Hitachi Ops Center Protector

7.10

Oracle Application Guide

This document is intended for database administrators who wants to protect Oracle Databases using Hitachi Ops Center Protector. It is assumed that the reader has a good working knowledge Oracle Database, Hitachi Block and NAS Storage administration and network administration.

MK-99PRT003-12
March 2025

Contents

Preface

This guide describes how to backup and restore Oracle Databases using Hitachi Ops Center Protector.

Ops Center Protector orchestrates the creation, retention and restoration of application-consistent and crash consistent snapshots and clones for Oracle Databases. Application data can be protected by creating snapshots or clones on Hitachi Block or NAS Storage. Data protection policies are combined with data flow diagrams to automate local and remote snapshots and replications for end-to-end data protection and recovery solutions. These snapshots and clones then can be used to revert production databases to specific points in time and to create copies for repurposing scenarios.

Software version

This document revision applies to Ops Center Protector version 7.10. Please refer to the accompanying Release Notes for information on what's changed in this release.

Intended audience

This document is intended for database administrators who wants to protect Oracle Databases using Hitachi Ops Center Protector. It is assumed that the reader has a good working knowledge Oracle Database, Hitachi Block and NAS Storage administration and network administration.

If you are new to Ops Center Protector, we recommend that you start by refering to the *Hitachi Ops Center Protector User's Guide* so that you understand the basic concepts, workflows and user interface.

Related documents

Main product guides:

- *Hitachi Ops Center Protector Software Release Notes*.
- *Hitachi Ops Center Protector Quick Start Guide*.
- *Hitachi Ops Center Protector User's Guide*.
- *Hitachi Ops Center Protector Oracle Application Guide*.
- *Hitachi Ops Center Protector VMware Application Guide*.
- *Hitachi Ops Center Protector Hyper-V Application Guide*.
- *Hitachi Ops Center Protector Microsoft SQL Application Guide*

Programming guides:

- *Hitachi Ops Center Protector REST API User Guide*.
- *Hitachi Ops Center Protector REST API Reference Guide*.
- *Hitachi Ops Center Protector REST API Change Log*.

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. ▪ Indicates emphasized words in list items.
Italic	▪ Indicates a document title or emphasized words in text. ▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`

Convention	Description
< > angle brackets	Indicates variables in the following scenarios: ▪ Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` ▪ Variables in headings.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
	Note	Calls attention to additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Important	Highlights information that is essential to the completion of a task.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	CAUTION	Warns the user of a hazardous situation that, if not avoided, could result in major or minor injury.
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1{,}000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1{,}000^3$ bytes
1 terabyte (TB)	1,000 GB or $1{,}000^4$ bytes
1 petabyte (PB)	1,000 TB or $1{,}000^5$ bytes
1 exabyte (EB)	1,000 PB or $1{,}000^6$ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1{,}024^2$ bytes
1 GB	1,024 MB or $1{,}024^3$ bytes
1 TB	1,024 GB or $1{,}024^4$ bytes
1 PB	1,024 TB or $1{,}024^5$ bytes
1 EB	1,024 PB or $1{,}024^6$ bytes

Accessing product documentation

Product user documentation is available on: https://docs.hitachivantara.com. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

The Hitachi Vantara Support Website is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send comments to doc.feedback@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Chapter 1: Before you begin

Supported configurations

Protector supports the following Oracle database configurations:

- Single instance with file systems.
- Single instance with Automatic Storage Management (ASM) (ASMlib or udev or afd on Linux, raw devices for AIX).
- Oracle RAC with ASM (ASMlib or udev or afd on Linux, raw devices for AIX).
- Linux device mapper multipathing. AIX native multipathing.
- Hitachi Dynamic Link Manager (HDLM).
- GPT/MBR partitioned disks with one primary partition for Linux, native disks partitions for AIX with one used partition.
- Container Databases (CDB) and plug-able databases (PDB).
- Flex ASM.
- Flex Cluster.
- DataGuard Primary and Standby.

If the Oracle data source is ASM, the following ASM protection modes are supported:

- External protection.

Prerequisites

It is important that the following prerequisites are met before you implement any of the Oracle Database protection policies described in this guide.

To ensure that your hardware and software environment is fully supported, please refer to https://compatibility.hitachivantara.com/assets/ops-protector.

For detailed information on installing the Ops Center Protector Master, and Client components, refer to the *Hitachi Ops Center Protector User's Guide*.

Application software prerequisites

Before Protector can interact with an Oracle Database to protect its data, ensure that your setup meets the following prerequisites:

- Oracle binaries must use separate disks from the database files and log files.
  - They can use any storage including local storage.
- Database files, redo logs and archive logs must use a single supported block storage array per database. If a filesystem is built on top of a volume group, each filesystem must be allocated to a separate volume group to maintain proper segregation.
- Database files and redo logs must be in separate ASM disk groups or filesystems. If a filesystem is built on top of a volume group, each filesystem must be allocated to a separate volume group to maintain proper segregation.
- Database files and archive logs must be in separate ASM disk groups or filesystems
- Redo logs and archive logs can be on the same ASM disk group or filesystem
- ASM disks must be partitioned. The ASM Data must be on the only partition of this disk. This is in accordance to the requirements of Oracle
- When using different filesystems to separate database files, redo/archive logs and binaries they need to use separate disks (LDEVs)

Multiple databases must not share ASM disk groups or filesystems

Block-based backups will only protect a **single database per backup**. If multiple databases share an ASM disk group or filesystem only the selected database is consistent on the backup and considered during restore and revert. Reverting a configuration with multiple databases on the same disks will lead to corruption of the databases which are not explicitly protected, as their data is reverted together with the selected database.

Special Files

- Oracle SP files should be located within the archive log ASM disk group or filesystem.
- ASM SP file must not be located in the data file location, as this will prevent reverts.
- Control files should be placed in the archive log ASM disk group or filesystem.

Database credentials

Protector will automatically determine which user to use in order to backup or restore the database. You can however specify custom users for Oracle and ASM related operations.

	Default user	Requirements for custom user
Oracle	OS user/owner of database `$ORACLE_HOME/bin/oracle`	user must be a member of a group with *sysdba* privileges
ASM	OS user/owner of GRID `$ORACLE_HOME/bin/oracle`	user must be a member of a group with *sysasm* privileges

Oracle RMAN SBT Integration

Oracle Recovery Manager (RMAN) is a backup and recovery tool which is supplied by Oracle with all current Oracle database versions. It provides capabilities to backup, restore and recover Oracle databases. As it is part of the database, many Oracle database administrators are very familiar with the tool and how to use it.

Hitachi Ops Center Protector integrates with Oracle RMAN using the SBT interface, which allows the database administrator to store data in datastores manged by Protector. The integration leverages Protectors **Unified Backup Infrastructure** (see *Hitachi Ops Center User's Guide*) to enable the RMAN backup to both on-site and cloud targets in a flexible and efficient way.

Ops Center Protector’s RMAN SBT integration allows backups and restores of any data supported by Oracle RMAN for SBT targets. This includes, but is not limited to:

- Oracle databases (full / incremental)
- Transaction logs
- Special files (e.g. control files)

About Oracle RMAN SBT integration

Hitachi Ops Center Protector integrates with Oracle RMAN using the SBT interface, which allows the database administrator to store data in datastores manged by Protector. The integration leverages Protector's **Unified Backup Infrastructure** (see *Hitachi Ops Center User's Guide*) to enable the RMAN backup to both on-site and cloud targets in a flexible and efficient way.

The Oracle RMAN SBT integration supports the full RMAN SBT feature set, including the backup of databases, archive logs and control files. The only exception to this are proxy backups which are not supported.

To configure the integration in Protector the following steps are required:

- Create a policy using the Oracle RMAN classsification and Access operation
  - Specify which databases are allowed, and which level of access is required
- Create a dataflow connecting all nodes which should have access to the data
  - Any storage supported by Protectors **Unified Backup Infrastructure** (see *Hitachi Ops Center User's Guide*) can be used as storage target
  - Any Oracle application node which should be able to access the data has to be on the dataflow
  - Oracle application nodes can be added or removed later, by modifying and re-activating the dataflow
- See Oracle RMAN SBT Integration (on page 12) for examples and more detailed instructions

To configure the RMAN the following steps are required:

- Dataflow must be created and activated in Protector
- Get the channel configuration using the **schedulershow command (on page 68)**
- Use the channel configuration in RMAN
- Use RMAN to backup or restore data using the channel

Note: All Oracle systems which need access to the SBT data, need to present on the dataflow and connected to the target node via an access operation. New nodes can be added at a later point in time by modifying the dataflow.

Hitachi Block prerequisites

The following prerequisites are mandatory if you plan to perform snapshotting and/or replication of Hitachi Block volumes. Please also refer to the Protector support matrices at https://compatibility.hitachivantara.com/assets/ops-protector .

- A machine (known as an ISM) must be assigned that controls the Block storage device. This node must be a supported Windows or Linux machine with the Protector Client software installed.

  

  Caution: ISM nodes and their associated CMDs used to control storage devices must not be shared with applications other than those forming part of the Ops Center suite.
- All primary data (paths or application data) to be snapshotted or replicated within the same data protection policy must exist on the same storage device.
- The block storage hardware must:
  - Support the data protection technologies you intend to use
  - Have the correct firmware version installed
  - Have the correct SVOS version installed
- For all replication types the P-VOLs must be setup in the host group

- In order to resize logical devices represented by the Block Host node that are part of a replication or snapshot pair the array account must have the Support Personal permission.
- For UR, journals must be set up, although for HM800 and later arrays Protector can create journals
- For GAD, the quorum disks or quorum-less disks must be provided. In most cases, one quorum device between participating storage systems is satisfactory. Please refer to the *Global-Active Device User Guide* for best practices
- For GAD, the array should be configured to allow virtualized LDEVs if they are required (where supported by the array)
- Port security must be enabled.
- Primary volumes must be set up using other Hitachi tools prior to selection in Protector
- For application consistent snapshots, the application must be installed and configured to use P-VOLs on a storage array, see the relevant application guide for details on the application configuration
- The password for authorizing a Block Device node must contain only useable CCI command characters: `A-Za-z0-9'-./:@\_`
- The device must have adequate shared memory (see Provisioning and Technical Guides)
- Pools must be created using Storage Navigator prior to selecting the Target Storage in Ops Center Protector:
  - For standard mode (non-cascading) TI the TI Pools must be set up
  - For cascade mode TI the Dynamic Provisioning Pools must be set up to also be a hybrid pool, otherwise a TI pool will also be required
  - For SI, TC, UR and GAD the Dynamic Provisioning Pools must be set up
- The following licensed features may be required depending on the features being used:
  - Dynamic Provisioning
  - Storage Navigator
  - Thin Image (for TI snapshot and RTI replication scenarios)
  - ShadowImage (for SI replication scenarios)
  - TrueCopy (for TC replication scenarios)
  - Universal Replicator (for UR replication scenarios)
  - Global-Active Device (for GAD replication scenarios)
  - Remote Replication Extended (for 3DC scenarios)
- The Protector ISM node controlling the block storage device must have:
  - The correct version of Hitachi CCI installed.
  - If CCI is not installed in the default location there are two options:
    1. Add a symbolic link from the default location to the install directory
    2. Configure Protector to use CCI in the custom location using the following instructions:

a. Stop the Protector services on the ISM node
b. Go to the directory <Protector home>\db\config
c. Make the change to all files matching hitachivirtualstorageplatform*.cfg
d. Change the <BinDirectory> value from C:/HORCM/etc to the correct installation path

```
<!-- Install directory of CCI, override to change
installation directory. -->

<BinDirectory>C:/HORCM/etc</BinDirectory>
```

e. Ensure the change has been made to all files at per 3 including the default one.
f. Start the Protector services on the ISM node

- Access to a dedicated Command Device (CMD) on the storage device, set up as follows:

  WARNING: When running the Analyzer probe server, API Configuration Manager, and Protector ISM Client on the same VM, all components share the same command device, but API Configuration Manager and Protector ISM Client must access the storage systems using different credentials. This means that API Configuration Manager and Protector ISM client must use different login accounts when accessing the storage system.

  - Security disabled
  - User authentication enabled
  - Device group definition disabled
  - The CMD must be visible to the host OS where the Protector proxy resides
  - The CMD must be offline
  - The CMD must be added to the meta_resource only.
  - Multiple active command devices may be visible to a Protector proxy as long as each one represents a different block storage device. Behaviour is undefined if multiple active command devices represent the same block storage device, unless these are configured in the Protector proxy node fail-over priority list.
  - Fibre channel and IP command devices are supported.
  - Multipath for Command Devices is supported

- A dedicated user (specified when creating the Hitachi Block Device node) for Protector must be created on the storage device with at least the following roles:
  - Storage Administrator (Provisioning)
  - Storage Administrator (Local Copy)
  - Storage Administrator (Remote Copy)
  - Security Administrator (View & Modify).

  The user must also have access to Resource Group 0 on the storage device.

- Fibre connectivity (including zoning) or iSCSI connectivity and pre-configured RCU paths between arrays for remote replication technologies
- If physical and software block devices are being configured in a single Protector environment it is essential that they do not share an ISM node.

Protecting archive logs and transaction logs for recovery

In addition to creating block based backups of Oracle databases and restoring them, Ops Center Protector can also assist with recovering a database and rolling it forward to a point in time newer than that captured by the snapshot.

Note: Restoring the Oracle database to the point in time captured in the snapshot, does not require any additional log or controlfile backups. This is only required, when the database should be recovered using additional information from the RMAN catalog.

Please ensure the following actions are complete to enable recovery and roll forward of block-based Oracle backups.

Use RMAN and the RMAN catalog, ideally with Protector‘s Oracle RMAN integration, to perform regular and frequent archive log backups

A recovery on a mount system is only possible with a backup of an archive log and corresponding controlfile. The contents and time of the archive log backups determine the latest transaction that can be recovered.

Ensure that controlfile and spfiles are protected with the archive logs

RMAN allows the current version of the controlfile (and spfile) to be backed up with archive logs. This is necessary to have all the information about backup sets, paths and logs available during recovery. To enable the automatic backup of these files, use 'configure controlfile autobackup on;' within RMAN. This is a one-time configuration for each specific database being protected.

Set 'control_file_record_keep_time' to the retention time of the snapshots

The recovery process starts with a restore of an appropriate controlfile to reduce the impact on the RMAN catalog. The controlfile holds the same information as the RMAN catalog. However, the controlfile has a limited size and holds the information for a limited time, only. The duration is defined via the parameter 'control_file_record_keep_time'. The default of this parameter is 7 days. It should be set to at least the number of days as the retention time of the backup. For example, if the backup has a retention period of 14 days, the following sqlplus command is used 'alter system set control_file_record_keep_time=14 scope=both;'

Chapter 2: Oracle Backup workflows

The following topics describe the steps required to configure policies and data flows to implement a number of different data protection scenarios.

For a detailed introduction on how to work with the Protector user interface, please refer to *Hitachi Ops Center Protector User's Guide*.

Block based workflows

This section addresses the workflows for block based backups.

How to create restore points with local snapshots

Before you begin

It is assumed that the following tasks have been performed:

- The Oracle Database application has been installed and any Protector prerequisites are met.
- The Protector Master software has been installed and licensed on a dedicated node.
- The Protector Client software has been installed on the source node where the Oracle Database application resides.
- The Protector Client software has been installed on the destination node that will act as a proxy for the Hitachi Block storage device. Note that for a Thin Image snapshot, the source and destination LDEVs are located on the same device.
- The storage device has been set up as per the Protector requirements and prerequisites.
- Permissions have been granted to enable the Protector UI, required activities and participating nodes to be accessed. In this example all nodes will be left in the default resource group, so there is no need to allocate nodes to user defined resource groups.

Ops Center Protector enables you to create a point-in-time snapshot of the Oracle database by storing the changes instead of copying the whole database. The snapshot is created using Thin Image technology. By creating a Thin Image snapshot, you can not only manage the storage space efficiently but also rapidly recover the database to a previous point in time.

Because Thin Image is differential, the primary volumes are required to reconstruct the entire data set, therefore if the primary data is lost then the snapshots are of no use. For this reason, Thin Image snapshots should not be relied upon for recovery from catastrophic primary data loss.

Note: Oracle backups are performed in two phases resulting in two snapshots. If the second phase fails the first phase snapshot may not be removed from the array.

The data flow and policy are as follows:

Figure 1 Hardware Snapshot Data Flow

Table 1 Oracle Snapshot Policy

Classification Type	Parameters	Value
Oracle Database	Database Selection	TestDb (The selected databases must be located on the same Block device)
	Backup Mode	Online

Operation Type	Parameters	Value	Assigned Nodes
Snapshot	Mode	Hardware	Oracle Database
	Hardware Type	Hitachi Block	
	RPO	8 Hours	
	Retention	1 Week	
	Run Options	Run on RPO	
	Source Options	Quiesce...	

