

NetBackup™ Web UI Oracle Administrator's Guide

Release 10.1.1

VERITAS™

Last updated: 2022-12-12

Legal Notice

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

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.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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	Managing Oracle	6
	About Oracle discovery	6
	Add an Oracle instance	8
	Add an Oracle instance group	9
	Clean up Oracle instance and databases	9
Chapter 2	Managing Oracle RAC	11
	Oracle Real Application Clusters (RAC)	11
	Add an Oracle Real Application Cluster (RAC)	12
	Edit or delete an Oracle RAC database	13
Chapter 3	Managing Oracle credentials	14
	Manage credentials for an instance or an Oracle RAC database	14
Chapter 4	Oracle Copilot with instant access and universal share	16
	Prerequisites when you configure an instant access Oracle database	16
	Hardware configuration requirement of instant access	18
	Things to consider before you configure an instant access mount point	18
	Backing up an Oracle database using Oracle copilot policy with universal share	19
	Configure an instant access mount	19
	View the livemount details of an instant access mount	20
	Configuring Auto Image Replication for Oracle instant access backups	21
	Delete an instant access mount	22
	NetBackup for Oracle terms	23
	Frequently asked questions	24

Chapter 5	Other Oracle configuration	27
	Load balance Oracle RAC instances	27
	Configure an Oracle Wallet with RAC within NetBackup	28

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 `nboradm` 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 14.

See [“Add an Oracle Real Application Cluster \(RAC\)”](#) on page 12.

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/opensv/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 8.

See [“Add an Oracle Real Application Cluster \(RAC\)”](#) on page 12.

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 8.

See [“Add an Oracle Real Application Cluster \(RAC\)”](#) on page 12.

See [“Edit or delete an Oracle RAC database”](#) on page 13.

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 28.
 - 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 27.

See [“Add an Oracle instance”](#) on page 8.

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 12.

See [“Add an Oracle instance”](#) on page 8.

See [“Clean up Oracle instance and databases”](#) on page 9.

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 **Username** 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.

For instant access using backup copies from cloud LSU (logical storage unit), the primary server and media server must be at NetBackup 10.0.1 or later.
 - The storage server must be NetBackup Appliance, Flex Appliance, Flex WORM, Flex Scale, Media Server Deduplication Pool (MSDP) AKS (Azure Kubernetes Services)/EKS (Amazon Elastic Kubernetes Service) deployment, and BYO on-premises or cloud-based that meets the earlier specified prerequisites.

For more information about limitations of instant access for cloud LSU (logical storage unit), refer to the `NetBackup Deduplication Guide`.

- Oracle Copilot supports a single universal share from NetBackup Appliance, Flex Appliance, Flex WORM, Flex Scale, MSDP AKS (Azure Kubernetes Services)/EKS (Amazon Elastic Kubernetes Service) deployment, and BYO on-premises and supports multiple universal shares from the Flex Scale cluster.

Note: Oracle Copilot with instant access is not supported on a universal share that has WORM enabled storage.

Hardware configuration requirement of instant access

Table 4-1 Hardware configuration

CPU	Memory	Disk
<ul style="list-style-type: none"> ■ 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. 	<ul style="list-style-type: none"> ■ 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. 	<p>Disk size depends on the size of your backup. Refer to the hardware requirements for NetBackup and Media Server Deduplication Pool (MSDP).</p>

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 multiple universal shares. 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/opensv/netbackup/bin/nbwmc stop`
- `/usr/opensv/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 universal shares with the NFS protocol.

Refer to the information on creating a universal share in the [NetBackup Web UI Administrator's Guide](#).

- 2 Mount all the universal shares on the Oracle clients.

- 3 Create an Oracle Copilot policy and then in Backup Selections, select the mount points of the universal shares.

Refer to the [NetBackup™ Copilot™ for Oracle Configuration Guide](#) for information about how to configure an Oracle copilot policy.

Refer to the **Recommendations when you configure an Oracle Copilot with universal shares** section in the [NetBackup for Oracle Administrator's Guide](#).

Refer to the **Troubleshooting issues related to Oracle Copilot with universal shares** section in the [NetBackup for Oracle Administrator's Guide](#).

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 names 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 20.

If you back up multiple universal shares and then create an instant access database, multiple instant access mounts are configured.

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 instant access mounts, it is recommended that you unmount them first from the Oracle clients.

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	<p>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.</p> <p>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.</p>
Incremental backup	<p>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.</p>

Term	Definition
Multilevel incremental backup	<p>RMAN lets you create multilevel backups. RMAN can create multilevel incremental backup. A value of 0 or 1 denotes each incremental level.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Differential incremental backup	<p>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.</p>
Cumulative incremental backup	<p>In a cumulative level 1 incremental backup, RMAN backs up all blocks that have changed since the most recent backup at level 0.</p> <p>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. Cumulative backups duplicate the work that previous backups did at the same level.</p>

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/opensv/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/opensv/pdde/vpfs/bin/vpfs_config.sh  
--configure_byo
```

Instant Access for BYO uses a self-signed certificate by default and only supports *.pem external certificate.

To configure the external certificate, perform the following steps:

How do I replace it with a certificate signed by external CA (*.pem certificate), if required?

- 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/opensv/pdde/vpfs/bin/vpfs_config.sh  
--configure_byo
```

Frequently asked questions

Answer

How can I disable media automount for the instant access livemount share in gnome?

Follow the guideline to disable the gnome automount:

<https://access.redhat.com/solutions/20107>

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.

How can I resolve the following issue in the `/var/log/vpfs/vpfs-config.log` file?

Perform the steps in the following order:

```
**** Asking the NetBackup
Webservice to trust the MSDP
webserver (spws) ****
/usr/opensv/netbackup/bin/nblibcurlcmd
failed (1):
```

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/opensv/netbackup/bin/bpplntcmd -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/opensv/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 12.

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:

```
nboradm -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 `nboradm` 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 12.

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.