White Paper

Dell PowerProtect Data Manager: Oracle RMAN Agent Backup and Recovery

Abstract

This white paper focuses on protecting an Oracle database using Dell PowerProtect Data Manager, the next-generation data protection platform.

October 2022

Revisions

Date	Description
July 2019	Initial release
February 2021	Revised
May 2021	Revised
July 2022	Revised for PowerProtect Data Manager version 19.11 release
October 2022	Revised for PowerProtect Data Manager version 19.12 release

Acknowledgments

Author: Vinod Kumar Kumaresan and Chetan Padhy

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third-party content is updated by the relevant third parties, this document will be revised accordingly.

Table of contents

Executive summary

Dell PowerProtect Data Manager software is an enterprise solution that provides software-defined data protection, deduplication, operational agility, self-service, and IT governance. PowerProtect Data Manager enables the transformation from traditional centralized protection to an IT-as-a-service model based on a self-service design. This design ensures that you can enforce compliance and other business rules, even when backup responsibilities are decentralized to individual database administrators and application administrators. Data Manager key features include:

- Software-defined data protection with integrated deduplication, replication, and reuse
- Data backup and recovery self-service operations from native applications that are combined with central IT governance
- Multicloud optimization with integrated cloud tiering
- SaaS-based monitoring and reporting

The modern, services-based architecture provides ease of deployment, scaling, and upgrading of Data Manager and integrates multiple data protection products within the Dell Data Protection portfolio to enable data protection as a service. Data Manager enables the protection of traditional workloads including Oracle, Exchange, SQL, SAP HANA, and file systems as well as Kubernetes containers and virtual environments.

Audience

This white paper is intended for customers, partners, and employees who want to better understand, evaluate, and explore Data Manager Integration with Oracle RMAN agent. Familiarity with PowerProtect Data Manager and DD series appliances is required.

Introduction

Data Manager integrates with the Oracle RMAN agent to check and monitor backup compliance against protection policies. The Oracle RMAN agent enables an application administrator to protect and recover the Oracle data on the application host.

1.1 Solution components

This section discusses PowerProtect Data Manager and Oracle RMAN agent backup components.

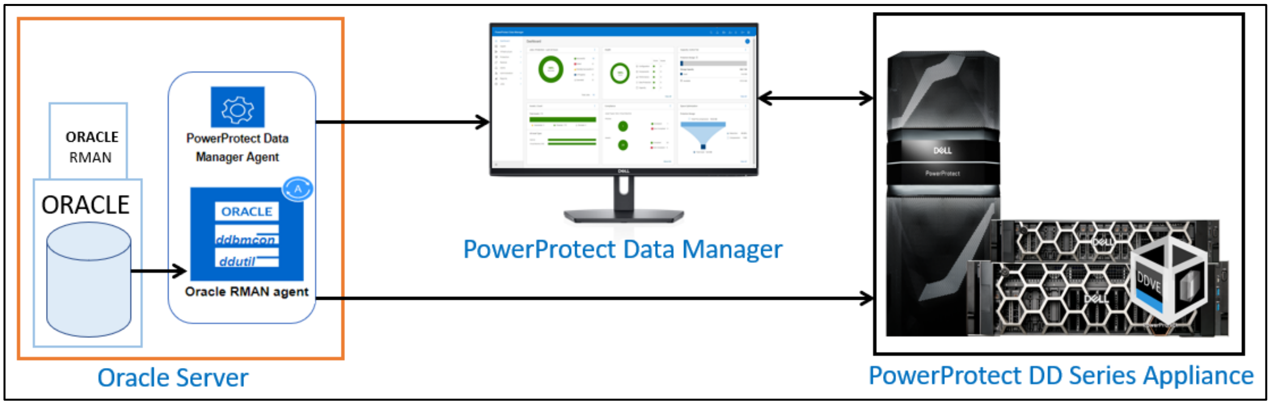

ORACLE RMAN
ORACLE
PowerProtect Data Manager Agent
ORACLE
ddbmcon
ddutil
Oracle RMAN agent
Oracle Server
PowerProtect Data Manager
DDVE
PowerProtect DD Series Appliance

Figure 1 PowerProtect Data Manager Oracle RMAN agent solution components overview

1.2 PowerProtect DD series appliances

Dell PowerProtect DD series appliances and older Data Domain systems are disk-based appliances that run DDOS to provide inline deduplication for data protection and disaster recovery (DR) in the enterprise environment. DD series appliances vary in storage capacity and data throughput. Systems are typically configured with expansion enclosures that add storage space.

DDOS features include:

- **Data integrity**: The DDOS Data Invulnerability Architecture protects against data loss from hardware and software failures.
- **Data Deduplication**: The file system deduplicates data by identifying redundant data during each backup and storing unique data once.
- **Restore operations**: File restore operations create little or no contention with backup or other restore operations.
- **DD Replicator**: DD Replicator sets up and manages the replication of backup data between two protection systems.
- **Multipath and load balancing**: In a Fibre Channel multipath configuration, multiple paths are established between a protection system and a backup server or backup destination array. When multiple paths are present, the system automatically balances the backup load between the available paths.
- **High availability**: The High Availability (HA) feature lets you configure two protection systems as an Active-Standby pair, providing redundancy in the event of a system failure. HA keeps the active and standby systems that are synchronized, so that if the active node were to fail due to hardware or software issues, the standby node can take over services and continue where the failing node left off.

- **Random I/O handling**: The random I/O optimizations in DDOS provide improved performance for applications and use cases that generate larger amounts of random read and write operations than sequential read and write operations.
- **System Administrator access**: System administrators can access the system for configuration and management using a command-line interface (CLI) or a user interface (UI).
- **Licensed features**: Feature licenses allow you to purchase only those features you intend to use. Some examples of features that require licenses are DD Boost, and capacity on demand (storage capacity increases).
- **Storage environment integration**: DDOS systems integrate easily into existing data centers.

1.3 PowerProtect Data Manager

PowerProtect Data Manager software is an enterprise solution that provides software-defined data protection, deduplication, operational agility, self-service, and IT governance.

Data Manager enables the transformation from traditional centralized protection to an IT-as-a-service model based on a self-service design. This design ensures that you can enforce compliance and other business rules, even when backup responsibilities are decentralized to individual database administrators and application administrators.

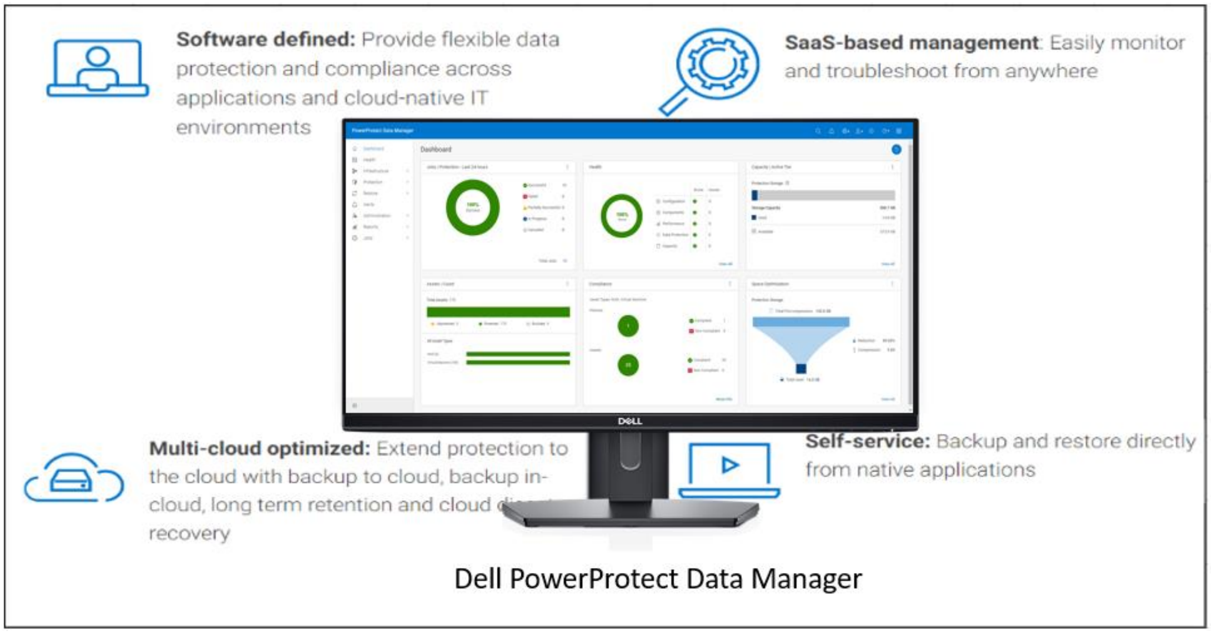

Software defined: Provide flexible data protection and compliance across applications and cloud-native IT environments
SaaS-based management: Easily monitor and troubleshoot from anywhere
Multi-cloud optimized: Extend protection to the cloud with backup to cloud, backup in-cloud, long term retention and cloud direct recovery
Self-service: Backup and restore directly from native applications
Dell PowerProtect Data Manager

Figure 2 PowerProtect Data Manager highlights

Data Manager key features include:

- Software-defined data protection with integrated deduplication, replication, and reuse
- Data backup and recovery self-service operations from native applications that are combined with central IT governance
- Multicloud optimization with integrated cloud tiering
- SaaS-based monitoring and reporting
- Modern services-based architecture for ease of deployment, scaling, and upgrading.

1.4 Oracle RMAN agent

The Oracle application agent allows an application administrator to protect and recover the Oracle RMAN application data on the application host. Oracle RMAN agent can be used alone by DBA to backup using RMAN scripts and transfer the data to DD series appliance. Data Manager agent integrates with the RMAN agent to check and monitor backup compliance against protection policies. Oracle RMAN agent has two main components:

- **ddbmcon**: The ddbmcon program is installed with the Oracle RMAN agent software and enables the Data Manager monitoring, management, and analysis of Oracle RMAN agent backups. During the Oracle RMAN agent installation, the ddbmcon program is installed in the $RMAN_HOME/bin directory. You cannot run the ddbmcon program manually. The program is only run by the PowerProtect Data Manager agent.
- **ddutil**: The ddutil program is also installed with the Oracle RMAN agent software. It enables DD series appliance command-line interface, which is used to create the lockbox, verify connectivity with DD series appliance, display or delete a backup, and perform various other manual operations that can be useful during self-service backup. For more details about command-line options, see the document *PowerProtect Data Manager for Oracle RMAN Agent User Guide.*

1.5 PowerProtect Data Manager agent

PowerProtect Data Manager agent is installed with Oracle RMAN agent. With the help of PowerProtect Data Manager agent administrators can monitor, manage, or analyze the Oracle RMAN agent backups on AIX or Linux. PowerProtect Data Manager agent can create and manage replication copies based on the protection policies. PowerProtect Data Manager agent performs these operations whether the backup is created by the DBA or by the Data Manager centralized backup scheduler. Data Manager with Oracle integration supports the following features and functionalities:

- Data Manager Centralized protection policy.
- Data Manager Self-Service protection policy.
- Oracle databases can be discovered by Data Manager automatically.
- Single Protection Policy (PLC) to manage the entire life cycle of data protection for Oracle database
- Centralized Oracle restore and recovery from the PowerProtect Data Manager UI
- Support of Oracle RMAN agent with Oracle 21c by the current version of PowerProtect Data Manager and the two previous versions. See PowerProtect Data Manager Compatibility Matrix for more details.

1.6 Oracle Recovery Manager server

Recovery Manager (RMAN) is an Oracle utility that can backup, restore, and recover database files. The product is a feature of the Oracle database server and does not require separate installation.

Recovery Manager is a client/server application that uses database server sessions to perform backup and recovery. It stores metadata about its operations in the control file of the target database and, optionally, in a recovery catalog schema in an Oracle database. You can invoke RMAN as a command-line executable from the operating system prompt or use some RMAN features through the Enterprise Manager UI.

Installation of the Oracle RMAN agent

Data Manager can manage and monitor data protection and replication for Oracle assets through integration with the Oracle RMAN agent. For configuring Data Manager with Oracle RMAN agent, the following two software components must be installed on the Oracle database host:

- Oracle RMAN Agent
- PowerProtect Data Manager agent

In an Oracle Real Application Clusters (RAC) environment, the Oracle RMAN agent and the PowerProtect Data Manager agent must be installed on each node in the Oracle RAC environment.

1.7 Deployment requirements

Ensure that you meet the prerequisites before you add an Oracle asset.

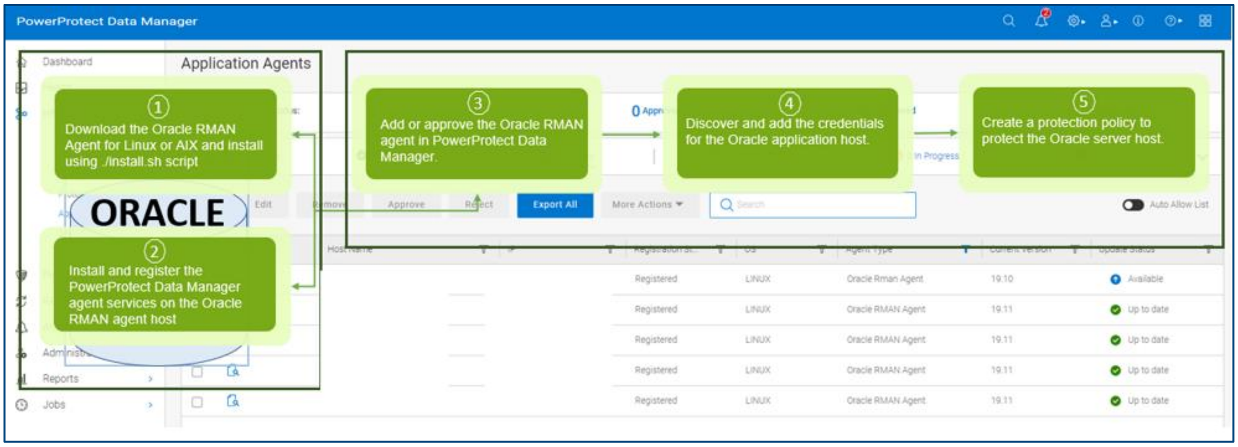
Verify that the environment meets the following requirements:

- Ensure that all clocks on both the Oracle host and Data Manager are time-synced to the local NTP server to ensure discovery of the backups
- Ensure that the Oracle host and the Data Manager network can see and resolve each other
- Ensure that port 7000 and 8443 is open on the Oracle host. Port 111,2049 and 2052 are open between DD series appliance and Oracle hosts
- Ensure that DD series appliances are added as the protection storage

1.8 Install and configure Oracle RMAN agent

1.8.1 Roadmap to protect Oracle database with PowerProtect Data Manager

Data Manager can manage and monitor data protection and replication for Oracle assets through integration with the Oracle RMAN agent.

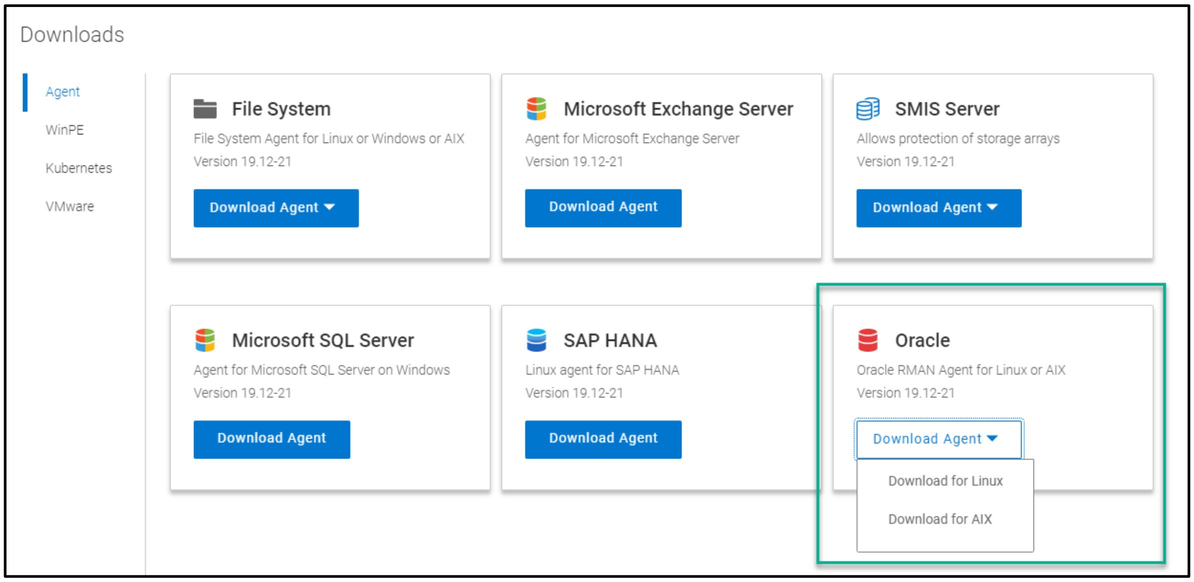


1. Download the Oracle RMAN Agent for Linux or AIX and install using ./install.sh script
2. Install and register the PowerProtect Data Manager agent services on the Oracle RMAN agent host
3. Add or approve the Oracle RMAN agent in PowerProtect Data Manager.
4. Discover and add the credentials for the Oracle application host.
5. Create a protection policy to protect the Oracle server host.

Host Name	Registration St...	OS	Agent Type	Current Version	Update Status
	Registered	LINUX	Oracle Rman Agent	19.10	Available
	Registered	LINUX	Oracle RMAN Agent	19.11	Up to date
	Registered	LINUX	Oracle RMAN Agent	19.11	Up to date
	Registered	LINUX	Oracle RMAN Agent	19.11	Up to date
	Registered	LINUX	Oracle RMAN Agent	19.11	Up to date

Figure 3 Oracle RMAN agent install and configure workflow

Oracle RMAN agent can be download from **Dashboard > System Settings**> **Downloads**.



File System
File System Agent for Linux or Windows or AIX
Version 19.12-21

Microsoft Exchange Server
Agent for Microsoft Exchange Server
Version 19.12-21

SMIS Server
Allows protection of storage arrays
Version 19.12-21

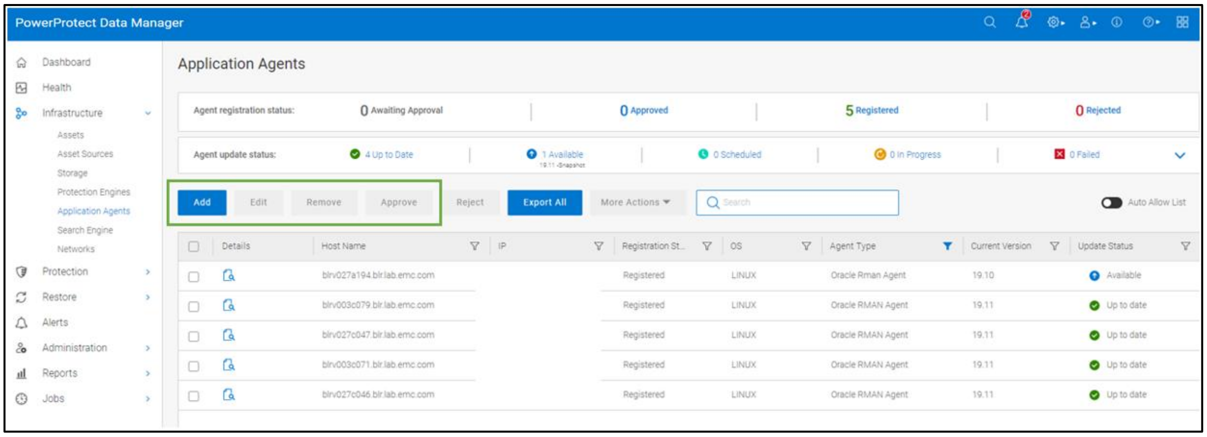
Microsoft SQL Server
Agent for Microsoft SQL Server on Windows
Version 19.12-21

SAP HANA
Linux agent for SAP HANA
Version 19.12-21

Oracle
Oracle RMAN Agent for Linux or AIX
Version 19.12-21

Figure 4 Oracle RMAN agent download

Use this option to add or approve the Oracle RMAN agent from **Infrastructure > Application Agents**.



