NetBackup™ Web UI Oracle Administrator's Guide

Release 10.0

Last updated: 2022-02-28

Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Veritas Technologies LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1 Introducing the NetBackup web user interface 6

About the NetBackup web UI 6
Terminology 7
Sign in to the NetBackup web UI 9
Sign out of the NetBackup web UI 11

Chapter 2 Monitoring NetBackup 12

The NetBackup dashboard 12
Job monitoring 12
Search for or filter jobs in the jobs list 13

Chapter 3 Managing Oracle 15

About Oracle discovery 15
Add an Oracle instance 17
Add an Oracle instance group 18
Clean up Oracle instance and databases 18

Chapter 4 Managing Oracle RAC 20

Oracle Real Application Clusters (RAC) 20
Add an Oracle Real Application Cluster (RAC) 21
Edit or delete an Oracle RAC database 22

Chapter 5 Managing Oracle credentials 23

Manage credentials for an instance or an Oracle RAC database 23

Chapter 6 Oracle Copilot with instant access and universal share 25

Prerequisites when you configure an instant access Oracle database 25
Hardware configuration requirement of instant access 27

Things to consider before you configure an instant access mount point 27
Backing up an Oracle database using Oracle copilot policy with universal share 28
Configure an instant access mount 28
View the livemount details of an instant access mount 29
Configuring Auto Image Replication for Oracle instant access backups 30
Delete an instant access mount 31
NetBackup for Oracle terms 31
Frequently asked questions 33

Chapter 7 Other Oracle configuration 36

Load balance Oracle RAC instances 36
Configure an Oracle Wallet with RAC within NetBackup 37

Introducing the NetBackup web user interface

This chapter includes the following topics:

- About the NetBackup web UI
- Terminology
- Sign in to the NetBackup web UI
- Sign out of the NetBackup web UI

About the NetBackup web UI

The NetBackup web user interface provides the following features:

- Ability to access the primary server from a web browser, including Chrome and Firefox. For details on supported browsers for the web UI, see the NetBackup Software Compatibility List.

  Note that the NetBackup web UI may behave differently for different browsers. Some functionality, for example a date picker, may not be available on all browsers. These inconsistencies are due to the capabilities of the browser and not because of a limitation with NetBackup.
- A dashboard that displays a quick overview of the information that is important to you.
- Role-based access control (RBAC) that lets the administrator configure user access to NetBackup and to delegate the tasks for workload protection.
- Protection of assets is achieved through protection plans, job management, and visibility of the protection status of assets.

- Workload administrators can create protection plans, manage credentials, subscribe assets to the protection plans that meet the SLO, monitor protection status, and perform self-service recovery of assets.

Note: The NetBackup web UI is best viewed at a 1280x1024 or higher screen resolution.

Access control in the NetBackup web UI

NetBackup uses role-based access control to grant access to the web UI. Access control is accomplished through roles.

- A role defines the operations that a user can perform and the features that the user can access in the web UI. For example, access to any workload assets, protection plans, or credentials.
- RBAC is only available for the web UI and the APIs.

  Other access control methods for NetBackup are not supported for the web UI and APIs, except for the Enhanced Auditing (EA).

Monitor NetBackup jobs

The NetBackup web UI lets administrators more easily monitor NetBackup job operations and identify any issues that need attention.

Protection plans: One place to configure schedules, storage, and storage options

Protection plans offer the following benefits:

- A default workload administrator can select the protection plans to use to protect assets.
- With the necessary RBAC permissions, a workload administrator can create and manage protection plans, including the backup schedules and storage that is used.
- When you select from your available storage, you can see any additional features available for that storage.

Self-service recovery

The NetBackup web UI makes it easy for a workload administrator to recover VMs, databases, or other asset types applicable to that workload.

Terminology

The following table describes the concepts and terms in web user interface.

Table 1-1 Web user interface terminology and concepts

Term	Definition
Asset group	See *intelligent group*.
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.
Backup now	An immediate backup of an asset. NetBackup performs a one-time, full backup of an asset using the selected protection plan. This backup does not affect any scheduled backups.
Intelligent group	Allows NetBackup to automatically select assets for protection based on the criteria (queries) that you specify. An intelligent group automatically stays up-to-date with changes in the production environment. These groups are also referred to as asset groups. These groups appear under the tab **Intelligent VM groups** or **Intelligent groups**.
Protection plan	A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once a protection plan is set up, assets can be subscribed to the protection plan.
RBAC	Role-based access control. The role administrator can delegate or limit access to the NetBackup web UI through the roles that are configured in RBAC. **Note:** The roles that you configure in RBAC do not control access to the NetBackup Administration Console.
Role	For RBAC, defines the operations that a user can perform and the assets or objects that they can access. For example, you can configure a role to manage recovery of specific databases and the credentials that are needed for backups and restores.
Storage	The storage to which the data is backed up, replicated, or duplicated (for long-term retention).
Subscribe, to a protection plan	The action of selecting an asset or an asset group to subscribe to a protection plan. The asset is then protected according to the schedule in the plan. The web UI also refers to *Subscribe* as *Add protection*.
Unsubscribe, from a protection plan	*Unsubscribe* refers to the action of removing protection or removing an asset or asset group from a plan.

Table 1-1 Web user interface terminology and concepts *(continued)*

Term	Definition
Workload	The type of asset. For example: VMware, RHV, AHV, Microsoft SQL, Oracle, Cloud, or Kubernetes.