Procedure

1. Locate the source *OS Host* node in the **Nodes Inventory** and check that it is authorized and online.

   This node represents the Protector Client installed on the Oracle server.
2. Create a new *Oracle Database* node using the Oracle Application Node Wizard (on page 38) and check that the node it is authorized and online.

The *Oracle Database* node type is grouped under **Application** in the **Node Type Wizard**. This node will be used in the dataflow to represent the Oracle Database setup to be protected.

a. Select the *OS Host* node identified above as the **Node running Oracle...**.

b. Specify the credentials for both the **Operating System** and **Database** users.

3. Locate the node in the **Node Inventory** that will control the Hitachi Block Device via a CMD (Command Device) interface and check that it is authorized and online.

   This node is used by Protector to orchestrate snapshot creation and is identified as the **Proxy Node** when creating the Hitachi Block Device node in the next step. This node is known as an ISM (Intelligent Storage Manager) node. The ISM node does not appear in the data flow.

4. Create a new Hitachi *Block Device* node (unless one already exists) using the **Block Storage Node Wizard** and check that it is authorized and online.

   The Hitachi *Block Device* node type is grouped under **Storage** in the **Node Type Wizard**. Note that this node does not appear in the snapshot data flow diagram, but is identified when assigning the snapshot policy.

5. Define a policy as shown in the table above using the **Policy Wizard**, Oracle Database Classification Wizard (on page 45) and **Snapshot Operation Wizard**.

   The *Oracle Database* classification is grouped under **Application** in the **Policy Wizard**.

6. Draw a data flow as shown in the figure above, that shows only the *Oracle Database* source node.

   At this stage the snapshot icon is not shown.

7. Assign the *Snapshot* operation to the *Oracle Database* source node. The *Oracle-Snapshot* policy will then be assigned automatically.
   The **Block Snapshot Operation Properties Dialog** is displayed.

8. Select the **Pool** by selecting the Hitachi *Block Device* node created in the steps above, followed by one of the available Thin Image *Pools*.

9. Leave the remaining parameters at their default settings, then click **OK**.

   The snapshot icon is now shown superimposed over the source node.

10. Compile and activate the data flow, checking carefully that there are no errors or warnings.

11. Locate the active data flow in the **Monitor Inventory** and open its **Monitor Details** page.

    The policy will be invoked repeatedly according to the RPO specified. The policy can also be manually triggered from the source node in the monitor data flow. You may want to manually trigger to create an initial snapshot.

12. Monitor the active data flow to ensure the policy is operating as expected.
    For a healthy data flow you will periodically see:

    - Snapshot jobs appearing in the **Jobs** area below the data flow that cycle through stages and ending in *Progress - Completed*.
    - Information messages appearing in the **Logs** area below the data flow indicating rules activation, storage handler and sequencer events.
    - Attachments to storage handler log events confirming which volumes are being snapshotted.

13. Review the status of the Hitachi *Block Device* to ensure snapshots are being created. New snapshots will appear periodically as dictated by the *RPO* of the policy. Old snapshots will be removed periodically as dictated by the *Retention Period* of the policy.

How to create restore points and full backups with snapshots of a local clone

Before you begin

It is assumed that the following tasks have been performed:

- The Oracle Database application has been installed and any Protector prerequisites are met.
- The Protector Master software has been installed and licensed on a dedicated node.
- The Protector Client software has been installed on the source node where the Oracle Database application resides.
- The Protector Client software has been installed on the node that will act as a proxy for the Hitachi Block storage device. Note that for a ShadowImage replication, the source and destination LDEVs are located on the same device.
- The storage device has been set up as per the Protector requirements and prerequisites.
- Permissions have been granted to enable the Protector UI, required activities and participating nodes to be accessed. In this example all nodes will be left in the default resource group, so there is no need to allocate nodes to user defined resource groups.

Snapshot of a local clone enables both rapid recovery to a point in time by using Thin Image snapshots, while providing an additional level of protection by creating a full clone of the database by using ShadowImage technology. Taking snapshots of the clone adds the additional benefit of being able to roll back the backup copy to a given restore point.

Because ShadowImage is an in-system replication technology, it does not provide protection against a disaster at the local site, since both the primary and secondary volumes are co-located.

The data flow and policy are as follows:

Figure 2 ShadowImage Replication with Local Thin Image Snapshots Data Flow

Table 2 Oracle Replication/Snapshot Policy

Classification Type	Parameters	Value
Oracle Database	Database Selection	TestDb (All the selected databases must be located on the same Block device)
	Backup Mode	Online

Operation Type	Parameter	Value	Assigned Nodes
Replicate	Run Options	Run on Schedule (see synch group schedule below)	Hitachi Block Device
	Souce Options	Quiesce...	
Snapshot	Mode	Hardware	Oracle Database
	Hardware Type	Hitachi Block	
	RPO	8 Hours	
	Retention	1 Week	
	Run Options	Run on Schedule (see synch group schedule below)	
	Source Options	Quiesce...	

Table 3 Synchronization Group Schedule

Trigger	N/A (this schedule defines a synchronization group name for local replications and snapshots. All parameters are ignored.)	Snapshot, Replication

Procedure

1. Locate the source *OS Host* node in the **Nodes Inventory** and check that it is authorized and online.

   This node represents the Protector Client installed on the Oracle server.
2. Create a new *Oracle Database* node using the Oracle Application Node Wizard (on page 38) and check that the node it is authorized and online.

   The *Oracle Database* node type is grouped under **Application** in the **Node Type Wizard**. This node will be used in the dataflow to represent the Oracle Database configuration to be protected.

   a. Select the *OS Host* node identified above as the **Node running Oracle...**.

   b. Optional - Specify the credentials for both the **Operating System** and **Database** users.
3. Locate the node in the **Nodes Inventory** that will control the Hitachi Block Devices via a CMD (Command Device) interface and check that it is authorized and online.

   This node is used by Protector to orchestrate replication of the LDEV and is identified as the **Proxy Node** when creating the Hitachi Block Device node in the next step. This node is known as an ISM (Intelligent Storage Manager) node. The ISM node does not appear in the data flow.
4. Create a new Hitachi *Block Device* node (unless one already exists) using the **Block Storage Node Wizard** and check that it is authorized and online.

   The Hitachi *Block Device* node type is grouped under **Storage** in the **Node Type Wizard**. The Hitachi Block Device node appears in the replication data flow as the destination node.
5. Define a policy as shown in the table above using the **Policy Wizard**. This policy contains operations for the local replication and snapshot.

   a. Define an *Oracle Database* classification using the Oracle Database Classification Wizard (on page 45).

      The *Oracle Database* classification is grouped under **Application** in the **Policy Wizard**.

   b. Define a *Replicate* operation using the **Replicate Operation Wizard**.

      ShadowImage replication runs as a batch operation triggered by the RPO of the snapshot.

   c. Define a local *Snapshot* operation using the **Snapshot Operation Wizard**.

      Thin Image snapshots run based on the RPO. However we also want to synchronize the snapshot with the replication. This is done by defining a trigger schedule that is applied to both the snapshot and replication operations.

   d. Define a *Trigger* schedule using the **Schedule Wizard**; accessed by clicking on **Manage Schedules** in the **Snapshot Operation Wizard** for the local snapshot.

      Only the trigger schedule name is required; the parameters are not relevant here since the RPO of the snapshot dictates when the replication operation is triggered.
6. Draw a data flow as shown in the figure above, that shows the *Oracle Database* source node connected to the Hitachi *Block Device* via a *Batch* mover.
7. Assign the to the *Oracle Database* source node.

8. Assign *Oracle-Replicate-Snaphot* policy's *Snapshot* operation to the *Oracle Database* source node.
   The **Block Snapshot Operation Properties Dialog** is displayed.
9. Select the **Pool** by selecting the local Hitachi *Block Device* node created in the steps above, followed by one of the available Thin Image *Pools*.
10. Leave the remaining snapshot parameters at their default settings, then click **OK**.
    The snapshot icon is now shown superimposed over the source node.
11. Assign the *Replicate* operation to the Hitachi *Block Device* node.
    The **Block Replication Operation Properties Dialog** is displayed.
12. Set the replication type to **In System Clone**, then choose a **Pool** from one of the available *Dynamic Pools*. Leave the remaining parameters at their default settings and click **OK**.
13. Compile and activate the data flow, checking carefully that there are no errors or warnings.
14. Locate the active data flow in the **Monitor Inventory** and open its **Monitor Details** page.

    The policy will be invoked automatically to create and then maintain the replication according to the policy. Snapshot and replication operations will be triggered synchronously on the source node according to the RPO.
15. Monitor the active data flow to ensure the policy is operating as expected.
    For a healthy data flow you will periodically see:
    - Replication and snapshot jobs appearing for the source node in the **Jobs** area triggered according to the RPO.
    - Information messages appearing in the **Logs** area below the data flow indicating rules activation, storage handler and sequencer events.
    - Attachments to storage handler log events confirming which volumes are being replicated.
16. Review the status of the Hitachi *Block Device* to ensure snapshots and replications are being created.
    New snapshots and a refreshed replication will appear periodically as dictated by the *RPO* of the policy. Old snapshots will be removed periodically as dictated by the *Retention Period* of the policy.

How to create restore points and DR backups with snapshots of a remote synchronous clone

Before you begin

It is assumed that the following tasks have been performed:

- The Oracle Database application has been installed and any Protector prerequisites are met.
- The Protector Master software has been installed and licensed on a dedicated node.
- The Protector Client software has been installed on the source node where the Oracle Database application resides.
- The Protector Client software has been installed on the nodes that will act as a proxy for both the primary and secondary Hitachi Block storage devices. Note that for a TrueCopy replication, the source and destination LDEVs are located on different devices.
- The storage devices have been set up as per the Protector requirements and prerequisites.
- Permissions have been granted to enable the Protector UI, required activities and participating nodes to be accessed. In this example all nodes will be left in the default resource group, so there is no need to allocate nodes to user defined resource groups.

Snapshot of a remote clone enables both rapid recovery to a point in time by using Thin Image snapshots, while providing an additional level of protection by creating a full remote clone of the database using Hitachi TrueCopy technology. In synchronous replication, the storage system signals each write completion only once it is performed on the primary and secondary volume (copy on write).

This setup provides partial protection against a disaster at the local site and full protection at the remote site as the primary and secondary volumes are geographically separated. If necessary, production can be moved quickly to the remote site while the local site is being recovered. Taking snapshots of the remote clone adds the additional benefit of being able to roll back the backup copy to a given restore point from the remote site.

The data flow and policy are as follows:

Figure 3 TrueCopy Replication with Local and Remote Thin Image Snapshots Data Flow

Table 4 Oracle Replication/Snapshot Policy

Classification Type	Parameters	Value
Oracle Database	Database Selection	TestDb (All the selected databases must be located on the same Block device)
	Backup Mode	Online

Operation Type	Parameter	Value	Assigned Nodes
Replicate	Run Options	N/A (TrueCopy is a continuous replication, so the Run option is ignored)	Secondary Hitachi Block Device
	Souce Options	Quiesce...	
Snapshot (on local device)	Mode	Hardware	Oracle Database
	Hardware Type	Hitachi Block	
	RPO	8 Hours	
	Retention	1 Week	
	Run Options	Run on Schedule (see synch group schedule below)	
	Source Options	Quiesce...	
Snapshot (on remote device)	Mode	Hardware	Secondary Hitachi Block Device
	Hardware Type	Hitachi Block	
	RPO	8 hours (this must match the local snapshot)	
	Retention	1 Week (this can differ from the local snapshot)	

Operation Type	Parameter	Value	Assigned Nodes
	Run Options	Run on Schedule (see synch group schedule below)	

Table 5 Synchronization Group Schedule

Trigger	N/A (this schedule defines a synchronization group name for local and remote snapshots. All parameters are ignored.)	N/A	Snapshot (local), Snapshot (remote)

Procedure

1. Locate the source *OS Host* node in the **Nodes Inventory** and check that it is authorized and online.

   This node represents the Protector Client installed on the Oracle server.
2. Create a new *Oracle Database* node using the Oracle Application Node Wizard (on page 38) and check that the node it is authorized and online.

   The *Oracle Database* node type is grouped under **Application** in the **Node Type Wizard**. This node will be used in the dataflow to represent the Oracle Database configuration to be protected.

   a. Select the *OS Host* node identified above as the **Node running Oracle...**.
   b. Optional - Specify the credentials for both the **Operating System** and **Database** users.
3. Locate the nodes in the **Nodes Inventory** that will control the primary and secondary Hitachi Block Devices via CMD (Command Device) interfaces and check that they are authorized and online.

   These nodes are used by Protector to orchestrate replication of the primary LDEV to the secondary and are identified as the **Proxy Node** when creating the primary and secondary Hitachi Block Device nodes in the next step. These nodes are known as ISM (Intelligent Storage Manager) nodes. The ISM nodes do not appear in the data flow.

4. Create new primary and secondary Hitachi *Block Device* nodes (unless ones already exists) using the **Block Storage Node Wizard** and check that they are authorized and online.

   The Hitachi *Block Device* node type is grouped under **Storage** in the **Node Type Wizard**. The secondary Hitachi Block Device node appears in the replication data flow as the destination node. The primary Hitachi Block Device node is represented in the data flow by the *Oracle Database* node where the primary LDEV is mounted.
5. Define a policy as shown in the table above using the **Policy Wizard**. This policy contains operations for the replication, local and remote snapshots.
   a. Define an *Oracle Database* classification using the Oracle Database Classification Wizard (on page 45).

      The *Oracle Database* classification is grouped under **Application** in the **Policy Wizard**.
   b. Define a *Replicate* operation using the **Replicate Operation Wizard**.

      TrueCopy replication runs as a continuous operation and thus no schedule needs to be defined.
   c. Define a local *Snapshot* operation using the **Snapshot Operation Wizard**.

      Thin Image snapshots run based on the RPO. However we also want to synchronize the local and remote snapshots. This is done by defining a trigger schedule that is applied to both the local and remote snapshot operations.
   d. Define a *Trigger* schedule using the **Schedule Wizard**; accessed by clicking on **Manage Schedules** in the **Snapshot Operation Wizard** for the local snapshot.

      Only the trigger schedule name is required; the parameters are not relevant here since the RPO of the local snapshot dictates when the local and remote snapshot operations are triggered.
   e. Define a remote *Snapshot* operation using the **Snapshot Operation Wizard**.

      To synchronize the local and remote snapshots, apply the same trigger schedule to this snapshot operation that was applied to the local snapshot operation.

      Note: The local and remote snapshots must have the same RPO, otherwise a rules compiler error will be generated.
6. Draw a data flow as shown in the figure above, that shows the *Oracle Database* source node connected to the secondary Hitachi *Block Device* via a *Continuous* mover.

   TrueCopy is a remote replication technology, so the Hitachi *Block Device* node shown on the data flow is the where the destination (SVOL) volume is located.
7. Assign the *Oracle-Replicate-Snaphot-Snapshot* policy to the *Oracle Database* source node.
8. Assign the local *Snapshot* operation to the *Oracle Database* source node.
   The **Block Snapshot Operation Properties Dialog** is displayed.
9. Select the **Pool** by selecting the local Hitachi *Block Device* node created in the steps above, followed by one of the available Thin Image *Pools*.
10. Leave the remaining snapshot parameters at their default settings, then click **OK**.

    The snapshot icon is now shown superimposed over the source node.
11. Assign the remote *Snapshot* operation to the remote Hitachi *Block Device* node.
    The **Block Snapshot Operation Properties Dialog** is displayed.

12. Select the **Pool** by selecting the remote Hitachi *Block Device* node created in the steps above, followed by one of the available Thin Image *Pools*.
13. Leave the remaining snapshot parameters at their default settings, then click **OK**.
    The snapshot icon is now shown superimposed over the destination node.
14. Assign the *Replicate* operation to the remote Hitachi *Block Device* node.
    The **Block Replication Operation Properties Dialog** is displayed.
15. Set the replication type to **Synchronous Remote Clone**, then choose a **Pool** from one of the available *Dynamic Pools*. Leave the remaining parameters at their default settings and click **OK**.
16. Compile and activate the data flow, checking carefully that there are no errors or warnings.
17. Locate the active data flow in the **Monitor Inventory** and open its **Monitor Details** page.