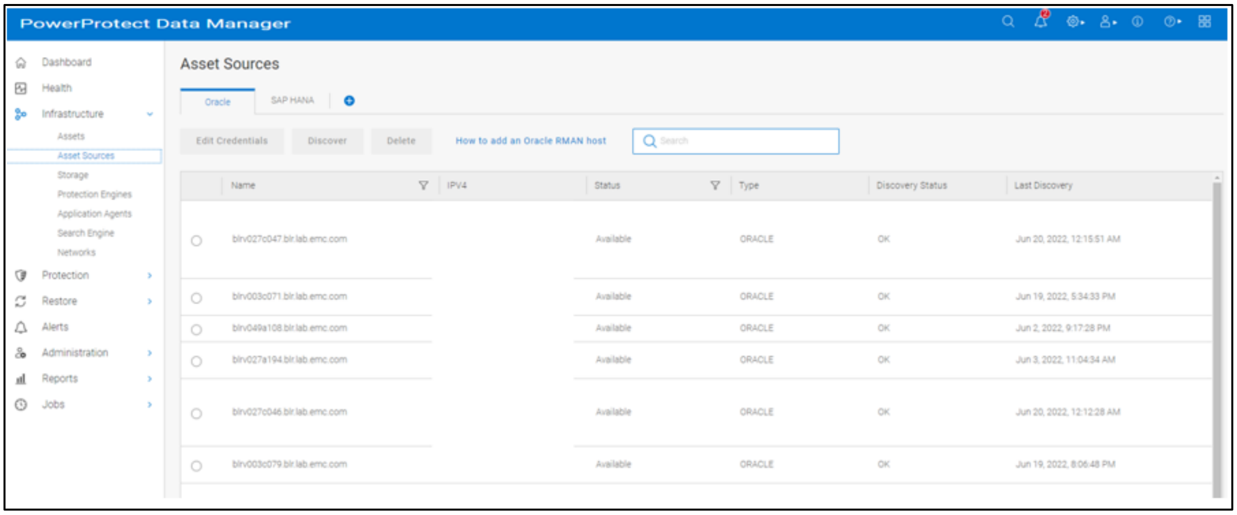
Application Agents

Agent registration status: 0 Awaiting Approval | 0 Approved | 5 Registered | 0 Rejected

Agent update status: 4 Up to Date | 1 Available 19.11 -Snapshot | 0 Scheduled | 0 In Progress | 0 Failed

□	Details	Host Name	IP	Registration St...	OS	Agent Type	Current Version	Update Status
□		blrv027a194.blr.lab.emc.com		Registered	LINUX	Oracle Rman Agent	19.10	Available
□		blrv003c079.blr.lab.emc.com		Registered	LINUX	Oracle RMAN Agent	19.11	Up to date
□		blrv027c047.blr.lab.emc.com		Registered	LINUX	Oracle RMAN Agent	19.11	Up to date
□		blrv003c071.blr.lab.emc.com		Registered	LINUX	Oracle RMAN Agent	19.11	Up to date
□		blrv027c046.blr.lab.emc.com		Registered	LINUX	Oracle RMAN Agent	19.11	Up to date

After you register an application host with PowerProtect Data Manager, you can use the **Asset Sources** window to discover an application host and modify the application host credentials. You must add credentials to the Oracle database so that PowerProtect Data Manager can access the database to create backups.

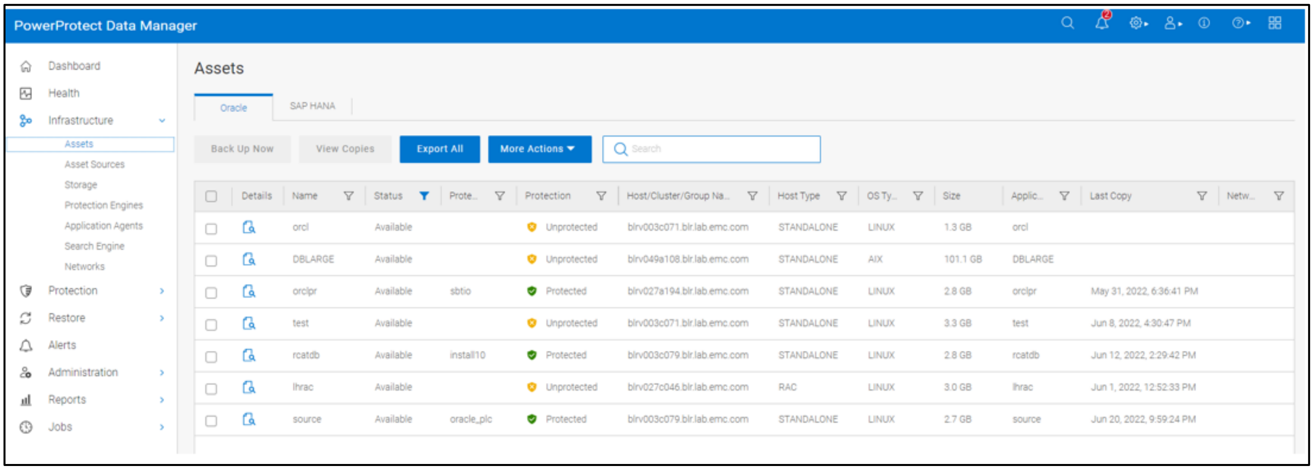


Asset Sources

Name	IPV4	Status	Type	Discovery Status	Last Discovery
blrv027c047.blr.lab.emc.com		Available	ORACLE	OK	Jun 20, 2022, 12:15:51 AM
blrv003c071.blr.lab.emc.com		Available	ORACLE	OK	Jun 19, 2022, 5:34:33 PM
blrv049a108.blr.lab.emc.com		Available	ORACLE	OK	Jun 2, 2022, 9:17:28 PM
blrv027a194.blr.lab.emc.com		Available	ORACLE	OK	Jun 3, 2022, 11:04:34 AM
blrv027c046.blr.lab.emc.com		Available	ORACLE	OK	Jun 20, 2022, 12:12:28 AM
blrv003c079.blr.lab.emc.com		Available	ORACLE	OK	Jun 19, 2022, 8:06:48 PM

Note: Starting with release 19.9, a new Oracle database discovery method is supported, which uses the `pmon` process without a dependence on `/etc/oratab` entries. The `/etc/oratab` file entries have the highest precedence for the discovery of Oracle database resources on the system, which enables the PowerProtect Data Manager operations.

Once the asset discovery is complete, the Oracle database assets are discovered in the **Infrastructure > Assets** section.



Assets

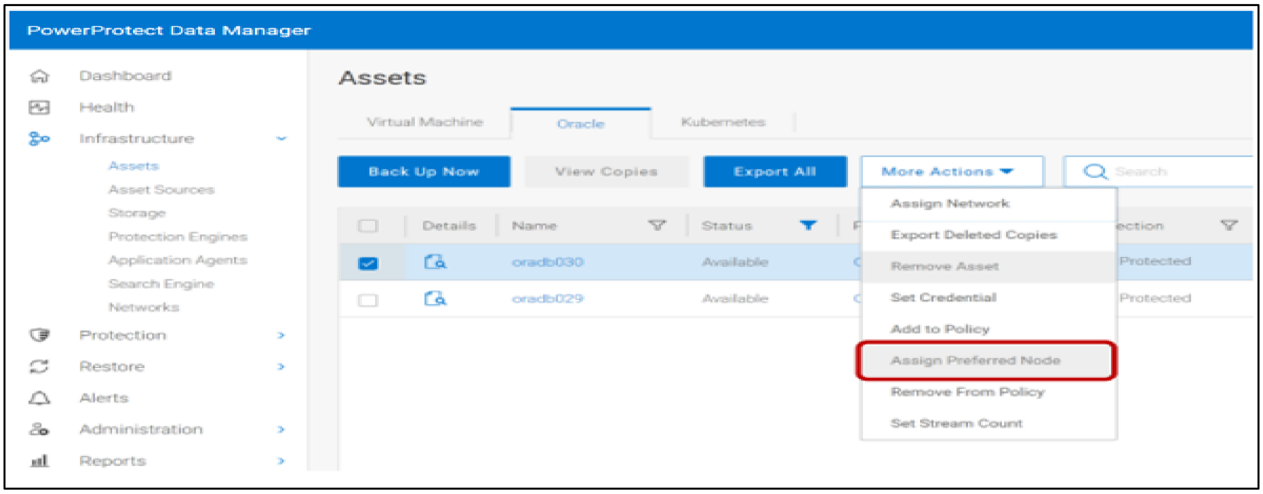
☐	Details	Name	Status	Prote...	Protection	Host/Cluster/Group Na...	Host Type	OS Ty...	Size	Applic...	Last Copy	Netw...
☐		orcl	Available		Unprotected	blrv003c071.blr.lab.emc.com	STANDALONE	LINUX	1.3 GB	orcl		
☐		DBLARGE	Available		Unprotected	blrv049a108.blr.lab.emc.com	STANDALONE	AIX	101.1 GB	DBLARGE		
☐		orclpr	Available	sbtio	Protected	blrv027a194.blr.lab.emc.com	STANDALONE	LINUX	2.8 GB	orclpr	May 31, 2022, 6:36:41 PM	
☐		test	Available		Unprotected	blrv003c071.blr.lab.emc.com	STANDALONE	LINUX	3.3 GB	test	Jun 8, 2022, 4:30:47 PM	
☐		rcatdb	Available	install10	Protected	blrv003c079.blr.lab.emc.com	STANDALONE	LINUX	2.8 GB	rcatdb	Jun 12, 2022, 2:29:42 PM	
☐		lhrac	Available		Unprotected	blrv027c046.blr.lab.emc.com	RAC	LINUX	3.0 GB	lhrac	Jun 1, 2022, 12:52:33 PM	
☐		source	Available	oracle_plc	Protected	blrv003c079.blr.lab.emc.com	STANDALONE	LINUX	2.7 GB	source	Jun 20, 2022, 9:59:24 PM	

Figure 5 Oracle assets section

See the *PowerProtect Data Manager for Oracle RMAN Agent User Guide.* for more details about how to install and configure Oracle RMAN agent with PowerProtect Data Manager.

1.8.2 Setting Oracle RAC Preferred Node Using Data Manager

Starting with Data Manager 19.12, you can set the Oracle RAC preferred node in the Data Manager user interface. This applies to a single/multi-asset based Oracle RAC environment.



☐	Details	Name	Status	F	ection
☑		oradb030	Available	C	Protected
☐		oradb029	Available	C	Protected

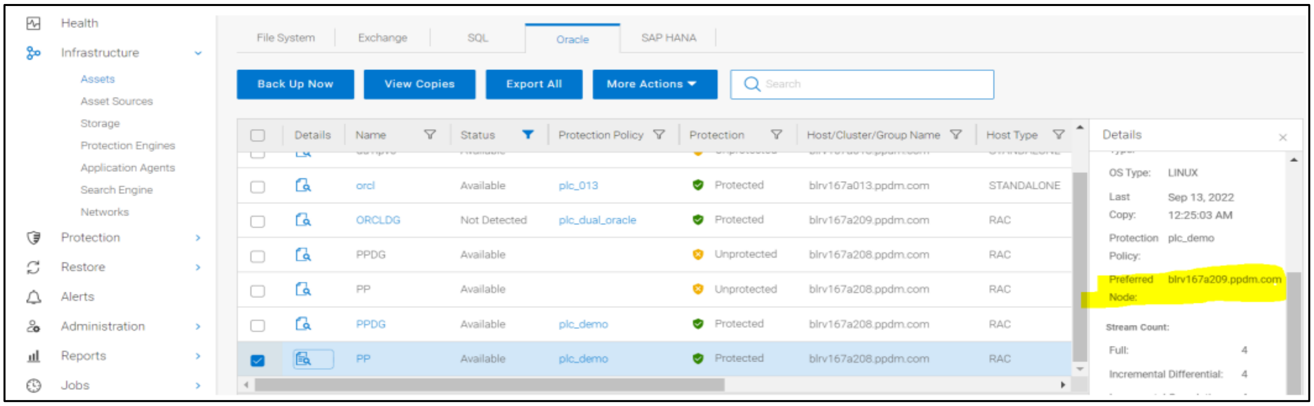
Note: The Preferred Node value from the config file gets migrated when the Data Manager server is upgraded from an older version. Adding/removing RAC nodes will automatically adjust the configuration.

The following are Oracle RAC preferred node UI features:

- The preferred node can be set with different AUTHs
- Any change in Preferred Node will take effect at the next triggered backup
- Preferred Node from UI takes precedence
- Decommissioning the preferred node will force Data Manager to use any other available node
- Shutting down the database or stopping the RMAN agent service on the preferred node will result in backup failure
- Works with both Linux and AIX platforms
- Compatible with older RMAN agent

2.2.2.1 Asset Details

After setting the Oracle preferred node in the Data Manager user interface, you can view which host is set as the Oracle RAC Preferred Node from Oracle Asset details.



□	Details	Name	Status	Protection Policy	Protection	Host/Cluster/Group Name	Host Type
□		orcl	Available	plc_013	Protected	blrv167a013.ppdm.com	STANDALONE
□		ORCLDG	Not Detected	plc_dual_oracle	Protected	blrv167a209.ppdm.com	RAC
□		PPDG	Available		Unprotected	blrv167a208.ppdm.com	RAC
□		PP	Available		Unprotected	blrv167a208.ppdm.com	RAC
□		PPDG	Available	plc_demo	Protected	blrv167a208.ppdm.com	RAC
☑		PP	Available	plc_demo	Protected	blrv167a208.ppdm.com	RAC

Details

OS Type: LINUX
Last Copy: Sep 13, 2022 12:25:03 AM
Protection Policy: plc_demo
Preferred Node: blrv167a209.ppdm.com

Stream Count:
Full: 4
Incremental Differential: 4

1.9 Authentication requirements

The Oracle RMAN agent program ddbmcon handles all communication between the Oracle RMAN agent and Data Manager. When the ddbmcon program performs discovery, backup, or deletion operations, it connects to the Oracle database. The following authentication methods are supported:

1. Database authentication
2. Oracle wallet authentication
3. Operating system authentication

The ddbmcon program tries all these authentication methods for each Oracle database instance. The program reports a connection error if it cannot connect to the database instance by using any of these methods. If one of these methods succeeds, the ddbmcon program ignores the other authentication methods and goes to retrieve the information as used by the Data Manager.

Ensure that you enable one of these three authentication methods for the ddbmcon program. For maximum ease of use, it is recommended that you enable the operating system authentication method. Both the database and Oracle wallet authentication methods require additional configuration steps on the Oracle host and parameter settings in the configuration file `rman_agent.cfg.` It is installed in the `$RMAN_AGENT_HOME/config` directory.

After you have set the authentication method, you can select the same in Data Manager UI during discovery and Policy Lifecycle (PLC) creation. For detailed instructions, see the *PowerProtect Data Manager for Oracle RMAN agent User Guide*.

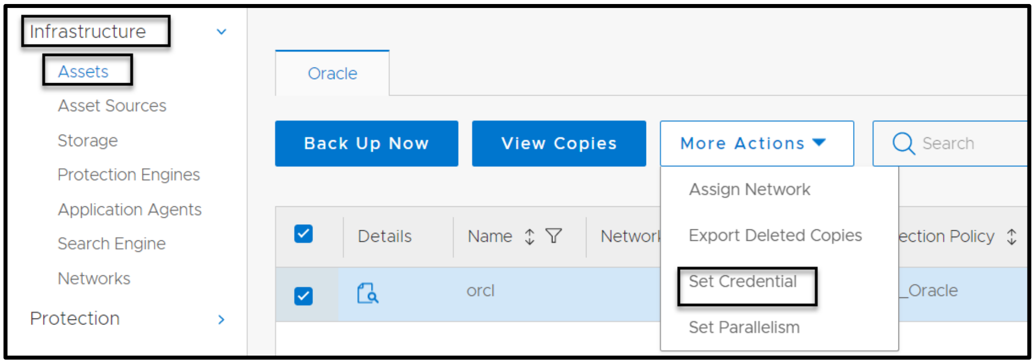
1.9.1 Setting Oracle assets credentials in Data Manager

Starting with Data Manager 19.7, you can optionally add and remove the credentials for one or more Oracle database assets simultaneously in the Data Manager UI. Following are few important points regarding adding credentials:

- You can only add the asset-level credentials when the Oracle host agent version is 19.7 or later.
- You can add Oracle assets with different Oracle operating system users or groups from the same asset source into a single protection policy.
- You can add multiple Oracle assets from multiple asset sources into a single protection policy.
- The Oracle assets can be associated with multiple credential types, where the supported database credential types are Oracle, Database User, and Wallet and the supported RMAN catalog credential types are Database User and Wallet.

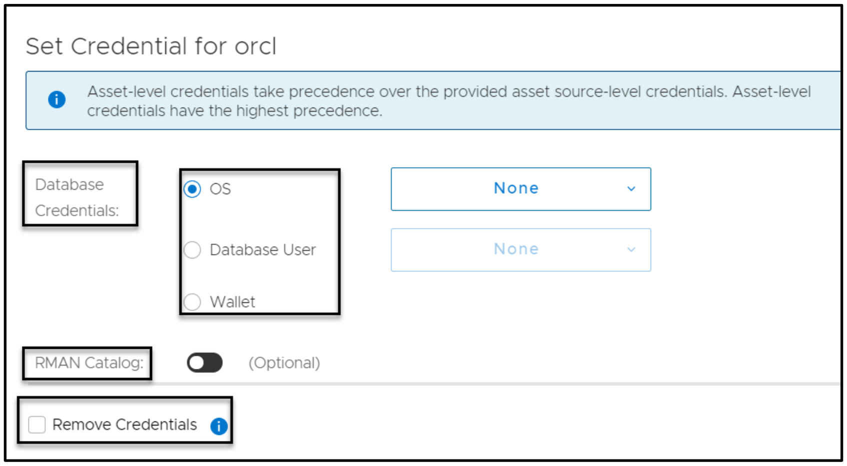
Use the following procedure to add or remove the credentials for the Oracle database assets.

1. In the Data Manager UI, select **Infrastructure** > **Assets**, and click the **Oracle** tab.
2. Select one or more assets by clicking the checkbox next to each required asset name.
3. Select More Actions > Set Credential.



4. In the **Set Credential** dialog box, add or remove the credentials for the selected Oracle assets:

To add the credentials for the assets, specify the required **operating system**, **Database User**, or **Wallet** settings for **Database Credentials**. When the asset is associated with an RMAN catalog, you can also specify the RMAN catalog credentials through the **Database User** or **Wallet** settings for **RMAN Catalog**.



Set Credential for orcl

Asset-level credentials take precedence over the provided asset source-level credentials. Asset-level credentials have the highest precedence.

Database Credentials: ● OS ○ Database User ○ Wallet

None

None

RMAN Catalog: (Optional)

□ Remove Credentials

Note: You can specify both the database credentials and RMAN catalog credentials in the Set Credential dialog box.

To remove the credentials for the assets, select **Remove Credentials**.

5. Click **Save** in the **Set Credential** dialog box.

Results

When you save the newly added credentials in the dialog box, Data Manager triggers an autoconfiguration job for the credential update in the respective clients.

After you add the credentials by using this procedure, the asset-level credentials are used for the selected assets during Oracle centralized backups, overriding the policy-level credentials.

Note: Credentials that you set at the asset level and asset source level supersede the credentials that you set at the protection policy level. Credentials at the asset level have the highest precedence.

1.10 Verification of database connectivity

You can run the ddutil command as the root user with the appropriate -v option to verify the connectivity from the ddbmcon program to the Oracle database. For detailed instruction check *PowerProtect Data Manager for Oracle RMAN agent User Guide*. The following subtopics describe the three supported levels of verification with the `ddutil -v` command:

1.10.1 System verification

To perform the system verification, run the ddutil -v system command as the root user.

The `ddutil -v system` command verifies the connectivity to the Oracle instances.

1.10.2 Asset verification

To perform the asset verification, run the `ddutil -v asset` command as the root user.

The command verifies the ability to read the Oracle database objects and provides similar output to the system verification command.

1.10.3 RMAN verification

To perform the RMAN verification, run the `ddutil -v rman` command as the root user. This verification is required only if you use an RMAN catalog.