Sign in to the NetBackup web UI

Authorized users can sign in to a NetBackup primary server from a web browser, using the NetBackup web UI.

For more information, refer to the *Authorized users* section in the *NetBackup™ Web UI Administrator’s Guide*.

The following sign-in options are available:

- Sign in with a username and password
- Sign in with a certificate or smart card
- Sign in with single sign-on (SSO)

Sign in with a username and password

Only authorized users can sign in to NetBackup web UI. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup primary server using a username and password

1 Open a web browser and go to the following URL.

https://*primaryserver*/webui/login

The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.

2 Depending on the sign-in options that are available, choose from the following:

- Enter your credentials and click **Sign in**.
- If the default method is not username and password, click **Sign in with username and password**. Then enter your credentials.

The following are example credentials:

For this type of user	Use this format	Example
Local user	*username*	**jane_doe**
Windows user	*DOMAIN\username*	**WINDOWS\jane_doe**

For this type of user	Use this format	Example
UNIX user	*username@domain*	**john_doe@unix**

Sign in with a certificate or smart card

You can sign in to NetBackup web UI with a smart card or digital certificate if you are an authorized user. Contact your NetBackup security administrator for more information.

To use a digital certificate that is not on a smart card, you must first upload the certificate to the browser's certificate manager. See the browser documentation for instructions or contact your certificate administrator for more information.

To sign in with a certificate or smart card

1. Open a web browser and go to the following URL.

   https://*primaryserver*/webui/login

   The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.

2. Click **Sign in with certificate or smart card**.
3. When your browser prompts you, select the certificate.

Sign in with single sign-on (SSO)

You can sign in to NetBackup web UI with the single sign-on (SSO) option if SAML is configured as an identity provider in your NetBackup environment. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup primary server using SSO

1. Open a web browser and go to the following URL.

   https://*primaryserver*/webui/login

   The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.

2. Click **Sign in with single sign-on**.
3. Follow the steps as provided by your administrator.

   On subsequent logons, NetBackup signs you in automatically to the primary server.

Sign out of the NetBackup web UI

Note that NetBackup automatically signs you out of the web UI after 24 hours, which is the maximum time that is allowed for a user session. After that time NetBackup requires that you sign in again. You can also sign out if you want to change the sign-in option that you want to use (username and password, smart card, or single sign-on (SSO)).

To sign out of the NetBackup web UI

◆ On the top right, click the profile icon and click **Sign out**.

Chapter 2

Monitoring NetBackup

This chapter includes the following topics:

- The NetBackup dashboard
- Job monitoring
- Search for or filter jobs in the jobs list

The NetBackup dashboard

The NetBackup dashboard provides a quick view of the details that are related to your role in your organization.

Table 2-1 The NetBackup dashboard

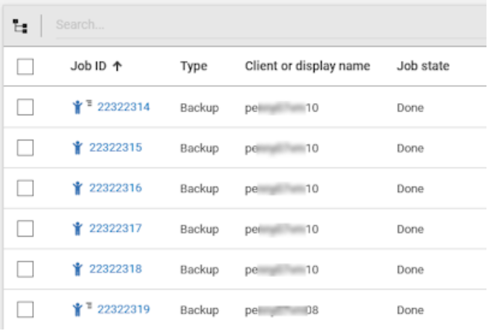
Dashboard widget	Description
Jobs	Lists job information, including the number of active and queued jobs and the status of attempted and completed jobs.

Job monitoring

Use the **Jobs** node in the Activity monitor to monitor the jobs in your NetBackup environment. The default view for jobs is the **List view** that contains the non-hierarchical list of all the jobs. You can also use the **Hierarchical view** to see the hierarchy of parent and child jobs.

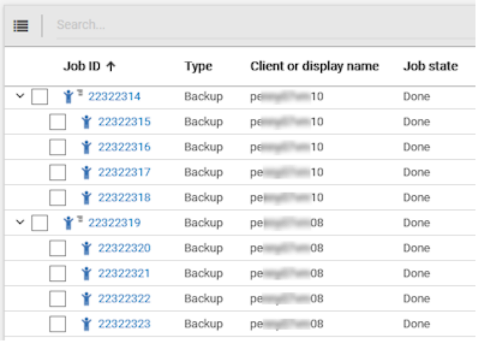
List view

Hierarchy view



Search...

□	Job ID ↑	Type	Client or display name	Job state
□	22322314	Backup	pe[redacted]10	Done
□	22322315	Backup	pe[redacted]10	Done
□	22322316	Backup	pe[redacted]10	Done
□	22322317	Backup	pe[redacted]10	Done
□	22322318	Backup	pe[redacted]10	Done
□	22322319	Backup	pe[redacted]08	Done



Search...

	Job ID ↑	Type	Client or display name	Job state
⌄ □	22322314	Backup	pe[redacted]10	Done
□	22322315	Backup	pe[redacted]10	Done
□	22322316	Backup	pe[redacted]10	Done
□	22322317	Backup	pe[redacted]10	Done
□	22322318	Backup	pe[redacted]10	Done
⌄ □	22322319	Backup	pe[redacted]08	Done
□	22322320	Backup	pe[redacted]08	Done
□	22322321	Backup	pe[redacted]08	Done
□	22322322	Backup	pe[redacted]08	Done
□	22322323	Backup	pe[redacted]08	Done

The type of jobs that you can view and manage depend on the RBAC role that you have. For example, a workload administrator (such as the Default VMware Administrator role) can view and manage only jobs for that workload. In contrast, the Administrator role lets you view and manage all NetBackup jobs.

