NetApp

Protected backup configuration and execution

SnapManager Oracle

NetApp
November 04, 2025

Table of Contents

Protected backup configuration and execution

You must configure SnapManager and Protection Manager to support database backup to secondary storage. The database administrator and the storage administrator must coordinate their actions.

Using SnapManager for Oracle to create the database profile for a local backup

The database administrators use SnapManager to create a database profile that will be used to initiate a backup to local storage on a primary storage system. The entire profile creation and backup creation processes are performed entirely in SnapManager; they do not involve Protection Manager.

A profile contains the information about the database being managed, including its credentials, backup settings, and protection settings for backups. By creating a profile, you do not need to specify database details each time you perform an operation on that database, instead just provide the profile name. A profile can reference only one database. That same database can be referenced by more than one profile.

1. Go to the SnapManager for Oracle client.

2. From the SnapManager Repositories tree, right-click the host you want associated with this profile, and select **Create Profile**.

3. In the Profile Configuration Information page, enter the following information and click **Next**.

   ◦ Profile name: payroll_prod

   ◦ Profile password: payroll123

   ◦ Comment: Production Payroll database

4. In the Database Configuration Information page, enter the following information and click **Next**.

   ◦ Database name: PAYDB

   ◦ Database SID: payrolldb

   ◦ Database host: Accept the default

     Because you are creating a profile from a host in the repository tree, SnapManager displays the host name.

5. In the second Database Configuration Information page, accept the following database information and click **Next**:

   ◦ Host Account, representing the Oracle user account: oracle

   ◦ Host Group, representing the Oracle group: dba

6. In the Database Connection Information page, select **Use database Authentication** to allow users to authenticate using database information.

   For this example, enter the following information and click **Next**.

   ◦ SYSDBA Privileged User Name, representing the system database administrator who has administrative privileges: sys

- Password (SYSDBA password): oracle
- Port to connect to database host: 1521

7. In the RMAN Configuration Information page, select **Do not use RMAN** and click **Next**.

    Oracle Recovery Manager (RMAN) is an Oracle tool that helps you back up and recover Oracle databases using block-level detection.

8. In the Snapshot Naming Information page, specify a naming convention for the Snapshots associated with this profile by selecting variables. The only variable that is required is the **smid** variable, which creates a unique snapshot identifier.

    For this example, do the following:

    a. In the Variable Token list, select the **{usertext}** variable and click **Add**.

    b. Enter "payroll.techco.com_" as the host name and click **OK**.

    c. Click **Left** until the host name appears just after "smo" in the Format box.

    d. Click **Next**.

    The Snapshot naming convention of smo_hostname_smoprofile_dbsid_scope_mode_smid becomes "smo_payroll.techco.com_payroll_prod2_payrolldb_f_a_x" (where the "f" indicates a full backup, the "a" indicates the automatic mode, and the "x" represents the unique SMID).

9. On the Perform Operation page, verify the information and click **Create**.

10. Click **Operation Details** to see information about the profile create operation and volume-based restore eligibility information.

Using Protection Manager to configure a secondary resource pool

To support backup of the database to secondary storage, the storage administrator uses Protection Manager to organize the secondary storage systems enabled with the SnapVault Secondary license into a resource pool for the backups.

Ideally, storage systems in a resource pool are interchangeable in terms of their acceptability as destinations for backups. For example, when developing the protection strategy for the payroll database, you, as the storage administrator, identified secondary storage systems with similar performance and quality of service levels that would be suitable members of the same resource pool.

You have already created aggregates of unused space on storage systems that you intend to assign to resource pools. This ensures that there is adequate space to contain the backups.

1. Go to Protection Manager's NetApp Management Console.

2. From the menu bar, click **Data** > **Resource Pools**.

    The Resource Pools window appears.

3. Click **Add**.

    The Add Resource Pool wizard starts.