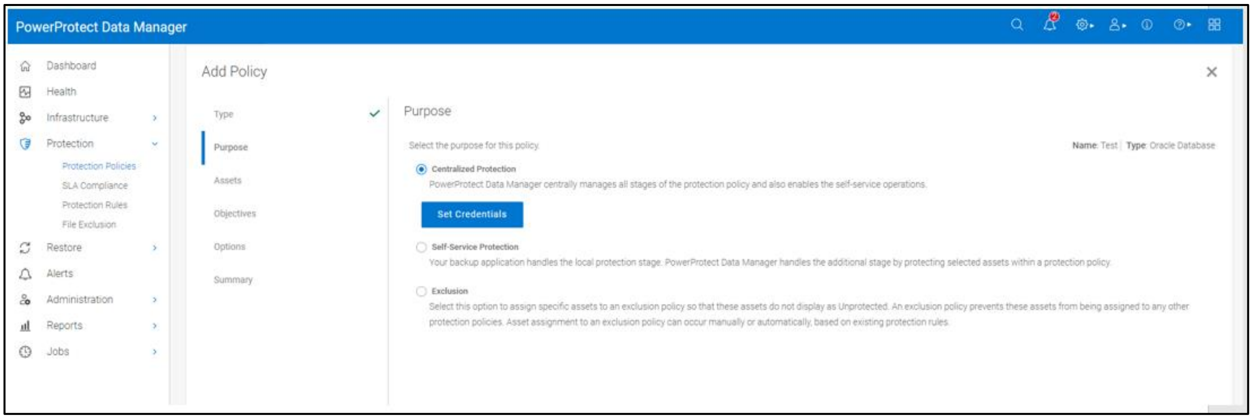
The ddutil -v rman command tests whether the ddbmcon program can connect to the target database and catalog database through an RMAN script, as required to perform an active deletion of Oracle backups.

Note: Database authentication or Oracle wallet authentication can be used to connect to an RMAN catalog. Operating system authentication cannot be used with the RMAN catalog. For more details, check *PowerProtect Data Manager Oracle RMAN agent User Guide*.

PowerProtect Data Manager protection policy

With Data Manager, the Oracle database protection task has been transferred from a backup administrator to the Oracle database administrator (or Oracle database owner). Data Manager creates Oracle database backups and manages remote replication copies based on the Protection Policy (PLC). Data Manager performs the backup and replication operations based on the protection policy and governed by the SLA. Oracle databases can be backed up through:

- Automatic backup by the Centralized Protection policy.
- Manual backup by the Oracle database administrator and governed by the Self-Service Protection policy.



Add Policy

Purpose

Select the purpose for this policy.

Name: Test | **Type**: Oracle Database

● **Centralized Protection**
PowerProtect Data Manager centrally manages all stages of the protection policy and also enables the self-service operations.

○ **Self-Service Protection**
Your backup application handles the local protection stage. PowerProtect Data Manager handles the additional stage by protecting selected assets within a protection policy.

○ **Exclusion**
Select this option to assign specific assets to an exclusion policy so that these assets do not display as Unprotected. An exclusion policy prevents these assets from being assigned to any other protection policies. Asset assignment to an exclusion policy can occur manually or automatically, based on existing protection rules.

Figure 6 Types of protection policies

Note:

- When you create protection policies for RAC databases, ensure that all nodes in the RAC environment are powered on and registered at the time of the protection policy creation. Otherwise, the protection might fail.
- RAC Node that will do the backup must be set by the DBA after the installation is complete using `IS_RAC_BACKUP_NODE =NODENAME` in `rman_agent.cfg` located in `$RMAN_AGENT_HOME/config`.
- For Oracle Instance Group assets, ensure that the maximum length of the hostname plus storage unit is 59. There are no special character limitations.
- Before you perform a backup on a weekly or monthly schedule from the protection policy, ensure that the Data Manager time zone is set to the local time zone. If the Data Manager time zone is not set to the local time zone, the weekly or monthly backup still runs but is triggered based on the Data Manager time zone.
- If applicable, complete all the virtual network configuration tasks before you assign any virtual networks to the protection policy. The *PowerProtect Data Manager Administration and User Guide* provides more information.

1.11 Centralized protection policy

When Data Manager admin creates a protection policy for Oracle databases, the centralized protection option enables the Data Manager to centrally manage the entire life cycle of data protection operations for the Oracle databases.

The data protection attributes are specified when the centralized protection policy is created: Type, purpose, credentials, assets, schedule, replication schedule, options, and SLA. After the protection policy creation is complete, the lockbox is automatically created for source and replication DD series appliance.

Attributes	**Attribute option**
Type of application	Oracle database
Purpose of the Protection Policy	Centralized Protection
Application Login Credentials	<Specify or select application login credentials>
Application Assets	<Select the desired Oracle databases>
Schedule	Backup Level

	Retention Period Backup start and end time <Specify or select the desired SLA> Replication schedule
Options	<Advanced options>
Summary	Check the option and Save.

1.12 Self-Service protection policy

When Data Manager admin creates a protection policy for Oracle databases, the self-service protection option enables the data owner to perform the manual backup operation from the command-line interface. The Data Manager prepares the environment to accommodate the manual backup operations. A few examples of these operations are creating a DD user with a password, creating a DD storage unit, enforcing the backup data retention. After the protection policy creation is completed, the lockbox is automatically created for source and replication DD series appliance.

The data protection attributes are specified when the self-service protection policy is created: Type, purpose, assets, retention, replication schedule, and SLA. Note that only the retention period and replication schedule can be specified in the schedule attribute in the self-service protection policy.

Attributes	**Attribute option**
Type of application	Oracle database
Purpose of the Protection Policy	Self-Service Protection
Application Assets	<Select the desired Oracle databases>
Schedule	Retention Period <Specify or select the desired SLA> Replication schedule
Summary	Check the option and Save.

Note: Data Manager can create and manage replication copies based on the protection policies. Data Manager performs these operations whether the backup is created by self-service policy or by the centralized backup policy.

Because Data Manager controls the replication, when the Oracle RMAN agent is deployed with Data Manager, the following self-service replication operations are disabled:

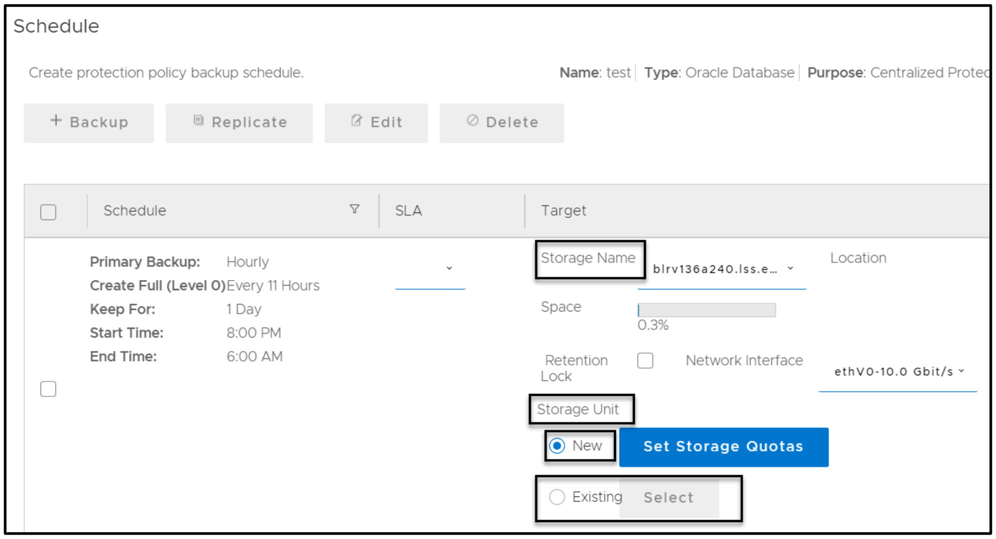
- Creation of multiple backup copies with the `RMAN BACKUP COPIES` command.
- MTree replication to create backup copies on a secondary DD series appliance.
- You can restore from replicated copies of backups that were performed with a previous version of Oracle RMAN agent.

- When you perform a self-service backup managed by Data Manager, the Data Manager protection policy settings for the given database override the target protection storage settings that are specified in the RMAN backup script. These settings include the Data Domain server hostname and storage unit name.

1.13 Storage unit consideration

When you create a protection policy, the Data Manager software can either create or reuse a storage unit on the specified DD system backup host, subject to limitations. All subsequent backups of assets in that protection policy go to this storage unit.

The storage unit set using Data Manager protection policy overrides the backup host and storage unit information from the script with the backup host and storage unit information from Data Manager. Both the manual backups and scheduled backups of these Oracle databases are sent to this storage unit. To display the storage units and their assigned databases on the Oracle RMAN agent host, run the `ddutil -s` command.



Schedule

Create protection policy backup schedule.

Name: test | **Type**: Oracle Database | **Purpose**: Centralized Protec

Primary Backup: Hourly
Create Full (Level 0) Every 11 Hours
Keep For: 1 Day
Start Time: 8:00 PM
End Time: 6:00 AM

Storage Name: blrv136a240.lss.e...
Location
Space: 0.3%
Retention Lock: □
Network Interface: ethV0-10.0 Gbit/s
Storage Unit
● New
○ Existing

Figure 7 Storage unit setup

Note: Oracle RMAN agent 19.6 and earlier releases do not support the mapping structure that allows protection policies to share the same storage unit. Backups of databases that are protected by older agents and different policies cannot target the same storage unit. Data Manager 19.7 and later releases contain logic that detects this condition when you add or edit a protection policy. The policy rules alert you to the conflict and fall back to the previous structure that mapped one policy to one storage unit. You can resolve this condition by upgrading the Oracle RMAN agent to release 19.7 or later.

1.14 Top-level directory changes

Only if the auto backup is enabled for the protected database and you have created a self-service protection policy for Oracle, complete the required top-level directory changes:

1. Log in to the Oracle host as an Oracle user.
2. To obtain the top-level directory information, run the following command:

```
/home/oracle/opt/dpsapps/rmanagent/ddutil -s
```

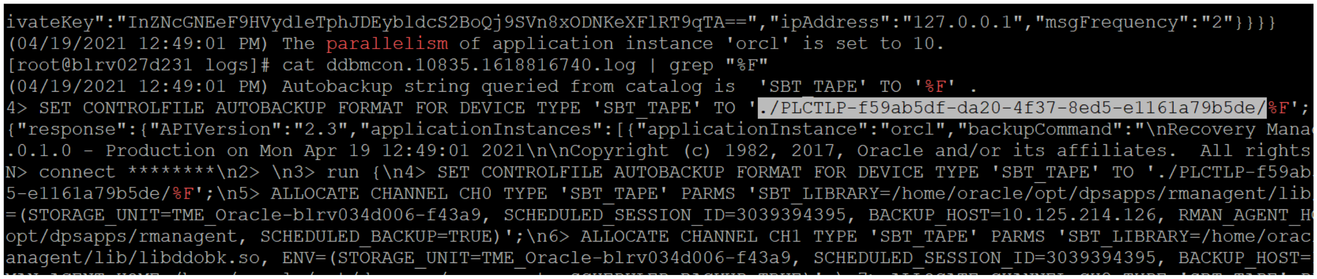
3. To complete the changes to the control file configuration for the Oracle database, run the following RMAN command, which includes the top-level pathname from the `ddutil -s` command output:

```
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE 'SBT_TAPE' TO './

< Top-Level Path>/%F';
```

After you run this command, all the database backup pieces including the auto backups will be written under the top-level directory created in the storage unit.

Note: This setting is required only if the backup is done using the self-service protection policy. For centralized protection policy, this setting is done automatically by Data Manager as seen in screenshot below.



```
ivateKey":"InZNcGNEeF9HVydleTphJDEybldcS2BoQj9SVn8xODNKeXFlRT9qTA==","ipAddress":"127.0.0.1","msgFrequency":"2"}}}}
(04/19/2021 12:49:01 PM) The parallelism of application instance 'orcl' is set to 10.
[root@blrv027d231 logs]# cat ddbmcon.10835.1618816740.log | grep "%F"
(04/19/2021 12:49:01 PM) Autobackup string queried from catalog is  'SBT_TAPE' TO '%F' .
4> SET CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE 'SBT_TAPE' TO './PLCTLP-f59ab5df-da20-4f37-8ed5-e1161a79b5de/%F';
{"response":{"APIVersion":"2.3","applicationInstances":[{"applicationInstance":"orcl","backupCommand":"\nRecovery Mana
.0.1.0 - Production on Mon Apr 19 12:49:01 2021\n\nCopyright (c) 1982, 2017, Oracle and/or its affiliates.  All rights
N> connect ********\n2> \n3> run {\n4> SET CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE 'SBT_TAPE' TO './PLCTLP-f59ab
5-e1161a79b5de/%F';\n5> ALLOCATE CHANNEL CH0 TYPE 'SBT_TAPE' PARMS 'SBT_LIBRARY=/home/oracle/opt/dpsapps/rmanagent/lib
=(STORAGE_UNIT=TME_Oracle-blrv034d006-f43a9, SCHEDULED_SESSION_ID=3039394395, BACKUP_HOST=10.125.214.126, RMAN_AGENT_H
opt/dpsapps/rmanagent, SCHEDULED_BACKUP=TRUE)';\n6> ALLOCATE CHANNEL CH1 TYPE 'SBT_TAPE' PARMS 'SBT_LIBRARY=/home/orac
anagent/lib/libddobk.so, ENV=(STORAGE_UNIT=TME_Oracle-blrv034d006-f43a9, SCHEDULED_SESSION_ID=3039394395, BACKUP_HOST=
```

Figure 8 Log of centralized protection policy showing automatic setup of the top-level directory

Oracle RMAN agent backup workflow

Oracle Database can be backed up using centralized protection policy and self-service protection policy. Based on the type of protection policy backup workflow changes. This section discusses workflow in each case.

1.15 Centralized protection backup

In the centralized protection backup, the entire backup life cycle is governed by Data Manager. There is no need for the DBA to create any RMAN scripts as all parameters are passed by Data Manager agent as per the backup options selected during protection policy creation.

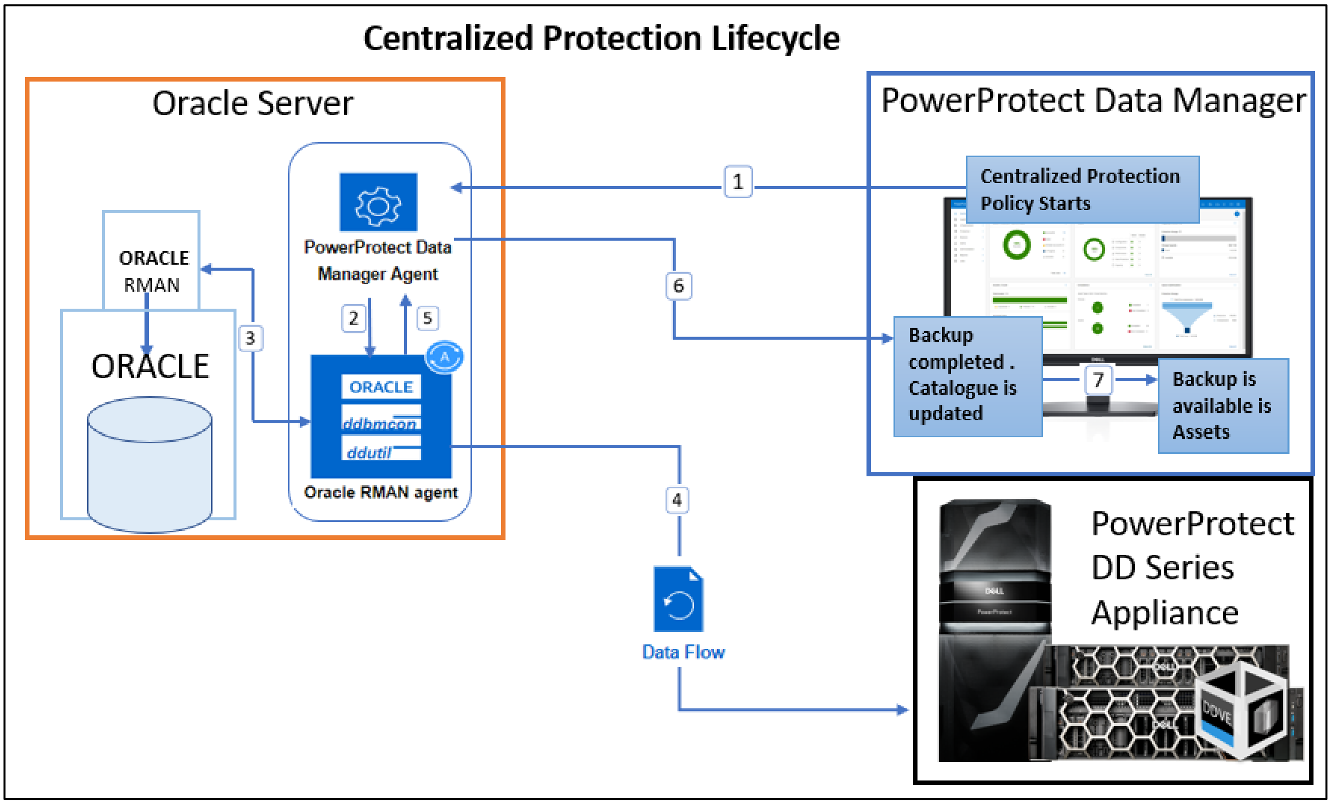

Centralized Protection Lifecycle
Oracle Server
ORACLE
RMAN
ORACLE
PowerProtect Data Manager Agent
ORACLE
ddbmcon
ddutil
Oracle RMAN agent
1
2
3
4
5
6
7
PowerProtect Data Manager
Centralized Protection Policy Starts
Backup completed . Catalogue is updated
Backup is available is Assets
Data Flow
PowerProtect DD Series Appliance

Figure 9 Centralized protection policy backup workflow

The backup workflow is as follows:

1. As scheduled, the centralized protection policy starts from Data Manager, and it communicates to the Agent service on Oracle client to start the backup process.
2. The agent service starts the Oracle RMAN agent and passes the information of assets that needs be backed up.
3. The Oracle RMAN agent connects to Oracle RMAN using the authentication provided, and Oracle RMAN starts Oracle databases backup and send it to Oracle RMAN agent.
4. The Oracle RMAN agent transfers the backup to DD series appliance, the number of streams used to transfer the data can vary based on the parallelism option selected for each asset.
5. When the data transfer is finished, Oracle RMAN agent sends the backup completion status to Agent service.
6. The agent service updates the backup status to Data Manager, and the backup catalog is updated with this information.

7. If the backup was successful, the backup copy is displayed in **Infrastructure > Assets > View Copies**.

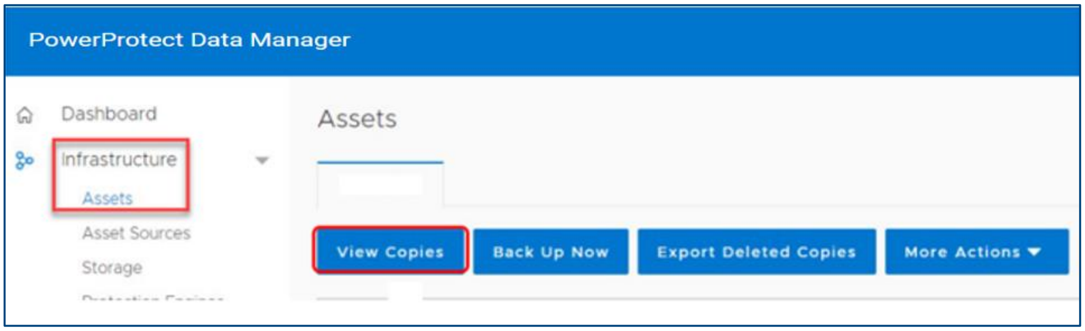
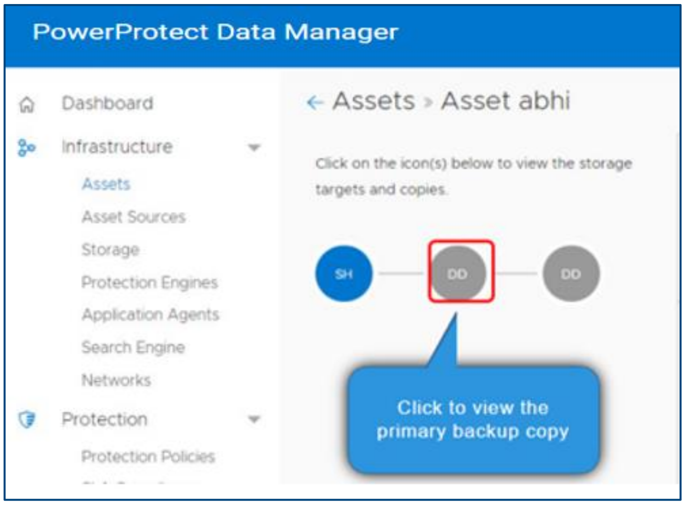


Figure 10 Check backup copies



Click on the icon(s) below to view the storage targets and copies.

