   This option ensures that if the database is not in the required state to create a backup, SnapManager automatically brings the database to the desired state to complete the operation.

4. On the Database, Tablespaces or Datafiles to Backup page, perform the following:
   a. Select **Backup Datafiles** to back up either the full database, selected data files, or selected tablespaces.
   b. Select **Backup Archivelogs** to back up the archive log files separately.
   c. Select **Prune Archivelogs** if you want to delete the archive log files from the active file system that is already backed up.

> If Flash Recovery Area (FRA) is enabled for archive log files, then SnapManager fails to prune the archive log files.

d. Select **Protect the backup** if you want to enable backup protection.

   This option is enabled only if the protection policy was selected while creating the profile.

e. Select **Protect Now** if you want to protect the backup immediately to the secondary storage overriding Protection Manager's protection schedule.

f. From the **Type** drop-down list, select the type of backup (offline or online) you want to create.

   If you select Auto, SnapManager creates a backup based on the current state of the database.

g. From the **Retention Class** drop-down list, select the retention class.

h. Select the **Verify backup using the Oracle DBVERIFY utility** check box if you want to ensure that the backed-up files are not corrupted.

5. In the **Schedule Name** field, enter a custom name of the schedule.

   You must not include spaces in the name.

6. On the Configure Backup Schedule page, perform the following:

   a. From the **Perform this operation** drop-down list, select the frequency of the backup schedule.

   b. In the **Start Date** field, specify the date when you want to initiate the backup schedule.

   c. In the **Start Time** field, specify the time when you want to initiate the backup schedule.

   d. Specify the interval in which backups will be created.

      For example, if you have selected the frequency as hourly and specify the interval as 2, then backups will be scheduled every 2 hours.

7. On the Task Enabling page, specify whether you want to perform tasks before and after backup operations are completed.

8. On the Perform Backup Schedule Operation page, verify the information and click **Schedule**.

9. 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