4. Complete the steps in the wizard to create the **paydb_backup_resource** resource pool.

Use the following settings:

- Name: Use **paydb-backup_resource**
- Space thresholds (use the defaults):
    - Space utilization thresholds: enabled
    - Nearly Full threshold (for resource pool): 80%
    - Full threshold (for resource pool): 90%

Using Protection Manager to configure secondary backup schedules

To support backup of the database to secondary storage, the storage administrator uses Protection Manager to configure a backup schedule.

Before configuring the schedule for secondary backups, the storage administrator confers with the DBA partner for the following information:

- The schedule that the DBA wants the secondary backups to follow.

In this case, once-daily backups occur at 7 p.m. and once-weekly backups occur on Saturday at 1 a.m.

1. Go to the Protection Manager's NetApp Management Console.
2. From the menu bar, click **Policies** > **Protection** > **Schedules**.

   The Schedules tab of the Protection Policies window is displayed.

3. Select the Daily schedule**Daily at 8:00 PM** in the list of schedules.
4. Click **Copy**.

   A new Daily schedule, **Copy of Daily at 8:00 PM**, is displayed in the list. It is already selected.

5. Click **Edit**.

   The Edit Daily Schedule property sheet opens to the Schedule tab.

6. Change the schedule name to **Payroll Daily at 7 PM**, update the description, then click **Apply**.

   Your changes are saved.

7. Click the **Daily Events** tab.

   The schedule's current Daily backup time of 8:00 p.m. is displayed.

8. Click **Add** and enter **7:00 PM** in the new time field, then click **Apply**.

   The schedule's current Daily backup time is now 7:00 p.m.

9. Click **OK** to save your changes and exit the property sheet.

Your new Daily schedule, **Payroll Daily at 7 PM**, is displayed in the list of schedules.

10. Select the Weekly schedule**Sunday at 8:00 PM plus daily** in the list of schedules.

11. Click **Copy**.

    A new Weekly schedule, **Copy of Sunday at 8:00 PM plus daily**, is displayed in the list. It is already selected.

12. Click **Edit**.

    The Edit Weekly Schedule property sheet opens to the Schedule tab.

13. Change the schedule name to **Payroll Saturday at 1 AM plus daily at 7 PM** and update the description.

14. From the **Daily Schedule** drop-down list, select the Daily schedule you just created, **Payroll Daily at 7 PM**.

    Selecting **Payroll Daily at 7 PM** means that this schedule defines when Daily operations occur when the **Payroll Saturday at 1 AM plus daily at 7 PM** schedule is applied to a policy.

15. Click **OK** to save your changes and exit the property sheet.

    Your new Weekly schedule, **Payroll Saturday at 1 AM plus daily at 7 PM**, is displayed in the list of schedules.

Using Protection Manager to configure a secondary backup protection policy

After configuring the backup schedule, the storage administrator configures a protected backup storage policy in which that schedule is to be included.

Before configuring the protection policy, the storage administrator confers with the DBA partner for the following information:

- Retention duration to specify for secondary storage

- Type of secondary storage protection required

The protection policy that is created, can be listed in SnapManager for Oracle by the DBA partner and assigned to a database profile for the data to be protected.

1. Go to Protection Manager's NetApp Management Console.

2. From the menu bar, click **Policies** > **Protection** > **Overview**.

   The Overview tab on the Protection Policies window is displayed.

3. Click **Add Policy** to start the Add Protection Policy wizard.

4. Complete the wizard with the following steps:

   a. Specify a descriptive policy name.

      For this example, enter **TechCo Payroll Data: Backup** and a description, then click **Next**.

b. Select a base policy.

For this example, select **Back up** and click **Next**.

c. In the Primary Data node policy property sheet, accept the default settings and click **Next**.

> (i) In this example, the local backup schedule that was configured in SnapManager is applied. Any local backup schedule that is specified using this method is ignored.

d. In the Primary Data to Backup connection property sheet, select a backup schedule.

For this example, select **Payroll Saturday at 1 AM plus daily at 7 PM** as your backup schedule, then click **Next**.