If you have an RBAC role that allows access to jobs, you can see the jobs list in the job hierarchy view. For example, the Default VMware Administrator role lets you see VMware jobs in the hierarchy view. However, if you only have access to one or more VMs (asset-level access), no jobs display in the job hierarchy view.

Search for or filter jobs in the jobs list

You can search for jobs in the Activity monitor or create filters to customize the jobs that are displayed.

Search for jobs in the jobs list

The search feature lets you search for the following job information: status code (complete status code #); policy name; client or display name; client; job ID (complete job ID #), or the job's parent ID.

Search for jobs in the jobs list

1 Click **Activity monitor > Jobs**.

2 In the **Search** box, type the keyword you want to find. For example, a client name or a status code number.

Filter the job list

To filter the job list

1. Click **Activity monitor > Jobs**.
2. In the toolbar, click the **Filter** icon.
3. Click on a filter that you created. Or, click **All jobs** to display all of the available jobs.

Managing Oracle

This chapter includes the following topics:

- About Oracle discovery
- Add an Oracle instance
- Add an Oracle instance group
- Clean up Oracle instance and databases

About Oracle discovery

The NetBackup Discovery Service (`nbdisco`) discovers Oracle database instances throughout the NetBackup environment. The discovery service reports to the primary server when it finds instances and databases to help you build an Oracle Intelligent Policy. The service polls the clients upon NetBackup installation and periodically after installation (every 4 hours). Instance management collects the discovered instances in an instance repository. The user can access this repository on the NetBackup web UI or by using the `nboraadm` command.

The NetBackup Discovery Service searches for instances and databases in different areas where Oracle is installed. The following areas are where the Discovery Service searches:

- Non-RAC Single instances are discovered by searching the `oratab` file on UNIX and from the registry on Windows.
- NetBackup looks for the Oracle health check files that are found in the Oracle home. These are not cleaned up when a database is deleted. You may need to delete them manually otherwise NetBackup can continue to find the databases that are deleted.

- Oracle RAC databases are discovered when NetBackup queries the Oracle Cluster Ready Services (CRS) using the Oracle Clusterware high availability API.

Oracle RAC in the web UI does not support upgrades from legacy script-based policies. Also, there is no web UI support for the configurations that are created using Appendix A or Appendix B in the NetBackup for Oracle Administrator's Guide.

To allow the NetBackup web UI to discover a RAC instance or cluster:

- Remove the Oracle RAC from any configuration that is setup using Appendix A or Appendix B in the NetBackup for Oracle Administrator's Guide.
- Remove any Oracle RAC from existing OIP policies in the current NetBackup Administrator's Console.

Note: When an Oracle RAC database is discovered, that database does not have a **Database ID**. A **Database ID** is required to manually add additional RAC instances to the database. You must register the RAC database and provide a **Database ID** before adding additional instances.

See "Manage credentials for an instance or an Oracle RAC database" on page 23.

See "Add an Oracle Real Application Cluster (RAC)" on page 21.

By default, this service is enabled to report instances. However, you can use the `REPORT_CLIENT_DISCOVERIES` client configuration entry to shut down or restart the service on a particular client. By default, `REPORT_CLIENT_DISCOVERIES` is not present in the Windows registry or the UNIX `bp.conf` file.

To change the default setting, use `bpsetconfig` to add or change the entry:

- In the Windows registry.
- In the `/usr/openv/netbackup/bp.conf` file on UNIX.

Use the following format: `REPORT_CLIENT_DISCOVERIES = TRUE | FALSE`

Set `REPORT_CLIENT_DISCOVERIES` to `FALSE` to shut down the discovery service. The service shuts down within 10 minutes and remains down on the client. To turn on the discovery service on that client, set `REPORT_CLIENT_DISCOVERIES` to `TRUE` or remove the entire entry. Then run `bp.start_all` on the client to restart the service.

To set this value on a client remotely, run the following command from the primary server:

```
echo REPORT_CLIENT_DISCOVERIES=FALSE | bpsetconfig -h clientname
```

Add an Oracle instance

In NetBackup, you can manually add an instance or allow NetBackup to scan for any Oracle instances. The NetBackup Discovery Service (`nbdisco`) discovers Oracle database instances throughout the NetBackup environment. All of the instances that are manually added or NetBackup discovers are populated in the **Instance** tab table.

Note: For more information about instance management, see *Instance management for an Oracle Intelligent Policy* in the NetBackup for Oracle Administrator's Guide.

To manually add an instance

1. On the left, click **Workloads** > **Oracle** and then click **Instances**.
2. In the **Instances** tab, click **Actions** and select **Add instance**.
3. Enter the required information for the instance.
4. (Optional) Enter the **Override default TNS_ADMIN path**if you need to override the default network administration directory on the client system. Enter the fully qualified path for the network administration directory on this host.
5. After all the required information for instance is entered, you can:
   - Click **Finish** to add the instance. Select this option to add the instance to NetBackup without credentials. The credentials can be added at a later time.
   - Click **Add and manage credentials** to add credentials for the instance at this time.