    The policy will be invoked automatically to create and then maintain the replication according to the policy. Snapshot operations will be triggered synchronously on the source and destination nodes according to the RPO.
18. Monitor the active data flow to ensure the policy is operating as expected.
    For a healthy data flow you will periodically see:
    - Replication and snapshot jobs appearing for the source node in the **Jobs** area triggered according to the RPO.
    - Snapshot jobs appearing for the destination node in the **Jobs** area synchronized to the local snapshot.
    - Information messages appearing in the **Logs** area below the data flow indicating rules activation, storage handler and sequencer events.
    - Attachments to storage handler log events confirming which volumes are being replicated.
19. Review the status of the local Hitachi *Block Device* to ensure snapshots are being created. Review the status of the remote Hitachi *Block Device* to ensure the replication is being performed and that snapshots are being created.
    New local and remote snapshots will appear periodically as dictated by the *RPO* of the policy. Old snapshots will be removed periodically as dictated by the *Retention Period* of the policy.

How to create restore points and DR backups with snapshots of a remote asynchronous clone

Before you begin

It is assumed that the following tasks have been performed:

- The Oracle Database application has been installed and any Protector prerequisites are met.
- The Protector Master software has been installed and licensed on a dedicated node.
- The Protector Client software has been installed on the source node where the Oracle Database application resides.
- The Protector Client software has been installed on the nodes that will act as a proxy for both the primary and secondary Hitachi Block storage devices. Note that for a TrueCopy replication, the source and destination LDEVs are located on different devices.
- The storage devices have been set up as per the Protector requirements and prerequisites.
- Permissions have been granted to enable the Protector UI, required activities and participating nodes to be accessed. In this example all nodes will be left in the default resource group, so there is no need to allocate nodes to user defined resource groups.

Snapshot of a remote clone enables both rapid recovery to a point in time by using Thin Image snapshots, while adding an additional level of protection by creating a full remote clone of the database using Universal Replicator (UR) technology. UR uses Journaling to perform volume consistent, asynchronous replication. In asynchronous replication, the storage system signals each write completion as soon as it is performed on the primary volume, it then transfers it to the secondary volume (copy after write).

UR journaling ensures the write order is completely guaranteed and the secondary volume is crash-recoverable at any point in time. However, if there is a long duration of link interruption between the primary and secondary sites, there might be a service level violation with increased RPO.

The data flow is as follows:

Figure 4 Universal Replicator with Local and Remote Thin Image Snapshots Data Flow

Procedure

1. Follow the procedure for How to create restore points and DR backups with snapshots of a remote synchronous clone (on page 24) using the same *Oracle-Replicate-Snaphot-*

Snapshot policy. However, when asigning the *Replicate* operation to the remote Hitachi *Block Device* node:

a. Set the replication type to **Asynchronous Remote Clone**.
b. Choose a **Pool** from one of the available *Dynamic Pools*.
c. Select the required **Source Journal** and **Destination Journal**.
d. Leave the remaining parameters at their default settings and click **OK**.
e. Then continue with the procedure.

RMAN based workflows

This section addresses the workflows for RMAN based backups.

How to allow read-only access to Oracle RMAN backups

Before you begin

It is assumed that the following tasks have been performed

- The Protector Master software has been installed and licenses on a dedicated node.
- The Protector Client software has been installed on all servers of the Oracle setup and the clients have been authorized on the Master.

This workflow describes the steps to follow when setting up Protectors RMAN SBT integration from scratch, so a database administrator can use Oracle RMAN to backup a database to an Ops Center Protector managed UBI datastore and allowing other nodes to only restore the data. A typical use case is a production system which has full access to create and restore backups, while a test system can only read and may not change the data.

As the goal is to achieve different levels of access for different Oracle Database nodes, you need to create separate policies. One for each level of access.

Note: In case multiple nodes or node groups require the same level of access to the same databases, the same policy can be used.

This example workflow uses a Gen2 Repository, however the workflow is identical for other datastore nodes like Amazon S3 or Hitachi Content Platform (HCP).

Figure 5 Oracle RMAN backup

Table 6 Oracle RMAN full access policy

Classification Type	Parameter	Value
Oracle RMAN	Allow Databases	Refer to Oracle RMAN Database Selection Wizard (on page 49) for details on how to allow databases access
	Deny Databases	Refer to Oracle RMAN Database Selection Wizard (on page 49) for details on how to deny databases access

Operation Type	Parameter	Value	Assigned Nodes
Access	Access Level	Read / Write	Repository, Amazon S3, Hitachi Content Platform(HCP)

Table 7 Oracle RMAN read only policy

Classification Type	Parameter	Value
Oracle RMAN	Allow Databases	Refer to Oracle RMAN Database Selection Wizard (on page 49) for details on how to allow databases access
	Deny Databases	Refer to Oracle RMAN Database Selection Wizard (on page 49) for details on how to deny databases access

Operation Type	Parameter	Value	Assigned Nodes
Access	Access Level	Read / Write	Repository, Amazon S3, Hitachi Content Platform(HCP)

Procedure

1. Locate the source and target *OS Host* nodes in the **Nodes Inventory** and check that they are authorized and online. These nodes represent the Protector Clients installed on the Oracle server.
2. Create a new *Oracle Database* node using the Oracle Application Node Wizard (on page 38) and check that the node it is authorized and online. The Oracle Database node type is grouped under Application in the Node Type Wizard. This node will be used in the dataflow to represent the Oracle Database setup to be protected.
3. Repate the step above and ensure there is an application **Oracle Database Application Node** representing the **Oracle setup** which we will only allow restores to.
4. Create a new *destination node*, for example a Repository, using the **Repository Storage Node Wizard** (see *Hitachi Ops Center User's Guide*) and check that it is authorized and online.

   The destination nodes, like the Repository node are grouped under Storage in the **Node Type Wizard** (see *Hitachi Ops Center User's Guide*). You can direct data from multiple nodes to a single repository so there is no need to create a new repository if a suitable one already exists.

   If a new Repository node is being created please the default Generation 2 type.

5. If a new Repository node is being created please the default Generation 2 type. Define the two policies as shown in the table above using the **Policy Wizard** (see *Hitachi Ops Center User's Guide*), Oracle RMAN Classification Wizard (on page 47) and the **Access Operation Wizard** (see *Hitachi Ops Center User's Guide*).
6. Draw a *data flow* as shown in the figure above, that shows the *Oracle Database* source node and the Oracle Database restore only node connected to the Repository destination node via a Batch mover, using the Data Flow Wizard.
7. Assign the *Oracle-RMAN-full-access policy* to the *Oracle Database source node* and to the repository node on the data flow.
8. Assign the *Oracle-RMAN-readonly policy* to the *Oracle Database source node* and to the repository node on the data flow.
9. Compile and activate the data flow, checking carefully that there are no errors.
10. Connect to the source Oracle Server command line (e.g. via SSH) and use the *schedulershow* (on page 68) command line utility to retrieve the *RMAN channel definition* for use on this server
11. In RMAN, on the source Oracle server, create a channel using the definition provided by **schedulershow (on page 68)** and use it to backup Oracle data. Please refer to the documentation provided by Oracle on how to backup and restore using an SBT channel.
12. Connect to the target Oracle server command line (e.g. via SSH) and use the **schedulershow (on page 68)** command line utility to retrieve the RMAN channel definition for use on this server
13. In RMAN, on the target Oracle server, create a channel using the definition provided by **schedulershow (on page 68)** and use it to re Oracle data. Please refer to the documentation provided by Oracle on how to backup and restore using an SBT channel.

Chapter 3: Restore workflows

The following topics describe the steps required to restore databases. These examples are performed from the **Restore Inventory**, however they can also be performed from the **Storage Inventory**. For a detailed introduction on how to work with the Protector user interface, please refer to *Hitachi Ops Center Protector User's Guide*.

When performing restore processing on an Oracle database, to prevent modifications of the existing configuration files and ensure they are available if required, Ops Center Protector always restores the following files to `$ORACLE_BASE/SnapShotBackup/<SID>/<BackupTimestamp>` on the server that is the target of the mount operation:

- `controlfile` (binary and ascii format),
- `spfile` (binary and ascii format),
- files recording the `startCN` and `endCN`,
- `oracle-Password` file,
- `init.ora` file

`controlfile`s and `SPfile`s are only copied if they are either in the same ASM Diskgroup or in the same directory with the database files or archive logs/redo logs.

ACFS is not supported (although the underlying ASM Diskgroup is copied).

The following files are not copied. A separate operation must be put in place if they are required:

- Database binaries
- External tables
- External LOBs (BFiles)
- Encryption wallets

How to mount a snapshot or clone for repurposing

A Block based clone or snapshot of an Oracle database can be used for repurposing by mounting it on a non-production server for development, test or analysis purposes. When using a Thin Image snapshots for repurposing, use a snapshot taken from a clone and not the production volume so that the performance of the production volume is not affected.

When mounting:

- The following configurations are supported:
  - Snapshots and clones from all supported backup types
  - The mounted DB runs on a single node (RAC is not supported when mounting)
- While it is possible to mount ASM based databases to any node, it is only possible to mount filesystem based databases on a node other than the source node.

  Note: The selected mount host must have a pre-existing LUN mounted from the corresponding storage device (this is required for the auto-discover feature to work). If not, then the mount operation fails.
- Protector Client software must be installed on the mount host.
- Only the backed up data files and a copy of the configuration files are included in the mounted snapshot or clone.

When unmounting:

- Protector stops and removes the recovered databases.

Procedure

1. Click **Restore** on the **Sidebar**.
2. Click the **Hitachi Block** button in the **Restore Dashboard**.
   The Hitachi **Block Restore Inventory** is displayed, but no results are initially shown.
3. Ensure the search criteria are displayed by clicking **Show Search**.
4. Enter the required search criteria to find the desired snapshots and replications, then click **Search**.
   All snapshots and replications meeting the search criteria will be displayed.
5. Select the snapshot or replication to be mounted.
6. Click **Mount**.
   The **Mount Operation Wizard** opens.
7. Select the **Application** mount option, specify the **Host Group**, **Host** and **Mount Location**, then click **Next**.
   The additional Mount Wizard - Select Oracle Restore Options (on page 51) are displayed.
8. Specify the **Recovery Options** then click **Finish**.
9. After mounting the snapshot or clone, it may be neccesary to perfom further manual recovery steps.

How to revert from a block snapshot or clone

An Oracle database can be reverted to an earlier state from a Block based snapshot or clone. Crash consistent snapshots cannot be reverted.

Note: Revert overwrites the original database and destroys all data in that database as a result.

Note: When a single backup contains data of multiple databases, reverting to the backup will corrupt all databases except the one which was selected for the backup and revert. Refer to the list of Supported configurations (on page 10) and the Application software prerequisites (on page 11) to avoid this situation.

Procedure

1. Click **Restore** on the **Sidebar**.
2. Click the **Hitachi Block** button in the **Restore Dashboard**.
   The **Block Restore Inventory** is displayed, but no results are initially shown.
3. Ensure the search criteria are displayed by clicking **Show Search**.
4. Enter the required search criteria to find the desired snapshots and replications, then click **Search**.
   All snapshots and replications meeting the search criteria will be displayed.
5. Select the snapshot or replication to be used to revert from.
6. Click **Revert**.
   The Revert Wizard - Configure Oracle Recovery Options (on page 62) of the **Block Snapshot Revert Wizard** are displayed.
7. Select the Oracle database **Recovery Options**, then click **Next**.
   The **Confirm Revert** page is displayed.
8. To ensure the user does not accidentally perform a revert, the text `REVERT` must be typed in uppercase prior to clicking **Finish**.
   The database is shutdown and the reversion process is performed.
9. Once reversion is complete, the database must be restarted manually by the database administrator who will need to choose how to recover the database (point-in-time, last known point, etc.).

How to allow Oracle RMAN to backup and restore from Protector managed datastores

Before you begin

It is assumed that the following tasks have been performed:

- The Protector Master software has been installed and licenses on a dedicated node.
- The Protector Client software has been installed on all servers of the Oracle setup and the clients have been authorized on the Master.

This workflow describes the steps to follow when setting up Protectors RMAN SBT integration from scratch, so a database administrator can use Oracle RMAN to backup a database to an Ops Center Protector managed UBI datastore. For illustration this workflow will use a Gen2 Repository, however the workflow is identical with other datastore nodes like Amazon S3 or Hitachi Content Platform (HCP).

Figure 6 Oracle RMAN Access

Table 8 Oracle RMAN full access policy

Classification Type	Parameter	Value
Oracle RMAN	Allow Databases	Refer to Oracle RMAN Database Selection Wizard (on page 49) for details on how to allow databases access
	Deny Databases	Refer to Oracle RMAN Database Selection Wizard (on page 49) for details on how to deny databases access

Table 9

Operation Type	Parameter	Value	Assigned Nodes
Access	Access Level	Read / Write	Repository, Amazon S3, Hitachi Content Platform(HCP)

Procedure

1. Locate the source *OS Host* node in the **Nodes Inventory** and check that it is authorized and online.

   This node represents the Protector Client installed on the Oracle server.
2. Create a new *Oracle Database* node using the Oracle Application Node Wizard (on page 38) and check that the node it is authorized and online.

   The *Oracle Database* node type is grouped under **Application** in the **Node Type Wizard**. This node will be used in the dataflow to represent the Oracle Database setup to be protected.

3. Create a new *destination node*, for example a Repository, using the **Repository Storage Node Wizard** (see *Hitachi Ops Center User's Guide*) and check that it is authorized and online.

   The destination nodes, like the Repository node are grouped under Storage in the **Node Type Wizard** (see *Hitachi Ops Center User's Guide*). You can direct data from multiple nodes to a single repository so there is no need to create a new repository if a suitable one already exists

   If a new Repository node is being created please the default Generation 2 type.
4. Define a policy as shown in the table above using the **Policy Wizard** (see *Hitachi Ops Center User's Guide*), Oracle RMAN Classification Wizard (on page 47) and the **Access Operation Wizard** (see *Hitachi Ops Center User's Guide*)
5. Draw a *data flow* as shown in the figure above, that shows the *Oracle Database* source node connected to the Repository destination node via a Batch mover, using the Data Flow Wizard.
6. Assign the *Oracle-RMAN-full-access policy* to the *Oracle Database source node* and to the repository destination node on the data flow.
7. Compile and activate the data flow, checking carefully that there are no errors.
8. Connect to the Oracle Server command line (e.g. via SSH) and use the *schedulershow* (on page 68) command line utility to retrieve the *RMAN channel definition* for use on this server
9. In RMAN create a channel using the definition provided by **schedulershow (on page 68)** and use it to backup and restore Oracle data. Please refer to the documentation provided by Oracle on how to backup and restore using an SBT channel

Chapter 4: Reference

This section provides salient reference information that supports the workflows detailed in this guide.

Nodes UI Reference

This section describes the Nodes UI pertaining to the node types that are used to backup Oracle Database.

Oracle Application Node Wizard

This wizard is launched when a new Oracle Database Node is added to the Nodes Inventory.

Note: If you have a clustered Oracle environment and add or remove nodes to or from the cluster, the Protector Oracle application node must be updated so that the Oracle environment can be rediscovered. Any active data flows including that node must be reactivated to update the rules.

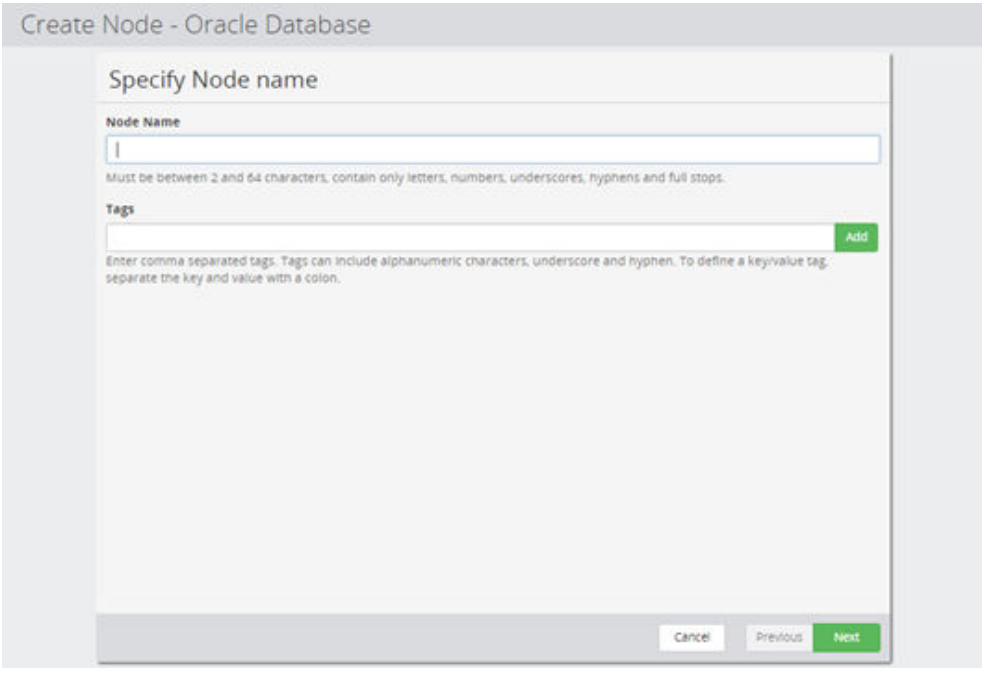

Figure 7 Oracle Database Node Wizard - Specify Node Name

Control	Description
Node Name	Enter a name for the Oracle node.
Tags	Modifies the tags of an existing object from the either the inventory screen or the details screen of the object.