In this example, the schedule that you selected includes both the weekly and daily schedules that you configured earlier.

e. In the Backup policy property sheet, specify the name for the backup node and the retention times for Daily, Weekly, or Monthly backups.

For this example, specify a Daily backup retention of 10 days and a Weekly backup retention of 52 weeks. After you complete each property sheet, click **Next**.

After all property sheets are completed, the Add Protection Policy wizard displays a summary sheet for the protection policy that you want to create.

5. Click **Finish** to save your changes.

The **TechCo Payroll Data: Backup** protection policy is listed among the other policies configured for Protection Manager.

The DBA partner can now use SnapManager for Oracle to list and assign this policy when creating the database profile for the data to be protected.

Using SnapManager for Oracle to create the database profile and assign a protection policy

You must create a profile in SnapManager for Oracle, enable protection in the profile, and assign a protection policy to create a protected backup.

A profile contains information about the database being managed, including its credentials, backup settings, and protection settings for backups. After you create a profile, you do not need to specify database details each time you perform an operation. A profile can reference only one database, but that same database can be referenced by more than one profile.

1. Go to the SnapManager for Oracle client.

2. From the Repositories tree, right-click the host, and select **Create Profile**.

3. On the Profile Configuration Information page, enter the profile details, and click **Next**.

You can enter the following information:

  ◦ Profile name: payroll_prod2

- Profile password: payroll123
- Comment: Production Payroll database

4. On the Database Configuration Information pages, enter the database details, and click **Next**.

   You can enter the following information:

   - Database name: PAYDB
   - Database SID: payrolldb
   - Database host: Accept the default. Because you are creating a profile from a host in the repository tree, SnapManager displays the host name.
   - Host Account, representing the Oracle user account: oracle
   - Host Group, representing the Oracle group: dba

5. On the Database Connection Information page, click **Use database Authentication** to allow users to authenticate using database information.

6. Enter the database connection details and click **Next**.

   You can enter the following information:

   - SYSDBA Privileged User Name, representing the system database administrator who has administrative privileges: sys
   - Password (SYSDBA password): oracle
   - Port to connect to database host: 1521

7. On the RMAN Configuration Information page, click **Do not use RMAN** and click **Next**.

   Oracle Recovery Manager (RMAN) is an Oracle tool that helps you back up and recover Oracle databases using block-level detection.

8. On the Snapshot Naming Information page, specify a naming convention for the Snapshots associated with this profile by selecting variables.

   The smid variable creates a unique snapshot identifier.

   Perform the following:

   a. In the Variable Token list, select usertext and click **Add**.
   b. Enter payroll.techco.com_ as the host name and click **OK**.
   c. Click **Left** until the host name appears just after smo in the Format box.
   d. Click **Next**.

   The Snapshot naming convention of smo_hostname_smoprofile_dbsid_scope_mode_smid becomes "smo_payroll.techco.com_payroll_prod2_payrolldb_f_a_x" (where "f" indicates a full backup, "a" indicates the automatic mode, and "x" represents the unique SMID).

9. Select **Protection Manager Protection Policy**.

   The **Protection Manager Protection Policy** enables you to select a protection policy that was configured by using NetApp Management Console.

10. Select **TechCo Payroll Data: Backup** as the protection policy from the protection policies retrieved from

NetApp Management Console, and click **Next**.

11. On the Perform Operation page, verify the information and click **Create**.

12. Click **Operation Details** to see information about the profile create operation and volume-based restore eligibility information.

    ◦ The assignment of a NetApp Management Console protection policy to the database profile automatically creates a nonconformant dataset, visible to the NetApp Management Console operator, with the name convention smo_<hostname>_<profilename>, or in this example: smo_payroll.tech.com_PAYDB.

    ◦ If the profile is not eligible for volume restore (also called "fast restore"), the following occurs:

        ▪ The **Results** tab indicates that the profile creation was successful and that warnings occurred during the operation.