     In the **Manage credentials for instance** screen, select one of the appropriate credential authentication methods from the list of **Instance credentials**.

     - Enter all required information for the selection. For all **Instance credentials** options, you can select **Use Oracle RMAN recovery catalog**.

     Click **Finish** to add this instance with credentials.

To add an instance with the Discovery option

1. On the left, click **Workloads** > **Oracle** and then click the **Instances** tab.
2. In the **Instances** tab, click **Actions** and select **Discover instances**.
3. Click **Start discovery**.
4. Add credentials for the instance per step 5.

To automatically register a new instance

1. On the left, click **Workloads** > **Oracle** and then click the **Instances** tab.
2. In the **Instances** tab, click **Actions** and select **Auto registration**.
3. Select the instance group from the **Select instance group** drop-down.
4. (Optional) Select **Override default UNIX TNS_ADMIN path** or **Override default Windows TNS_ADMIN path** and enter the path.
5. Click **Save**.

Add an Oracle instance group

NetBackup lets you create an instance group that includes instances with a common set of credentials. You can create a default instance group for newly-discovered instances. Oracle RAC databases cannot be added to an instance group.

To add an Oracle instance group

1. On the left, click **Workloads** > **Oracle** and then click **Instance groups**.
2. In the **Instance groups** tab, click **Actions** and select **Add instance group**.

   Note: Instance group names cannot be localized. NetBackup does not support non-US ASCII characters in the instance group name.

3. Enter the required information.
4. Enter the credential information for the **Instance credentials** option you select.

   The credential options change based on the option that is selected in **Instance credentials**.

5. Click **Finish**.

See “Add an Oracle instance” on page 17.

See “Add an Oracle Real Application Cluster (RAC)” on page 21.

Clean up Oracle instance and databases

NetBackup can automatically remove orphaned instances and databases if they are not registered or are no longer discoverable. Orphaned instances are the databases that were discovered at one time but were never registered. This operation is done automatically once you set the number of days.

To set up automatic cleanup of instances

1. On the left, click **Workloads** > **Oracle** and then click **Instances**.
2. In the **Instances** tab, click **Actions** and select **Instances cleanup**.
3. Set the number of days and then click **Cleanup**.

See “Add an Oracle instance” on page 17.

See “Add an Oracle Real Application Cluster (RAC)” on page 21.

See “Edit or delete an Oracle RAC database” on page 22.

Chapter 4

Managing Oracle RAC

This chapter includes the following topics:

- Oracle Real Application Clusters (RAC)
- Add an Oracle Real Application Cluster (RAC)
- Edit or delete an Oracle RAC database

Oracle Real Application Clusters (RAC)

In a Real Application Clusters (RAC) environment, many Oracle database instances exist on separate servers, each with direct connectivity to a single Oracle database. All the servers can run transactions concurrently against the same database. Should any single server or instance fail, processing continues on the surviving servers.

RAC supports all Oracle backup features that are available in exclusive mode, including online backups and offline backups of an entire database or individual tablespaces.

Currently, only the NetBackup web UI has full RAC support for Oracle policies. This manual contains only the information that is needed to add an Oracle RAC to the web UI.

To manage classic policies you must use the NetBackup Administration Console. However, Oracle policies protecting an Oracle RAC can be managed in the NetBackup web UI. See the NetBackup for Oracle Administrator’s Guide for full details on creation and management of an Oracle policy.

Note: Any nodes of the Oracle RAC cluster that is used in backups, must be running a NetBackup client. The version should be the same version across the cluster. For Oracle RAC OIP support the NetBackup 8.3 client is required.

Add an Oracle Real Application Cluster (RAC)

Use this procedure to add an Oracle RAC and the appropriate credentials. Once an Oracle RAC is added, you can create a policy in the web UI to schedule a backup of the Oracle RAC.

Add an Oracle RAC

1. On the left, click **Workloads** > **Oracle** and then click **RAC databases**.
2. In the **RAC databases** tab, click **Actions** and select **Add RAC**.
3. Enter all the required information for the Oracle RAC database and then click **Next**.
4. Enter all the required information for an Oracle RAC instance and then:
   - Click **Finish** to add the Oracle RAC and the instance. Select this option to add the RAC to NetBackup without credentials. The credentials can be added at a later time.
   - Click **Add and manage credential** to add credentials for the Oracle RAC database at this time. Choose the credential option for this RAC:
     - **Use Oracle Wallet**. Enter the Oracle Wallet folder location. The folder location must be on a file system.

       Using Oracle Wallet requires these items:
       - The same path for each node of the cluster.
       - Each instance must have its own entry in a shared wallet.
       - You must put a specific connection identifier in the wallet.
         For more information about the connect identifier:
         See “Configure an Oracle Wallet with RAC within NetBackup” on page 37.
       - A single instance must have the path to the wallet and the Net service name (TNS alias).
     - **RAC database credentials**. Enter a username and password.
     - **Use Oracle RMAN recovery catalog**. Select this option and enter a username, password, and the Net service name (TNS alias). This option can be used with Oracle Wallet but it must be the same wallet as the database connection.

   Enter the appropriate credential information for the Oracle RAC and then click **Add credentials**.

See “Load balance Oracle RAC instances” on page 36.

See “Add an Oracle instance” on page 17.

Edit or delete an Oracle RAC database

Edit an Oracle RAC database

Use this procedure to edit the information that is entered for the Oracle RAC database.

Edit an Oracle RAC database

1. On the left, click **Workloads** > **Oracle** and then click **RAC databases**.
2. In the **RAC databases** tab, click the Actions menu for the RAC and select **Edit**.

   Also, you can click **Edit RAC database** on the top right of the page when viewing the **Oracle RAC database** details page.
3. Enter the required information and then click **Next**.

   Changing the **RAC type** is optional when editing an Oracle RAC.

   Editing the **Backup host** is optional.

   You cannot edit the **Database unique name** or the **Database ID**.
4. Enter the required information and then click **Save**.

Delete an Oracle RAC database

Use this procedure to delete an Oracle RAC.

Delete an Oracle RAC database

1. On the left, click **Workloads** > **Oracle** and then click **RAC databases**.
2. In the **RAC databases** tab, click the Actions menu for the Oracle RAC database and select **Delete**.
3. Click **OK**.

See “Add an Oracle Real Application Cluster (RAC)” on page 21.

See “Add an Oracle instance” on page 17.

See “Clean up Oracle instance and databases” on page 18.

Managing Oracle credentials

This chapter includes the following topics:

- Manage credentials for an instance or an Oracle RAC database

Manage credentials for an instance or an Oracle RAC database

You can add or update credentials for instances and RAC databases at any time. When you manually add an instance or a RAC database, you can choose not to include the credentials at time of entry. After the discovery service adds new instances and RAC databases to the repository, you can add credentials. NetBackup provides a way to enter the proper credentials for your instance and RAC databases.

When an Oracle RAC database is discovered, that database does not have a **Database ID**. A **Database ID** is required to manually add additional RAC instances to the database. You must register the RAC database and provide a **Database ID** before adding additional instances.

To add credentials for an instance

1 On the left, click **Workloads** > **Oracle** and then click **Instances**.

2 In the **Instances** tab, click the Actions menu for the instance and select **Manage credentials**.

3 In the **Manage credentials for instance** screen, select one of the appropriate credential authentication methods:

   - Select **Add to group and register using group credentials** to register the instance using group credentials. Select the instance group name from the drop-down.

- Select **Use instance credentials** to register using the instance credentials. Select the credential option for this instance and enter all required information.

4 Click **Finish**.

To add credentials for a RAC database

1 On the left, click **Workloads** > **Oracle** and then click **RAC databases**.

2 In the **RAC databases** tab, click the Actions menu for the instance and select **Manage credentials**.

3 In the **Manage credentials for RAC database** screen, select one of the appropriate credential authentication methods:

- Select **Use Oracle Wallet** to use the credentials that are located in the Oracle Wallet. For non-RAC installations, the instance net service name must be stored in the Oracle Wallet as defined in Oracle's wallet documentation.
- Select **RAC database credentials** and enter the correct **User name** and **Password** for the database.
- (Optional) Enter credentials for the **Oracle RMAN recovery catalog credentials** section.

4 Click **Add credentials**.

Oracle Copilot with instant access and universal share

This chapter includes the following topics:

- Prerequisites when you configure an instant access Oracle database
- Things to consider before you configure an instant access mount point
- Backing up an Oracle database using Oracle copilot policy with universal share
- Configure an instant access mount
- View the livemount details of an instant access mount
- Configuring Auto Image Replication for Oracle instant access backups
- Delete an instant access mount
- NetBackup for Oracle terms
- Frequently asked questions

Prerequisites when you configure an instant access Oracle database

The following prerequisites apply when you configure Oracle instant access databases:

Prerequisites:

- For Build Your Own (BYO) server, the operating system version must be same as the latest appliance operating system version that is RHEL 7.6 and later.
- For BYO server, NGINX is installed on the storage server.
  - The NGINX version must be same as the one in the corresponding official RHEL version release. You need to install it from the corresponding RHEL yum source (EPEL).
  - Ensure that the `policycoreutils` and `policycoreutils-python` packages are installed from the same RHEL yum source (RHEL server). Then run the following commands:
    - `semanage port -a -t http_port_t -p tcp 10087`
    - `setsebool -P httpd_can_network_connect 1`
- For BYO server, the `/mnt` folder on the storage server cannot be mounted by any mount points directly. User mount points must be mounted to its subfolders.
- For BYO server, enable the `logrotate` permission in SELinux using the following command:

  ```
  semanage permissive -a logrotate_t
  ```
- Instant access is only supported for Oracle backup images when the following conditions are met:
  - The backup is an Oracle Copilot incremental merge (**Whole Database-Datafile Copy Share** and **Database Backup Shares**).

    For more information, see *Backup Selections tab* in the NetBackup for Oracle Administrator's Guide.
  - The backup is a full database backup.
  - The primary server, media server, storage server, and client version must be NetBackup 10.0 or later. The NetBackup appliance must be running software version 4.0 or later.
  - The storage server must be an appliance or BYO that meets the earlier specified prerequisites.

Hardware configuration requirement of instant access

Table 6-1 Hardware configuration

CPU	Memory	Disk
■ Minimum 2.2-GHz clock rate. ■ 64-bit processor. ■ Minimum 4 cores; 8 cores recommended. For 64 TB storage, the Intel x86-64 architecture requires eight cores.	■ 16 GB (For 8 TB to 32 TB of storage) 1 GB RAM for 1 TB storage. ■ 32 GB of RAM for more than 32 TB storage. ■ An additional 500 MB of RAM for each live mount.	Disk size depends on the size of your backup. Refer to the hardware requirements for NetBackup and Media Server Deduplication Pool (MSDP).