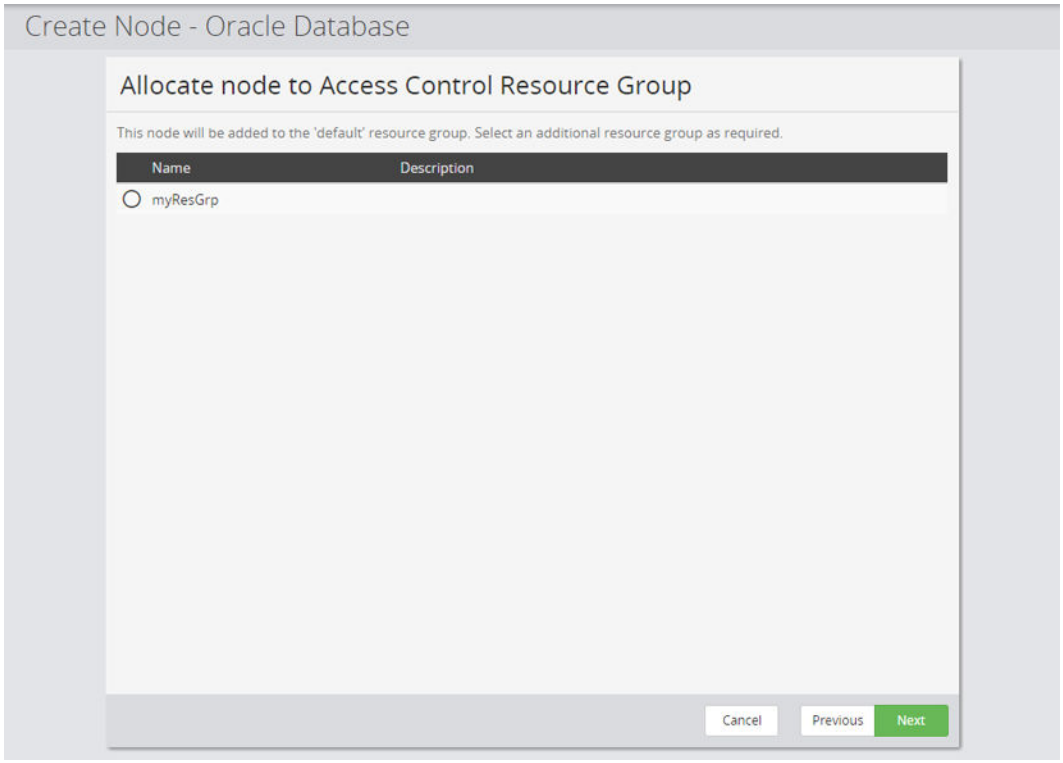

Figure 8 Oracle DB Node Wizard - Allocate node to Access Control Resource Group

Control	Description
Resource Groups	Select the resource group(s) to which this node will be allocated for the purposes of RBAC. All nodes are automatically allocated to the 'default' resource group.

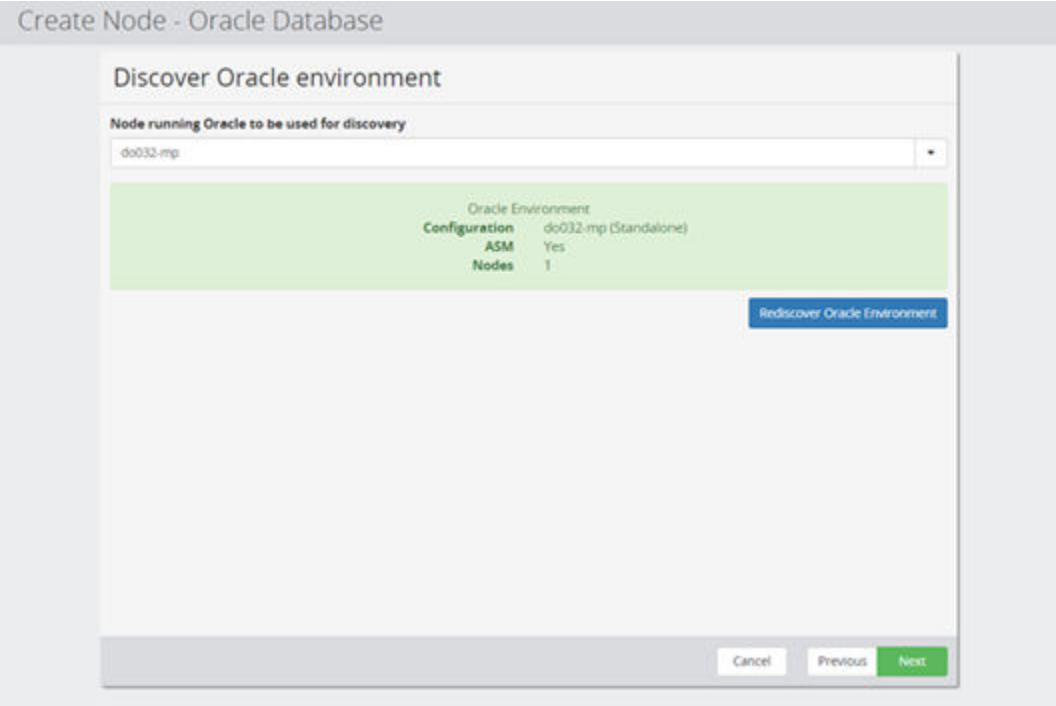

Figure 9 Oracle DB Node Wizard - Discover Oracle environment

Control	Description
Node running Oracle to be used for discovery	Select the Protector client node that communicates with the Oracle server. This node will then discover the Oracle environment.
Rediscover Oracle Environment	Click this button to refresh the cached details.

Note:

- If your Oracle setup uses ASM you can optionally specify which user is used to manage ASM.
- If your Oracle setup does not use ASM, this dialog will not be displayed.

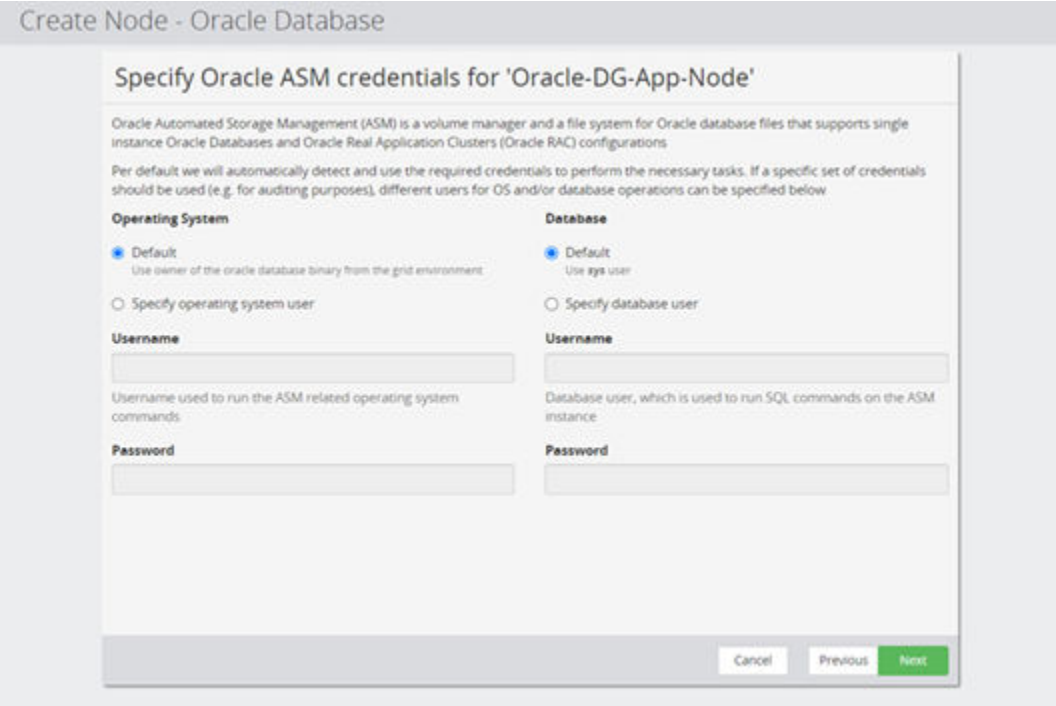

Figure 10 Oracle DB Node Wizard - Specify Oracle ASM credentials

Control	Description
Operating System	Select one of the following: ▪ Default - use the default owner of the Oracle database from the grid environment. ▪ Specify operating system user - specify the operating system user for the Oracle database.
Domain	For non-default operating system user only. If a Windows operating system is used, enter the domain name of the system to access Oracle ASM.
Username	For non-default operating system user only. Enter the Oracle Database username for the Oracle ASM.
Password	For non-default operating system user only. Enter the operating system username's password for the Oracle ASM.
Database	Select one of the following: ▪ Default - use the default database user to execute the SQL commands on the Oracle ASM instance ▪ Specify database user - specify the Oracle Database user who can execute the SQL commands on the Oracle ASM instance

Control	Description
Username	For non-default database user only. Enter the Oracle Database username of the user who can execute the SQL commands on the Oracle ASM instance.
Password	For non-default database user only. Enter the password of the user who can execute the SQL commands on the Oracle ASM instance.

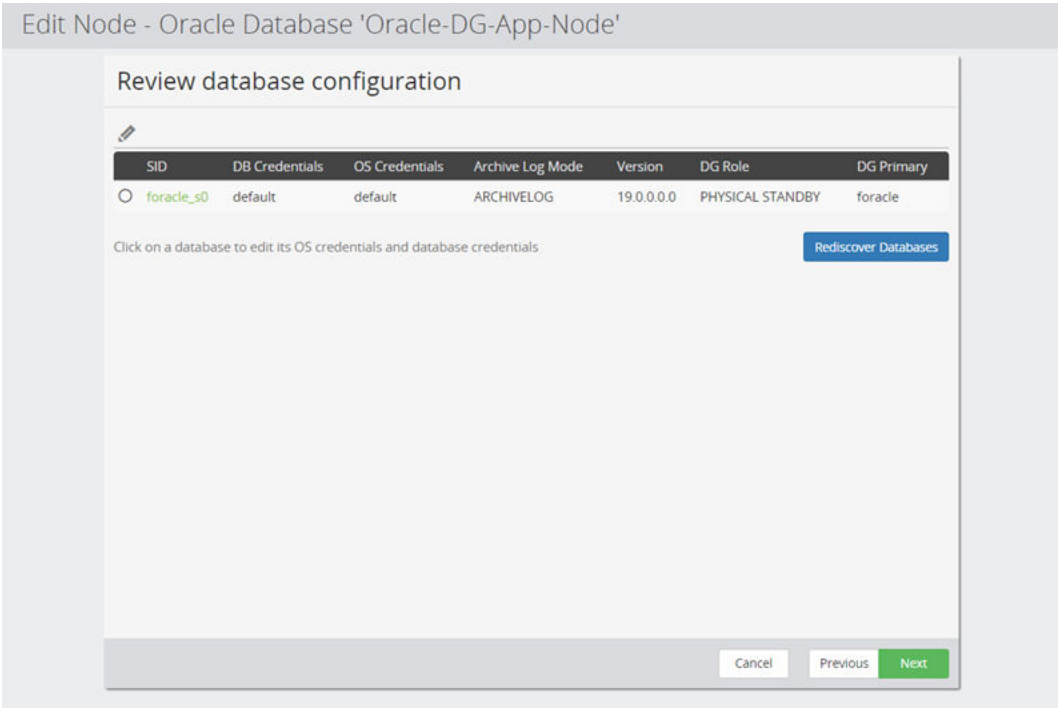

Figure 11 Oracle DB Node Wizard - Review database configuration

Control	Description
SID	Click on a database's SID to open the **Specify Database credentials** dialog (see below).
Rediscover Databases	Click this button to refresh the cached details.
DB Credentials	Displays the credentials based on the SID for database connection.
OS Credentials	Displays the OS credentials for system connection.
RMAN Catalog	Displays Oracle connection to the RMAN Catalog Database.
Archive Log Mode	Displays the archivelog information in archivelog mode.

Control	Description
Version	Displays the version number of Oracle Database.
DG Role	Displays the DataGuard roles Physical Standby, Logical Standby or Primary.
DG Primary	Displays the DataGuard Primary database name if the DG Role is Standby.

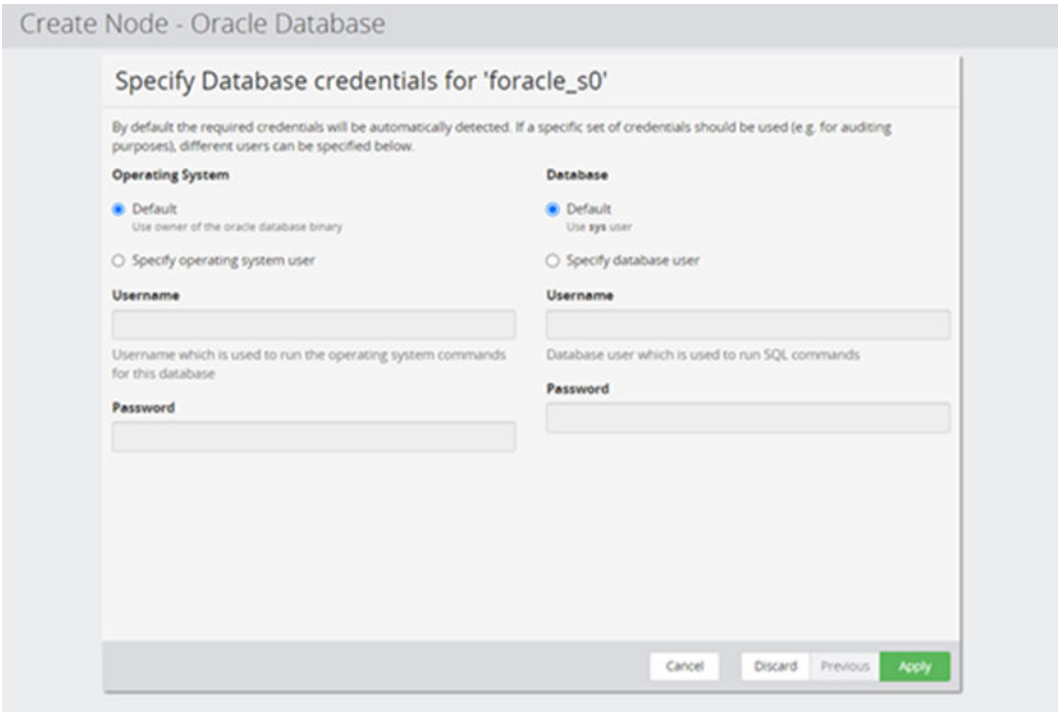

Figure 12 Oracle DB Node Wizard - Specify Database credentials

Control	Description
Operating System	Select one of the following: ▪ Default - use the owner of the Oracle database binary. ▪ Specify operating system user - specify the operating system user.
Domain	For non-default operating system user only. If a Windows operating system is used, enter the domain name of the system to access Oracle ASM.
Username	For non-default operating system user only. Enter the username which is used to run the operating system commands for this database.

Control	Description
Password	For non-default operating system user only. Enter the username's password.
Database	Select one of the following: ▪ Default - use the default database user to execute the SQL commands on the Oracle ASM instance ▪ Specify database user - specify the database user who can execute the SQL commands on the Oracle ASM instance
Username	For non-default database user only. Enter the username of the user who can execute the SQL commands.
Password	For non-default database user only. Enter the password of the user who can execute the SQL commands.