        ▪ The **Operation Details** tab includes a WARNING log, which states the profile is not eligible for fast restore and explains why.

Using Protection Manager to provision the new dataset

After the smo_paydb dataset is created, the storage administrator uses Protection Manager to assign storage system resources to provision the dataset's Backup node.

Before provisioning the newly created dataset, the storage administrator confers with the DBA partner for the name of the dataset specified in the profile.

In this case, the dataset name is smo_payroll.tech.com_PAYDB.

1. Go to Protection Manager's NetApp Management Console.

2. From the menu bar, click **Data** > **Datasets** > **Overview**.

   The Datasets tab of the Datasets window displays a list of datasets that includes the dataset that was just created through SnapManager.

3. Locate and select the **smo_payroll.tech.com_PAYDB** dataset.

   When you select this dataset, the graph area displays the smo_paydb dataset with its backup node unprovisioned. Its conformance status is flagged as nonconformant.

4. With the smo_paydb dataset still highlighted, click **Edit**.

   The Protection Manager's NetApp Management Console displays the Edit Dataset window for the **smo_payroll.tech.com_PAYDB** dataset. The window's navigation pane displays configuration options for the dataset's primary node, backup connection, and backup node.

5. From the navigation pane, locate the options for the dataset's backup node and select **provisioning/resource pools**.

   The Edit Dataset window displays a setting for default provisioning policy and a list of available resource pools.

6. For this example, select the **paydb_backup_resource** resource pool and click **>**.

   The selected resource pool is listed in the "Resource Pools for this node" field.

7. Click **Finish** to save your changes.

The Protection Manager automatically provisions the secondary backup node with resources from the paydb_backup_resource resource pool.

Using SnapManager for Oracle to create a protected backup

When creating a backup for this example, the DBA selects to create a full backup, sets backup options, and selects protection to secondary storage. Although the backup is initially made on local storage, because this backup is based on a protection-enabled profile, the backup is then transferred to secondary storage according to the protection policy's schedule as defined in Protection Manager.

1. Go to the SnapManager for Oracle client.
2. From the SnapManager Repository tree, right-click the profile containing the database that you want to back up, and select **Backup**.

   The SnapManager for Oracle Backup Wizard starts.

3. Enter Production_payroll as the label.
4. Enter Production payroll Jan 19 backup as the comment.
5. Select **Auto** as the type of backup that you want to create.

   This allows SnapManager to determine whether to perform an online or offline backup.

6. Select **Daily** or **Weekly** as the frequency of the backup.
7. To confirm that the backup is in a valid format for Oracle, check the box next to **Verify backup**.

   This operation uses Oracle DBVerify to check the block format and structure.

8. To force the state of the database into the appropriate mode (for example, from open to mounted), select **Allow startup or shutdown of database, if necessary**, and click **Next**.
9. In the Database, Tablespaces, or Datafiles to Backup page, select **Full Backup** and click **Next**.
10. To protect the backup on secondary storage, check **Protect the Backup** and click **Next**.
11. In the Perform Operation page, verify the information you supplied and click **Backup**.
12. In the progress page, view the progress and results of the backup creation.
13. To view the details of the operation, click **Operation Details**.

Using SnapManager for Oracle to confirm backup protection

Using SnapManager for Oracle, you can view a list of backups associated with a profile, determine whether the backups were enabled for protection, and view the retention class (daily or weekly, in this example).

At first, the new backup in this example shows as scheduled for protection, but not yet protected (in the SnapManager graphical user interface and in the backup show command output). After the storage

administrator ensures that the backup has been copied to secondary storage, SnapManager changes the backup protection state from "Not protected" to "Protected" in both the graphical user interface and with the backup list command.

1. Go to the SnapManager for Oracle client.
2. In the SnapManager Repository tree, expand the profile to display its backups.
3. Click the **Backups/Clones** tab.
4. In the Reports pane, select **Backup Details**.
5. View the Protection column and ensure that the status is "Protected."