Things to consider before you configure an instant access mount point

The instant access feature enhances the Oracle Intelligent Policy and gives you options to protect an Oracle database using a universal share on a NetBackup appliance or BYO server. This feature gives you better control of backups when an Oracle database backup is placed in a database share by the DBA. This feature also lets you choose a database share as the destination for the first backup copy. The backup copy is a full set of database data file copies created, incrementally updated, and protected by NetBackup.

For more information about universal share, refer to NetBackup Administrator's Guide, Volume I.

Note the following about the instant access Oracle feature:

- The oracle copilot backup with universal share can only be used for instant access and cannot be used for Oracle Copilot instant recovery.
- For instant access to work following an upgrade of NetBackup, first restart the NetBackup Web Service on the primary server. Run the following commands:
  - `/usr/openv/netbackup/bin/nbwmc stop`
  - `/usr/openv/netbackup/bin/nbwmc start`

Backing up an Oracle database using Oracle copilot policy with universal share

Before you configure Oracle copilot instant access, you must back up the Oracle database using the Oracle copilot policy with universal share.

To back up Oracle copilot with universal share

1. Create a universal share with the NFS protocol.

   Refer to the information on creating a universal share in the `NetBackup Web UI Administrator's Guide`.

2. Mount the universal share on the Oracle client.

3. Create an Oracle Copilot policy and then in Backup Selections, select the mount point of the universal share.

   Refer to the NetBackup™ Copilot™ for Oracle Configuration Guide for information about how to configure an Oracle copilot policy.

Configure an instant access mount

You can configure an instant access database from a full backup. The full backup must come from an Oracle copilot backup with data file copies in the NetBackup universal share.

You can configure an instant access Oracle database from the web UI or use the REST API.

Configure an instant access mount

1. On the left, select **Workloads > Oracle**.

2. On the **Databases** tab, click the database for which you want to configure the instant access database.

3. Click the **Recovery points** tab, then click the date on which the backup occurred.

   The available images appear in rows with the backup timestamp for each image.

4. Right-click on the backup image and click **Actions > Configure instant access mount**.

   Note: This option is only displayed if the recovery point supports instant access.

   ---

5 Enter the host name where you want to configure the instant access mount for the database.

6 Click **Configure**.

7 After the instant access job starts, click on the **Restore activity** tab to view the progress.

See "View the livemount details of an instant access mount" on page 29.

View the livemount details of an instant access mount

To view the livemount details of an instant access mount

1 On the left, select **Workloads > Oracle**.

2 Click the **Instant access databases** tab.

The tab lists the instant access databases.

3 On the **Instant access databases** tab, click on the database name to see its details.

Clone of	Instant access database for which you configured the instant access mount.
Storage server	Name of the storage server.
Mount ID	Unique ID for an instant access livemount.
Export path	Exported instant access livemount path from the storage server.
Recovery point time	Date when the recovery point was created.
Created on	Date when the instant access livemount was created.
Retention	Time period for which you want the instant access mount to be retained.

4 To save the full export path to your Clipboard, click on the copy-to-clipboard icon next to the export path in the details listing.

Configuring Auto Image Replication for Oracle instant access backups

You must add replication to the stream and the snap storage lifecycle policies (SLPs) to ensure that the SLP metadata is replicated for restore from an instant access backup image.

Oracle copilot with universal share's SLP (storage life policy) must include the backup from snapshot operation. The backup can only be used for Instant Access. Instant Recovery (nborair) is not supported.

To configure Auto Image Replication for Oracle instant access backups

1. Configure Auto Image Replication between two NetBackup master servers.

   For more information about configuring Auto Image Replication, refer to the NetBackup™ Administrator's Guide, Volume I.

2. For Oracle instant access create the following storage lifecycle policies (SLPs):

   - stream-slp for backup
   - snap-slp for backup from snapshot

   For more information about configuring storage lifecycle policies, refer to the NetBackup™ Administrator's Guide, Volume I.

3. Sign in to the NetBackup web UI.

4. On the left, click **Storage > Storage lifecycle policies** and select the **stream-slp** policy.

5. In the **Backup** operation, click **Actions** and select **Add child**.

6. On the **Properties** pane, select the **Replication** operation and then select the **Target import SLP**.

7. Click **Create** to add the child.

8. On the NetBackup web UI, click **Storage > Storage lifecycle policies** and select the **snap-slp** policy.

9. In the **Snapshot** and **Backup from Snapshot** operations, click **Actions** and select **Add child**.

10. On the **Properties** pane, select the **Replication** operation and then select the **Target import SLP**.

11. Click **Create** to add the child.

    Replication then runs successfully for **Backup** and **Backup from Snapshot** operations in both SLPs.

Delete an instant access mount

You can delete the instant access mount when it is no longer used.

To delete an instant access mount

1 On the left, select **Workloads > Oracle**.

2 Click the **Instant access databases** tab.

The tab lists the instant access databases.

3 Select **Actions > Remove Instant access mount > Delete**.

Ensure that you run the RMAN crosscheck command after the mount is deleted.