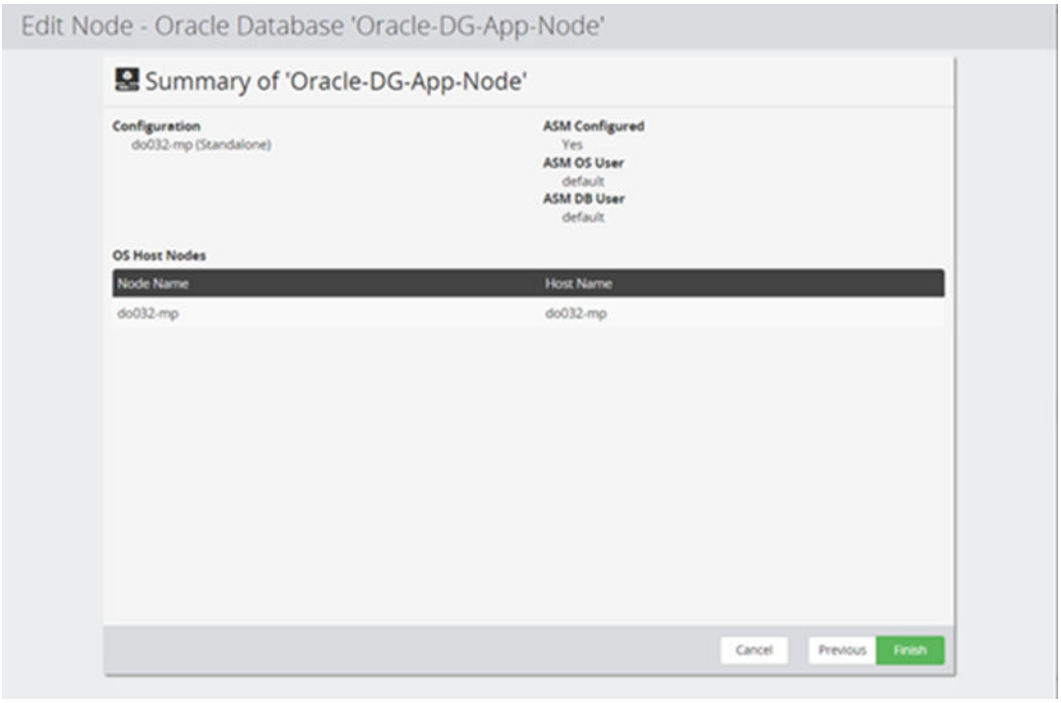

Figure 13 Oracle DB Node Wizard - Summary

Control	Description
Summary	Summary of the selected configuration.

Policies UI Reference

This section describes the Policies UI pertaining to the node types that are used to backup Oracle Database.

Oracle Database Classification Wizard

This wizard is launched when a new Oracle Database classification is added to a Policy.

The Oracle Database classification is used to define which databases are to be protected.

Note: When used in combination with a storage hardware backup operation, Protector will discover the underlying hardware paths at runtime. For Hitachi Block storage hardware based backups, all the paths must exist on the same block hardware device.

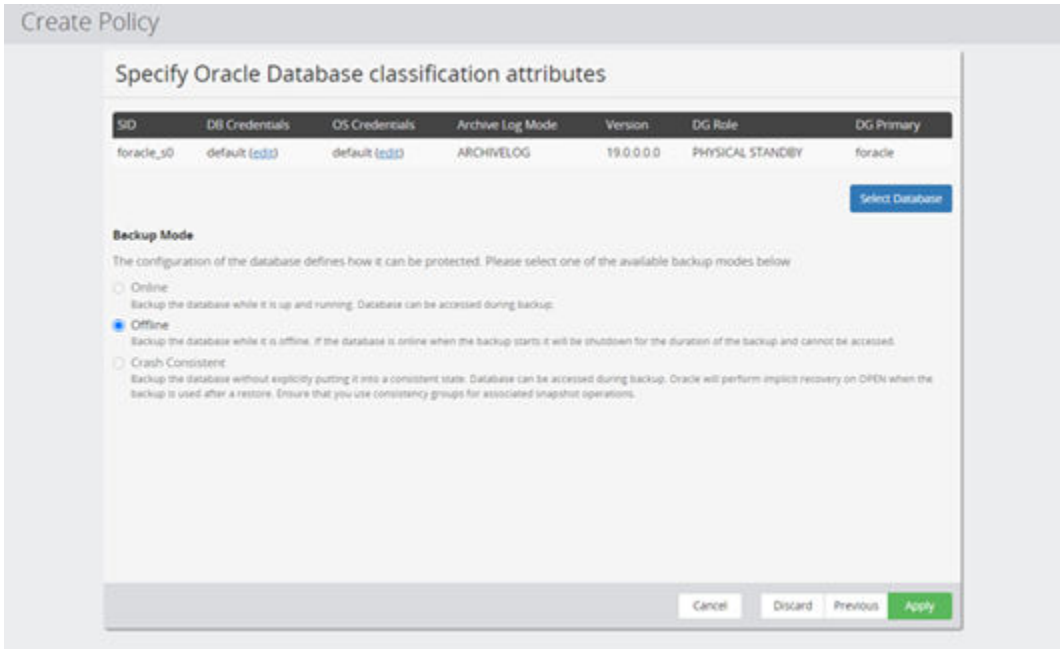

Figure 14 Oracle Database Wizard - Specify Oracle Database classification attributes

Control	Description
Databases	Lists the currently selected databases.

Control	Description
	Only the databases listed are backed up. ▪ For block based policies - Databases are discovered only once, when the policy is defined. ▪ For host based policies - This classification is not currently supported.
Select Database	Click to open the Select Database dialog shown below.
Backup Mode	Select one of the following: ▪ Online – Available only if Oracle Database is running in `ARCHIVELOG` mode. Oracle is briefly quiesced while an application consistent snapshot is made. ▪ Offline – Available always. Oracle is taken offline while an application consistent snapshot is made. ▪ Crash Consistent – Available only in Version 12c and if Oracle Database is running in `ARCHIVELOG` mode. Oracle remains running while a crash consistent snapshot is taken. **Note:** ▪ If the DataGuard Role is PHYSICAL STANDBY, backup mode is auto selected as Offline. ▪ If the Backup Mode is set to Online, ensure that Quiesce configured applications before backup is selected in the **Snapshot/Replicate Operation Attributes Wizard**. ▪ If the Backup Mode is set to Crash Consistent, ensure that the Use consistency group option is selected in the **Snapshot/Replicate Operation Properties Dialog** on the data flow.

Figure 15 Oracle Database Wizard - Select Oracle Databases Dialog

Control	Description
Oracle Node	Select a node representing the Oracle server hosting the database(s) to be selected for backup.
Filter database by name	Filters the databases list below to show only those entries that contain the filter string.
Databases	Select the database(s) to be backed up from the list.
Refresh	Click this button to refresh the cached details and clear the name filter.

Oracle RMAN Classification Wizard

This wizard is launched when a new Oracle RMAN classification is added to a Policy.

The Oracle RMAN classification allows to conveniently specify, which databases can or cannot access Oracle RMAN data using the access operation.

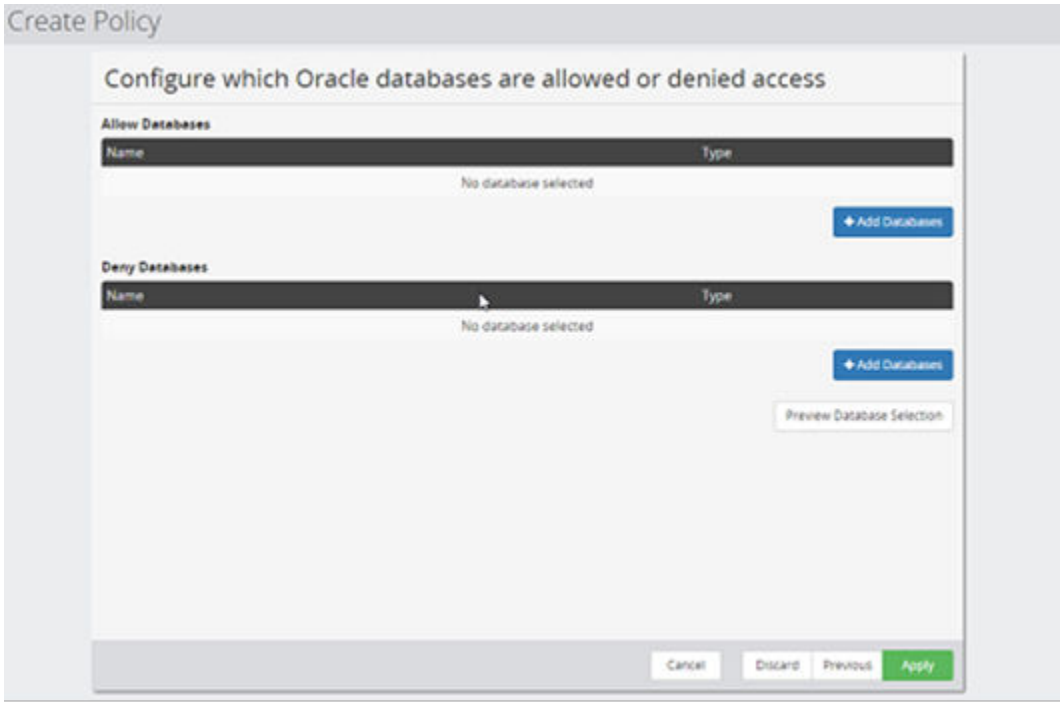

Figure 16 Oracle RMAN Wizard - Specify Oracle Databases (Allowed / Denied Access)

Control	Description
Allow Databases	Lists the databases that will be allowed access for Oracle RMAN access operations.
Add Databases	Opens the Oracle RMAN Database Selection Wizard (on page 49) to enable databases to be added to the **Allow Databases** list above.

Control	Description
Deny Databases	Lists the databases that will not be allowed access for Oracle RMAN access operations.
Add Databases	Opens the Oracle RMAN Database Selection Wizard (on page 49) to enable databases to be added to the "Deny Databases" list above.
Preview Database Selection	Click this button to preview the which databases are allowed access for an existing Oracle Database node.

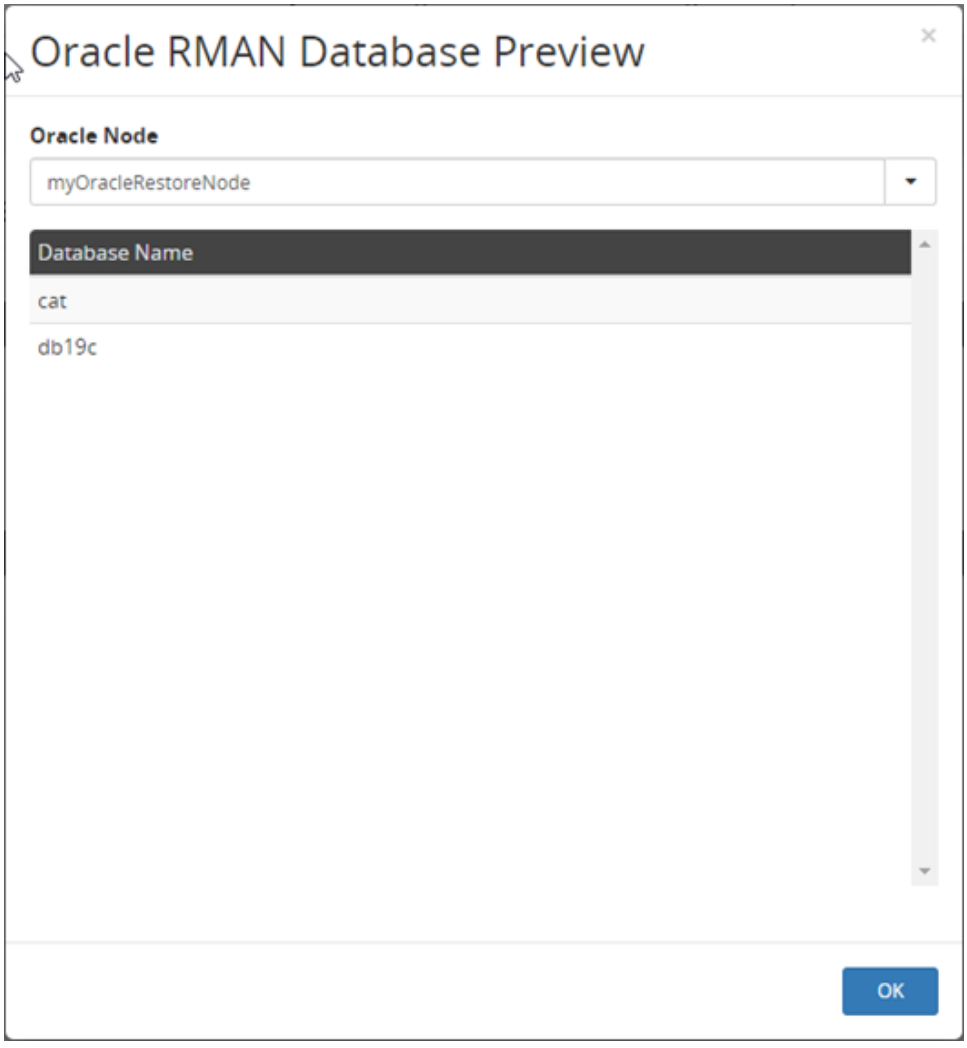

Figure 17 Oracle RMAN Database Preview

Control	Description
Oracle Node	Select a node representing the Oracle setup, which should be previewed.
Database List	List all databases on this node which would be allowed access with the defined classification.

Oracle RMAN Database Selection Wizard

This wizard is launched when a user adds entries to the list of allowed or denied databases in an Oracle RMAN classification.

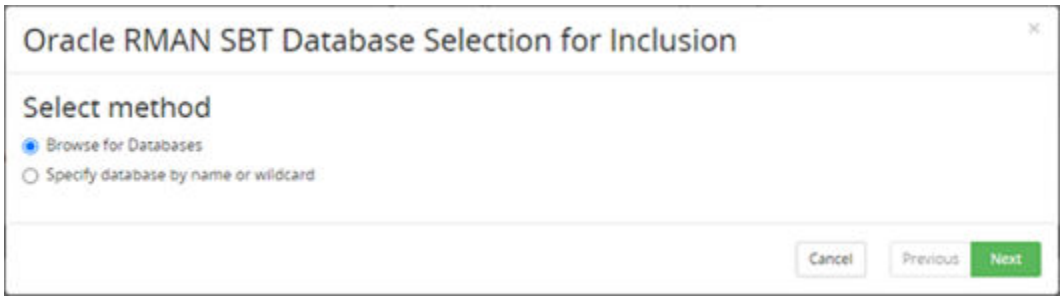

Figure 18 Oracle Database Selection – Select method

Control	Description
Browse for databases	Select this option to browse an existing Oracle node for databases. See **Oracle Database Selection – Browse by** below.
Specify databases by name or wildcard	Select this option specify a database by name pattern match. See **Oracle Database Selection – Specify name or wildcard** below.

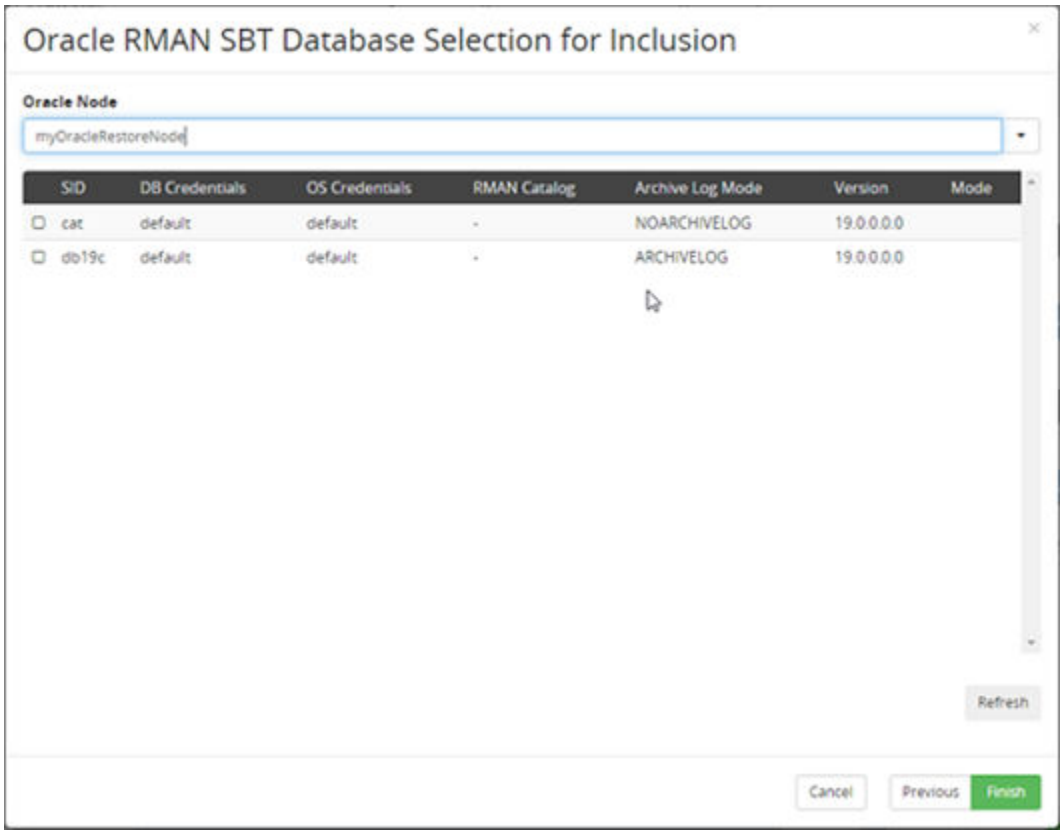

Figure 19 Oracle Database Selection – Browse by

Control	Description
Oracle Node	Select an Oracle database application node to browse for databases.
Database List	Lists the databases which exist on the selected node. You can select one or more databases.
Refresh	Refreshes the list of databases for the selected node. This operation may take a few minutes.