Figure 11 Checking available backup copies of Oracle host

1.15.1 Backup levels for centralized protection

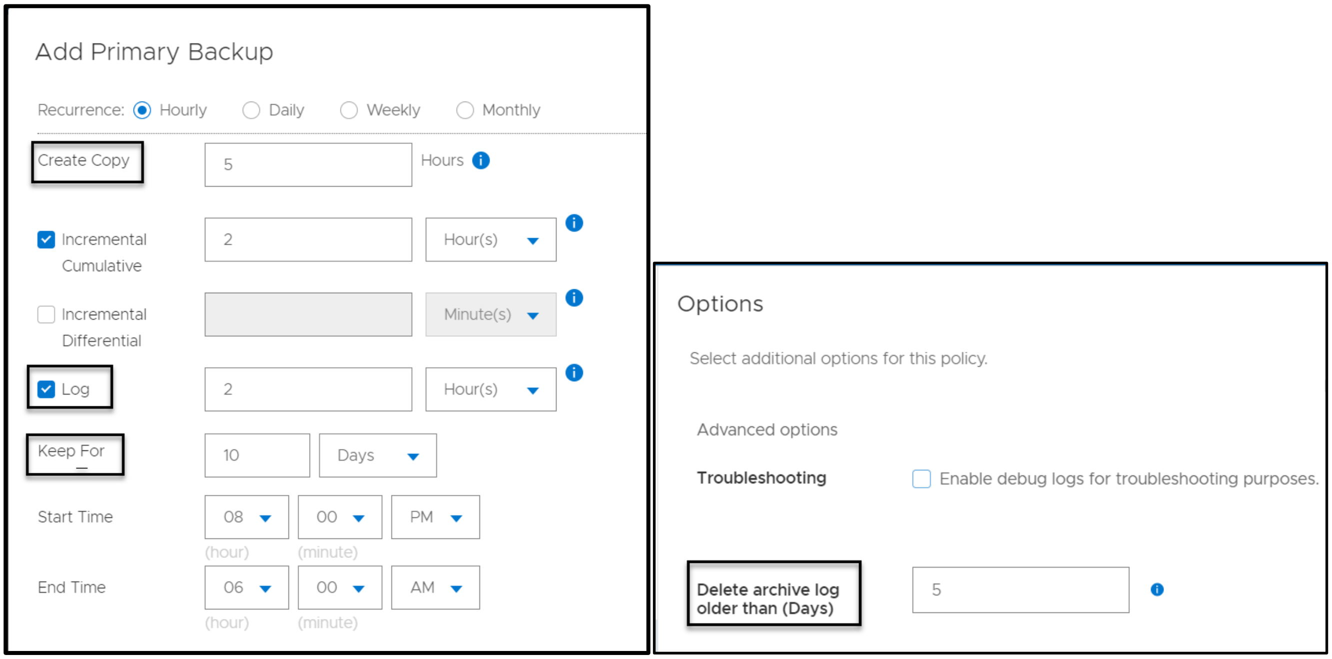
The backup levels available during centralized protection policy are explained in table below:

Backup level	Description	Minimum frequency recommendation
Full	Backs up all the data.	Daily
Incremental Cumulative	Backs up only the data that has changed since the last full backup.	12 hours
Incremental Differential	Backs up only the data that has changed since the last incremental differential backup, or the last full backup if there are no other incremental differential backups.	6 hours

Log	Backs up the archived logs	30 minutes

You can define in what intervals these backups should run. Option to delete the logs after successful backup is also available under **Options**->**Delete archive log older than (Days).**

Note: To delete the archived logs that are older than the specified number of days, ensure that the log backup option is enabled when you create the backup schedule. To delete the archived logs immediately after the log backups, set the flag option in `rman_agent.file`, available in the directory `$RMAN_AGENT_HOME/config` with the entry `DELETE_ARCHIVE_LOGS=TRUE`.



Add Primary Backup

Recurrence: ● Hourly ○ Daily ○ Weekly ○ Monthly

Create Copy: 5 Hours

☑ Incremental Cumulative: 2 Hour(s)

☐ Incremental Differential: Minute(s)

☑ Log: 2 Hour(s)

Keep For: 10 Days

Start Time: 08 (hour) 00 (minute) PM

End Time: 06 (hour) 00 (minute) AM

Options

Select additional options for this policy.

Advanced options

Troubleshooting: ☐ Enable debug logs for troubleshooting purposes.

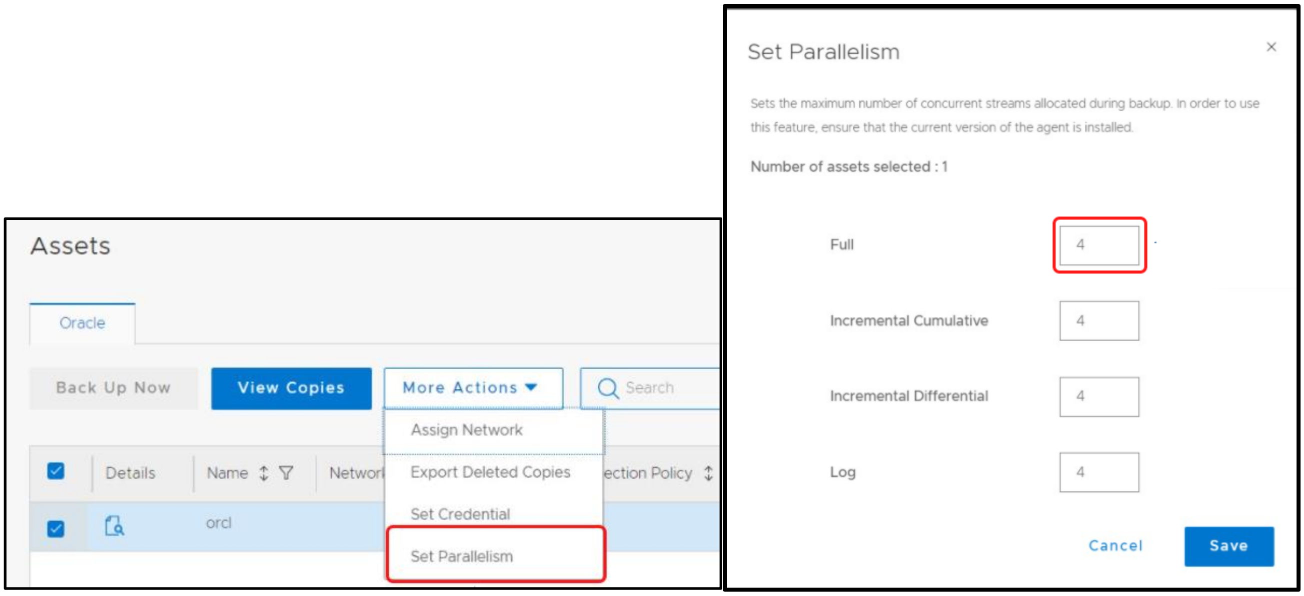
Delete archive log older than (Days): 5

1.15.2 Enable multistream backup

To enable multistream Oracle backups for a centralized protection policy, you can set the parallelism value as the number of Oracle backup channels in the Data Manager UI. As an alternative, you can set the `PARALLELISM` parameter in the configuration file `rman_agent.cfg`.

Determine the required number of Oracle backup channels based on the system capacity. With the parallelism setting, you can override the number of backup channels from the Oracle RMAN agent client side. In the Data Manager UI, perform the following steps to set the parallelism for multistream backups:

1. Select Infrastructure > Assets > Oracle.
2. Select the Oracle asset. Select **More Actions** > **Set Parallelism**.



Set Parallelism

Sets the maximum number of concurrent streams allocated during backup. In order to use this feature, ensure that the current version of the agent is installed.

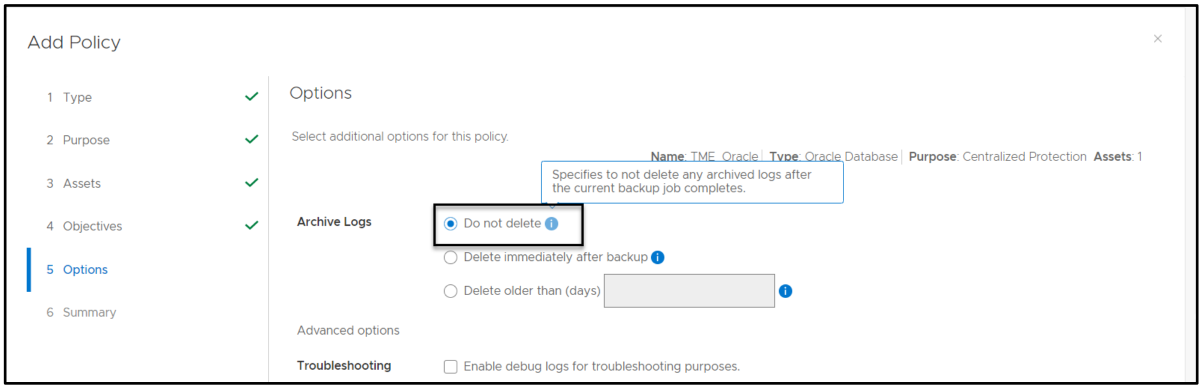
Number of assets selected : 1

Full	4
Incremental Cumulative	4
Incremental Differential	4
Log	4

1.15.3 Archive log backup

While setting up the centralized protection policy under **Options** page, select the settings for archive logs deletion from the production Oracle host using one of the following options:

- **Do not delete**: Select this option to prevent the deletion of archived logs during backups. To delete the archived logs, the database administrator must run the delete command manually



Options

Select additional options for this policy.

Name: TME_Oracle | **Type**: Oracle Database | **Purpose**: Centralized Protection **Assets**: 1

Specifies to not delete any archived logs after the current backup job completes.

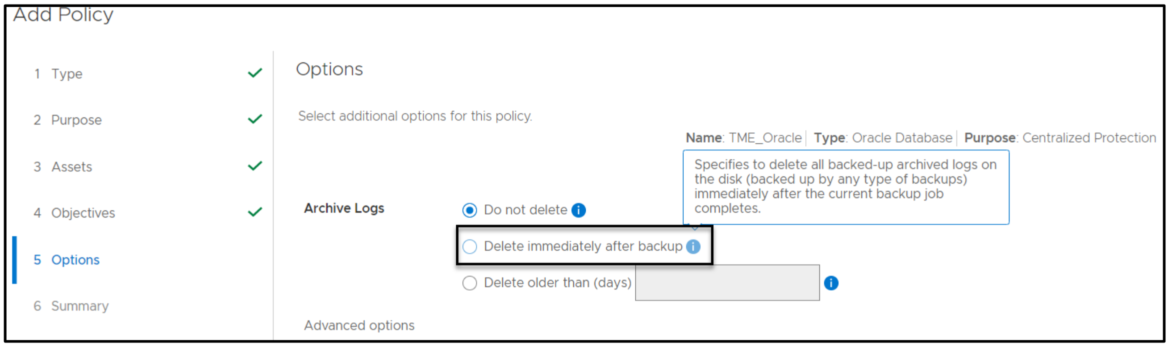
Archive Logs ● Do not delete
○ Delete immediately after backup
○ Delete older than (days)

Advanced options

Troubleshooting □ Enable debug logs for troubleshooting purposes.

Figure 12 Archive log setting (1)

- **Delete immediately after backup**: Select this option to enable the deletion of archived logs immediately after all the backup types that are performed through the protection policy



Add Policy

1 Type ✓
2 Purpose ✓
3 Assets ✓
4 Objectives ✓
5 Options
6 Summary

Options

Select additional options for this policy.

Name: TME_Oracle | **Type**: Oracle Database | **Purpose**: Centralized Protection

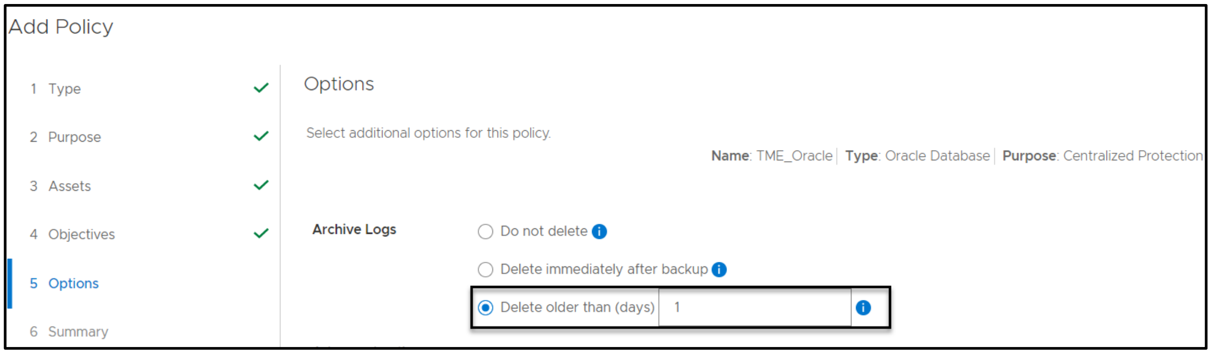
Specifies to delete all backed-up archived logs on the disk (backed up by any type of backups) immediately after the current backup job completes.

Archive Logs
● Do not delete ⓘ
○ Delete immediately after backup ⓘ
○ Delete older than (days) ⓘ

Advanced options

Figure 13 Archive log setting (2)

- **Delete older than (days)**: Select this option to enable the deletion of the available archived logs that are older than the specified number of days, for all the backup types that are performed through the protection policy. Set the number of days after which the archived logs are deleted.



Add Policy

1 Type ✓
2 Purpose ✓
3 Assets ✓
4 Objectives ✓
5 Options
6 Summary

Options

Select additional options for this policy.

Name: TME_Oracle | **Type**: Oracle Database | **Purpose**: Centralized Protection

Archive Logs
○ Do not delete ⓘ
○ Delete immediately after backup ⓘ
● Delete older than (days) 1 ⓘ

Figure 14 Archive log setting (3)

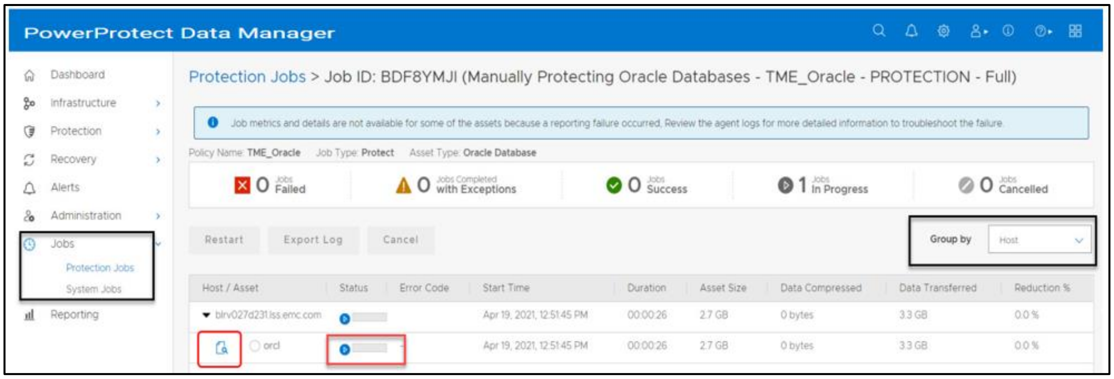
1.15.4 Monitoring jobs and task for centralized protection policy

Use the **Protection Jobs** and **System Jobs** windows in the PowerProtect Data Manager UI to monitor the status of Oracle backup and to view details about failed, in progress, or recently completed jobs. To perform analysis or troubleshooting, you can view a detailed log of a failed job or task.

You can also view details for a job group and individual jobs and tasks. When you click the job ID next to the job entry, the **Job ID Summary** window displays the information for only this job group, job, or task. This information enables you to monitor the status of individual jobs and tasks, view job and task details, and perform certain operations on jobs and tasks.

Use the **Group by** filter in the **Job ID Summary** window to view the application assets that are protected for all hosts in a protection job group. You can filter jobs by host for Microsoft SQL, Exchange databases, Oracle databases, File Systems, and SAP HANA databases.

To filter application assets by hostname, click the job ID for the job group, and then select **Group by** > **Host**. To display all assets in the job group, select **Group by** > **None**.



Protection Jobs > Job ID: BDF8YMJI (Manually Protecting Oracle Databases - TME_Oracle - PROTECTION - Full)

Job metrics and details are not available for some of the assets because a reporting failure occurred. Review the agent logs for more detailed information to troubleshoot the failure.

Policy Name: **TME_Oracle** Job Type: **Protect** Asset Type: **Oracle Database**

0 Jobs Failed | 0 Jobs Completed with Exceptions | 0 Jobs Success | 1 Jobs In Progress | 0 Jobs Cancelled

Group by: Host

Host / Asset	Status	Error Code	Start Time	Duration	Asset Size	Data Compressed	Data Transferred	Reduction %
blrv027d231.lss.emc.com			Apr 19, 2021, 12:51:45 PM	00:00:26	2.7 GB	0 bytes	3.3 GB	0.0 %
orcl			Apr 19, 2021, 12:51:45 PM	00:00:26	2.7 GB	0 bytes	3.3 GB	0.0 %

Figure 15 Monitoring backup using filter option Group by Host

Note: For Oracle hosts, the **Group by >Host** selection shows the job progress as 0% and then successful 100% once completed which means it will not show real-time progress. This is a known limitation with Oracle database backups. For more filter options and details, see the document *PowerProtect Data Manager Administration and User Guide.*

1.16 Self-service protection backup

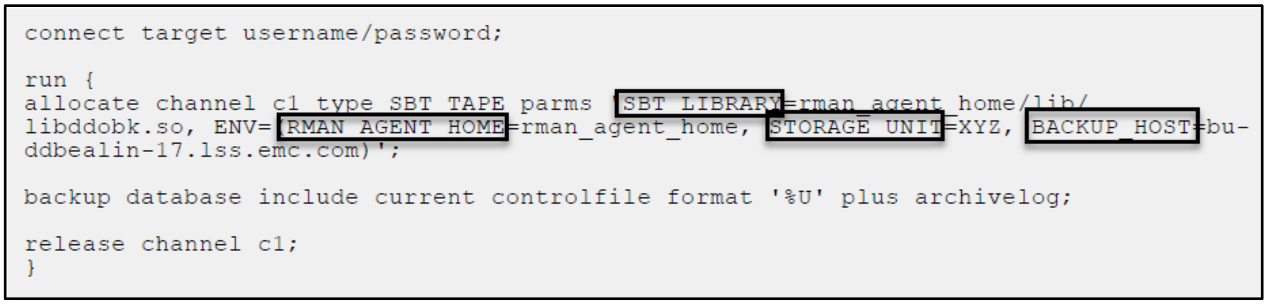
When the Data Manager admin creates a protection policy for Oracle databases, the self-service protection option enables the data owner to perform the manual backup operation from the command-line interface. In this option, the DBA creates their own RMAN scripts to back up the data directly to the DD series appliance using only the Oracle RMAN agent and Data Manager agent service to do the discovery every hour to check if the RMAN catalog is updated with any new backups.

To identify the storage unit and DD series appliance hostname, run the `ddutil -s` command on the Oracle client. Only if the autobackup is enabled for the protected database and you have created a self-service protection policy for Oracle, complete the required top-level directory changes as explained in Top-level directory changes.

Following information is needed before performing the self-service protection of Oracle database. These parameters are required in the RMAN scripts:

- `SBT_LIBRARY`-The installation directory of the DD Boost library file - `libddobk.so`. The default installation directory is: `$RMAN_AGENT_HOME/lib`
- `STORAGE_UNIT`-The name of DD series appliance storage unit, which is created automatically when you add the protection policy. To display the storage units and their assigned databases on the Oracle RMAN agent host, run the `ddutil -s` command
- `BACKUP_HOST`-The hostname or IP address of the DD series appliance.
- `RMAN_AGENT_HOME`-The Oracle RMAN Agent software installation directory.

The following example shows an RMAN script that performs a full backup of the database and its archive logs:



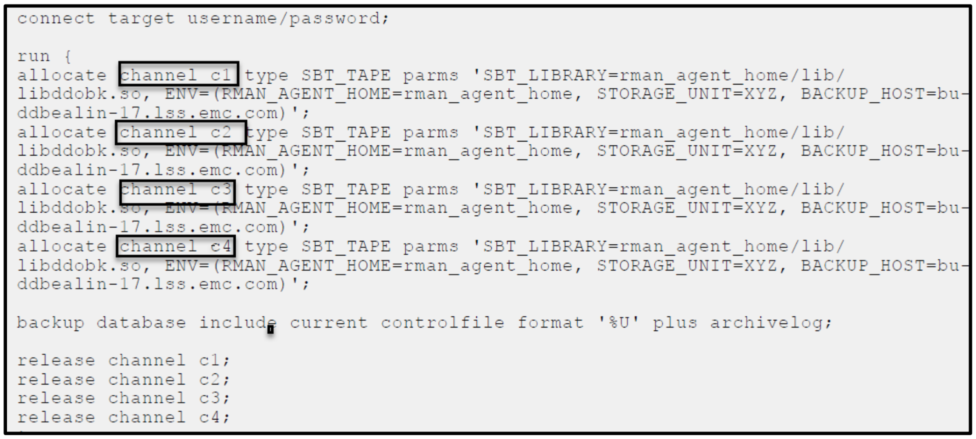
```
connect target username/password;

run {
allocate channel c1 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so, ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ, BACKUP_HOST=bu-
ddbealin-17.lss.emc.com)';

backup database include current controlfile format '%U' plus archivelog;

release channel c1;
}
```

Figure 16 Script for full backup and its archive logs with one channel



```
connect target username/password;

run {
allocate channel c1 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so, ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ, BACKUP_HOST=bu-
ddbealin-17.lss.emc.com)';
allocate channel c2 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so, ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ, BACKUP_HOST=bu-
ddbealin-17.lss.emc.com)';
allocate channel c3 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so, ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ, BACKUP_HOST=bu-
ddbealin-17.lss.emc.com)';
allocate channel c4 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so, ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ, BACKUP_HOST=bu-
ddbealin-17.lss.emc.com)';

backup database include current controlfile format '%U' plus archivelog;

release channel c1;
release channel c2;
release channel c3;
release channel c4;
```

Figure 17 Allocated more channels for parallel backup using RMAN script

The backup workflow is as follows:

1. The DBA starts the Oracle RMAN script and script starts the Oracle database backup.
2. Oracle RMAN connects with Oracle RMAN agent to start the data transfer.
3. The Oracle RMAN agent opens connections with the DD series appliance and starts the data transfer.
4. When the backup is completed, the backup catalog information is passed from Oracle RMAN agent to Data manager agent service on client.
5. The PowerProtect Data Manager agent updates Data Manager with the backup status.
6. Data Manager updates the catalog information and sets the retention for oracle backup as per the self-service policy.
7. You can now see the backup copies under **Infrastructure** > **Assets** > **View Copies**.

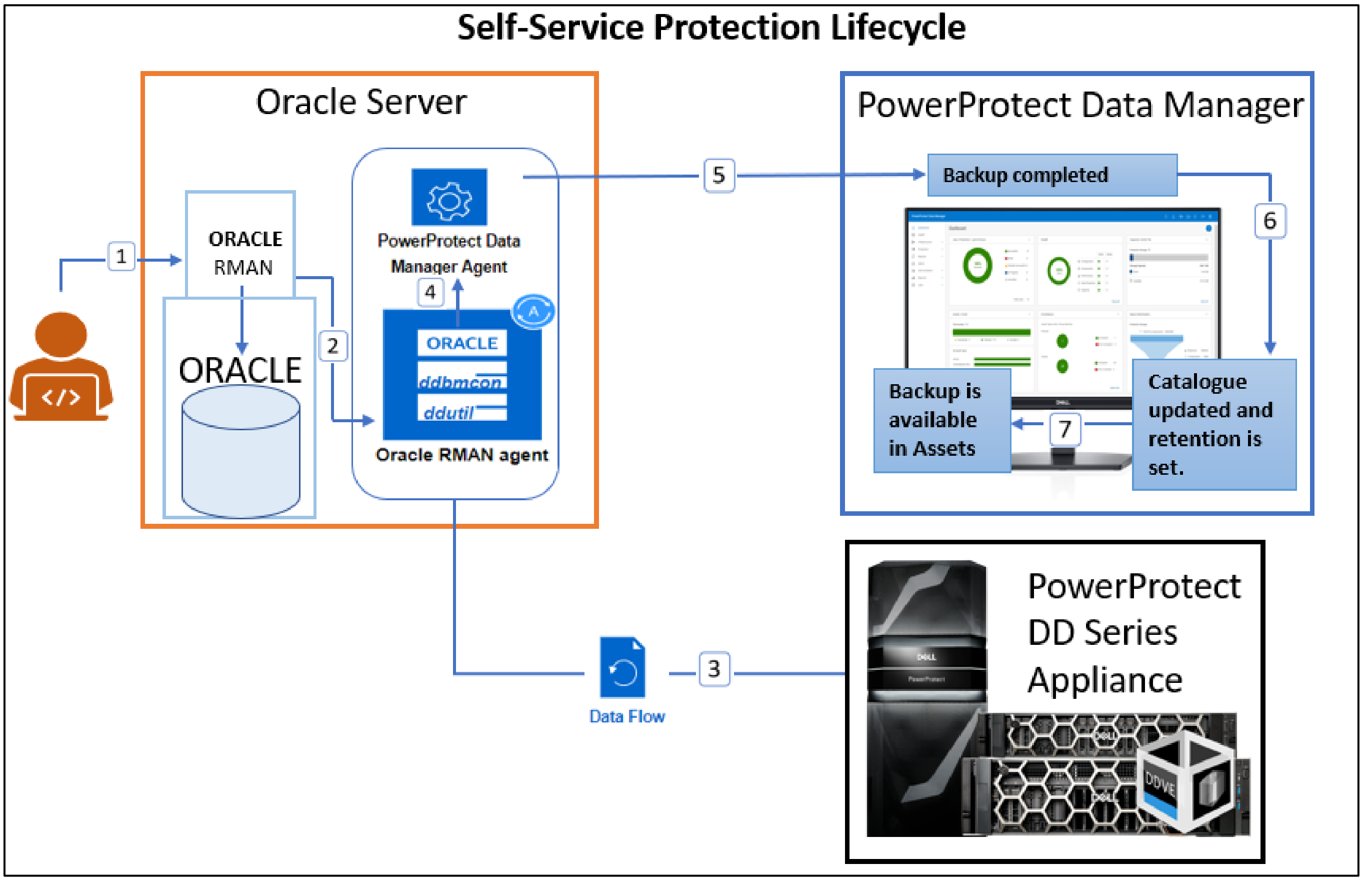

Self-Service Protection Lifecycle
Oracle Server
1
ORACLE RMAN
ORACLE
2
PowerProtect Data Manager Agent
4
ORACLE
ddbmcon
ddutil
Oracle RMAN agent
5
PowerProtect Data Manager
Backup completed
6
Backup is available in Assets
7
Catalogue updated and retention is set.
Data Flow
3
PowerProtect DD Series Appliance

Figure 18 Self-service protection policy backup workflow

Oracle RMAN recovery

With Data Manager, you can perform centralized restore and recovery of Oracle backups from Data Manager UI or an Oracle database recovery on the Oracle database host by running one of the supported Oracle backup or recovery tools.

- Oracle Recovery Manager (RMAN) with rman command
- Oracle Enterprise Manager UI

1.17 Centralized restore and recovery of Oracle backups

Starting with Data Manager 19.11, you can perform centralized Oracle restore and recovery from the PowerProtect Data Manager UI when the Oracle Server data has been backed up through a protection policy. The centralized Oracle restore and recovery operations include the restore and recovery of a full online database, restore of only archive logs, and disaster recovery of an entire database.

You can perform the following types of centralized restore and recovery of Oracle Server backups:

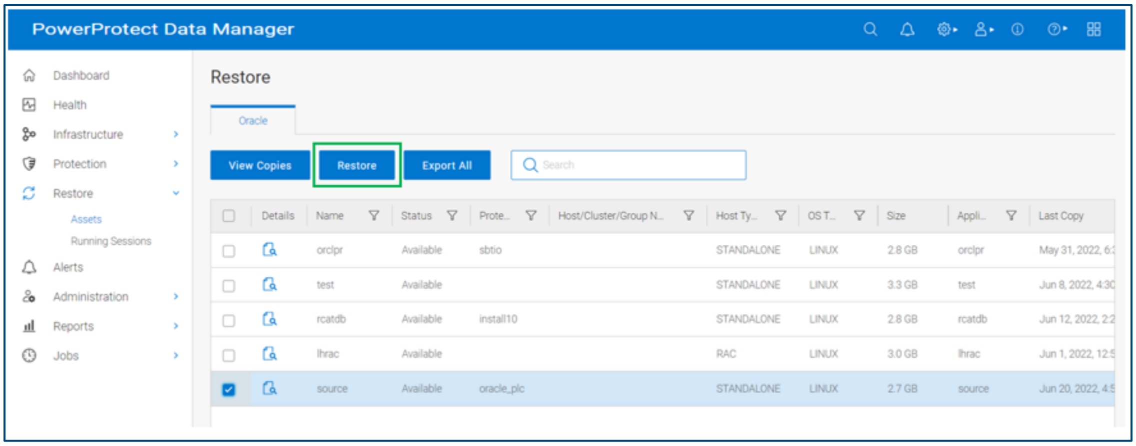
- Centralized restore and recovery of a full online database without restore of the control file
- Centralized restore of only archive logs without restore of the control file
- Centralized disaster recovery of an entire database, including the spfile and control file

Using a centralized restore from the PowerProtect Data Manager UI, you can restore the Oracle database or archive logs for a single asset. You can perform the centralized restore to either the original Oracle Server host or an alternate host with the following requirements:

- The Oracle RMAN agent software must be installed and configured on the alternate host.
- The alternate host must be an Oracle server host that is a discovered asset of PowerProtect Data Manager.

Optionally, you can select to perform a dry run of any centralized restore and recovery operation to either the original host or an alternate host. The dry run option creates the required RMAN restore scripts but does not perform an actual restore or recovery. RMAN script will be created in the $RMAN_AGENT_HOME/ tmp directory on the selected target host. You can use the RMAN restore scripts that the dry run creates to perform a self-service restore as required.

Centralized restore and recovery operations can be performed from the **Restore > Assets > Oracle** window in the PowerProtect Data Manager UI.



□	Details	Name	Status	Prote...	Host/Cluster/Group N...	Host Ty...	OS T...	Size	Appli...	Last Copy
□		orclpr	Available	sbtio		STANDALONE	LINUX	2.8 GB	orclpr	May 31, 2022, 6:
□		test	Available			STANDALONE	LINUX	3.3 GB	test	Jun 8, 2022, 4:30
□		rcatdb	Available	install10		STANDALONE	LINUX	2.8 GB	rcatdb	Jun 12, 2022, 2:2
□		lhrac	Available			RAC	LINUX	3.0 GB	lhrac	Jun 1, 2022, 12:5
☑		source	Available	oracle_plc		STANDALONE	LINUX	2.7 GB	source	Jun 20, 2022, 4:5

Figure 19   Centralized restore and recovery of Oracle backups

1.17.1 Centralized Oracle restore and recovery of a full online database

A centralized restore and recovery of an online Oracle database supports the following features:

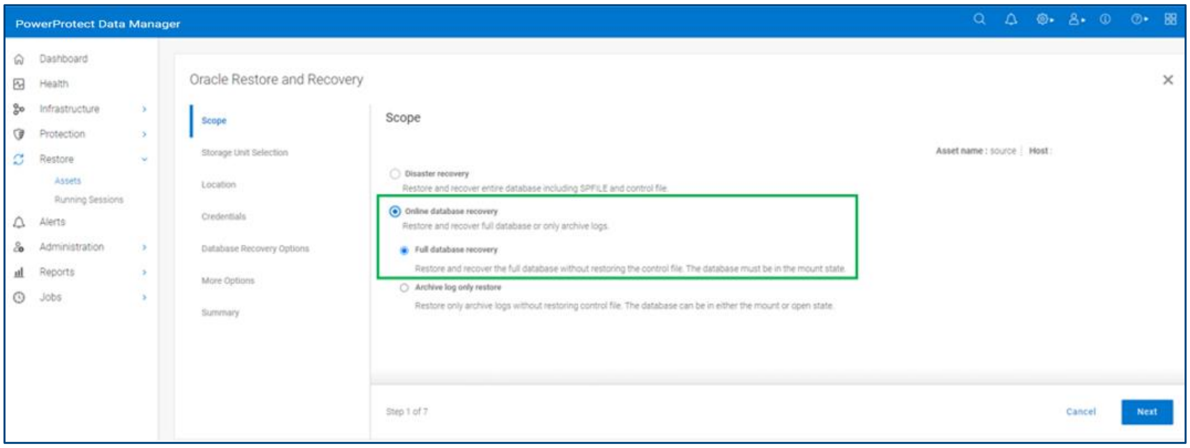
- Restore and recovery to the original Oracle host.
- Restore and recovery to an alternate Oracle host.
- Point-in-time restore and recovery, based on time, SCN, or log sequence.
- Dry run of the database restore and recovery.

Note: A centralized restore and recovery of an Oracle database is allowed only when the backup copies location is listed as LOCAL or Local_Recalled in the Location column in the PowerProtect Data Manager UI. (To see the Location column, go to Infrastructure > Assets, select the asset on the Oracle tab, click View Copies, and then click the storage icon on the left.) To recall a cloud tier backup before you perform a centralized restore, follow the procedure “Restore the cloud tier backups to DD” mentioned in the

For any centralized restore to an alternate host, ensure that the alternate host is an Oracle Server host that is a discovered asset of PowerProtect Data Manager.

Note: If the alternate host is not included in the list of available hosts, follow the instructions to install and configure the Oracle RMAN agent on the alternate host. Ensure that the Oracle Server host is registered to the same PowerProtect Data Manager server.

You can use the PowerProtect Data Manager UI to perform a centralized restore and recovery of a full Oracle database backup without the control file.



Scope

Asset name : source | **Host :**

○ **Disaster recovery**
Restore and recover entire database including SPFILE and control file.

● **Online database recovery**
Restore and recover full database or only archive logs.

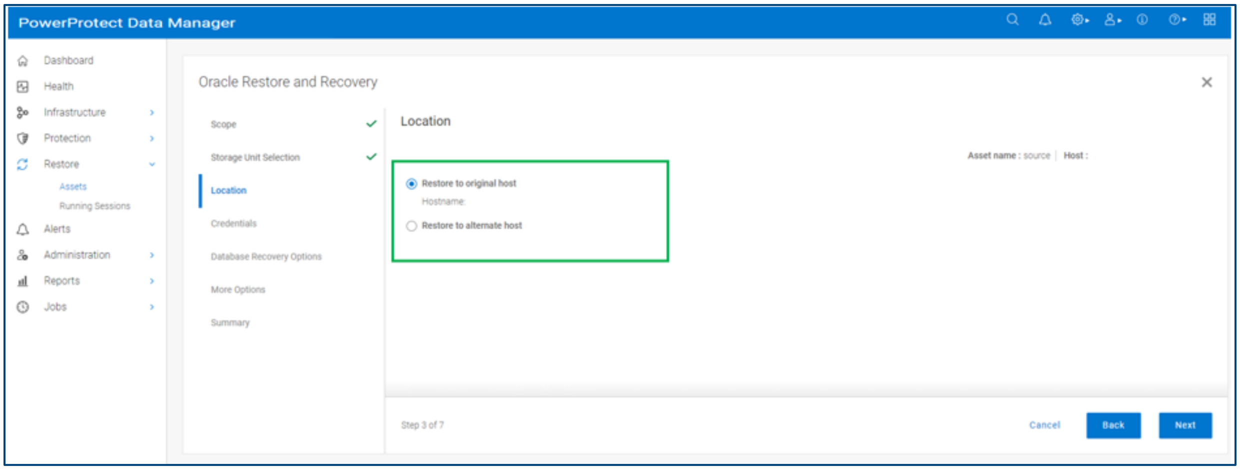
● **Full database recovery**
Restore and recover the full database without restoring the control file. The database must be in the mount state.

○ **Archive log only restore**
Restore only archive logs without restoring control file. The database can be in either the mount or open state.

Step 1 of 7

Use the **Location** page to select the preferred type of restore.

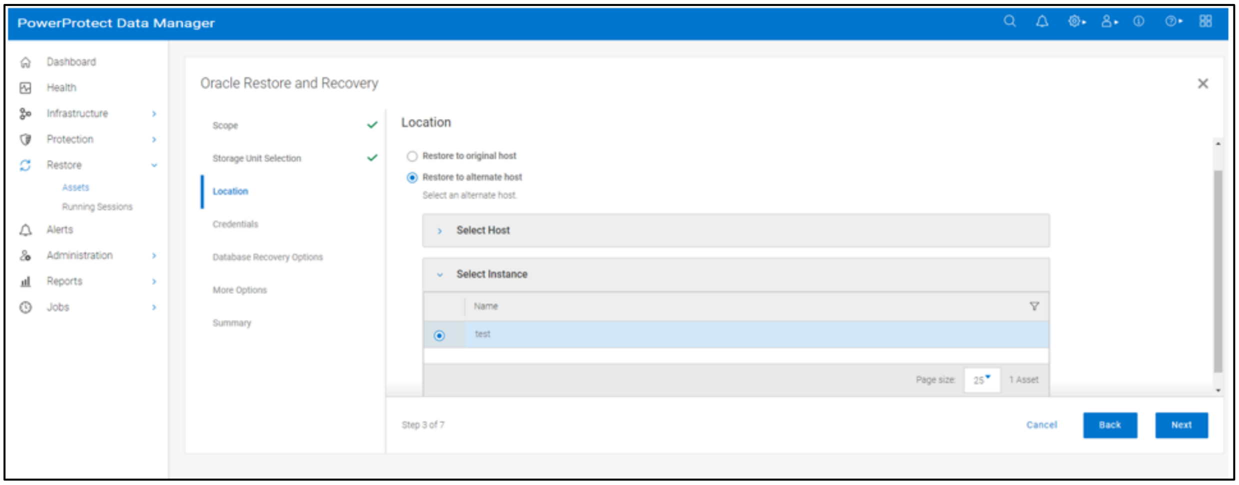
The option **Restore to original host** specifies to restore to the original host with the displayed hostname. If the original host is part of a RAC cluster, select the available node hostname from the list.



● Restore to original host

○ Restore to alternate host

The **Restore to alternate host** option specifies to restore to an alternate host. Select the alternate hostname from the list, and then select the required instance name.



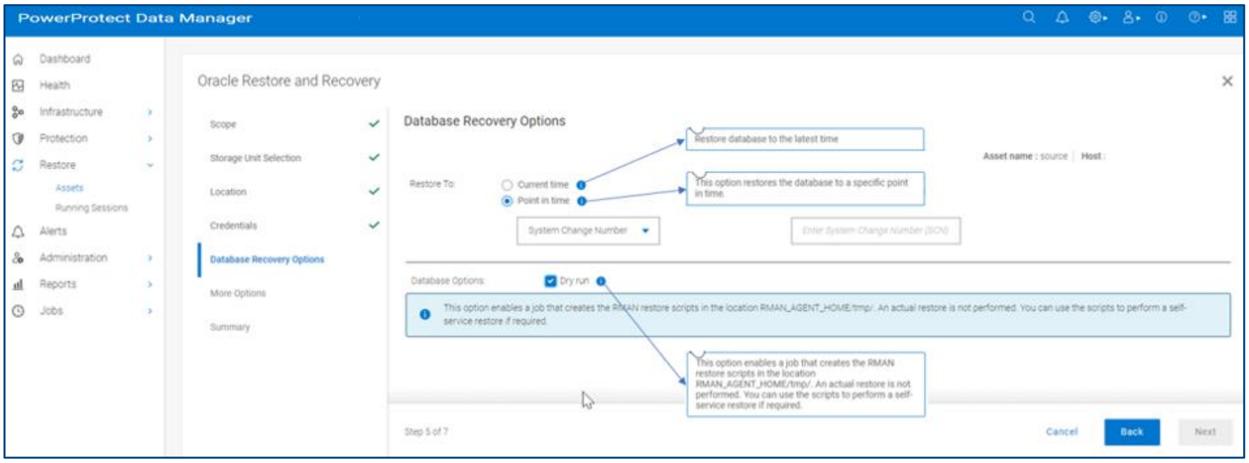
○ Restore to original host

● Restore to alternate host

Select an alternate host.

	Name
●	test

The **Database Recovery Options** page is shown below.



Restore To: ○ Current time ● Point in time

Restore database to the latest time

This option restores the database to a specific point in time.

Database Options: ☑ Dry run

This option enables a job that creates the RMAN restore scripts in the location RMAN_AGENT_HOME/tmp/. An actual restore is not performed. You can use the scripts to perform a self-service restore if required.

This option enables a job that creates the RMAN restore scripts in the location RMAN_AGENT_HOME/tmp/. An actual restore is not performed. You can use the scripts to perform a self-service restore if required.

The **Restore To** setting enables you to select Current time or Point in time.

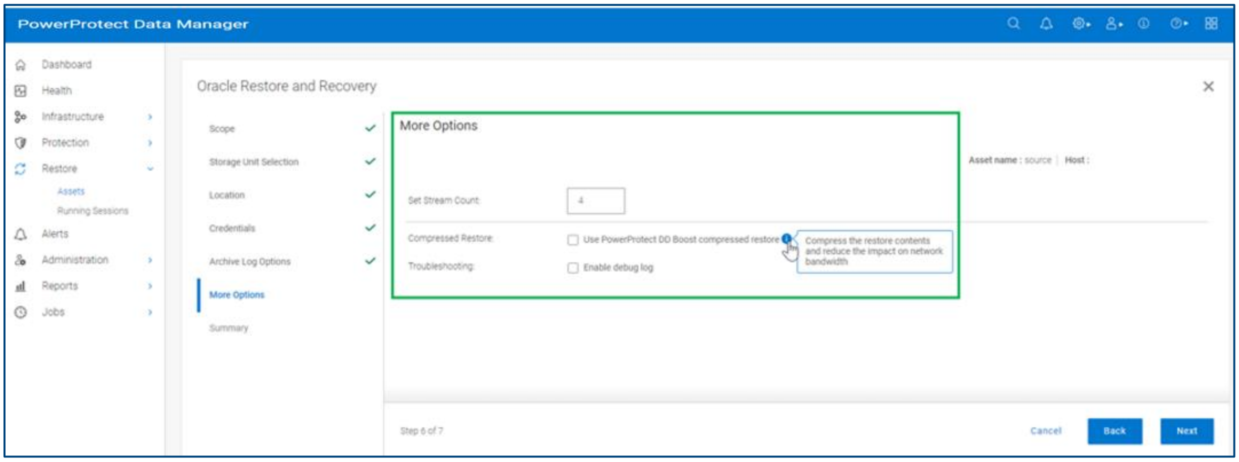
The **Current time** is the latest backup time in the control file.

For **Point in time**, select one of the following options from the menu:

- **System Change Number:** Enter the System Change Number (SCN) in the text box.
- **Timestamp:** Enter the date and time in the text box or click the icon to display a calendar and select the date and time.
- **Log Sequence:** Enter the log sequence in the text box.
- **Database Options**: Select **Dry Run** if you do not want to run an actual restore and recovery.

Use the **More options** page to specify the required options:

- **Set Stream Count**: Enter an integer stream count in the text box, if required. The default stream count is 4. The maximum stream count is 255
- **Compressed Restore**: To enable restore compression and reduce the impact on the network bandwidth, select **Use PowerProtect DD Boost (compressed restore).**
- **Troubleshooting**: To enable troubleshooting, select **Enable debug log**.



More Options

Asset name : source | Host :

Set Stream Count: 4

Compressed Restore: □ Use PowerProtect DD Boost compressed restore

Compress the restore contents and reduce the impact on network bandwidth

Troubleshooting: □ Enable debug log

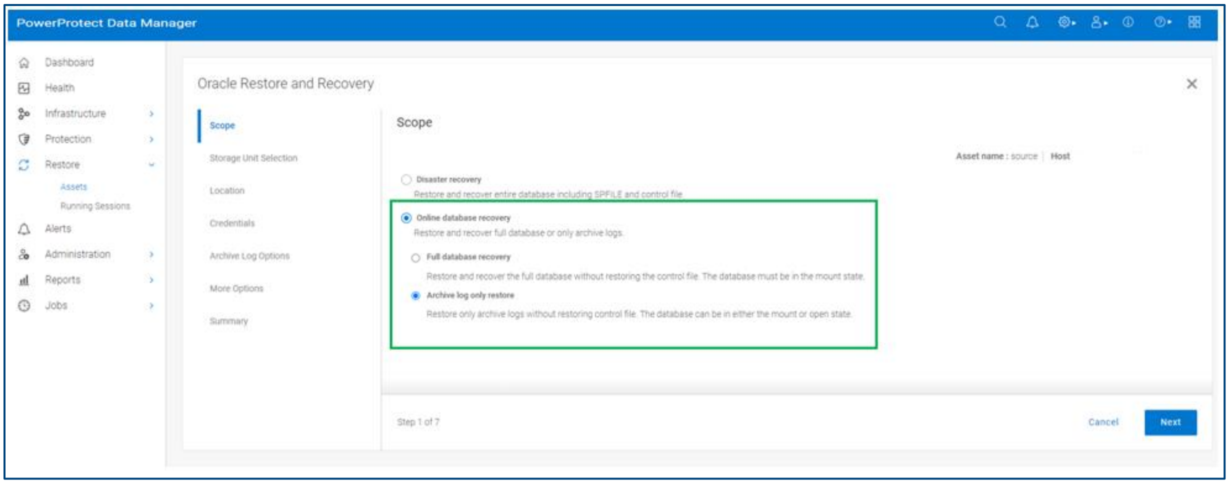
1.17.2 Centralized Oracle restore of archive logs

A centralized restore of only Oracle archive logs supports the following features:

- Restore to the original Oracle host
- Restore to an alternate Oracle host
- Restore of a specific range of archive logs, based on time, SCN, or log sequence
- Dry run of the archive log restore

You can use the PowerProtect Data Manager UI to perform a centralized restore of an Oracle archive logs backup without the control file.

Use the **Scope** page to select online database recovery and to choose Archive log only restore.



Oracle Restore and Recovery

Scope

Asset name : source | Host

○ Disaster recovery
Restore and recover entire database including SPFILE and control file.

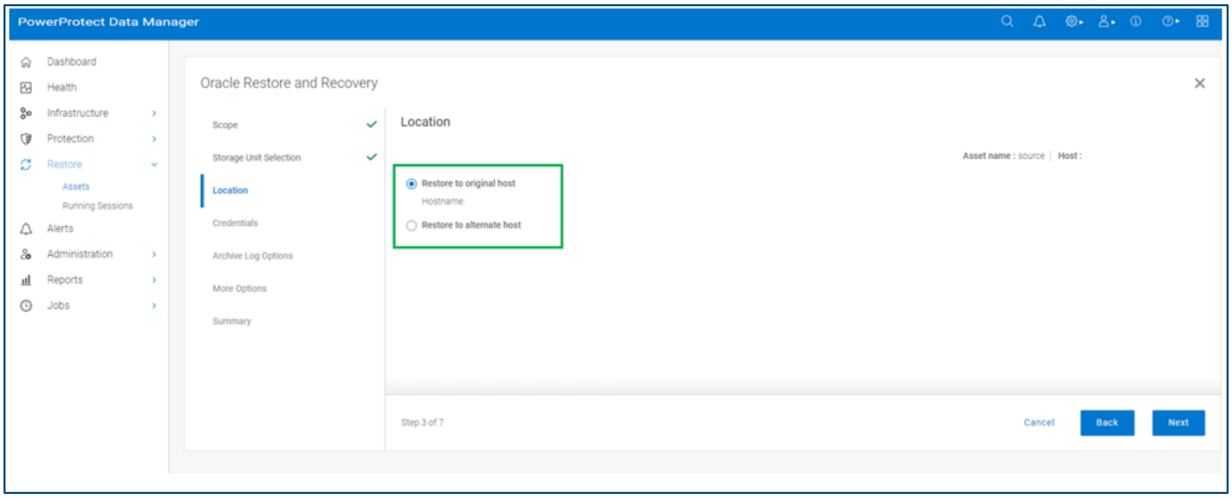
● Online database recovery
Restore and recover full database or only archive logs.

○ Full database recovery
Restore and recover the full database without restoring the control file. The database must be in the mount state.

● Archive log only restore
Restore only archive logs without restoring control file. The database can be in either the mount or open state.

Step 1 of 7

Use the **Location** page to select the preferred type of restore.



Oracle Restore and Recovery

Location

Asset name : source | Host :

● Restore to original host
Hostname:

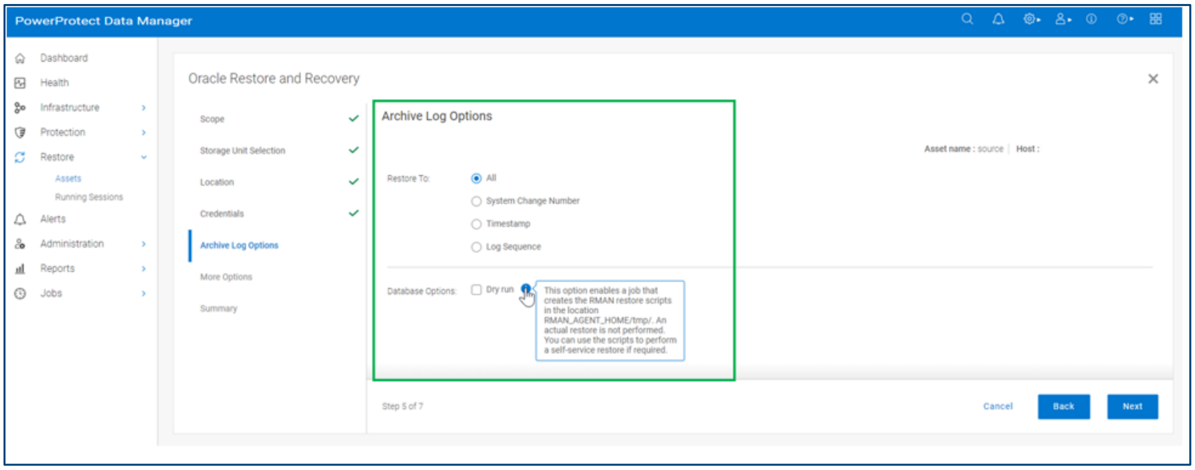
○ Restore to alternate host

Step 3 of 7

The **Restore to original host** setting enables restoring to the original host with the displayed hostname. If the original host is part of a RAC cluster, select the available node hostname from the list.

The **Restore to alternate host** setting specifies restoring to an alternate host. Select the alternate hostname from the list, and then select the required instance name.

Use the **Archive Log Options page** to select the required options.



Oracle Restore and Recovery

Archive Log Options

Asset name : source | Host :

Restore To: ● All ○ System Change Number ○ Timestamp ○ Log Sequence

Database Options: □ Dry run

This option enables a job that creates the RMAN restore scripts in the location RMAN_AGENT_HOME/tmp/. An actual restore is not performed. You can use the scripts to perform a self-service restore if required.

Step 5 of 7

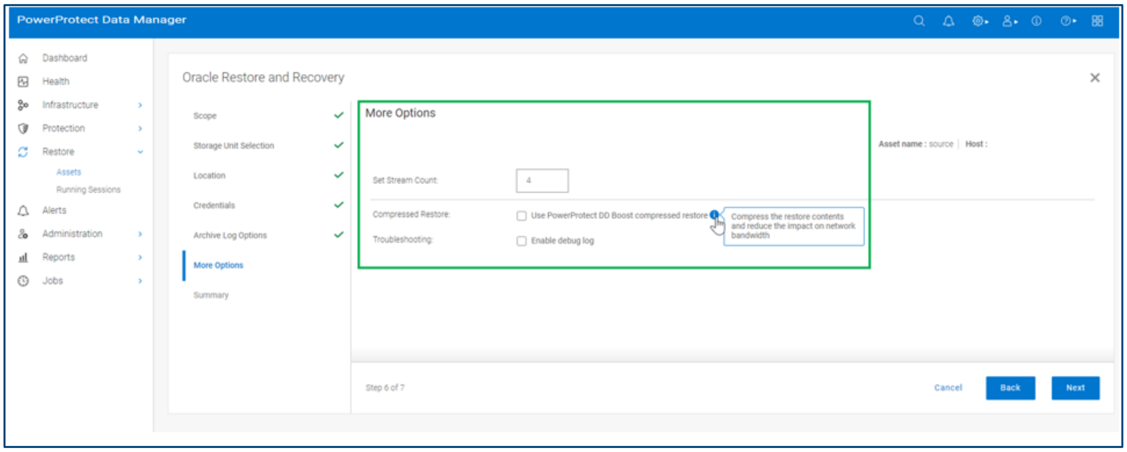
Restore To: Select one of the following options:

- **All**: Specifies to restore all the archive logs of the database asset
- **System Change Number**: Specifies to restore the archive logs for the SCN range. Type the SCN start and end values in the text boxes
- **Timestamp**: Specifies to restore the archive logs for the timestamp range. Type or select the timestamp start and end values in the text boxes
- **Log Sequence**: Specifies to restore the archive logs for the log sequence range. Type the log sequence start and end values in the text boxes

Database options: Select Dry Run if you do not want to run an actual restore.

Use the **More Options** page to specify the required options:

- **Set Stream Count**: Enter an integer stream count in the text box, if required. The default stream count is 4. The maximum stream count is 255
- **Compressed Restore**: To enable restore compression and reduce the impact on the network bandwidth, select **Use PowerProtect DD Boost (compressed restore).**
- **Troubleshooting**: To enable troubleshooting, select **Enable debug log.**



Oracle Restore and Recovery

More Options

Asset name : source | Host :

Set Stream Count: 4

Compressed Restore: □ Use PowerProtect DD Boost compressed restore

Compress the restore contents and reduce the impact on network bandwidth

Troubleshooting: □ Enable debug log

Step 6 of 7

1.17.3 Centralized disaster recovery of an Oracle database

A centralized Oracle disaster recovery supports the following features:

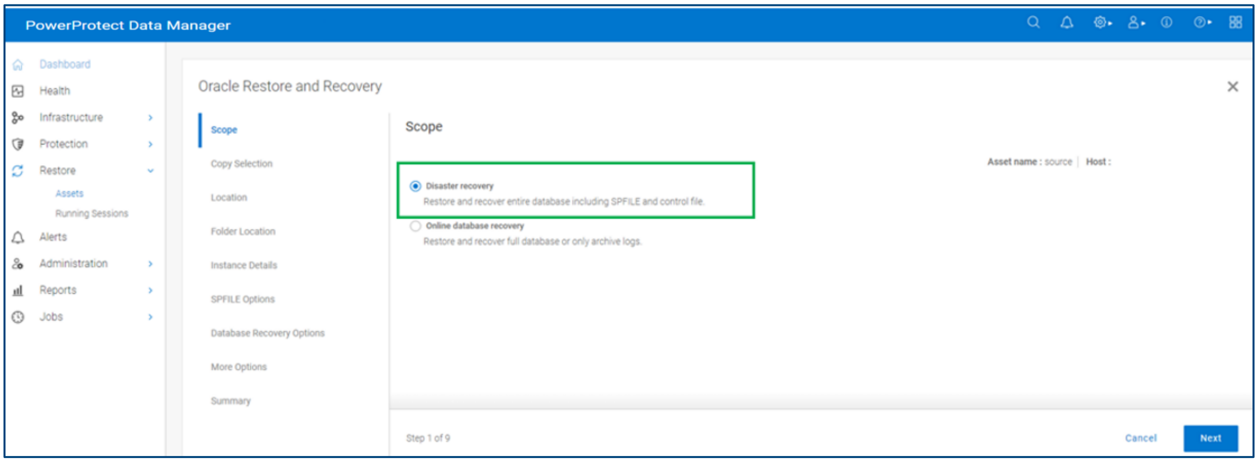
- Restore to the original Oracle host
- Restore to an alternate Oracle host

Note: You can use the disaster recovery for Oracle testing and development purposes, for example, to validate the Oracle backups on an alternate host.

- Change of the database ID (DBID) of the restored database after disaster recovery
- Relocation of the Oracle data files
- Customization of Oracle startup parameter settings in the spfile of the Oracle database
- Point-in-time restore and recovery, based on time, SCN, or log sequence
- Dry run of the disaster recovery

You can use the PowerProtect Data Manager UI to perform a centralized disaster recovery of an Oracle database including the spfile and control file.

Use the **Scope page** to select Disaster recovery option.



Scope

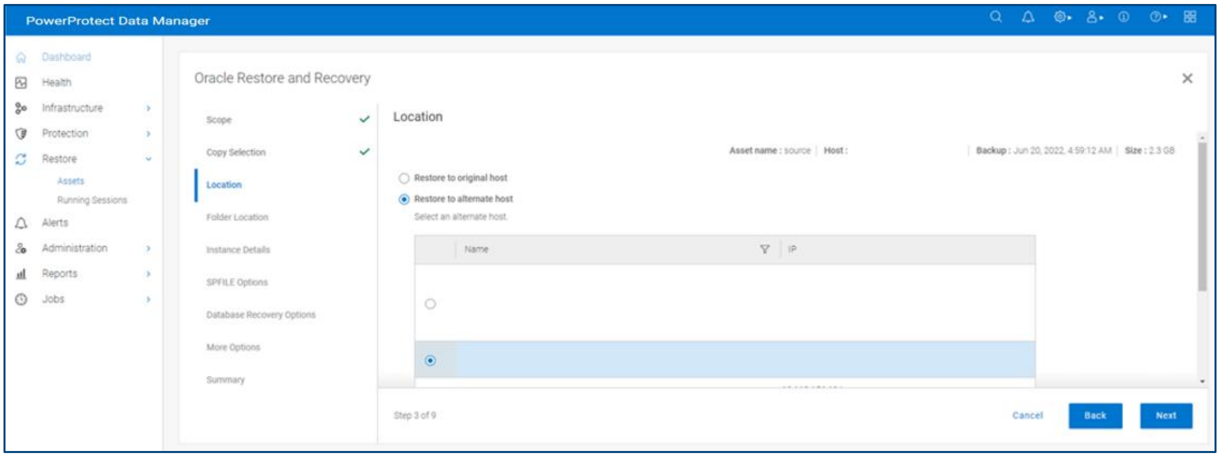
Asset name : source | Host :

● Disaster recovery
Restore and recover entire database including SPFILE and control file.

○ Online database recovery
Restore and recover full database or only archive logs.

This option restores and recovers the entire database, including the spfile and control file. You can use this option to restore the Oracle database to the original host or to an alternate host with a different database ID (DBID) than the original production host. The restore to the alternate host is usually used for test and development purposes.

Use the **Location page** to select the preferred type of restore.



Location

Asset name : source | Host : | Backup : Jun 20, 2022, 4:59:12 AM | Size : 2.3 GB

○ Restore to original host

● Restore to alternate host

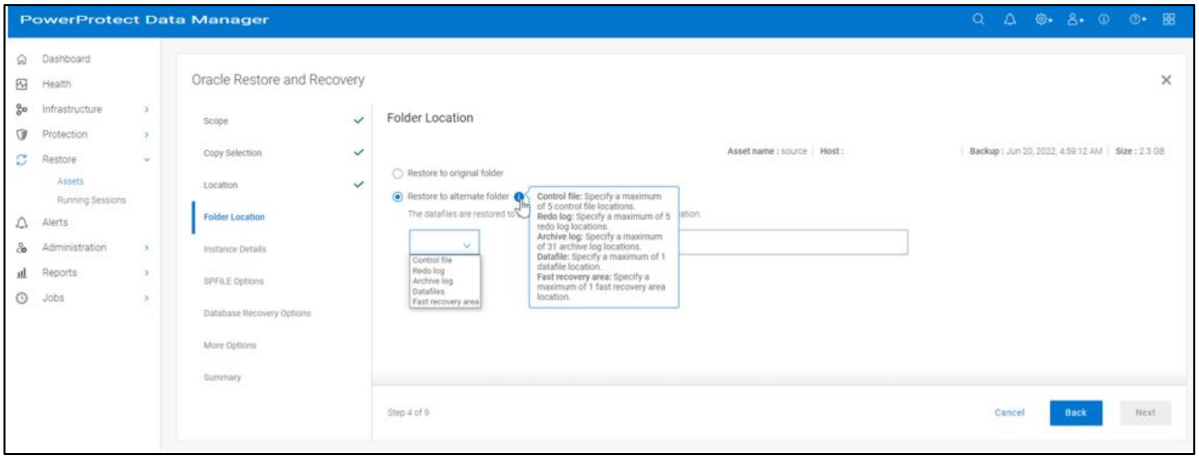
Select an alternate host.

Step 3 of 9

The **Restore to original host** option specifies restoring to the original host with the displayed hostname. If the original host is part of a RAC cluster, select the available node hostname from the list.

The **Restore to alternate host** option specifies restoring to an alternate host. Select the alternate hostname from the list

Use the **Folder Location page** to select one of the following options.



Folder Location

Asset name : source | Host : | Backup : Jun 20, 2022, 4:59:12 AM | Size : 2.3 GB

○ Restore to original folder

● Restore to alternate folder

The datafiles are restored to ation.

Control file: Specify a maximum of 5 control file locations.
Redo log: Specify a maximum of 5 redo log locations.
Archive log: Specify a maximum of 31 archive log locations.
Datafile: Specify a maximum of 1 datafile location.
Fast recovery area: Specify a maximum of 1 fast recovery area location.

Step 4 of 9

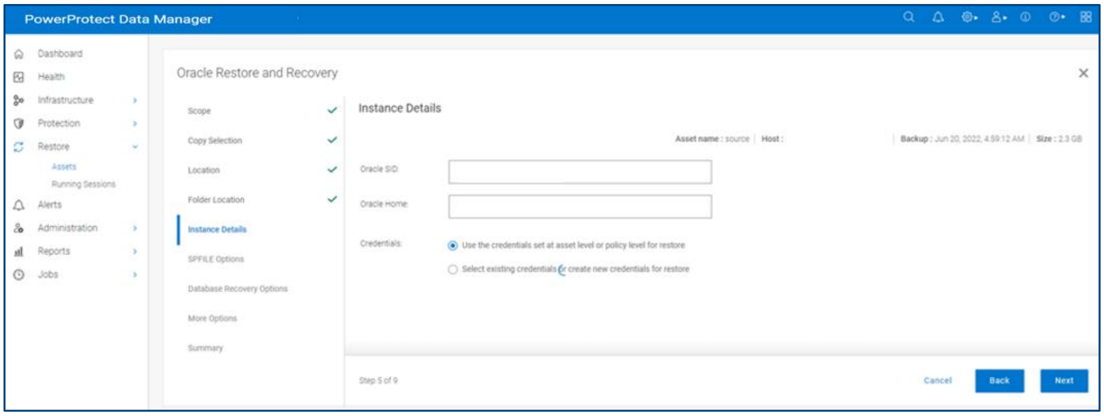
- Restore to original folder

Note: When you select to restore the Oracle data files to the original location, the original database is overwritten.

- Restore to alternate folder

To specify an alternate location, select Archive log, Control file, Datafiles, Fast recovery area, or Redo log from the menu, and then type the alternate location in the text box. For each additional alternate location, click the + icon, select the file type from the menu, and type the alternate location in the text box.

Use the **Instance Details page** to specify the required settings:



Oracle Restore and Recovery

Instance Details

Asset name : source | **Host :** | **Backup :** Jun 20, 2022, 4:59:12 AM | **Size :** 2.3 GB

Oracle SID:

Oracle Home:

Credentials: ● Use the credentials set at asset level or policy level for restore
○ Select existing credentials or create new credentials for restore

Step 5 of 9

- **Oracle SID:** Enter the Oracle instance system ID (SID) in the text box.
- **Oracle Home**: Enter the valid Oracle home pathname in the text box.

  Note: The Oracle home pathname must not include a final space or slash (/).

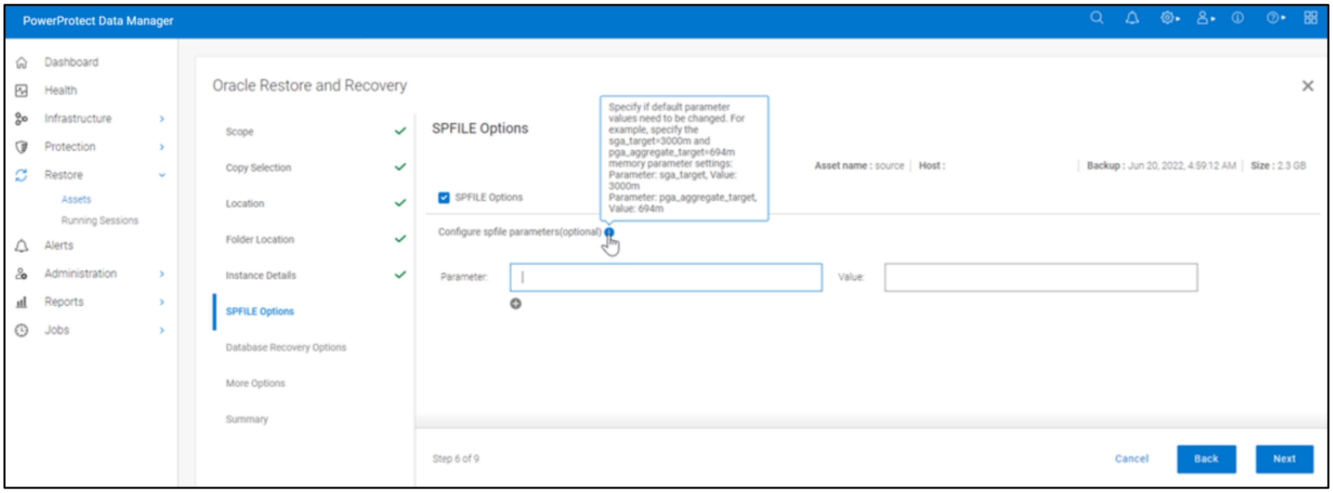
- **Credentials**: Select one of the following options:

  – Use the credentials set at asset level or policy level for restore.

  Note: Credentials at the asset level take precedence over credentials at the protection policy level.

  – Select the existing credentials or create new credentials for restore.

Use the **SPFILE Options** page to specify the required settings.



Oracle Restore and Recovery

SPFILE Options

Asset name : source | **Host :** | **Backup :** Jun 20, 2022, 4:59:12 AM | **Size :** 2.3 GB

☑ SPFILE Options

Configure spfile parameters(optional)

Specify if default parameter values need to be changed. For example, specify the sga_target=3000m and pga_aggregate_target=694m memory parameter settings:
Parameter: sga_target, Value: 3000m
Parameter: pga_aggregate_target, Value: 694m

Parameter: | Value:

Step 6 of 9

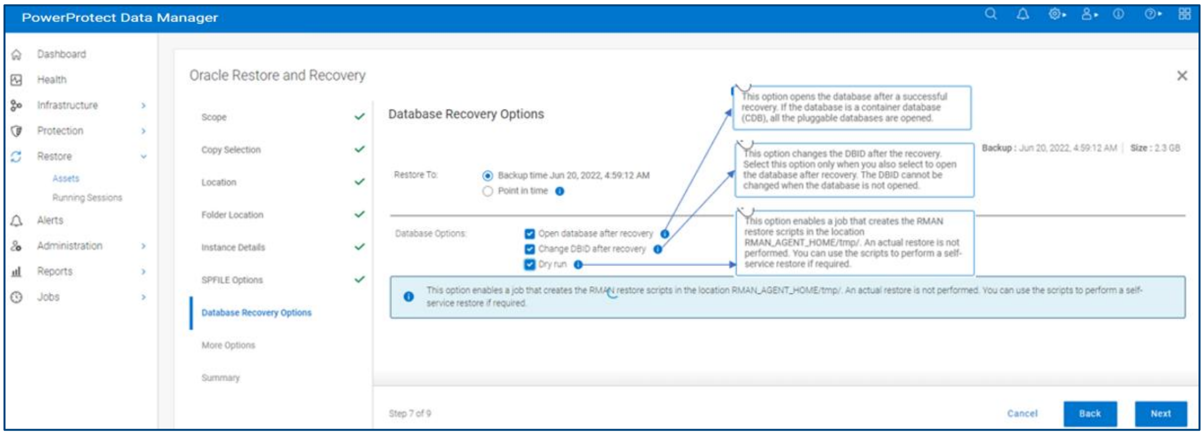
- **SPFILE Options:** Select this option to specify the restore of the spfile during the disaster recovery. This option is selected by default when the selected copy contains the spfile.

  Note: If you do not select this option to restore the spfile, you must create the spfile manually and start the database instance in no mount mode.

- **Configure SPFILE Parameters**: To change a default spfile parameter setting, type the parameter name in the Parameter text box and the parameter value setting in the **Value** text box. For each additional parameter setting that you want to change, click the + icon and then type the parameter name and value in the new blank text boxes.

For more details about configuring SPFILE parameters, see the document [PowerProtect Data Manager Oracle RMAN Agent User Guide]() for detailed steps.

Use the **Database Recovery Options** page to select the required options.



Database Recovery Options

Backup : Jun 20, 2022, 4:59:12 AM | **Size :** 2.3 GB

Restore To: ● Backup time Jun 20, 2022, 4:59:12 AM ○ Point in time

Database Options: ☑ Open database after recovery ☑ Change DBID after recovery ☑ Dry run

This option opens the database after a successful recovery. If the database is a container database (CDB), all the pluggable databases are opened.

This option changes the DBID after the recovery. Select this option only when you also select to open the database after recovery. The DBID cannot be changed when the database is not opened.

This option enables a job that creates the RMAN restore scripts in the location RMAN_AGENT_HOME/tmp/. An actual restore is not performed. You can use the scripts to perform a self-service restore if required.

This option enables a job that creates the RMAN restore scripts in the location RMAN_AGENT_HOME/tmp/. An actual restore is not performed. You can use the scripts to perform a self-service restore if required.

Step 7 of 9

- **Restore To**: Select Backup time (backup end time of selected backup copy) or Point in time.

  For **Point in time**, select one of the following options from the menu:
  - **System Change Number:** Type the System Change Number (SCN) in the text box.
  - **Timestamp:** Type the date and time in the text box or click the icon to display a calendar and select the date and time.
  - **Log Sequence**: Type the log sequence in the text box.

- **Database Options**: Select any required options from the list:

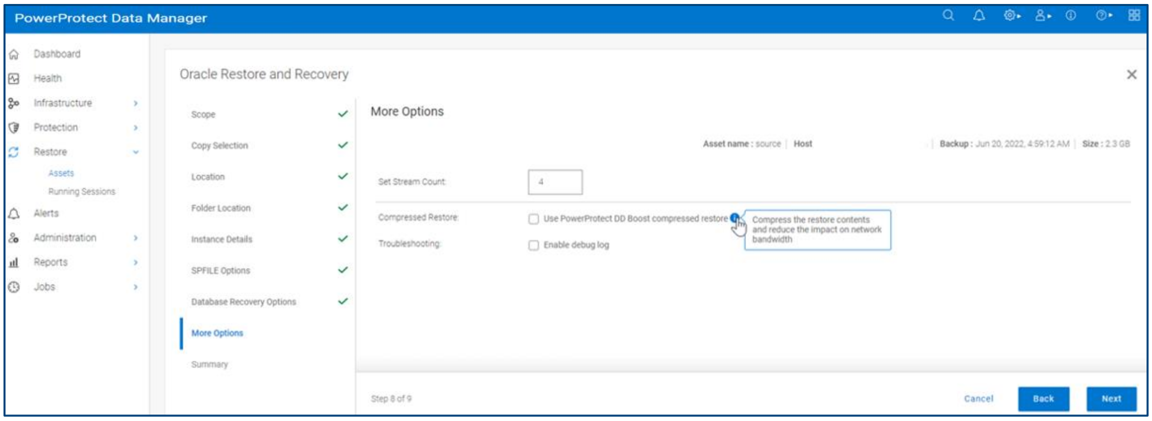
  - **Open database after recovery**: This option opens the database after the recovery. If the database is a container database (CDB), all the pluggable databases are opened.

  - **Change DBID after recovery**: This option changes the DBID after the recovery. Select this option only when you also select to open the database after the recovery. When the database is unopened, the DBID cannot be changed.

Note: When you select the Change DBID after recovery option, the asset is discovered automatically in PowerProtect Data Manager after a successful restore with the DBID change. When you do not select this option, the restored asset is not discovered automatically.

  - Dry run

Use the **More Options** page to specify the required options.



Oracle Restore and Recovery

More Options

Asset name : source | Host | Backup : Jun 20, 2022, 4:59:12 AM | Size : 2.3 GB

Set Stream Count: 4

Compressed Restore: □ Use PowerProtect DD Boost compressed restore

Compress the restore contents and reduce the impact on network bandwidth

Troubleshooting: □ Enable debug log

Step 8 of 9

- **Set Stream Count**: Type an integer stream count in the text box, if required. The default stream count is 4. The maximum stream count is 255.
- **Compressed Restore**: To enable restore compression and reduce the impact on the network bandwidth, select Use PowerProtect DD Boost compressed restore.
- **Troubleshooting**: To enable troubleshooting, select Enable debug log.

Centralized Oracle restore and recovery includes the following limitations:

- You cannot perform a cross-OS platform restore.
- You cannot perform a quick recovery.
- You cannot perform a centralized restore of an Oracle backup performed by a stand-alone Oracle RMAN agent before the agent was registered with PowerProtect Data Manager.

1.18 Self-service restores of Oracle databases

You can perform database restores directly to the Oracle application host by using the Oracle RMAN agent or you can restore an Oracle backup of a source client for disaster recovery or for a cross-restore to an alternate client host.

The restore workflow is as follows:

1. Oracle DBA starts the restore using RMAN recovery script.
2. Oracle RMAN connects to Oracle RMAN Agent and passes the information of assets to be recovered.
3. Oracle RMAN agents connects to DD series appliance and requests the data for recovery.
4. Data transfer starts from DD series appliance.
5. After recovery of database is completed, the script displays the completion status.

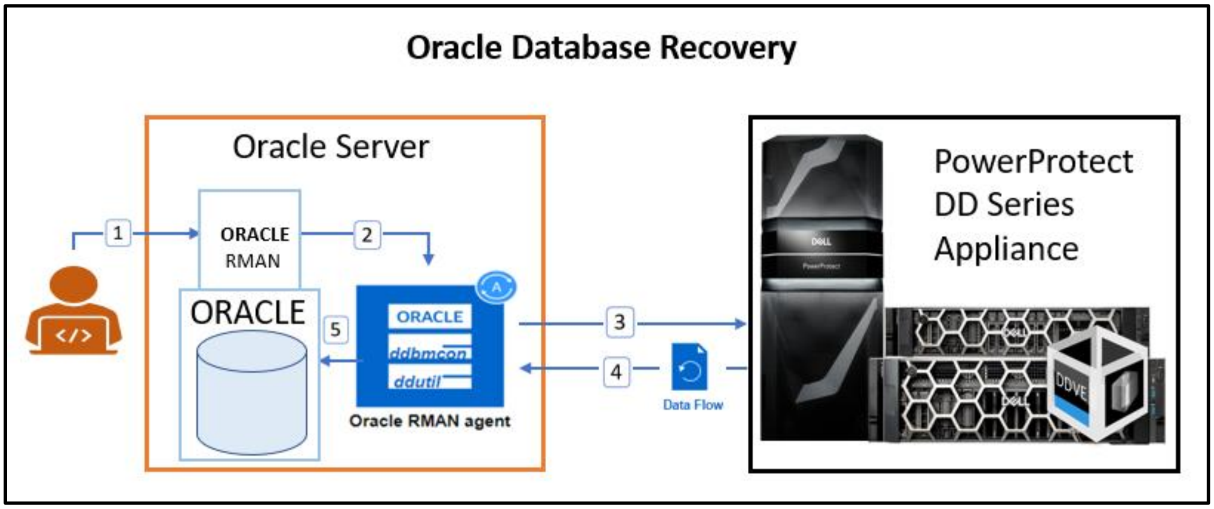


Figure 20 Self-service Oracle database restore workflow

To perform an Oracle database restore, you must prepare the database and then run an RMAN script to restore the data. The *RMAN documentation* provides detailed information about how to prepare the database and create the RMAN restore script. The documentation also describes all the supported restore features.

The following information is required before the Oracle database recovery operation:

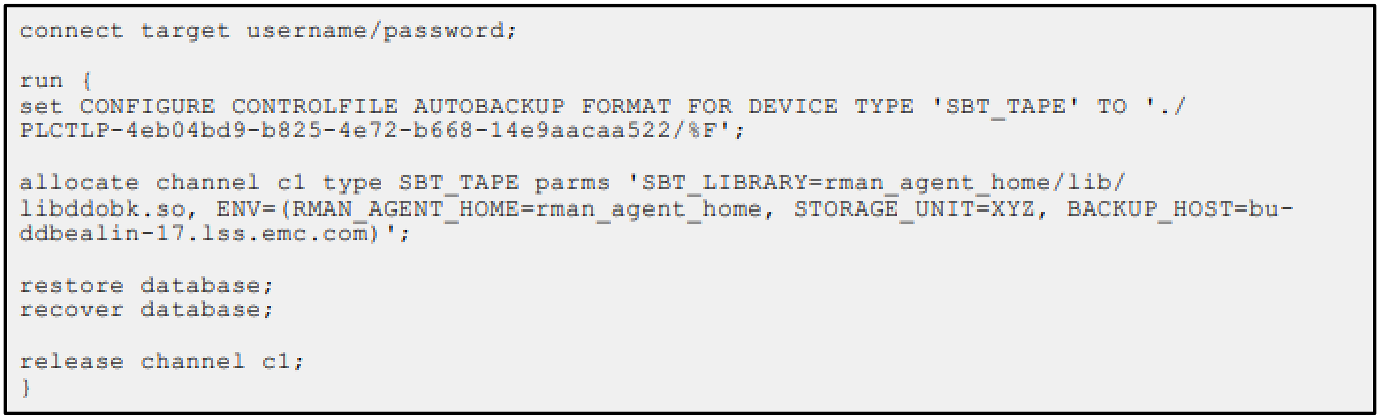
- SBT_LIBRARY: The installation directory of the DD Boost library file - libddobk.so. The default installation directory is: $RMAN_AGENT_HOME/lib
- STORAGE_UNIT: The name of DD series appliance storage unit, which is created automatically when you add the protection policy. To display the storage units and their assigned databases on the Oracle RMAN agent host, run the ddutil -s command
- BACKUP_HOST: The hostname or IP address of the DD series appliance.
- RMAN_AGENT_HOME: The Oracle RMAN Agent software installation directory.

To identify the storage unit and DD hostname, run the ddutil -s command on the Oracle client. For example, run the following command in the $RMAN_AGENT_HOME/bin directory:

```
./ddutil -s
```

Specify the storage unit, top-level pathname, and DD hostname in the RMAN restore script.

The following example shows an RMAN script that performs a complete restore of the database to the current time, after the database has been prepared:



```
connect target username/password;

run {
set CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE 'SBT_TAPE' TO './
PLCTLP-4eb04bd9-b825-4e72-b668-14e9aacaa522/%F';

allocate channel c1 type SBT_TAPE parms 'SBT_LIBRARY=rman_agent_home/lib/
libddobk.so, ENV=(RMAN_AGENT_HOME=rman_agent_home, STORAGE_UNIT=XYZ, BACKUP_HOST=bu-
ddbealin-17.lss.emc.com)';

restore database;
recover database;

release channel c1;
}
```

Figure 21 Restore script

Note: To increase the parallelism of the restore, you can allocate more channels.

For detailed steps to restore an Oracle application host or to restore to an alternate host, see *PowerProtect Data Manager Oracle RMAN Agent User Guide.*

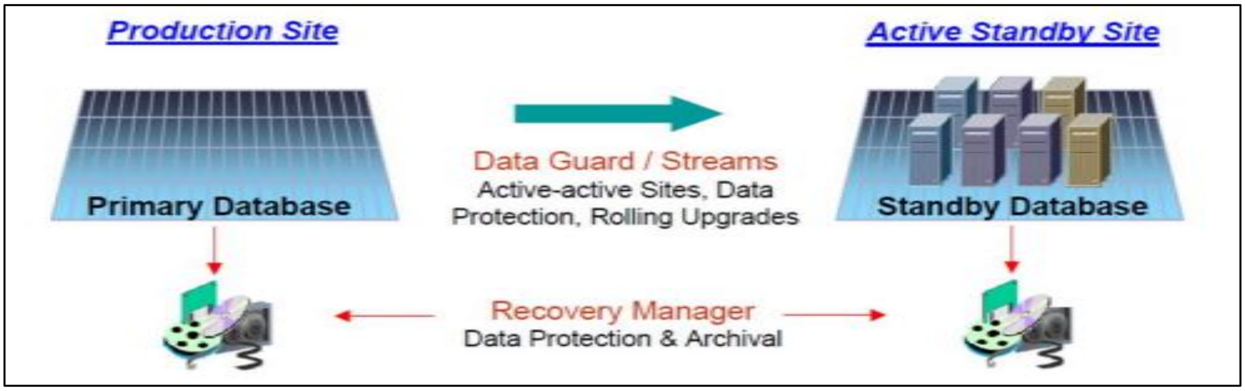
Oracle Data Guard support

Data Guard provides a comprehensive set of services that create, maintain, manage, and monitor one or more standby databases to enable production Oracle databases to survive disasters and data corruption. Data Guard maintains these standby databases as transitionally consistent copies of the production database.

Oracle Data Guard ensures high availability, data protection, and disaster recovery for enterprise data. It is common at large enterprise sites to deploy critical Oracle databases in High Availability mode or Data Guard mode.

1.19 Data Guard configuration

Data Guard configuration consists of one primary database and one or more standby databases. The standby databases will be always in sync with the primary database.

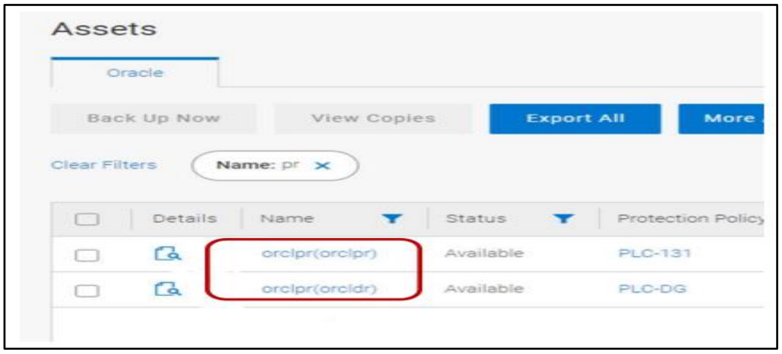


1.20 Data Guard: standalone mode support

Starting with version 19.12, Data Manager supports standalone mode assets that simplify the management of primary/standby node protection and recovery for users.

The following are Oracle RAC preferred node UI features:

- The Data Guard asset name is displayed in the format DBNAME(DBUNQIUE)
- The user can use a single instance of Data Manager to protect all Data Guard nodes
- Each database in a Data Guard configuration is considered a separate entity with its individual protection schedule and workflow
- No role or correlation is shown between databases in a Data Guard configuration
- This is supported on both Linux and AIX



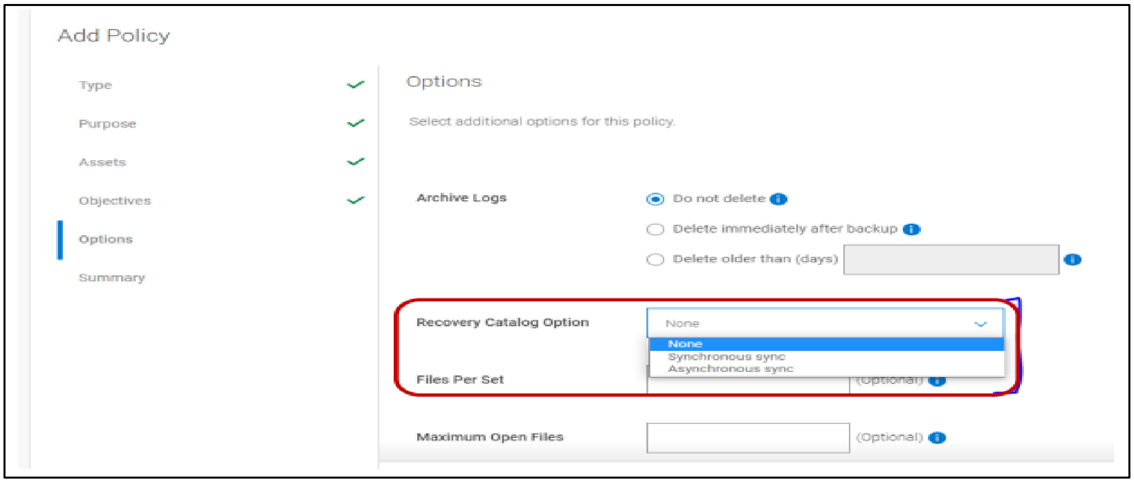
□	Details	Name	Status	Protection Policy
□		orclpr(orclpr)	Available	PLC-131
□		orclpr(orcldr)	Available	PLC-DG

1.21 Data Guard: the recovery catalog option

In the Data Guard environment, it is recommended that the user use a recovery catalog to manage the RMAN metadata for all physical databases, including primary and standby databases.

RMAN uses the recovery catalog as the single source of truth for the Data Guard environment. RMAN does not automatically resynchronize every database in the Data Guard environment when connected as TARGET to one database in the environment.

This option is applicable only for centralized protection in an Oracle Data Guard environment. This option resynchronizes the recovery catalog either synchronously or asynchronously with backup copies after each backup.



Options

Select additional options for this policy.

Archive Logs: ● Do not delete; ○ Delete immediately after backup; ○ Delete older than (days)

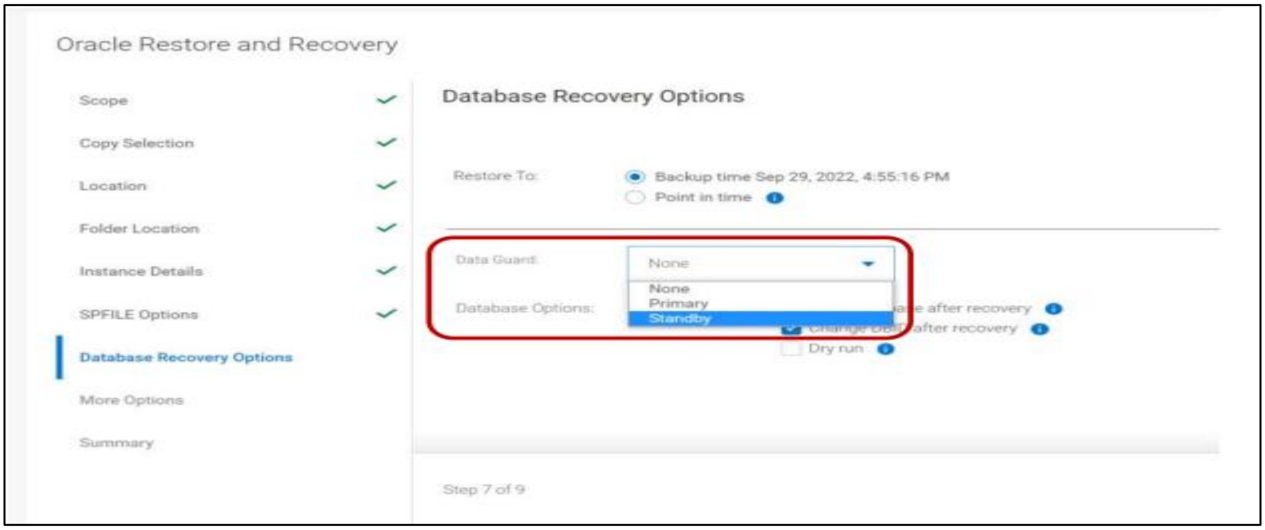
Recovery Catalog Option: None

Files Per Set: (Optional)

Maximum Open Files: (Optional)

1.22 Data Guard: the disaster recovery option

The disaster recovery option helps to restore the database as either a primary or standby database in a Data Guard configuration to a specified point in time. The user can bring up a standby database using a primary or standby database backup, or bring up a primary database using a primary or standby database backup (by using spfile/pfile).



Database Recovery Options

Restore To: ● Backup time Sep 29, 2022, 4:55:16 PM; ○ Point in time

Data Guard: None

Database Options: ...e after recovery; ☑ Change DBID after recovery; □ Dry run

Step 7 of 9

Note: After a disaster recovery, have an administrator get the Data Guard in sync.

1.23 Data Guard: self-service protection

For self-service protection, synchronize the recovery catalog in separate RMAN sessions at regular intervals to update the recovery catalog with the current metadata from the target database control file.

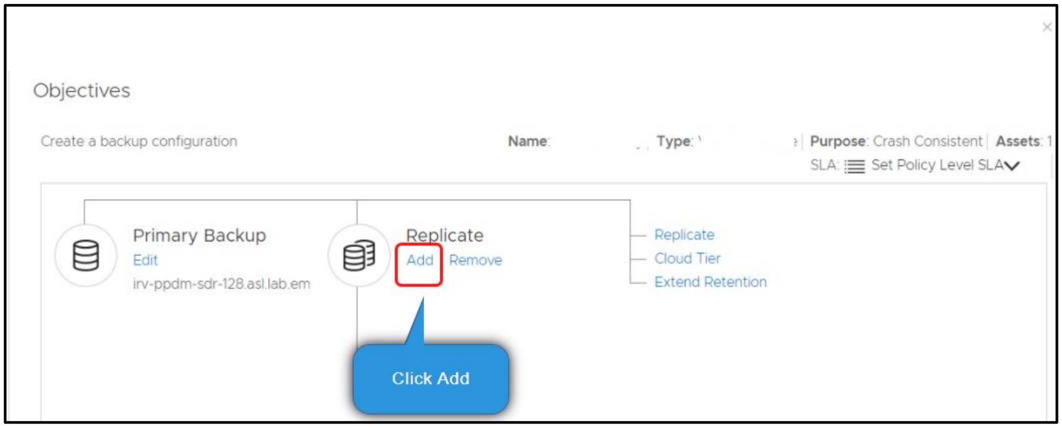
The user can run the resync catalog command to initiate a full resynchronization of the recovery catalog.

To enable self-service backups for an Oracle RAC Data Guard configuration, add the `DB_UNIQUE_NAME` parameter to the RMAN script ALLOCATE CHANNEL.

Replication and DD Cloud Tier

During the protection policy creation self-service or centralized, you can add the replication to a remote PowerProtect DD series appliance as the replication target.

In a protection policy, click **Replicate** next to **Primary Backup**, **Primary Retention**, or **Extend Retention**. An entry for **Replicate** is created to the right of the primary or extended retention backup schedule. Under **Replicate**, click **Add**. The **Add Replication** dialog appears.



Objectives

Create a backup configuration

Name:

Type:

Purpose: Crash Consistent | **Assets**: 1

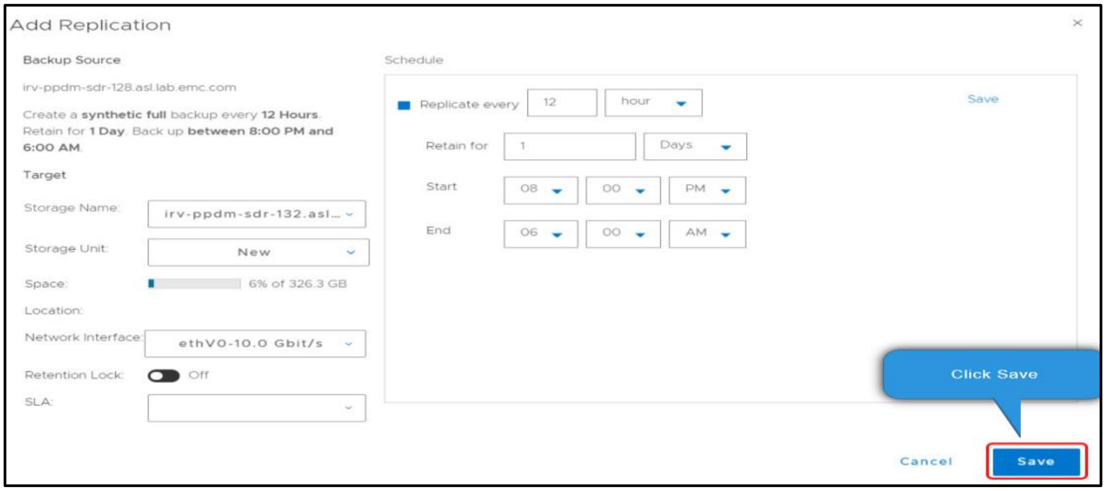
SLA: Set Policy Level SLA

Primary Backup
Edit
irv-ppdm-sdr-128.asl.lab.em

Replicate
Add Remove

Figure 22 Replication configuration

Complete the schedule details in the **Add Replication** dialog and click **Save** to save your changes.



Add Replication

Backup Source

irv-ppdm-sdr-128.asl.lab.emc.com

Create a **synthetic full** backup every **12 Hours**. Retain for **1 Day**. Back up **between 8:00 PM and 6:00 AM**.

Target

Storage Name: irv-ppdm-sdr-132.asl...

Storage Unit: New

Space: 6% of 326.3 GB

Location:

Network Interface: ethV0-10.0 Gbit/s

Retention Lock: Off

SLA:

Schedule

Replicate every 12 hour

Retain for 1 Days

Start 08 00 PM

End 06 00 AM

Figure 23 Replication schedule

Data Manager cloud tier feature works in tandem with the DD Cloud Tier feature to move Data Manager backups from DD series appliance to the cloud. This provides long-term storage of Data Manager backups by seamlessly and securely tiering data to the cloud. From the Data Manager UI, you configure cloud tier to move Data Manager backups from DD series appliance to the cloud, and you can perform seamless recovery of these backups. DD series appliance cloud storage units must be preconfigured on the DD series appliance before they are configured for cloud tier in the Data Manager UI. The *PowerProtect Data Manager Administration Guide* provides more information.

Both Oracle centralized and self-service protection policies support cloud tiering. You can create the cloud tier schedule from both primary and replication stages. Schedules must have a minimum weekly recurrence and a retention time of 14 days or greater. Ensure that the DD series appliance is set up for cloud tiering and follow the below step:

1. Click **Cloud Tier** next to **Primary Backup** or **Extend Retention,** or if adding a cloud stage for a replication schedule that you have added, click **Cloud Tier** under **Replicate**. An entry for **Cloud Tier** is created to the right of the primary or extended retention backup schedule, or below the replication schedule.

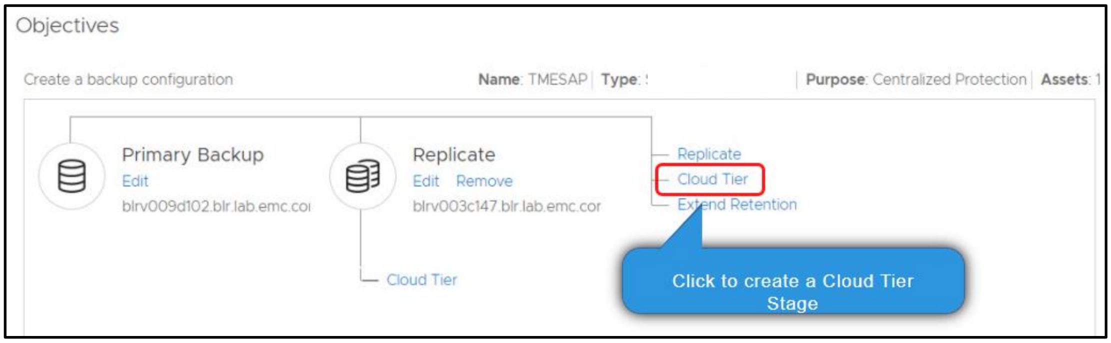

Objectives
Create a backup configuration
Name: TMESAP | Type:
Purpose: Centralized Protection | Assets: 1
Primary Backup
Edit
blrv009d102.blr.lab.emc.coi
Replicate
Edit Remove
blrv003c147.blr.lab.emc.cor
Replicate
Cloud Tier
Extend Retention
Cloud Tier
Click to create a Cloud Tier Stage

Figure 24 Cloud Tier Configuration

2. Under the entry for **Cloud Tier**, click **Add**.

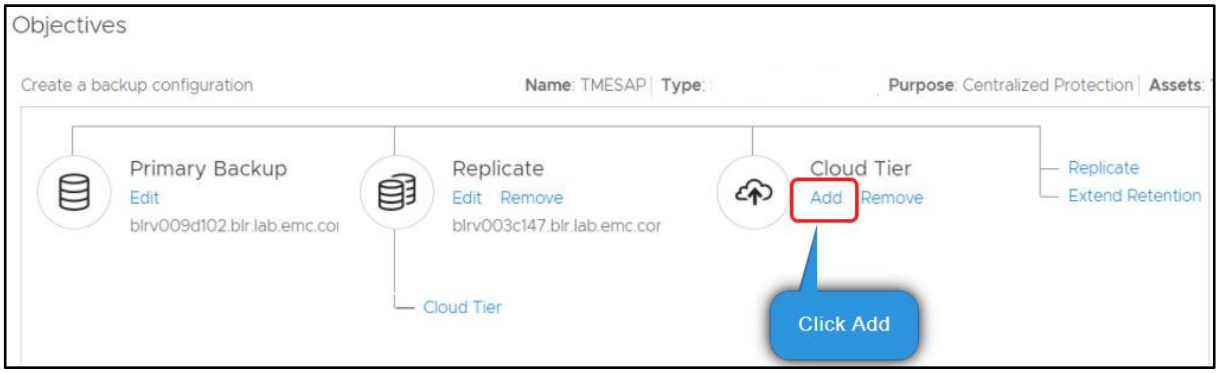
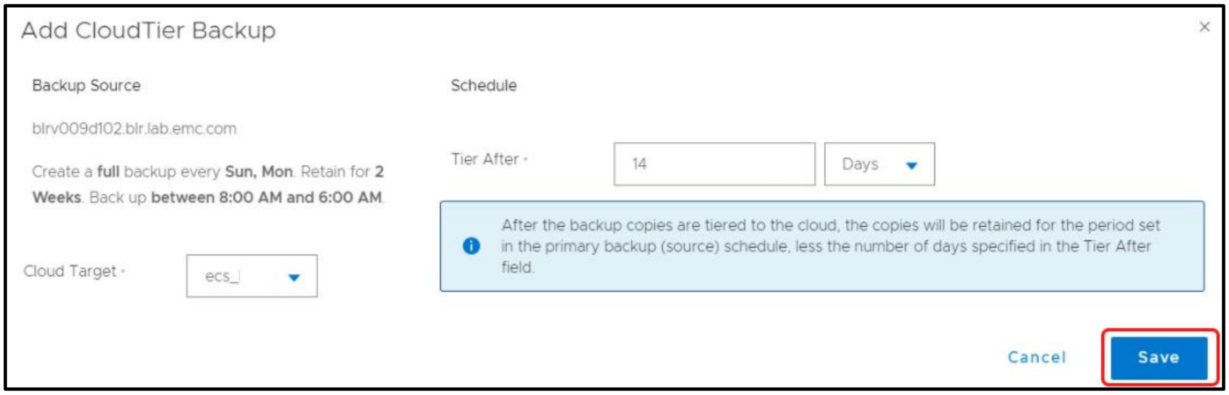


Figure 25 Cloud Tier Configuration

3. The **Add Cloud Tier Backup** dialog appears, with summary schedule information for the parent node to indicate whether you are adding this cloud tier stage for the primary backup schedule, the extended retention backup schedule, or the replication schedule.

Complete the schedule details in the **Add Cloud Tier Backup** dialog, and click **Save** to save your changes.



Add CloudTier Backup

Backup Source

blrv009d102.blr.lab.emc.com

Create a **full** backup every **Sun, Mon**. Retain for **2 Weeks**. Back up **between 8:00 AM and 6:00 AM**.

Cloud Target * ecs_

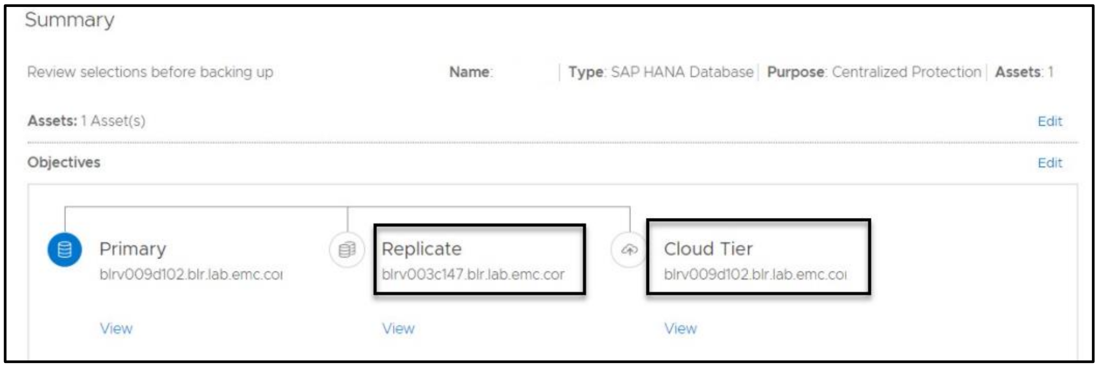
Schedule

Tier After * 14 Days

After the backup copies are tiered to the cloud, the copies will be retained for the period set in the primary backup (source) schedule, less the number of days specified in the Tier After field.

Figure 26 Cloud Tier Configuration

4. The Protection Policy Summary Lists **Replicate** and **Cloud Tier**.



Summary

Review selections before backing up

Name: | **Type**: SAP HANA Database | **Purpose**: Centralized Protection | **Assets**: 1

Assets: 1 Asset(s)

Objectives

Primary blrv009d102.blr.lab.emc.cor

Replicate blrv003c147.blr.lab.emc.cor

Cloud Tier blrv009d102.blr.lab.emc.coı

Figure 27 Replication and DD Cloud Tier

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

The Data Protection Info Hub provides expertise that helps to ensure customer success with Dell data protection products.

A.1 Related resources

- PowerProtect Data Manager for Oracle RMAN agent User Guide
- PowerProtect Data Manager Administration and User Guide
- PowerProtect Data Manager Deployment Guide
- DDOS Administration Guide

PowerProtect Data Manager E-LAB Navigator: Provides compatibility information, including specific software and hardware configurations that PowerProtect Data Manager supports. To access E-LAB Navigator, go to PowerProtect Data Manager Compatibility Matrix.