4 After an instant access mount share is deleted, perform an RMAN crosscheck of the share before the next backup to prevent failures.

5 Specify the "disk" type instead of a "SBT_TAPE" type. Use the default `<NetBackup_policyname>`. Or, if the datafile copy tag is changed in the **Oracle** tab, use that tag name in place of `<NetBackup_policyname>`.

Example command:

```
Run {

Allocate channel ch00 type 'disk';

crosscheck backup tag <Netbackup_policyname>;

delete noprompt expired backup;

crosscheck copy <Netbackup_policyname>;

delete noprompt expired copy;

release channel ch00;

}
```

NetBackup for Oracle terms

The table describes the important terms that might be new to an Oracle database administrator or a NetBackup administrator.

Term	**Definition**
Full backup	A full backup backs up all the blocks into the backup set, skipping only data file blocks that have never been used. Note that a full backup is not the same as a whole database backup; "full" is an indicator that the backup is not incremental. A full backup has no effect on subsequent incremental backups, which is why it is not considered part of the incremental strategy. In other words, a full backup does not affect which blocks are included in subsequent incremental backups.
Incremental backup	An incremental backup is a backup of only those blocks that have changed since a previous backup. Oracle lets you create and restore incremental backups of data files, tablespaces, and a database. You can include a control file in an incremental backup set, but the control file is always included in its entirety. No blocks are skipped.
Multilevel incremental backup	RMAN lets you create multilevel backups. RMAN can create multilevel incremental backup. A value of 0 or 1 denotes each incremental level. A level 0 incremental backup, which is the base for subsequent incremental backups, copies all blocks containing data. You can create a level 0 database backup as backup sets or image copies. The only difference between a level 0 incremental backup and a full backup is that a full backup is never included in an incremental strategy. Thus, an incremental level 0 backup is a full backup that happens to be the parent of incremental backups whose level is greater than 0. The benefit to performing multilevel incremental backups is that you do not back up all of the blocks all of the time. Incremental backups at a level greater than zero (0) only copy the blocks that were modified. Hence, the backup size can be significantly smaller and the backup might require much less time. The size of the backup file depends solely upon the number of blocks that are modified and the incremental backup level.
Differential incremental backup	In a differential level 1 backup, RMAN backs up all blocks that have changed since the most recent incremental backup at level 1 (cumulative or differential) or level 0. For example, in a differential level 1 backup, RMAN determines which level 1 backup is the most recent backup. RMAN backs up all blocks that have been modified after that backup. If no level 1 is available, then RMAN copies all blocks that have changed since the base level 0 backup.

Term	Definition
Cumulative incremental backup	In a cumulative level 1 incremental backup, RMAN backs up all blocks that have changed since the most recent backup at level 0. Cumulative incremental backups reduce the work that is needed for a restore. The cumulative incremental backup ensures that you only need one incremental backup from any particular level at restore time. Cumulative backups require more space and time than differential incremental backups, because they duplicate the work that previous backups did at the same level.

Frequently asked questions

Here are some frequently asked questions for Oracle instant access.

Frequently asked questions	Answer
How can I enable the Oracle instant access feature on BYO after storage is configured or upgraded without the NGINX service installed?	Perform the steps in the following order: **1** Install the required NGINX service version. **2** Run the command: `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo` **3** Ensure that the new BYO NGINX configuration entry `/etc/nginx/conf.d/byo.conf` is part of the HTTP section of the original `/etc/nginx/nginx.conf` file.
How can I resolve the following issue in the vpfs-config.log file that is raised from? `Verifying that the MSDP REST API is available via https on port 10087`	Perform the steps in the following order: **1** Install the `policycoreutils` and `policycoreutils-python` packages through the yum tool. **2** As required by SELinux for NGINX, add the following rules to bind on the 10087 port. ■ `semanage port -a -t http_port_t -p tcp 10087` ■ `setsebool -P httpd_can_network_connect 1` **3** Run the following command: `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`

Frequently asked questions	Answer
Instant Access for BYO uses a self-signed certificate by default and only supports *.pem external certificate. How do I replace it with a certificate signed by external CA (*.pem certificate), if required?	To configure the external certificate, perform the following steps: **1** If the new certificate is already generated (the certificate must contain long and short host names for the media server), go to step 5. **2** Create the RSA public or private key pair. **3** Create a certificate signing request (CSR). The certificate must contain long and short host names for the media server. **4** The external Certificate Authority creates the certificate. **5** Replace `<PDDE Storage Path>/spws/var/keys/spws.cert` with the certificate and replace `<PDDE Storage Path>/spws/var/keys/spws.key` with the private key. **6** Run the following command to reload the certificate: `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`
How can I disable media automount for the instant access livemount share in gnome? If the automount is enabled, the source folder is mounted from the livemount share in gnome and smaller disks appear. In this scenario, the instant access feature does not work properly. The mounted disk content source is from the `.../meta_bdev_dir/...` folder under livemount share, while the mount target is in the `/run/media/...` folder.	Follow the guideline to disable the gnome automount: https://access.redhat.com/solutions/20107

Frequently asked questions	Answer

How can I resolve the following issue in the `/var/log/vpfs/vpfs-config.log` file?
`**** Asking the NetBackup Webservice to trust the MSDP webserver (spws) **** /usr/openv/netbackup/bin/nblibcurlcmd failed (1):`
	Perform the steps in the following order:
	1 Ensure that your NetBackup primary server is up and there is no firewall blocking the connection between the primary server and storage server.
	2 Run the following command on storage server to verify the connection status:
	`/usr/openv/netbackup/bin/bpclntcmd -pn`
	3 Wait for the NetBackup primary server to start and for an established connection between the NetBackup primary server and storage server. Then run the following command:
	`/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`

Other Oracle configuration

This chapter includes the following topics:

- Load balance Oracle RAC instances
- Configure an Oracle Wallet with RAC within NetBackup

Load balance Oracle RAC instances

NetBackup can be set up to load balance the instances that makeup the Oracle RAC. Use this feature to distribute the backup load across all of the instances and to exclude any Oracle RAC instances from the backup.

To load balance Oracle RAC instances

1 On the left, click **Workloads** > **Oracle** and then click **RAC databases**.

2 In the **RAC databases** tab, click the Actions menu for the Oracle RAC database and select **Load balance**.

3 In the **Select number of instances to load balance**, select the number of instances to include for load balancing.

If you select **All**, all instances in the Oracle RAC are available for load balancing.

4 In the table, select the instance or instances you want to move up or down in priority.

5 Click **Move up** or **Move down** to move the instances.

Click **Move up** to move the instance or instances to the top of the list.

Click **Move down** to move the instance or instances to the bottom of the list.

6 (Optional) If you select **Do not use** in the action menu on the right, that instance moves to the **RAC instances excluded from backup** table.

NetBackup does not use this instance when backup operations are performed.

7 Click **Save**.

See "Add an Oracle Real Application Cluster (RAC)" on page 21.

Configure an Oracle Wallet with RAC within NetBackup

The configuration and setup of the Oracle Wallet in NetBackup is a two-step process. You add descriptors first, then you register the wallet. In the cases of Oracle RAC, your descriptors must enumerate the list of RAC instances that comprise your RAC cluster.

NetBackup Oracle Wallet prerequisites:

- The Oracle wallet location must be accessible from all nodes of the RAC cluster.
- Using a shared location is encouraged for maintainability.
  An example storage location can be: An Oracle ACFS file system that is mounted on each node or an NFS share accessible to each node. The mount point of the shared location must be the same on each node.
- If the wallet is not in a shared location, it must be in an identically duplicate location on each node of the RAC cluster. The full contents of the wallet must also be duplicated on each node of the RAC cluster.

To configure Oracle Wallet with RAC in NetBackup:

1 Retrieve the RAC connect descriptors for all instances in the RAC database. Place the list of connect descriptors in a text file for easy access at step 2. Use one of the following methods:

   Get RAC connect descriptors from the NetBackup web UI:

   - On the left, click **Workloads** > **Oracle** and then click **RAC databases**.
   - Click **RAC connect descriptors** from the action menu on the right in the RAC database row.
   - Copy each full RAC connect descriptor by highlighting the text save the connector for later use.

   Get RAC connect descriptors from the NetBackup CLI:

   - Use the `nboraadm` command to retrieve the connect descriptors:

```
nboraadm -list_rac_instances
-rac_db_unique_name RAC_DB_NAME -show_connect_descriptor
```

- Copy the connect descriptors from the screen or use the `'>'` command to create a file with the connect descriptors.

Manually create the RAC connect descriptors:

- If you don't have this information, use the web UI Oracle RAC functionality or `nboraadm` to retrieve the information needed. You need to retrieve the scan name, service name, and port number for the given RAC database. If the RAC instances for the RAC database are not known, use either interface to collect the list of instance names.
- For each instance of a RAC, you must insert this information to create a connect descriptor. Insert the scan name, service name, and port number (from RAC database), as well as the instance name (from RAC instance) into the following example:

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=<INSERT SCAN NAME>)(PORT=<INSERT PORT NUMBER>))
(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=<INSERT SERVICE NAME>)
(INSTANCE_NAME=<INSERT INSTANCE NAME>)))
```

2 Add the connect descriptors with the Oracle `MKSTORE` utility. The descriptors are case-sensitive and must match exactly to what is in NetBackup.

```
mkstore -wrl /db/orac183/wallet/ -CreateCredential
'(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=exampleScanName.veritas.com)
(PORT=1521))(CONNECT_DATA=(SERVER=DEDICATED)
(SERVICE_NAME=orac183.veritas.com)(INSTANCE_NAME=orac1831)))'
testUser testPassword
```

```
mkstore -wrl /db/orac183/wallet/ -CreateCredential
'(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=exampleScanName.veritas.com)
(PORT=1521))(CONNECT_DATA=(SERVER=DEDICATED)
(SERVICE_NAME=orac183.veritas.com)(INSTANCE_NAME=orac1832)))'
testUser testPassword
```

3 Register the RAC with the wallet path using the web UI.

See “Add an Oracle Real Application Cluster (RAC)” on page 21.

To register the RAC with the wallet path from the CLI, run `nboraadm -register_rac_db`.

If the RAC is registered for the first time from discovery, you need to include the `dbid`. From the CLI, run `nboraadm -register_rac_db -rac_db_unique_name`.

4 (Optional) If you get an error when you attempt to register the RAC, review the error message. Compare the descriptors in the error message with what you generated in step 1 and what you inserted into your Oracle wallet.