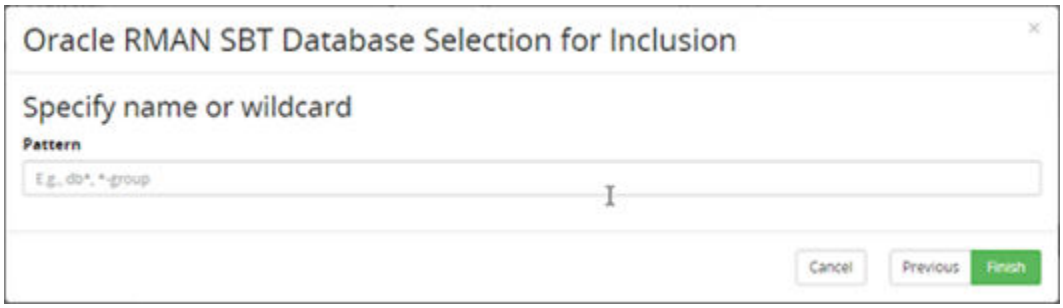

Figure 20 Oracle Database Selection – Specify name or wildcard

Control	Description
Pattern	Enter a case insensitive pattern that will be used to match the database by name. The '*' character can be used to match any sequence of characters. E.g.: IH_* would match any database type whose name begins with IH_. **Note:** Protector evaluates the pattern every time Oracle RMAN tries to access the data. If new databases are added later, they will still be allowed or denied access, depending if they match the pattern or not.

Restore UI Reference

This section describes the Restore UI pertaining to the node types that are used to backup Oracle Database.

Mount Wizard - Select Oracle Restore Options

When mounting block snapshots or replications created by a policy containing an *Oracle Database* classification, Protector will display the following additional wizard pages that allows application specific options to be configured:

Note: To perform the mount operation, a snapshot should be available.

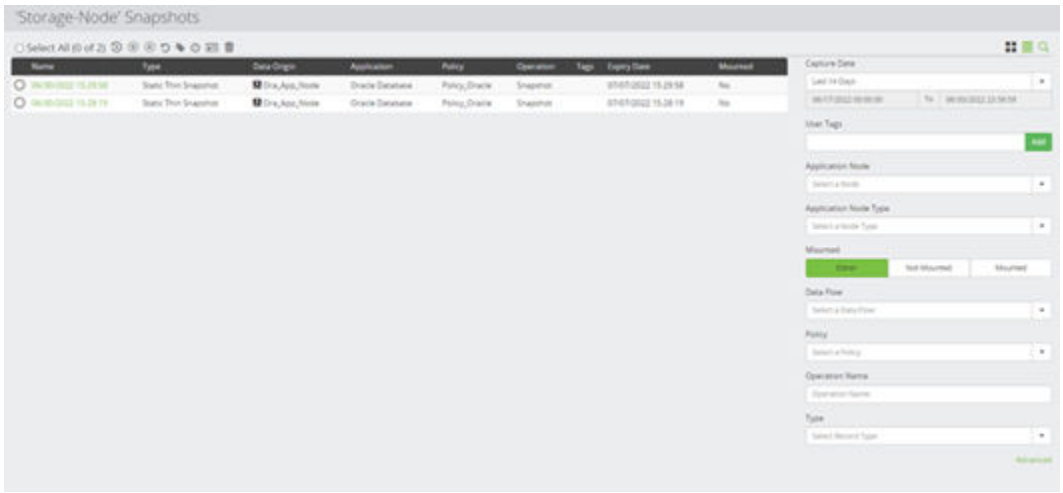

Figure 21 Snapshot to be mounted

Table 10 List of Snapshots to be mounted

Control	Description
Name	Displays the name of the snapshots to be mounted.
Type	Displays the type of the snapshot.
Data Origin	Displays the Application Node that was used to create the snapshot.
Application	Displays the application on which the snapshot is running.
Policy	Displays the policy associated with the snapshot.
Operation	Displays the type of the operation for the snapshot.
Tags	Displays the tags associated with that snapshot.
Expiry Date	Displays the expiry date for the snapshot.
Mounted	States the status of the snapshot if it is mounted or not mounted.
Filter on Capture Date	Filters the snapshot on the date range on which it was created.
Filter on User Tags	Filters the displayed results based on Tags.
Filter on Application Node	Filters the snapshot by the name of the node.
Filter on Application Node Type	Filters the snapshot on the type of the Application node.
Filter on Mounted	Filters the snapshot by either Mounted or Not Mounted.
Filter on Data Flow	Filters the snapshot based on the Data Flow associated with a snapshot.
Filter on Operation Name	Filters the snapshot so that only entries with the specified Operation Name are displayed.
Filter on Type	Filters the snapshot based on its type.
Filter on Advanced Query String	Provides advanced search capabilities, allowing users to create filters based on combinations of API properties (see the API reference guide for more details).

Control	Description
Search	Returns the result on Advanced Query String.

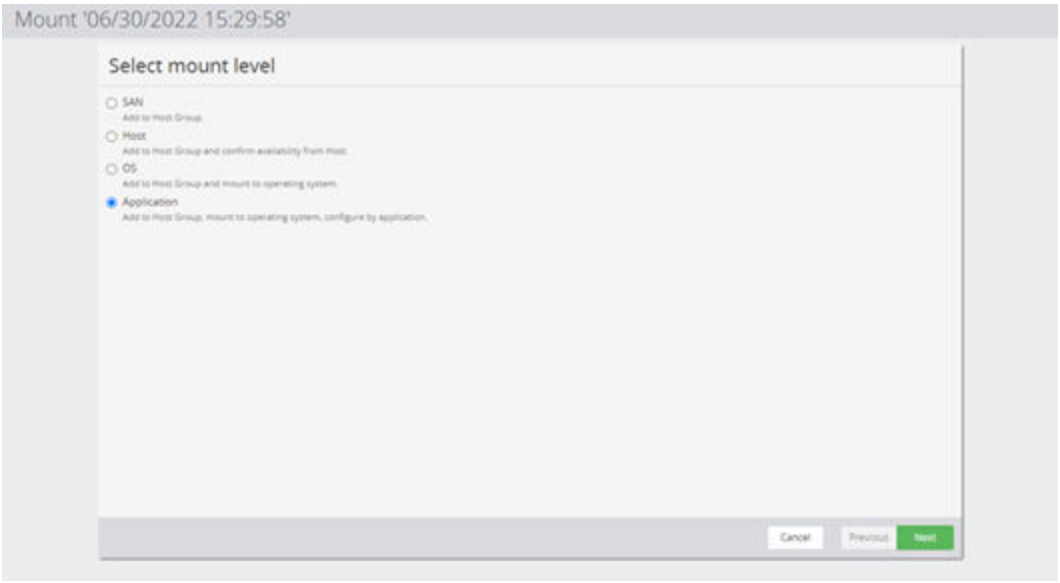

Figure 22 Select Mount Level

Table 11 Oracle - Select Mount Level

Control	Description
SAN	Add this record to a Host Group.
Host	Add this record to a Host Group and confirm availability from Host.
OS	Add this record to a Host Group and mount to operating system.
Application	Add this record to a Host Group, mount to operating system configure by application (This will include ASM operations).

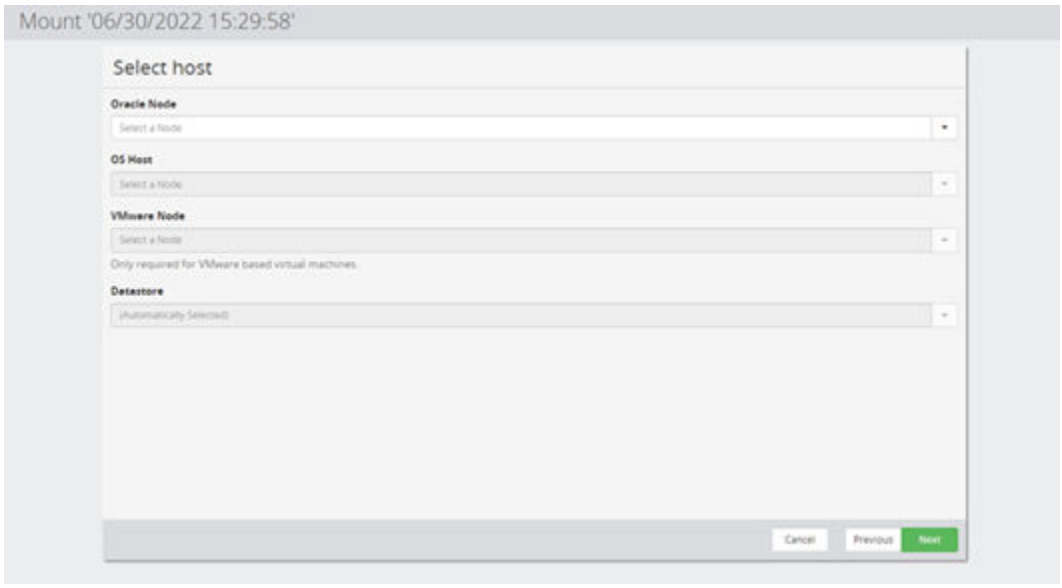

Figure 23 Oracle Mount - Select Host

Table 12 Oracle - Select Host

Control	Description
Oracle node	The oracle node where the user will mount the snapshot representing the target Oracle app server environment.
OS Host	The node which hosts the Oracle application node.
VMware Node	Select the VMware Host or vCenter where the VM's disks will be mounted.
Datastore	Select the Datastore where the disk will be mounted.

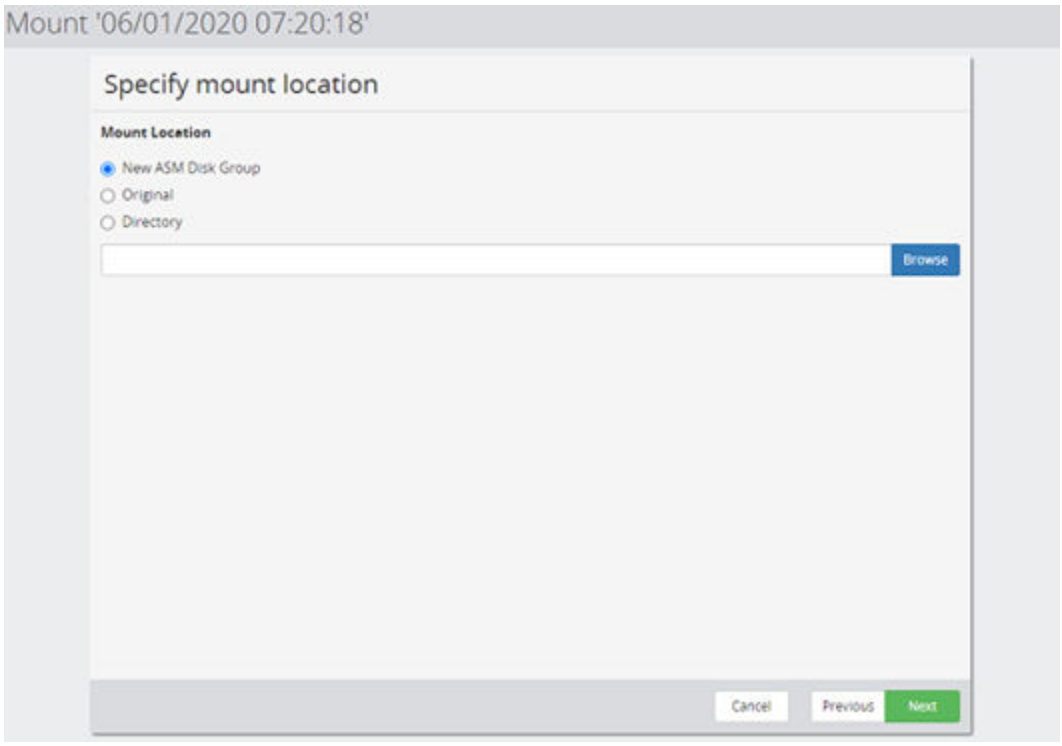

Figure 24 Mount Wizard - Specify Mount Location

Control	Description
New ASM Disk Group	Mount the ASM disk groups using a new generated name to avoid conflicts with the original database or existing ASM disk groups. The new disk group name is auto generated. It comprises the original name and a numeric suffix, allowing for multiple copies of the same database to be mounted to a single host. **Note:** This option is only valid for backups of ASM based Oracle databases. The option will be disabled automatically if Protector detects a filesystem based Oracle database in a backup created with Protector 7.1 or newer.
Original	Mount the database using the same ASM disk groups or filesystem paths as the original database the backup was created from. If the path or disk group name is in use by an existing database, the mount will fail.

Control	Description
Directory	Mount the database to the provided path. If the path in use by an existing database, the mount will fail. **Note:** This option is only valid for backups of filesystem based Oracle databases. The option will be deactivated automatically, if Protector detects an ASM based Oracle database in a backup created with Protector 7.1 or newer.

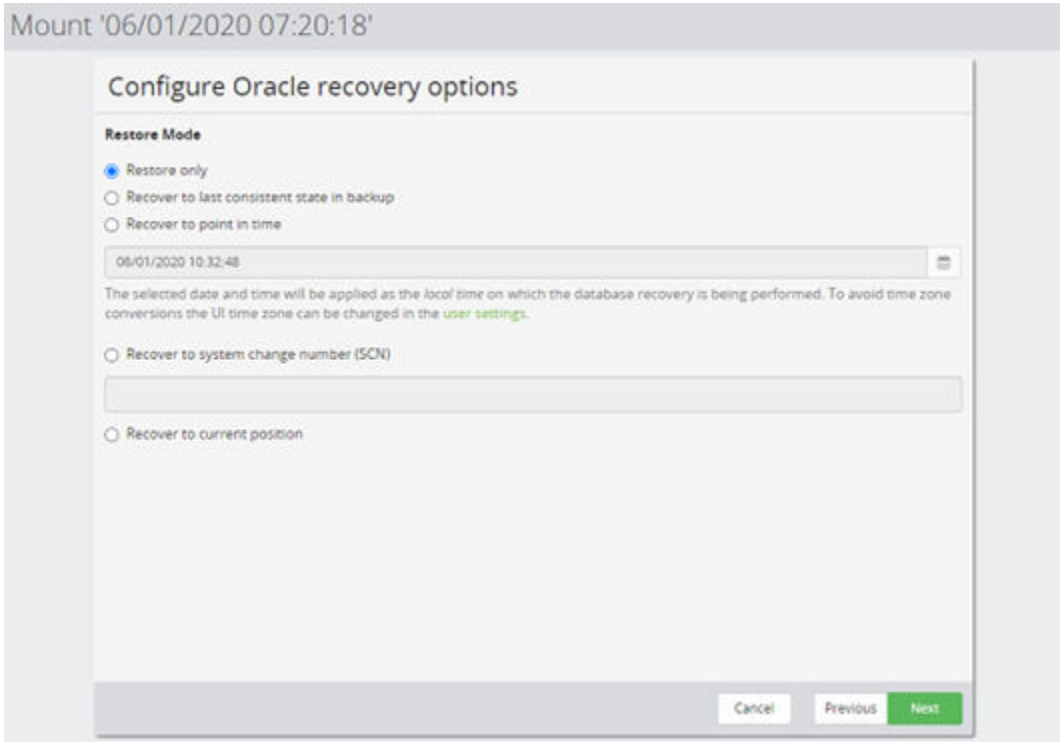

Figure 25 Mount Wizard - Select Oracle Restore Options

Control	Description	Logs Reset Post Mount	Requires RMAN catalog	Requires control/ spfile in RMAN backup
Restore only	The database is simply mounted. It is left to the database administrator to recover manually.	No	No	No

Control	Description	Logs Reset Post Mount	Requires RMAN catalog	Requires control/ spfile in RMAN backup
Recover to last consistent state in backup	The database is recovered to the consistent state which was captured by the backup. The database is brought online. This type of mount can be performed with the data in the backup alone.	Depends (see note 1)	No	No
Recover to point in time	A timestamp is entered which defines the point in time to recover. This requires a connection to the RMAN catalog and logs which are shared with/ available to the host. **Note:** This is not applicable for DataGuard configuration.	Depends (see note 1)	Yes	Yes (see note 2)
Recover to system change number (SCN)	A system change number is entered which defines the change point to recover. This requires a connection to the RMAN catalog and logs which are shared with/available to the host. **Note:** This is not applicable for DataGuard configuration.	Depends (see note 1)	Yes	Yes (see note 2)
Recover to current position	The database is recovered to the most current position possible. This requires a connection to the RMAN catalog and logs which are shared with/available to the host.	Depends (see note 1)	Yes	Yes (see note 2)

Control	Description	Logs Reset Post Mount	Requires RMAN catalog	Requires control/ spfile in RMAN backup
	Note: ▪ When mounting, the current position is the latest point in time which is provided by the archive logs referenced in RMAN catalog. It does not include any archive logs or redo logs on the source machine which have not been backed up via RMAN. ▪ This is not applicable for DataGuard configuration.			

Note: (1) In the table above, logs will only be reset when Open Database is selected in the **Post Recovery Options** page of the wizard (see below).

Caution: (2) In the table above, for some recovery scenarios the RMAN catalog needs to hold a control file. RMAN can be configured to add a control/spfile backup every time an archive log backup is performed.

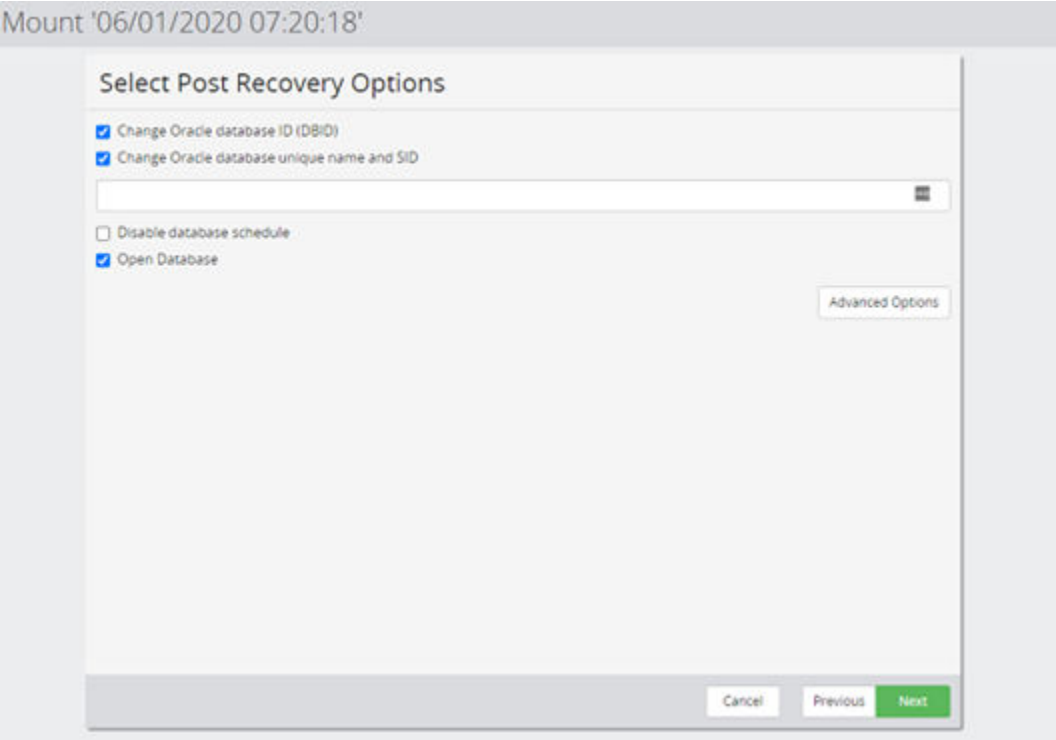

Figure 26 Mount Wizard - Select Post Recovery Options

Control	Description
Change Oracle database ID (DBID)	Creates a new DBID for the database. **Tip:** A DBID is a unique, Oracle generated number identifying each database. It is found in control files as well as datafile headers and is used to determine which database that file belongs to.
Change Oracle database unique name and SID	A new unique name and SID can be specified for the database. **Tip:** This changes the `unique_database_name` which is also used as the SID.
Disable database schedule	Disables database internal tasks scheduled for this database. **Tip:** The Oracle scheduler allows the administrator to schedule SQL commands as jobs. By selecting this option existing schedules will be disabled.
Open Database	If selected, then after recovery the database will placed in the *OPEN* state using the *RESETLOGS* or *NORESETLOGS* option, as per the requirements of the database. Otherwise the database will be left in the *MOUNT* state.
Advanced Options	Opens the **Advanced Options** page of the wizard.

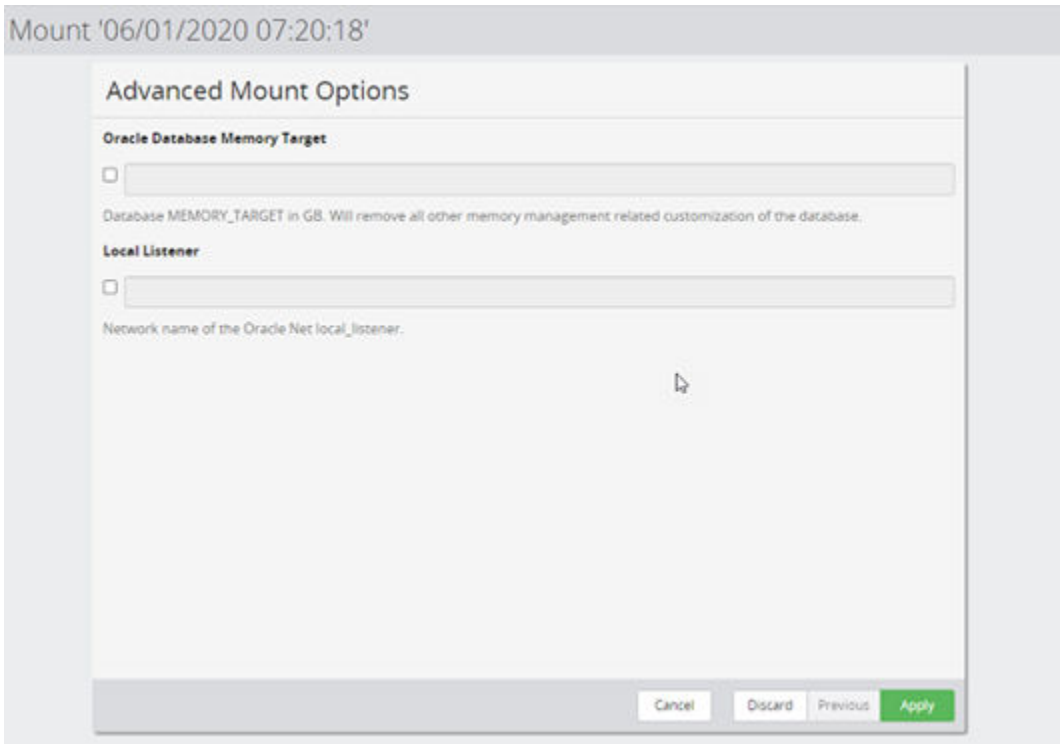

Figure 27 Mount Wizard - Advanced Mount Options

This page of the wizard is not be displayed if Restore only or Recover to last consistent state in backup is selected in a previous step.

Control	Description
Oracle database Memory Target	Sets the database `MEMORY_TARGET` in GB. Entering a value here will remove all other memory management related customization of the database. **Tip:** This allows Oracle databases from very powerful source systems to be deployed on less powerful systems. The PGA and SGA memory areas will be managed by Oracle within the given memory target.
Local Listener	Sets the network name of the Oracle Net `local_listener`.

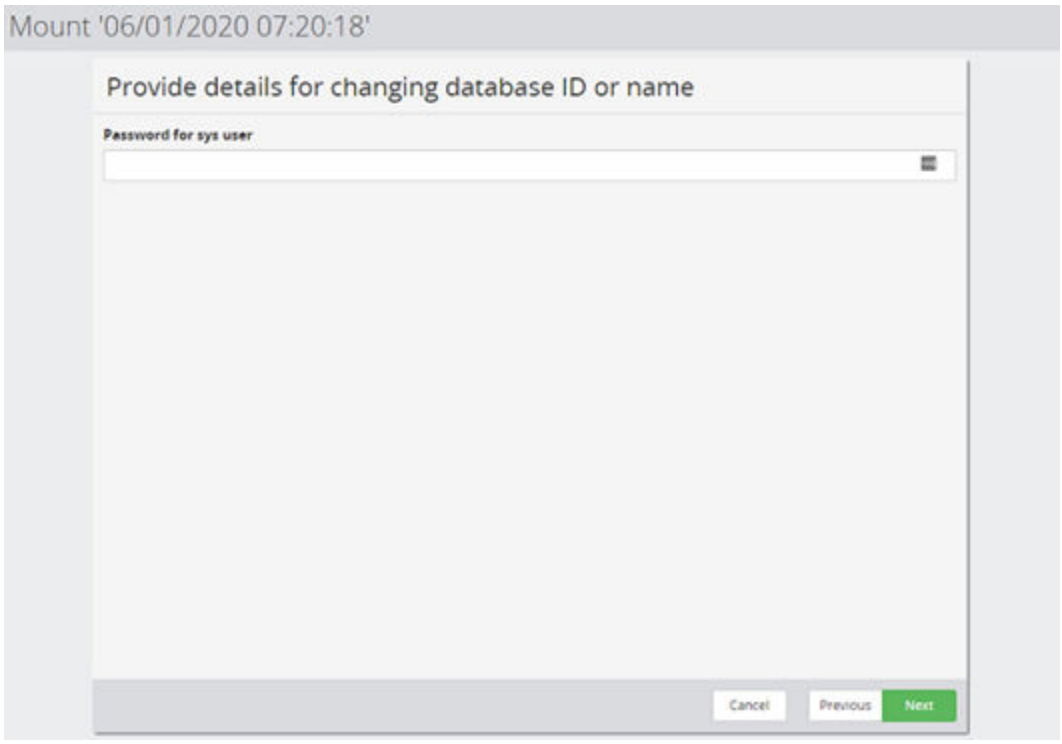

Figure 28 Mount Wizard - Provide details for changing database ID or name

This page of the wizard will only be displayed if either Change Oracle database ID (DBID) or Change Oracle database unique name and SID options are selected in a previous step.

Control	Description
Password for sys user	Depending on the Oracle version: ▪ Oracle 11g: The sys user password is required to change the Oracle database ID or database unique name. ▪ Oracle 12 or newer: This field can be left empty.

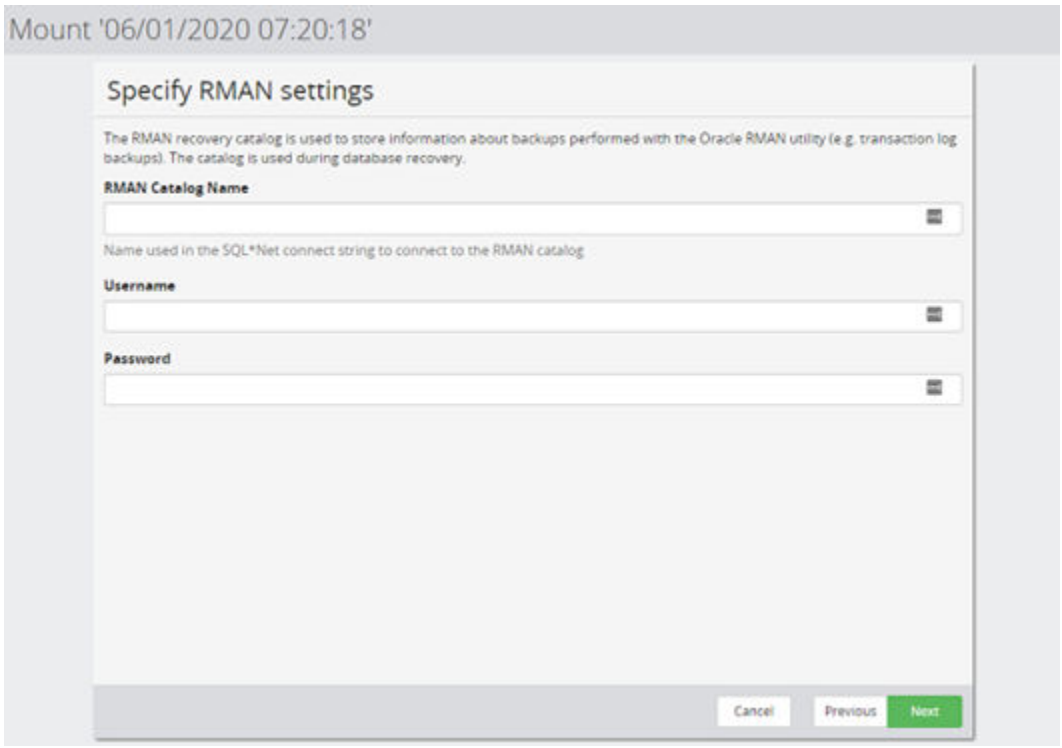

Figure 29 Mount Wizard - Specify RMAN credentials

This page of the wizard is not displayed if Restore only or Recover to last consistent state in backup is selected in a previous step.

Control	Description
RMAN Catalog Name	For RMAN only. Enter the RMAN Catalog Name as it is entered in the SQL*Net connect string to connect to the RMAN catalog.
Username	For RMAN only. Enter the username for the RMAN catalog.
Password	For RMAN only. Enter the password for the RMAN catalog.

Revert Wizard - Configure Oracle Recovery Options

When reverting snapshots or local replications created by a policy containing an *Oracle Database* classification, Protector will first display the following wizard page that allows application specific options to be configured.

Note: If an Oracle app node is of type DataGuard Standby then snapshot cannot be reverted.

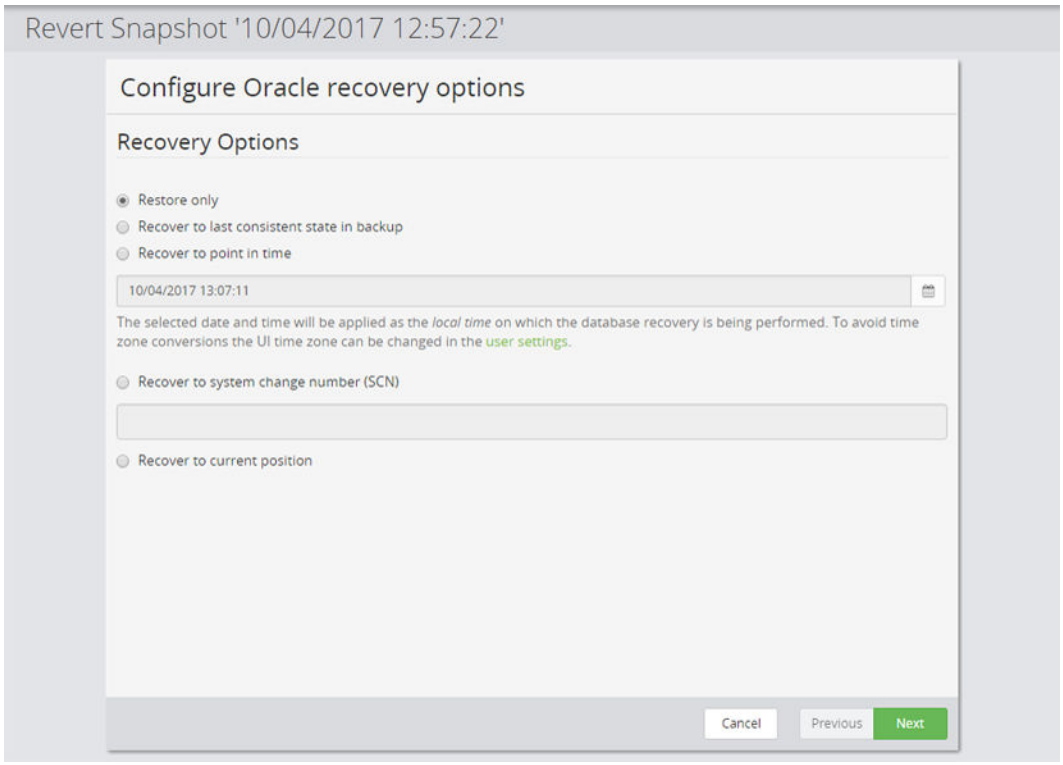

Figure 30 Revert Wizard - Configure Oracle Recovery Options

Control	Description	Logs Reset Post Recovery
Restore only	The database is simply reverted and it is left to the database administrator to recover manually.	No
Recover to last consistent state in backup	The database is recovered to the consistent state which was captured by the backup. The database is brought online. This type of revert can be performed with the data in the backup alone; no RMAN catalogue is required.	Yes
Recover to point in time	A timestamp is entered (in 24 hour format: YYYY-MM-DD:HH:MM:SS), which defines the point in time to recover. The time entered must be after the time the snapshot was created and before the last available transaction. This option requires a connection to the RMAN catalog and logs which are shared with/available to the host.	Yes

Control	Description	Logs Reset Post Recovery
Recover to system change number (SCN)	A system change number is entered which defines the change point to recover. The SCN entered must be after the snapshot was created and before the last available transaction. This option requires a connection to the RMAN catalog and logs which are shared with/available to the host.	Yes
Recover to current position	The database is recovered to the most current position possible. Because access to the latest redo logs is available, it is possible to recover to the last transaction. This requires a connection to the RMAN catalog and logs which are shared with/available to the host.	No

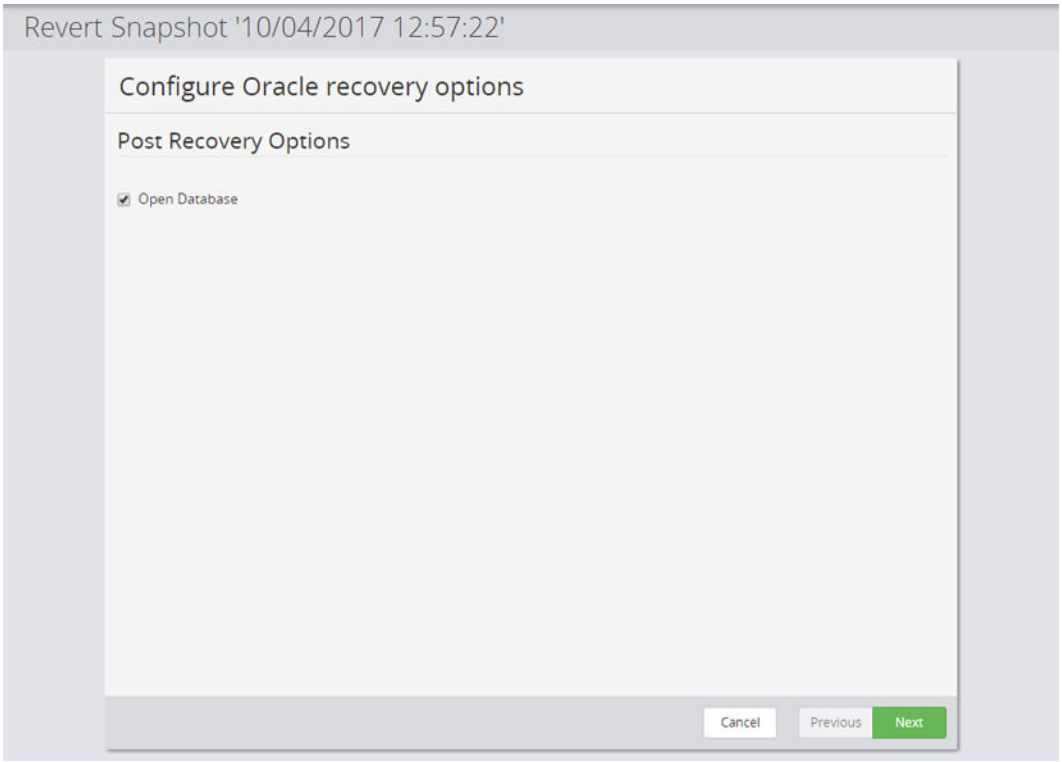

Figure 31 Revert Wizard - Post Recovery Options

Control	Description
Open Database	If selected, then after recovery the database will placed in the *OPEN* state using the *RESETLOGS* or *NORESETLOGS* option, as per the requirements of the database. Otherwise the database will be left in the *MOUNT* state.

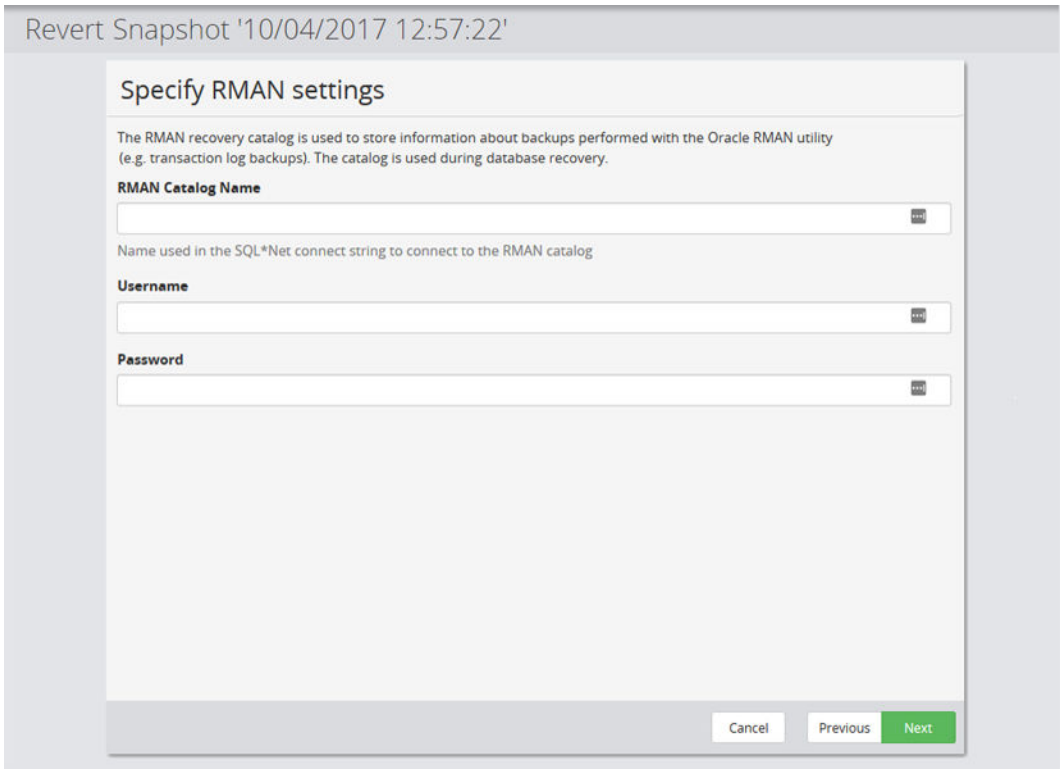

Figure 32 Revert Wizard - Specify RMAN Credentials

This page of the wizard is not displayed if Restore only or Recover to last consistent state in backup is selected in a previous step.

Control	Description
RMAN Catalog Name	For RMAN only. Enter the RMAN Catalog Name as it is entered in the SQL*Net connect string to connect to the RMAN catalog.
Username	For RMAN only. Enter the username for the RMAN catalog.
Password	For RMAN only. Enter the password for the RMAN catalog.

Chapter 5: Troubleshooting

This chapter provides guidelines for how to troubleshoot issues that might occur when using Ops Center Protector.

Troubleshooting Oracle Database

This section provides guidelines for how to troubleshoot issues that might occur when using Oracle Databases.

An online backup or mount fails

Problem:

In the event of a failure, Protector attempts to revert the operations performed up to the point of the failure, but success cannot be guaranteed.

Solution:

If an Oracle online backup fails, then check that the operations described in the attachments to the log entry `backupOnline Worksteps` are reverted. It is especially important that the step `endOnlineBackup` is performed. If not then execute the steps described in the attachment to the log entry `endOnlineBackup`.

If an Oracle offline backup fails, check that the database is started.

If a mount fails then check if the status of the snapshot is mounted. If so, then perform an un-mount. In addition to this, check that an eventual ASM Diskgroup (**`asmcmd lsdg`**) is un-mounted and removed from the resource group (**`asmcmd umount`** *ASM_DISKGROUP*; **`srvctl remove diskgroup -g`** *ASM_DISKGROUP*). Do not try to issue a mount operation to another server, prior a successful un-mount operation.

Failed to discover Oracle environment when creating application node

Problem:

The following error message is seen when attempting to discover an Oracle Environment in the ‘Create Node – Oracle Database’ section:

```
Failed to discover Oracle Environment
```

Solution:

1. Click **Rediscover Oracle Environment**

Note: If click fails, continue with the below steps.

2. Ensure that Oracle is running. If not, start Oracle and repeat the discover process.
3. Edit the file `/etc/nsswitch.conf`
   a. Using a suitable editor, open the file `/etc/nsswitch.conf`
   b. Locate the line that starts with `hosts` and comment it out with a `#`
   c. Copy the line and re-order it so that `dns` is first and `files` is last. E.g.:

```
#hosts: files dns myhostname
hosts: dns myhostname files
```

   d. Save the file.
   e. Attempt to discover the Oracle Environment again. The edited file should be picked up straight away and thus it should not be necessary to restart or reboot.

Oracle database snapshot fails to mount

Problem:

The following error message is logged if you attempt to mount an Oracle database snapshot to a location where one is already mounted:

```
Handler call failed: [...] ASM Diskgroups [...] mounted
```

Solution:

You cannot mount a second snapshot of the database to a location where one is already mounted.

RAC lock on database failed

The following error message is logged, during online snapshot operations, for all but one node in a RAC environment:

```
Handler call failed: [...] RAC Lock Database failed, check if [...]
```

Only one RAC node will succeed to lock the database prior to online snapshotting, all other nodes in the RAC will fail.

Solution:

Check that the operation has succeeded on exactly one of the RAC nodes.

Cannot find Oracle database metadata files on mount

Problem:

The metadata files relating to the mounted Oracle database files cannot be located.

Solution:

The following information message is logged when an Oracle database is mounted:

```
OracleHandler [...]: mount for 'Oracle DB: [...]' finished [...]
```

The attachment lists the destination paths where the Oracle metadata files have been placed.

Error when reverting on ASM in normal/high redundancy mode

Problem:

If you attempt to revert a database running on ASM in normal or high redundancy mode, the following warning message is logged during backup operations, followed by the error message:

```
Handler call failed: [...] normal or high redundancy used; revert
not possible with one mirror
```

Solution:

ASM normal/high redundancy modes are currently not supported.

Warning during backup if data/redo files in the same directory

Problem:

The following warning message is logged during backup operations when the data and redo files of the Oracle database are located in the same directory:

```
OracleHandler [...]: Oracle Database Files and Redo in the [...]
```

Solution:

It is not recommended to have redo logs and data on the same physical disks, as this may cause unusable backups for anything other than crash consistent backups. Please refer to **Oracle application software prerequisites** for more information.

Oracle RAC RPO based policy creates more snapshots than expected

Problem:

When using the 'All Day' schedule option for an Oracle RAC policy and relying on the RPO setting alone, more snapshots than expected may be created. This can happen if rules are activated while one node in the RAC is busy or restarting, causing the activation time to be offset for that node.

Solution:

Try using the ‘Scheduled Time’ option rather than an RPO. Also check that the RAC nodes’ times are synchronized.

Listing Oracle RMAN channel configurations with schedulershow

schedulershow is a CLI tool that is used to aid the Oracle database administrator to configure Oracle RMAN to save and restore data using a datastore managed by Ops Center Protector. It provides the following functionality.

- List the Oracle RMAN dataflows active on the current node
- Create a sample RMAN channel definition for a dataflow operation

In order for a node to store or access any data in a Protector managed datastore using Oracle RMAN, the node has to be part of a dataflow and granted access using the access operation. Once the dataflow is compiled and distributed, it can be listed with schedulershow and Oracle RMAN can access it using an SBT channel.

Table 13 Command line options

Abbreviated Argument	Full Argument	Description
`-h`	`--help`	Display help.
`-c`	`---config <trigger>`	Display RMAN channel configuration for a dataflow. The command provides a list of valid triggers when running the it without parameters..

Usage Example

List all Oracle RMAN dataflows active on this node

```
app/bin/schedulershow

Application DataFlow Source OperationName Storage Trigger

Oracle mysampledf1 myOracleNode Access myRepository
1f04eeec33b10190b79ea6d47a65f3943f5a9de0c1a5d1557afeb420ea604046

Oracle Demo2 myOracleNode Access myRepository
6e7b941d5e73ec5a3ce72b64e70c36c56e6d12f76a379d0982d130d1b505a895
```

Get the Oracle RMAN channel definition for a dataflow

```
app/bin/schedulershow -c
1f04eeec33b10190b79ea6d47a65f3943f5a9de0c1a5d1557afeb420ea604046

# Application = Oracle

# DataFlow=mysampledf1

# Source=myOracleNode

# OperationName=Access

# Storage=myRepository

#
Trigger=1f04eeec33b10190b79ea6d47a65f3943f5a9de0c1a5d1557afeb420ea60
4046

DEVICE TYPE 'SBT_TAPE' PARMS

'SBT_LIBRARY=/opt/hitachi/protector/app/lib/
libhsbt.so,SBT_PARMS=(TRIGGER=1f04eeec33b10190b79ea6d47a65f3943f5a9d
e0c1a5d1557afeb420ea604046)'
```

Glossary

Archive
A copy that is created for long-term retention.

Asynchronous journalling
Transactions are written to disk and also placed in a journal log file, to protect against data loss in the event of a system failure. Transactions from the log file are sent to the destination machine.

Asynchronous replication
Transactions are held in memory before being sent over the network. If the network is unavailable then transactions are written to disk and sent to the destination machine when the connection is re-established. Asynchronous replication is optimal for connections with sporadic efficiency.

Backup
A copy that is created for operational and disaster recovery.

Bandwidth throttling
Used to control when and what proportion of available network bandwidth is used by Ops Center Protector for replication.

Batch backup
A process by which the repository is updated periodically using scheduled resynchronizations. This method involves a scan of the source machine's file system, but only the changed bytes are transferred and stored. This method is useful for data that does not change often, such as data contained on the operating system disk. Linux based source nodes are only able to perform batch backups.

Clone
An operation where a copy of the database is created in another storage location in a local or remote site.

Continuous Data Protection (CDP)
A method of capturing the state of a file system in near real time. CDP shares much of the functionality of Live Backup, except that RPO is measured in minutes, data is retained for a much shorter period of time and is not indexed by the MDS. Typically, CDP and Live Backup are used in conjunction. CDP is only supported on source nodes running the Microsoft Windows operating system.

Data flow
Identifies the data sources, movers and destinations participating in a backup, along with interconnection paths between them. Policies are assigned to each node to determine what type of data is backed up.

Data source
A machine hosting a file system or application where the Protector client software is installed.

Deduplication
A method of reducing the amount of storage space that your organization requires, to archive data, by replacing multiple instances of identical data with references to a single instance of that data.

Destination node
A machine that is capable of receiving data for the purposes of archiving. This machine might be the Ops Center Protector Repository or Block device.

License key

A unique, alphanumeric code that is associated with the unique machine ID that is generated during the Ops Center Protector installation. The license key must be activated in order to use the software.

Live backup

A backup technique that avoids the need for bulk data transfers by continuously updating the repository with changes to the source file system. This is similar to CDP but with longer retention periods and RPOs being available. Live backups perform byte level change updates whereas batch backups perform block level change updates.

Master node

The machine that controls the actions of other nodes within the Ops Center Protector network.

Metadata Store (MDS)

Records metadata that describes items that are held in repositories. The MDS supports indexing of stored data, thus enabling fast searches when locating data for restoration.

Mover

Defines the type of data movement operation to be performed between source and destination nodes, during the creation of a data flow. Batch movers perform block level data transfers on a scheduled basis, whereas continuous movers perform byte level data transfers on a near-continuous basis.

Node Group

Multiple machines of the same type can be assigned to one or more node groups. Within the Data Flow page, you can assign policies to nodes within node groups en-mass.

Policy

A configurable data protection objective that is mapped to machines or groups, and to the data management agents that implement the policy. Multiple policies can be assigned to a single node.

Recovery Point Objective (RPO)

The frequency at which a backup will occur. This governs the point in time to which data can be recovered should a restore be needed.

Replication

An operation where a copy of the data is created in another local or remote location automatically.

Repository

A destination node that stores data from one or more source nodes. The Ops Center Protector Repository supports batch backup, archiving, and versioning policies.

Snapshot (Thin Image)

A point in time copy of the data that is based on references to the original data.

Source node

Any node (server, workstation or virtual machine) that hosts data to be protected by Ops Center Protector. The source node has an Active Data Change Agent, which is responsible for monitoring the host file system and performing the relevant actions defined by the policies. Nodes need to be configured as a source node if they need to transfer locally stored data to a destination node, or implement data tracking, blocking and auditing functions. A node can be both a source and destination simultaneously.

Synchronous replication

Transactions are transferred to the remote storage device immediately and the write operation is signaled as completed only once data is confirmed as written to both primary and secondary volumes. Synchronous replication is optimal for connections with high efficiency.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1{,}000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1{,}000^3$ bytes
1 terabyte (TB)	1,000 GB or $1{,}000^4$ bytes
1 petabyte (PB)	1,000 TB or $1{,}000^5$ bytes
1 exabyte (EB)	1,000 PB or $1{,}000^6$ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1{,}024^2$ bytes
1 GB	1,024 MB or $1{,}024^3$ bytes
1 TB	1,024 GB or $1{,}024^4$ bytes
1 PB	1,024 TB or $1{,}024^5$ bytes
1 EB	1,024 PB or $1{,}024^6$ bytes

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact