Veritas NetBackup™ for Oracle Administrator's Guide

UNIX, Windows, and Linux

Release 8.1

VERITAS™

Veritas NetBackup™ for Oracle Administrator's Guide

Last updated: 2017-09-26

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

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

Introduction

This chapter includes the following topics:

What's new about NetBackup for Oracle

NetBackup contains new features for Copilot using a new command and a single-step restore to ASM storage.

NetBackup Copilot Instant Recovery for Oracle

The Copilot functionality is extended with the introduction of a new command called `nborair`. The `nborair` command can determine if an image is available for Oracle Copilot instant recovery. The functionality is not in the GUI at this time.

See "Creating an instant recovery point from an Oracle Copilot image" on page 142.

See "Deleting an instant recovery point for Oracle Copilot instant recovery" on page 144.

For information about this command, see the NetBackup Commands Reference Guide

Single-step restore to ASM storage

Use RMAN to restore to ASM storage after creating a recovery point using `nborair`. The functionality is not in the GUI at this time.

See "Single-step restore to ASM storage from a Copilot recovery point" on page 151.

Authorized locations for script-based policies

During a backup, NetBackup checks for scripts in the default script location or the authorized location(s). Use the `nbsetconfig` to configure authorized locations or place the script in the default location.

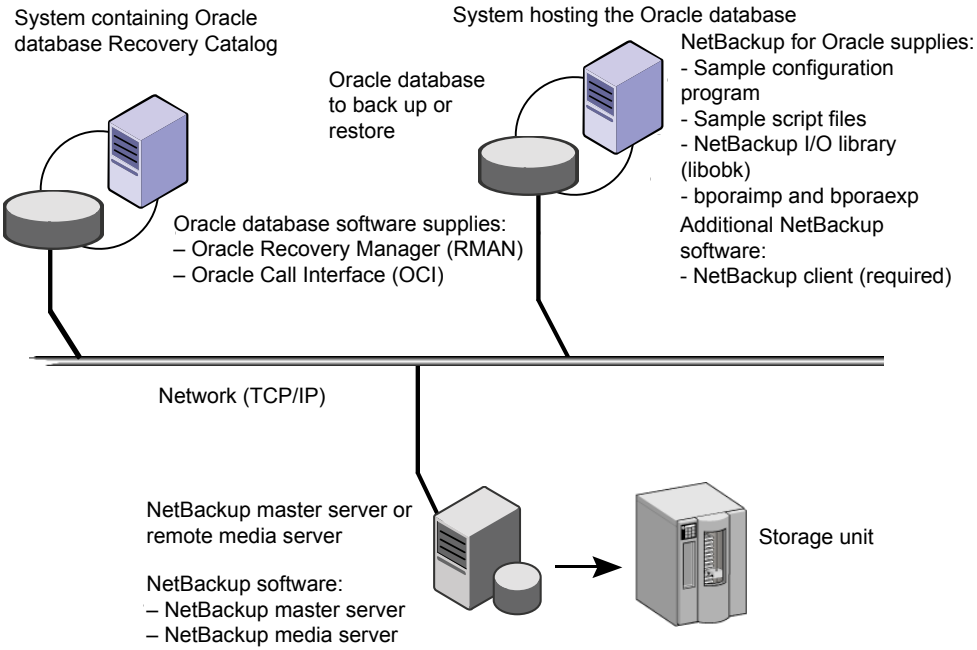
See "Registering authorized locations used by a NetBackup database script-based policy" on page 337.

About NetBackup for Oracle

NetBackup integrates the database backup and recovery capabilities of the Oracle Recovery Manager (RMAN) with the backup and recovery management capabilities of NetBackup.

Figure 1-1 shows the major components in a NetBackup configuration. The server that hosts the Oracle database must be a NetBackup client. The master server must also have NetBackup for Oracle licensed.

Figure 1-1 NetBackup for Oracle on a sample network



NetBackup for Oracle features

The following table shows the NetBackup for Oracle main features:

Table 1-1 NetBackup for Oracle features

Feature	Description
Media and device management	All devices that the Media Manager supports are available to NetBackup for Oracle.

Table 1-1 NetBackup for Oracle features *(continued)*

Feature	Description
Scheduling facilities	NetBackup scheduling facilities on the master server can be used to schedule automatic and unattended Oracle backups. This feature also lets you choose the times when these operations can occur. For example, to prevent interference with normal daytime operations, you can schedule your database backups to occur only at night.
Multiplexed backups and restores	NetBackup for Oracle lets you take advantage of NetBackup's multiplexing capabilities. Multiplexing directs multiple data streams to one backup device, thereby reducing the time necessary to complete the operation.
Transparent Oracle and regular file system backup and restore operations	All backups and restores run simultaneously and transparently without any action from the NetBackup administrator. The database administrator can run database backup and restore operations through NetBackup. An administrator or any other authorized user can use NetBackup to run database backups and restores. If you use the command line interface, templates, or scripts, you must use script- or template-based Oracle policies. These policies use Oracle's Recovery Manager (RMAN) as if NetBackup were not present.

Table 1-1 NetBackup for Oracle features *(continued)*

Feature	Description
Oracle Instance management	An Oracle instance discovery service automatically polls the clients throughout the NetBackup environment every five minutes. The service collects the discovered instances in an instance repository. The user can view the instances on the NetBackup Administration Console or by using the `nboraadm` command. You can create the instance groups that each contain a set of instances that are registered with a common set of credentials. A default instance group can be created for the newly discovered instances that are then automatically registered into this group. You select Oracle instances and instance groups to be part of an Oracle backup policy. You can create the policy for the default instance group to make sure that all newly created instances are automatically protected. Oracle DBAs can use the `nboraadm` command on the NetBackup client to manage instances, instance groups, and their credentials. This command is very useful in environments where the Oracle credentials are known only by the DBAs and not by the NetBackup administrators.
Sharing the same storage units that are used for other file backups	You can share the same devices and media that are used for other backups or give Oracle exclusive use of certain devices and media. NetBackup for Oracle can use the Media Manager, disk, PureDisk storage units, etc.
Centralized and networked backup operations	From the NetBackup master server, you can schedule database backups or start them manually for any client or instance. The Oracle databases can also reside on the hosts that are different from the devices on which NetBackup stores the backups.

Table 1-1 NetBackup for Oracle features *(continued)*

Feature	Description
Graphical user interfaces	NetBackup provides the following graphical user interfaces for client users and administrators: ■ Backup, Archive, and Restore user interface ■ NetBackup Administration Console for Java ■ NetBackup OpsCenter NetBackup OpsCenter is the web-based graphical user interface that is used to perform an Oracle Guided Recovery cloning operation. See "About OpsCenter Guided Recovery" on page 156. A database administrator or NetBackup administrator can start backup or restore operations for Oracle from the NetBackup graphical user interface on the master server.
Templates	The NetBackup for Oracle database wizards can create backup and recovery templates for script- or template-based Oracle policies. You can launch the backup wizard and the recovery wizard from the Backup, Archive, and Restore (BAR) interface. The wizards generate platform-independent templates containing the configuration information that the software uses when it performs backups and restores. The wizard-generated templates do not support all the features native to Oracle. You may want to write a customized backup or restore script in a scripting language that the operating system defines. You can use a template as the base for a script.
Oracle Guided Recovery cloning	Guided Recovery clones an Oracle database from a backup, and simplifies the process of creating a new database from backups of an existing database. Guided Recovery uses an Oracle cloning wizard that executes on the OpsCenter graphical user interface.
Parallel backup and restore operations	NetBackup for Oracle supports the parallel backup and restore RMAN capabilities. For example, you can run more than one tape device at a time for a single Oracle backup or restore. This capability reduces the time necessary to complete the operation.
Compression	Compression increases backup performance over the network and reduces the size of the backup image that NetBackup writes to the storage unit.

Table 1-1 NetBackup for Oracle features *(continued)*

Feature	Description
Support for Replication Director	Replication director can be used to create snapshots of the Oracle database. The snapshots can then be replicated to other NetApp disk arrays or backup the snapshot to a storage unit. To use Replication Director, the Oracle database must exist on a NetApp NAS disk array. Replication Director is not supported on SAN storage at this time. Oracle snapshot backups that use Replication Director are supported on UNIX and Linux platforms only.
Support on a NetBackup appliance for backup to an appliance share (Copilot)	**Note:** This feature requires a NetBackup appliance running software version 2.7.1 or later. This feature enhances the Oracle Intelligent Policy by giving you options for protecting an Oracle database using a share on a NetBackup appliance. 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. You must create a share on the appliance for this option using the NetBackup Appliance Shell Menu. Oracle backups only work on an NFS share on the NetBackup appliance. For more information about how to set up the share, see Creating a share from the NetBackup Appliance Shell Menu in the Veritas NetBackup 52xx and 5330 Appliance Administrator's Guide.
Immediate backup for Oracle DBA	The Oracle DBA can start an immediate backup from the client using the `nboraadm -immediate` command. The Oracle DBA can start the backup instead of waiting for the backup to be initiated based on the NetBackup schedule. This command option is useful if the Oracle DBA wants to perform a backup before maintenance. The command must be initiated from the client where the instance resides.

Table 1-1 NetBackup for Oracle features *(continued)*

Feature	Description
Support for Container and Pluggable databases	Oracle 12c introduced the container databases (CDB) and pluggable databases (PDB). The Oracle Intelligent Policy is enhanced and allows a backup to include single or multiple PDBs. This feature also lets you select one or more Oracle 12c instances along with non-Oracle 12c instances in OIP.

NetBackup for Oracle terminology

Table 1-2 explains some Oracle terms as they pertain to NetBackup.

Table 1-2 Oracle terms

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.

Table 1-2 Oracle terms *(continued)*

Term	Definition
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.
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, however, because they duplicate the work that previous backups did at the same level.

NetBackup for Oracle operation using the Oracle Intelligent Policy

The Oracle Intelligent Policy feature lets you create a policy that specifies one or more Oracle instances to be backed up. You manage instances in an instance repository available on the NetBackup Administration Console. The instance

repository contains all discovered and manually created Oracle instances that reside in the NetBackup environment. Instance management lets you add, change, delete, and register instances with a set of credentials.

See "Instance management for an Oracle Intelligent Policy" on page 55.

To create an Oracle Intelligent Policy, you can use the **Policy Configuration Wizard** or the **Policies** utility. The **Policy Configuration Wizard** is easier to use because it guides you through the setup process by automatically choosing the best values for most configurations. But the wizard does not present all policy configuration options (for example, calendar-based scheduling). After you create a policy, you can use the **Policies** utility to configure the options that are not part of the wizard.

Policy creation includes assigning instances to the policy. The Oracle Intelligent Policy does not require you to know how RMAN functions or how to use the templates and scripts. The feature is instance-based and not template-scripting based.

See "Creating an Oracle Intelligent Policy (OIP)" on page 70.

NetBackup for Oracle includes a library of functions that enable RMAN to use NetBackup. On UNIX, NetBackup uses the RMAN SBT_LIBRARY parameter to link the RMAN server software with the media management API library that NetBackup for Oracle installs. On Windows, the NetBackup for Oracle library is located in `c:\Windows\system32`.

See "Installing NetBackup for Oracle" on page 27.

When you back up Oracle database instances, each resultant backup set contains at least one backup piece from the target database. You must give each backup piece a unique name. Several substitution variables are available to aid in generating unique names. The policy utility provides a set of default file name formats for the backup pieces. NetBackup considers the backup piece name as the file being backed up, so this name must be unique in the catalog.

To override any of the default file name formats, select **Specify backup file name formats**. You can change the formats for the various backup file names for data files, archived redo logs, the control file, and the Fast Recovery Area (FRA). Ensure that the format that is specified for all RMAN backup piece names ends with `_%t` to guarantee that each backup piece has a unique name in the catalog. NetBackup uses this timestamp as part of its search criteria for catalog images. Without this timestamp, performance may degrade as the NetBackup catalog grows.

For a backup, the following items apply:

- The `rman` command starts the requested operation on the databases.
- When the process requires media to store backup data, RMAN issues a backup request to start a user-directed backup.

- The NetBackup media server connects to NetBackup for Oracle on the client. NetBackup for Oracle on the client sends the database data to the NetBackup media server which saves the data to secondary storage. A restore operation works in essentially the same manner except that RMAN issues a restore request. Then NetBackup retrieves the data from secondary storage and sends it to NetBackup for Oracle on the client.
- RMAN supports parallel operations, so that a single `rman` command can start more than one backup, or restore on the NetBackup system.
- The status for an RMAN operation is stored in the RMAN catalog or in the database control file. This same status appears in the output of the RMAN command that is used to run the backup or restore. This status is the only status that a database administrator must check to verify that a backup or restore has been successful.
- You can see the RMAN script and RMAN output in the details of the controlling job (`bphdb`) in the Activity Monitor.
- NetBackup also logs status, but only for its own part of the operation. The database administrator cannot use the NetBackup status to determine whether `rman` was successful. Errors can occur in `rman` that do not affect NetBackup and are not recorded in its logs.

Logging the RMAN input and output on a client

NetBackup has the ability to log the RMAN input and output that is logged locally on the client and also sent to the Activity Monitor. The `RMAN_OUTPUT_DIR` entry specifies which directory to place the RMAN input and output locally on the client for Oracle Intelligent Policy backups. The log is only created when a backup is run using an Oracle Intelligent Policy (OIP) and the file is continuously updated during the RMAN backup. Only one `RMAN_OUTPUT_DIR` entry per client is allowed in a Windows environment. In a UNIX environment, each user can place the output in a different location by adding the `RMAN_OUTPUT_DIR` entry to `$HOME/bp.conf` file. The value in the `$HOME/bp.conf` file takes precedence if it exists. NetBackup does not clean up the log files so the Oracle user has to clean up the log files manually.

You must use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. The directory that is specified must exist and the Oracle user needs to have permission to create files within the directory.

Use the following format:

`RMAN_OUTPUT_DIR` = *directory_name*

The *directory_name* is a directory to which the Oracle user has permission to create files within the directory.

For information about these commands, see the NetBackup Commands Reference Guide.

The file name has a specific format that includes the client name, policy name (OIP), schedule type, date stamp (yyyymmdd), and timestamp (hhmmss). The following is an example of how the file name looks in the directory:

`orac121_backuppolicyname_full_20160201_184157_GMT.log`

The following are examples of `RMAN_OUTPUT_DIR` entires:

Windows: *install_path*`\oracle\oracle_logs\RMAN`

UNIX: `/oracle/oracle_logs/rman`

NetBackup for Oracle operation using a script- or template-based policy

The following are prerequisites for performing Oracle backups to a storage unit:

- On Windows, access to the NetBackup library
- On UNIX, linking with NetBackup
- Generating unique file names

NetBackup users or automatic schedules can start database backups by specifying a template or a shell script in the file list of the Oracle policy. The template or the shell script specifies the backup commands that RMAN performs on the client.

On Windows, NetBackup for Oracle includes a library of functions that enable RMAN to use NetBackup. This library is in `c:\Windows\system32`.

On UNIX, NetBackup for Oracle includes a library of functions that enable RMAN to use NetBackup. You can link to this library.

See "About linking Oracle RMAN with NetBackup for UNIX" on page 37.

When you use the RMAN `backup` command, each resulting backup set contains at least one backup piece (data file, data file copy, control file, or archive log) from the target database. You must give each backup piece a unique name using the `format` operand. Several substitution variables are available to aid in generating unique names. You can specify the `format` operand in the `backup` command. NetBackup considers the backup piece name as the file being backed up, so this name must be unique in the catalog.

For a backup, the following items apply:

- The `rman` command starts the requested operation on the databases.

- When the process requires media to store backup data, RMAN starts a user-directed backup by issuing a backup request.
- The NetBackup media server connects to NetBackup for Oracle on the client. NetBackup for Oracle on the client sends the database data to the NetBackup media server which saves the data to secondary storage. A restore operation works in essentially the same manner except that RMAN issues a restore request. Then NetBackup retrieves the data from secondary storage and sends it to NetBackup for Oracle on the client.
- RMAN supports parallel operations, so a single `rman` command can start more than one backup, or restore on the NetBackup system.
- The status for an RMAN operation is stored in the RMAN catalog or in the database control file. This same status appears in the output of the RMAN command that runs the backup or restore. This status is the only status that a database administrator must check to verify that a backup or restore has been successful.
- NetBackup also logs status, but only for its own part of the operation. The database administrator cannot use the NetBackup status to determine whether `rman` was successful. Errors can occur in `rman` that do not affect NetBackup and are not recorded in its logs.

About Oracle RMAN

RMAN performs a wide variety of automated backup and recovery functions. During a backup or a restore, RMAN provides the interface to the databases, and it extracts and inserts data.

To start a database backup or restore, the database administrator runs the `rman` command. You can run this command from the command line, a script, or an application such as NetBackup. The RMAN script is used as a parameter to the `rman` command and specifies the operations to be performed (for example, backup or restore). The RMAN script also defines other components of the operation such as the database objects to be backed up or restored.

During a backup or restore, RMAN controls the data streams going into or out of a database. RMAN can access storage devices when it is integrated with a media management system, such as the system that NetBackup provides.

RMAN provides true incremental backups. An incremental backup backs up data files and includes only the blocks that have been changed since the last incremental backup. For more information on the backup and recovery process, see your Oracle documentation.

Table 1-3 explains Oracle RMAN terms as they pertain to NetBackup.

Table 1-3 Oracle RMAN terms

Term	Definition
backup set	A backup set is a backup of one or more data files, control files, SPFILEs, and archived redo log files. Each backup set consists of one or more binary files called backup pieces. Backup pieces are written in a proprietary format that only RMAN can create or restore.
instance	An Oracle database instance consists of a System Global Area (SGA) and the Oracle background processes. When Oracle starts a database, it allocates an SGA and starts Oracle background processes. The SGA is de-allocated when the instance shuts down.
Real Application Clusters (RAC)	RAC is an option that allows multiple concurrent instances to share a single physical database.
RMAN	RMAN backs up, restores, and recovers database files. RMAN starts Oracle database server processes on the target database. These Oracle database server processes perform the backup and restore. RMAN performs backup and recovery procedures, and it greatly simplifies the tasks that administrators perform during these processes. However, RMAN cannot directly manage the storage devices and media that are used in its backups. So it must be integrated with an application that has these capabilities. NetBackup for Oracle provides device and media management capabilities by integrating RMAN with NetBackup and its media management software. Also, RMAN can access NetBackup's automatic scheduling facilities and its graphical interfaces.
RMAN repository	An RMAN recovery catalog or the database control file is a repository for the information that RMAN uses and maintains. RMAN uses this information to determine how to run requested backup and restore actions.
`rman` command	The `rman` command starts an RMAN backup or restore.

Table 1-3 Oracle RMAN terms *(continued)*

Term	Definition
RMAN script	The RMAN script specifies the commands for RMAN to perform (for example, backups and restores). For information on RMAN commands and script files, see your Oracle documentation. The following directory contains example RMAN shell scripts: Windows: *install_path*\NetBackup\dbext\Oracle\samples\rman UNIX: /usr/openv/netbackup/ext/db_ext/oracle/samples/rman These example scripts run RMAN commands and are fully commented to explain the features that are used. You can review these examples and use them as a starting point for developing backup, restore, and recovery scripts.

For more information on RMAN terminology, see your Oracle documentation.

About the Oracle recovery catalog

The recovery catalog is a repository of information. RMAN uses the information in the recovery catalog to determine how to perform requested backup and restore actions.

The recovery catalog contains information about the following software components:

- Data file and archive log backup sets and backup pieces.
- Data file copies.
- Archived redo logs and their copies.
- Tablespaces and data files on the target database.
- Stored scripts. These are named, user-created sequences of RMAN and SQL commands.

Oracle recommends that you use RMAN with a recovery catalog, especially if you have 20 or more data files. However, you are not required to maintain a recovery catalog with RMAN.

For information on the benefits and disadvantages of using a recovery catalog, see your Oracle documentation.

Chapter 2

NetBackup for Oracle QuickStart

This chapter includes the following topics:

Installing NetBackup for Oracle

Before you can create an Oracle Intelligent Policy, you need to install NetBackup for Oracle and use the instance management facility.

To install NetBackup for Oracle

1. Verify that the NetBackup for Oracle agent is supported on your operating system and platform.

   See "Verifying the operating system and platform compatibility" on page 35.

2. Make sure that you meet the server requirements and client requirements of NetBackup for Oracle.

   See "NetBackup server and client requirements" on page 36.

3. Install NetBackup if it is not already on your system.

   Note: The Oracle database agent is installed as part of the NetBackup client installation.

   For more information on NetBackup installation, see the NetBackup Installation Guide.

Registering Oracle database instances

The Oracle Discovery Service discovers Oracle database instances in the NetBackup environment and collects them in an instance repository. You must register all the discovered instances that you want to protect by assigning them credentials. An Oracle policy accepts only registered instances.

You can register instances individually or add them to an instance group where they assume the credentials of the group. You can also manually add an instance and assign it a set of credentials at that time. The Oracle database user is required to have a certain level of credentials. The Oracle database user must have `SYSBACKUP` or `SYSDBA` privileges (based on version of Oracle).

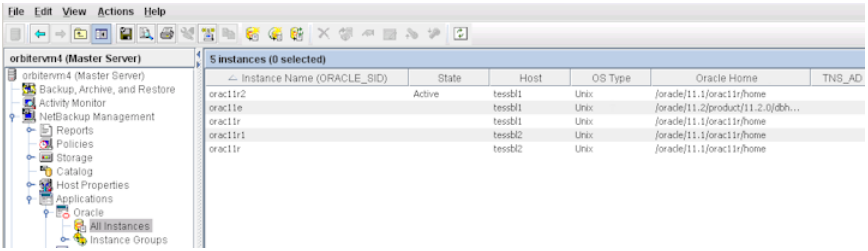
Use the **NetBackup Administration Console** or the `nboraadm` command on the CLI to access the repository for instance registration. The `nboraadm` command is available on the NetBackup master server and the NetBackup clients. This command is available because users such as the DBAs may not have access to the master server. The NetBackup administrator uses `nboraadm` on the master server to control the list of users and clients that have access to `nboraadm` on the NetBackup client.

To register Oracle database instances

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Applications > Oracle**.

2. The Oracle entry in the left pane contains two items:

- Click **Instances** to display the list of instances. The list includes the names of instances that you have added and the instances that the Oracle Discovery Service has discovered. The following is an example of the screen that appears:



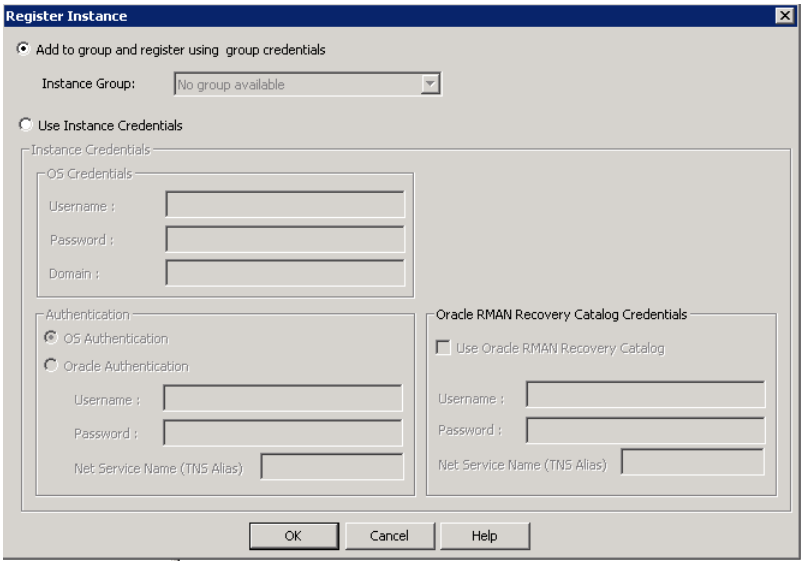
- Click **Instance Groups** to create an instance group to which you can then add instances with the same credentials.

Procedures are available about how to create an instance group.

See "Creating an Oracle database instance group" on page 30.

3 Select one or more instances on the instance list. Use the **Ctrl** and **Shift** keys as needed to select multiple instances.

4 Select **Actions > Register**. The following **Register Instance** panel appears.



5 Do one of the following:

- If you have already created an instance group, select**Add to group and register using group credentials** to add the instance(s) to the group. Select the instance group name from the **Instance Group** pulldown menu. The instance assumes the credentials of the instance group. Click **OK** to continue.
- Click **Use Instance Credentials**. Enter the instance credentials and click **OK**.

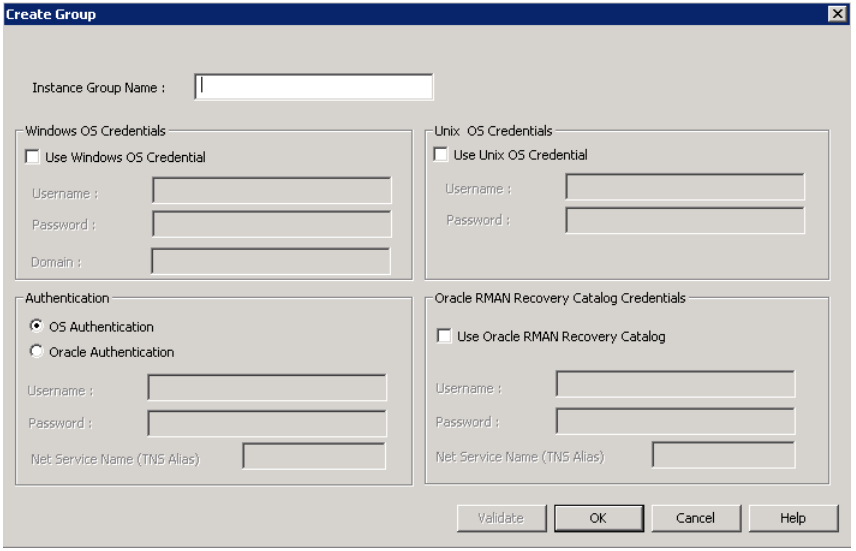
6. The credentials are validated and a Validation Report dialog shows the results. You can save the credentials even if the validation fails. Click **OK** to display the **Instances** list again.
7. Verify that the **Instances** list shows the date-time when you registered the instance. The instance is now available to select for an Oracle Intelligent Policy.
8. Repeat for all other instances that you want registered individually or as part of an instance group.

Creating an Oracle database instance group

This procedure 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. Then you can create a policy that uses this instance group to automatically protect the new instances.

To create an Oracle database instance group

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Applications > Oracle**.
2. Right-click **Instance Groups** and select **New Instance Group**. The following **Create Group** dialog appears.



3. Enter the **Instance Group Name** in the text window, then fill in the appropriate credentials, and click **OK**.

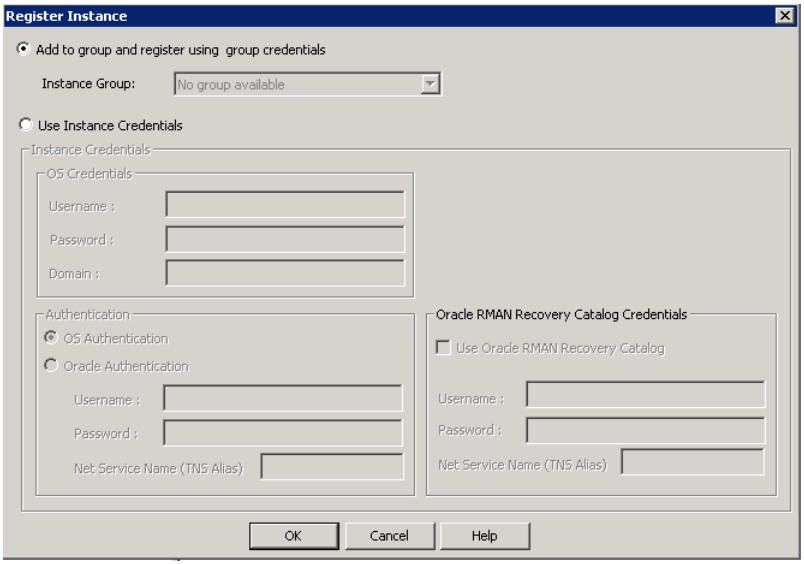
Note: Instance group names cannot be localized.

The newly created instance group name appears in the right pane.

Click **Help** for help entering the appropriate credentials. If necessary, contact the Oracle database administrator for the correct set of credentials.

4. To assign individual instances to this instance group, click **Instances** in the left pane to display the list of instances.

5 Right-click the desired instance and select **Register** to display the following **Register Instance** panel. You can use the **Ctrl** and **Shift** keys to select multiple instances for registering.



6 Make sure **Add to group and register using group crendentials** is selected. Use the **Instance Group** pulldown menu to select the instance group that you want the instance to be added to, then click **OK**.

7 Repeat for each instance that you want included in the instance group.

8 You may want to make this instance group the default for all newly discovered instances. If so, all newly discovered instances are automatically added to this instance group. More information is available about auto-registering an instance group.

See "Automatic Registration of an instance group" on page 65.

Creating an Oracle policy

The easiest method to set up a backup policy is to use the **Policy Configuration Wizard**. This wizard guides you through the setup process by automatically choosing the best values for most configurations.

See "About Oracle Intelligent Policies (OIP)" on page 68.

Not all policy configuration options are presented through the wizard (for example, calendar-based scheduling and the Data Classification setting). After the policy is

created, modify the policy in the **Policies** utility to configure the options that are not part of the wizard.

Use the following procedure to create a policy using the Policy Configuration Wizard.

To create a policy with the Policy Configuration Wizard

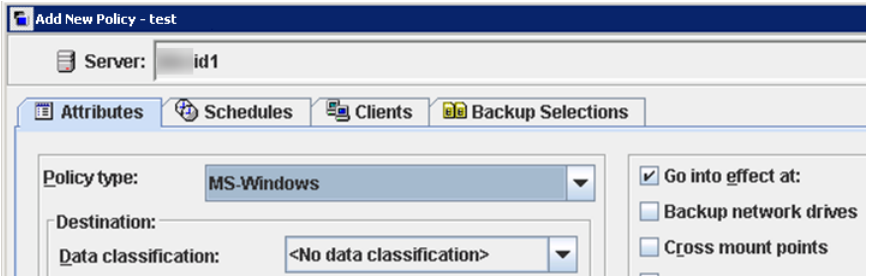
1. In the **NetBackup Administration Console**, in the left pane, click **NetBackup Management**.
2. In the right pane, click **Create a Policy** to begin the **Policy Configuration Wizard**. The first panel of the Policy Configuration Wizard appears.
3. Select **Oracle - Backup Oracle data** on the panel, then click **Next**.
4. Follow the prompts. Click **Help** on any wizard panel for assistance while running the wizard.

Use the following procedure to create a policy without using the **Policy Configuration Wizard**.

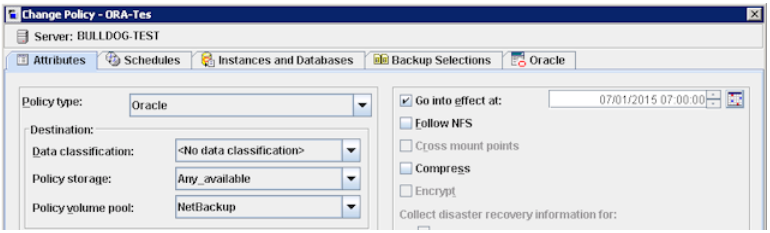
To create a policy without the Policy Configuration Wizard

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Policies**.
2. On the **Actions** menu, click **New > New Policy**.
3. Type a unique name for the new policy in the **Add a New Policy** dialog box. If necessary, clear the **Use Policy Configuration Wizard** check box, then click **OK**.

   The **Attributes** tab of the **Add New Policy** dialog box appears along with the following set of tabs across the top of the panel:



4 In the **Policy Type** pulldown menu, select **Oracle**. This action causes the tabs across the top of the panel to change to the following:



5 The **Add New Policy** panels contain some default conditions and some parameters that you must specify. The default values are the best values for most configurations. However, you may need to customize the parameter settings on one or more of the tabs.

The dialog contains the following set of tabbed pages:

- **Attributes** tab. Default values are automatically selected on the **Attributes** tab. More information is available about these attributes.
  See the NetBackup Administrator's Guide, Volume I.
- **Schedules** tab. More information is available about this tab.
  See the NetBackup Administrator's Guide, Volume I.
- **Instances and Databases** tab. On this page, select the instances and instance groups that you want backed up for the policy. An Oracle Intelligent Policy (OIP) must include either the **Protect Instances and Databases** or the **Protect instance groups** option. More information is available about this tab.
  See "Instances and Databases tab" on page 77.
- **Backup Selections** tab. More information is available about the attributes on this tab.
  See "Backup Selections tab" on page 79.
- **Oracle** tab. More information is available about the attributes on this tab.
  See "Oracle tab" on page 81.

6 To protect the newly discovered instances, you may have to create the instance group first, then set up a policy for the default instance group.

See "Automatic Registration of an instance group" on page 65.

Chapter 3

Installing NetBackup for Oracle

This chapter includes the following topics:

Verifying the operating system and platform compatibility

Verify that the NetBackup for Oracle agent is supported on your operating system or platform.

To verify operating system and compatibility

1. Go to the following webpage:

   http://www.netbackup.com/compatibility

2. In the list of documents, click on the following document:

   Application/Database Agent Compatibility List

3. For information on support for Snapshot Client, see the following document:

   Snapshot Client Compatibility List

NetBackup server and client requirements

Every NetBackup server includes the NetBackup client software by default. Therefore, you can use NetBackup for Oracle on a NetBackup server or client (if NetBackup for Oracle is supported on that platform).

Verify that the following requirements are met for the NetBackup server:

- The NetBackup server software is installed and operational on the NetBackup server. The NetBackup server platform can be any that NetBackup supports.
  See the NetBackup Installation Guide.
- One or more Oracle database instances must exist.
- Make sure that you configure any backup media that the storage unit uses.
  The number of media volumes that are required depends on several things:
  - The devices used
  - The sizes of the databases that you want to back up
  - The amount of data that you want to archive
  - The size of your backups
  - The frequency of backups or archives

  See the NetBackup Administrator's Guide, Volume I.
- Verify that the NetBackup client software is installed on the computer that has the databases you want to back up.
  If the database is clustered, you must use the same version of NetBackup on each node in the cluster.

See "About the license for NetBackup for Oracle" on page 37.

Requirements for using NetBackup for Oracle in a NetBackup cluster

If you plan to use NetBackup for Oracle on a NetBackup server configured in a NetBackup cluster, verify the following requirements:

- NetBackup supports your cluster environment.
  See the Software Compatibility List (SCL).
- The NetBackup server software is installed and configured to work in a NetBackup cluster.
  See the NetBackup Installation Guide.
  See the NetBackup Clustered Master Server Administrator's Guide.

- The NetBackup client software is installed and operational on each node to which NetBackup can failover.
- A valid license for NetBackup for Oracle must exist on each node where NetBackup server resides.

About the license for NetBackup for Oracle

The NetBackup for Oracle agent is installed with the NetBackup client software. No separate installation is required. A valid license for the agent must exist on the master server.

More information is available on how to add licenses.

See the NetBackup Administrator's Guide, Volume I.

For a NetBackup cluster, a valid license for NetBackup for Oracle must exist on each node where NetBackup server resides.

About linking Oracle RMAN with NetBackup for UNIX

Before writing to a storage unit, link the Oracle database server software with the NetBackup API library installed by NetBackup for Oracle. Oracle uses this library when it needs to write to or read from the devices that NetBackup media manager supports.

To link your Oracle software with the NetBackup API library, use one of the following methods:

- (Recommended) Use the SBT_LIBRARY parameter in the PARMS section of the allocate channel in the RMAN script. In the run block of the RMAN script, modify the ALLOCATE statement so that the SBT_LIBRARY parameter points to the NetBackup API library. For example:

```
ALLOCATE CHANNEL CH00 TYPE 'SBT_TAPE' PARMS 'SBT_LIBRARY=
   /usr/openv/netbackup/bin/libobk.so64.1';
```

- Use the linking script that NetBackup provides.
- Create the links manually.

The linking process differs depending on your hardware platform, your Oracle database server release level, and your OS level. This topic does not address all the supported combinations, but it specifies OS level differences.

The default location for the NetBackup API library is `/usr/openv/netbackup/bin`. The name of the NetBackup API library differs depending on your platform.

Table 3-1 lists the library names for the supported platforms.

Table 3-1 NetBackup API libraries

Platform	Oracle	Library name
AIX	64-bit	libobk.a64
HP Itanium	64-bit	libobk.so
Linux x86	64-bit	libobk.so64
Linux Itanium	64-bit	libobk.so
IBM pSeries	64-bit	libobk.so
IBM zSeries	64-bit	libobk.so
Solaris (SPARC)	64-bit	libobk.so.64.1
Solaris (x86)	64-bit	libobk.so.1

Verifying environment variables and shutting down Oracle

The following procedure describes how to correctly define your environment variables and how to shut down the Oracle database instances.

To verify environment variables and shutdown Oracle database instances

1. Make sure that your Oracle environment variables are defined.

   Define the variables as follows:

   `ORACLE_HOME` The directory path to the Oracle software location.

   `ORACLE_SID` The name of the Oracle database instance.

2. Become the Oracle user.

   ```
   su - oracle
   ```

3. Determine if you need to link or re-link the library with NetBackup.

   See “Linking Oracle RMAN with NetBackup on UNIX platforms” on page 39.

4. If this installation is an upgrade and the SBT_LIBRARY parameter is not in use, restart the Oracle database instance.

Linking Oracle RMAN with NetBackup on UNIX platforms

The procedures in this topic show how to link RMAN with NetBackup. The automatic method is preferred. Use the manual method only if the link script fails or if you receive Oracle messages to indicate that manual linking is required.

Link the library with NetBackup when you license NetBackup for Oracle for the first time.

For more information about what Oracle database release that NetBackup for Oracle supports, review the Application/Database Agent Compatibility List.

To automatically link Oracle RMAN with NetBackup

1. Run the `oracle_link` script that is located in `/usr/openv/netbackup/bin/`.

   This script determines the Oracle version level and then links Oracle with the NetBackup API library. This script writes output to /tmp/make_trace.<pid>. To change the trace file location, change the MAKE_TRACE variable in the `oracle_link` script.

2. If this installation is an upgrade, restart the Oracle database instance.

To manually link Oracle RMAN with NetBackup, follow the instructions in one of the platform-specific sub-topics:

- See "Manually linking AIX (64-bit)" on page 39.
- See "Manually linking HP Itanium (64-bit)" on page 40.
- See "Manually linking Linux x86 (64-bit)" on page 41.
- See "Manually linking IBM pSeries or zSeries" on page 42.
- See "Manually linking Solaris x86 (64-bit)" on page 42.
- See "Manually linking Solaris SPARC (64-bit)" on page 43.

Manually linking AIX (64-bit)

To manually link AIX (64-bit)

1. Type the following `cd` command to change directories:

   ```
   cd $ORACLE_HOME/lib
   ```

2. Type the following `ls` command to determine whether the Oracle library exists:

   ```
   ls -l libobk.*
   ```

3 (Conditional) Use the `mv` command to move the Oracle library to an alternate location.

Perform this step if the output from step 2 shows that `libobk.a` exists.

For example:

```
mv libobk.a libobk.a.orig
```

4 Type the following `ln` command to create a new link:

```
ln -s /usr/openv/netbackup/bin/libobk.a64 libobk.a
```

5 If you run into problems and cannot re-link Oracle with the NetBackup API library, you can rollback what you have done. Enter the following:

```
cd $ORACLE_HOME/lib64
    mv libobk.so.orig libobk.so
```

Manually linking HP Itanium (64-bit)

To manually link HP Itanium (64-bit)

1 Type the following `cd` command to change directories:

```
cd $ORACLE_HOME/lib
```

2 Type the following `ls` command to determine whether the Oracle library exists:

```
ls -l libobk.so
```

3 (Conditional) Use the `mv` command to move the Oracle library to an alternate location.

Perform this step if the output from step 2 shows that `libobk.so`.

For example:

```
mv libobk.so libobk.so.orig
```

4 Type the following `ln` command to create new links:

```
ln -s /usr/openv/netbackup/bin/libobk.so  libobk.so
```

5 If you run into problems and cannot re-link Oracle with the NetBackup API library, you can rollback what you have done. Enter the following:

```
cd $ORACLE_HOME/lib64
    mv libobk.so.orig libobk.so
```

Manually linking Linux x86 (64-bit)

To manually Linux x86 (64-bit)

1 Type the following `cd` command to change directories:

```
cd $ORACLE_HOME/lib
```

2 Type the following `ls` command to determine whether the Oracle library exists:

```
ls -l libobk.so
```

3 (Conditional) Use the `mv` command to move the Oracle library to an alternate location.

Perform this step if the output from step 2 shows that `libobk.so` is present.

For example:

```
mv libobk.so libobk.so.orig
```

4 Type the following `ln` command to create a new link:

```
ln -s /usr/openv/netbackup/bin/libobk.so64 libobk.so
```

5 If you run into problems and cannot re-link Oracle with the NetBackup API library, you can rollback what you have done. Enter the following:

```
cd $ORACLE_HOME/lib64
    mv libobk.so.orig libobk.so
```

Manually linking IBM pSeries or zSeries

To link manually IBM pSeries or zSeries

1. Type the following `cd` command to change directories:

   ```
   cd $ORACLE_HOME/lib
   ```

2. Type the following `ls` command to determine whether the Oracle library exists:

   ```
   ls -l libobk.so
   ```

3. (Conditional) Use the `mv` command to move the Oracle library to an alternate location.

   Perform this step if the output from step 2 shows that `libobk.so` is present.

   For example:

   ```
   mv libobk.so libobk.so.orig
   ```

4. Type the following `ln` command to create a new link:

   ```
   ln -s /usr/openv/netbackup/bin/libobk.so libobk.so
   ```

5. If you run into problems and cannot re-link Oracle with the NetBackup API library, you can rollback what you have done. Enter the following:

   ```
   cd $ORACLE_HOME/lib64
       mv libobk.so.orig libobk.so
   ```

Manually linking Solaris x86 (64-bit)

To manually link Solaris x86 (64-bit)

1. Type the following `cd` command to change directories:

   ```
   cd $ORACLE_HOME/lib
   ```

2. Type the following `ls` command to determine whether the Oracle library exists:

   ```
   ls -l libobk.so
   ```

3 Use the `mv` command to move the Oracle library to an alternate location. Perform this step if the output from step 2 shows that `libobk.so` is present.

For example:

```
mv libobk.so libobk.so.orig
```

4 Type the following `ln` command to create a new link:

```
ln -s /usr/openv/netbackup/bin/libobk.so.1 libobk.so
```

5 If you run into problems and cannot re-link Oracle with the NetBackup API library, you can rollback what you have done. Enter the following:

```
cd $ORACLE_HOME/lib64
    mv libobk.so.orig libobk.so
```

Manually linking Solaris SPARC (64-bit)

To manually link Solaris (64-bit)

1 Type the following `cd` command to change directories:

```
cd $ORACLE_HOME/lib
```

2 Type the following `ls` command to determine whether the Oracle library exists:

```
ls -l libobk.so
```

3 (Conditional) Use the `mv` command to move the Oracle library to an alternate location.

Perform this step if the output from step 2 shows that `libobk.so` is present.

For example:

```
mv libobk.so libobk.so.orig
```

4 Type the following `ln` command to create a new link:

```
ln -s /usr/openv/netbackup/bin/libobk.so64.1 libobk.so
```

5 If you run into problems and cannot re-link Oracle with the NetBackup API library, you can rollback what you have done. Enter the following:

```
cd $ORACLE_HOME/lib64
    mv libobk.so.orig libobk.so
```

Chapter 4

Oracle policy configuration

This chapter includes the following topics:

Preparing for NetBackup for Oracle configuration

The major part of configuring NetBackup for Oracle is to create and configure the Oracle policies. The following topics prepare you to configure NetBackup for Oracle policies:

- See "About Oracle policy configuration" on page 46.
- See "Permissions for NetBackup for Oracle log directories" on page 47.
- See "NetBackup for Oracle backup policy types" on page 48.
- See "Configuring the logon account for the NetBackup Client Service for NetBackup for Oracle" on page 113.
- See "Configuring the Maximum jobs per client for NetBackup for Oracle" on page 54.

About Oracle policy configuration

NetBackup offers two ways to configure an Oracle policy.

- Oracle Intelligent Policies. This method lets you create a single policy to protect multiple Oracle database instances that are spread over multiple clients. You select Oracle database instances for a policy from a repository of instances that are automatically discovered in the NetBackup environment. Among the features that these policies provide is the ability to schedule frequent backups of archived redo logs. These backups are accomplished in minutes instead of hours or days.
- Script- or template-based policies. This method lets you create an Oracle backup policy by using a script or template that is based on a list of clients.

A backup policy for a database defines the backup criteria for a specific group of instances (Oracle Intelligent Policy) or clients (script- or template-based policy).

The Intelligent Oracle Policy includes the following criteria:

- Storage unit and media to use
- Policy attributes
- Backup schedules. Automatic schedule and archive log schedule.
- Instances to be backed up
- Backup selections: Whole database, tablespaces, data files, FRA

The script- or template-based policy includes the following criteria:

- Storage unit and media to use
- Policy attributes
- Backup schedules: Automatic schedule and application schedule.
- Clients to be backed up
- Backup templates or script files to be run on the clients

To back up the database environment, define at least one script- or template-based Oracle policy with the appropriate schedules and clients. Or, you can configure a single Oracle Intelligent Policy that includes all instances.

Most requirements for database policies are the same as for file system backups. In addition to the policy attributes for Oracle, other attributes are available that you should consider.

See the NetBackup Administrator's Guide, Volume I.

Permissions for NetBackup for Oracle log directories

In UNIX, NetBackup uses the `/usr/openv/netbackup/logs` directory tree for the recording of troubleshooting information. NetBackup also uses this directory tree for progress and communication updates to users and other NetBackup applications. Restrictive permissions on these directories can not only disable the collection of troubleshooting data, but also prevent the application itself from functioning correctly.

Backup operations and restore operations fail when permissions are too restrictive. We recommend that you make all of the `/usr/openv/netbackup/logs` directories and subdirectories readable and writeable by all users (777 permissions). However, security requirements may prohibit global read-write access. If so, you can restrict permissions of specific directories to a single group or user. If you do restrict permissions, you have to make sure that these restrictions do not affect backup and restore operations. This means that all operations must be initiated using a process that has read and write access to the `/usr/openv/netbackup/logs` directory and subdirectories.

Check that the `/usr/openv/netbackup/logs/user_ops` directory tree has 777 permissions. The items in this directory need to be accessible for the applications to operate correctly.

If you restrict permissions on the other directories that are located in `/usr/openv/netbackup/logs`, backup and restore operations are not affected. However, troubleshooting efforts may be hindered when processes do not have the appropriate permissions to update their designated debug logs.

In Windows, a situation can occur during backup and restore jobs of Oracle 12c where no debug log files are created in the `dbclient` and `bpdbsbora` folders. In the Oracle 12c release, an Oracle user can be a Windows built-in account (`LocalSystem` or `LocalService`) or a standard Windows user account. This issue is the result of security permissions for standard (non-administrator) Windows user accounts.

If a standard (non-administrator) Windows user account is used, the Oracle user may not have the proper privileges to write to the `dbclient` and `bpdbsbora` folders. To avoid this issue, change the Windows security permissions of the `dbclient` and `bpdbsbora` folders to give the Oracle user **Full control** permissions.

You need to review permissions on the `user_ops` folder and subfolders. By default, these folders are writeable by all users. If restrictive settings have been configured, ensure that full access is granted for any standard Windows user account that is used. Otherwise, backup and restore operations can fail.

For more information about how restrictive settings can cause issues during backups, restores, or troubleshooting, refer to the following article:

http://www.veritas.com/docs/TECH52446

Oracle Home User permissions when NetBackup SAN Client is used

To use the NetBackup SAN Client to protect Oracle on Windows, the Oracle user must have administrator privileges. Starting with Oracle Database 12c Release 1 (12.1), Oracle Database on Windows supports the use of Oracle Home User. The Oracle Home User is specified at the time of Oracle Database installation and is used to run the Windows services for the Oracle home. The Oracle Home User that is used to run Windows services is similar to the Oracle user for Oracle Database on Linux.

For more information, refer to the Oracle document "Supporting Oracle Home User on Windows" at the following location:

http://docs.oracle.com/cd/E16655_01/win.121/e10714/oh_usr.htm

To use NetBackup SAN Client, make sure to select **Use Windows Built-in Account** during Oracle Database installation. Making this selection enables the Windows services for the Oracle home to run as `LocalSystem` or `LocalService`.

NetBackup for Oracle backup policy types

Table 4-1 shows the Oracle backup policy types you can specify.

Table 4-1 Oracle backup types

Backup type	Description
Application Backup – Script- or template-based policy using streamed data only	The Application Backup schedule enables user-controlled NetBackup operations from the client. These operations include those initiated from the client and those initiated by an automatic schedule on the master server. NetBackup uses the Application Backup schedule when the user starts a backup manually. Configure at least one Application Backup schedule for each database policy. The Default-Application-Backup schedule is configured automatically as an Application Backup schedule.

Table 4-1 Oracle backup types *(continued)*

Backup type	Description
Full Backup – Script-based policy	Stream-based backup: The specified script in the **Backup Selections** tab is executed. If the script is set up properly, RMAN initiates a full stream based backup (full or incremental level 0). **Note:** The **Application Backup** schedule properties (For example: storage and retention) are used. RMAN proxy backup: The specified script in the **Backup Selections** tab is executed. If the script is set up properly, RMAN initiates a proxy backup. **Note:** The **Full Backup** schedule properties (For example: storage and retention) are used for the proxy portion of the backup. The **Application Backup** schedule properties (For example: storage and retention) are used for the streamed portion of the backup.
Differential Incremental backup – Script-based policy	Stream-based backup: The specified script in the **Backup Selections** tab is executed. If the script is set up properly, RMAN initiates a stream-based incremental level 1 backup. **Note:** The **Application Backup** schedule properties (I.E. storage, retention, etc.) are used. RMAN proxy backup: This backup type should only be used for BLI backups. If you do not use a proxy backup for a BLI backup, then a **Full Backup** schedule should be used. The specified script in the **Backup Selections** tab is executed. If the script is set up properly, RMAN initiates a proxy backup. **Note:** The **Differential Incremental Backup** schedule properties (I.E. storage, retention, etc.) are used for the proxy portion of the backup. The **Application Backup** schedule properties (I.E. storage, retention, etc.) are used for the streamed portion of the backup.

Table 4-1 Oracle backup types *(continued)*

Backup type	Description
Cumulative Incremental backup – Script-based policy	Stream-based backup: The specified script in the **Backup Selections** tab is executed. If the script is set up properly, RMAN initiates a stream-based incremental level 1 cumulative backup. **Note:** The **Application Backup** schedule properties (I.E. storage, retention, etc.) are used. RMAN proxy backup: This backup type should only be used for BLI backups. If you do not use a proxy backup for a BLI backup, then a **Full Backup** schedule should be used. The specified script in the **Backup Selections** tab is executed. If the script is set up properly, RMAN initiates a proxy backup. **Note:** The **Cumulative Incremental Backup** schedule properties (I.E. storage, retention, etc.) are used for the proxy portion of the backup. The **Application Backup** schedule properties (I.E. storage, retention, etc.) are used for the streamed portion of the backup.
Full Backup – Template based policy	Stream-based backup: The specified template in the **Backup Selections** tab is executed. Dynamically generates an RMAN script that initiates an incremental level 0 backup. **Note:** The **Application Backup** schedule properties (I.E. storage, retention, etc.) are used. RMAN proxy backup (Policy is defined to perform a snapshot): The specified template in the **Backup Selections** tab is executed. Dynamically generates an RMAN script that initiates a proxy backup. **Note:** The **Full Backup** schedule properties (I.E. storage, retention, etc.) are used for the proxy portion of the backup. The **Application Backup** schedule properties (I.E. storage, retention, etc.) are used for the streamed portion of the backup.

Table 4-1 Oracle backup types *(continued)*

Backup type	Description
Differential Incremental backup – Template based policy	Stream-based backup: The specified template in the **Backup Selections** tab is executed. Dynamically generates an RMAN script that initiates a Differential Incremental (INCREMENTAL LEVEL 1) backup. **Note:** The **Application Backup** schedule properties (I.E. storage, retention, etc.) are used. RMAN proxy backup (Policy is defined to perform a snapshot): The specified template in the **Backup Selections** tab is executed. If the policy has **Perform block level incremental backups** selected, the generated script causes RMAN to initiate a proxy backup. Conversely, if the policy does not have **Perform block level incremental backups** selected, the generated script causes RMAN to initiate a Differential Incremental (INCREMENTAL LEVEL 1) backup. **Note:** The **Differential Incremental Backup** schedule properties (I.E. storage, retention, etc.) are used for the proxy portion of the backup. The **Application Backup** schedule properties (I.E. storage, retention, etc.) are used for the streamed portion of the backup.

Table 4-1 Oracle backup types *(continued)*

Backup type	Description
Cumulative Incremental backup – Template based policy	Stream-based backup: The specified template in the **Backup Selections** tab is executed. Dynamically generates an RMAN script that initiates a Cumulative Incremental (INCREMENTAL LEVEL 1 CUMULATIVE) backup. **Note:** The **Application Backup** schedule properties (I.E. storage, retention, etc.) are used. RMAN proxy backup (Policy is defined to perform a snapshot): The specified template in the **Backup Selections** tab is executed. If the policy has **Perform block level incremental backups** selected, the generated script causes RMAN to initiate a proxy backup. Conversely, if the policy does not have **Perform block level incremental backups** selected, the generated script causes RMAN to initiate a Cumulative Incremental (INCREMENTAL LEVEL 1 CUMULATIVE) backup. **Note:** The **Cumulative Incremental Backup** schedule properties (I.E. storage, retention, etc.) are used for the proxy portion of the backup. The **Application Backup** schedule properties (I.E. storage, retention, etc.) are used for the streamed portion of the backup.
Full Backup – OIP Policy	Stream-based backup: Dynamically generates an RMAN script on each client for the instance(s) and or instance group(s) defined in the **Instances and Databases** tab. The script initiates an Incremental Full (INCREMENTAL LEVEL 0) backup. RMAN proxy backup (Policy is defined to perform a snapshot): Dynamically generates an RMAN script on each client for the instance(s)and or instance group(s) defined in the **Instances and Databases** tab to initiate a proxy backup. **Note:** The **Full Backup** schedule properties (I.E. storage, retention, etc.) are used for both the streamed and the proxy data.

Table 4-1 Oracle backup types *(continued)*

Backup type	Description
Differential Incremental backup – OIP Policy	Stream-based backup: Dynamically generates an RMAN script on each client for the instance(s) and or instance group(s) defined in the **Instances and Databases** tab. The script initiates a Differential Incremental (INCREMENTAL LEVEL 1) backup. RMAN proxy backup (Policy is defined to perform a snapshot): ■ The policy has **Perform block level incremental backups** selected. An RMAN script is dynamically generated on each client for the instance(s)and or instance group(s) defined in the **Instances and Databases** tab to initiate a proxy backup. ■ The policy does not have **Perform block level incremental backups** selected. An RMAN script is dynamically generated on each client for the instance(s) and or instance group(s) defined in the **Instances and Databases** tab. A Differential Incremental (INCREMENTAL LEVEL 1) backup is initiated. **Note:** The **Differential Incremental Backup** schedule properties (I.E. storage, retention, etc.) are used for both the streamed and the proxy data.

Table 4-1 Oracle backup types *(continued)*

Backup type	Description
Cumulative Incremental backup – OIP Policy	Stream-based backup: Dynamically generates an RMAN script on each client for the instance(s) and or instance group(s) defined in the **Instances and Databases** tab. The script initiates a Cumulative Incremental (INCREMENTAL LEVEL 1 CUMULATIVE) backup. RMAN proxy backup (Policy is defined to perform a snapshot): ■ The policy has **Perform block level incremental backups** selected. An RMAN script is dynamically generated on each client for the instance(s)and or instance group(s) defined in the **Instances and Databases** tab to initiate a proxy backup. ■ The policy does not have **Perform block level incremental backups** selected. An RMAN script is dynamically generated on each client for the instance(s)/instance group(s) defined in the **Instances and Databases** tab. A Cumulative Incremental (INCREMENTAL LEVEL 1 CUMULATIVE) backup is initiated. **Note:** The “Cumulative incremental backup” schedule properties (I.E. storage, retention, etc.) are used for both the streamed and the proxy data.
Archived redo log backup – OIP Policy Only	The policy dynamically generates an RMAN script on each client for the instance(s) and or instance group(s) defined in the **Instances and Databases** tab. The policy initiates a stream-based archive redo log backup. **Note:** The frequency is granular down to intervals of minutes.

Configuring the Maximum jobs per client for NetBackup for Oracle

The following procedure shows how to set the **Maximum jobs per client** attribute.

To configure the maximum jobs per client

1. In the left pane of the NetBackup Administration Console, expand **NetBackup Management > Host Properties**.
2. Select **Master Server**.
3. In the right pane, double-click the server icon.

4 Click **Global Attributes**.

5 Change the **Maximum jobs per client** value to 99.

The **Maximum jobs per client** specifies the maximum number of concurrent backups that are allowed per client. The default is 1.

You can use the following formula to calculate a smaller value for the maximum jobs per client setting:

Maximum jobs per client = *number_of_streams* X *number_of_policies*

Refer to the following definitions:

number_of_streams	The number of backup streams between the database server and NetBackup. Each separate stream starts a new backup job on the client.
number_of_policies	The number of policies of any type that can back up this client at the same time. This number can be greater than one. For example, a client can be in two policies to back up two different databases. These backup windows can overlap.

For Oracle backups and restores, the number of jobs is difficult to determine. This difficulty exists because Oracle internally determines when and how many streams to run in parallel to optimize performance.

Note: Enter a large enough value for the **Maximum jobs per client** attribute to meet the number of jobs that Oracle runs. You may need to experiment with different values at your site.

Instance management for an Oracle Intelligent Policy

The NetBackup Discovery Service runs on all clients in the environment and reports to the master server when it finds instances of applications. This service helps you to build an Oracle Intelligent Policy by finding Oracle instances and displaying them in the **NetBackup Administration Console** and the **Instances and Databases** tab. When NetBackup is installed, the service checks the local client host for Oracle database instances and also checks 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 Administration Console or by using the `nboraadm` command.

DBAs can run `nboraadm` on a NetBackup client if the backup administrator enables access to `nboraadm` by running the following command on the master server:

```
# nboraadm -add_dba <client_name> <user_name>
```

See the `nboraadm` description in the NetBackup Commands Reference Guide.

All instances that you want backed up as part of an Oracle Intelligent Policy must be registered with credentials. Instance management lets you assign credentials to individual instances as well as instance groups. The instances in an instance group share the same set of credentials. You can direct the discovery service to assign the new instances that it discovers to an instance group. The Oracle database user is required to have a certain level of credentials. The Oracle database user must have `SYSBACKUP` or `SYSDBA` privileges (based on version of Oracle).

See "About the NetBackup Discovery Service" on page 56.

See "Manually adding an Oracle database instance to the repository" on page 58.

See "Registering an Oracle database instance" on page 61.

See "Creating an Oracle database instance group" on page 30.

See "About Oracle database instance groups" on page 64.

See "Adding an instance to an instance group" on page 64.

See "Automatic Registration of an instance group" on page 65.

See "About instance actions" on page 67.

See "About Oracle Intelligent Policies (OIP)" on page 68.

See "Oracle database upgrade effect on Oracle Intelligent Policies" on page 72.

About the NetBackup Discovery Service

The NetBackup Discovery Service (`nbdisco`) discovers Oracle database instances throughout the NetBackup environment. The discovery service reports to the master server when it finds instances of applications to help you build an Oracle Intelligent Policy. The service polls the clients upon NetBackup installation and periodically after installation (every 5 minutes). Instance management collects the discovered instances in an instance repository. The user can access this repository on the **NetBackup Administration Console** or by using the `nboraadm` command.

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.

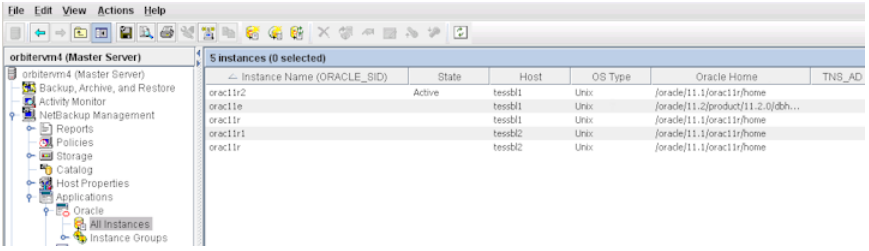
To set this value on a client remotely, run the following command from the master server:

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

Viewing the Oracle database instance repository

You can view a complete list of all Oracle database instances. In the **NetBackup Administration Console**, in the left pane, expand the **Applications** node, then expand the **Oracle** node. The two items under the **Oracle** node are Instances and Instance Groups.

When you click **All Instances**, the following is an example of the instance list in the right pane.



You can click on one of the instances to select it for an operation. You can also select multiple instances for an operation with the following exceptions:

- You can select only one instance at a time to view properties.
- You can register multiple instances simultaneously only if the OS type is the same (UNIX or Windows).

The instances are listed with the following column information:

Instance Name The instance name (ORACLE_SID).

State	The current state of the instance. Possible values are: ■ Blank - The instance is not yet registered and cannot be protected using an Intelligent Oracle Policy. ■ Active - Credentials have been provided for the instance. An Intelligent Oracle Policy can protect the instance. ■ Inactive - If the instance is added to a policy, it is not included in the backup. An administrator can inactivate an instance to take it offline (for example, for upgrades).
Host	Specifies the host where the Oracle database resides.
OS Type	Specifies the operating system of the host. Valid values are Windows and UNIX.
ORACLE_HOME	The file path of the Oracle home directory where the instance resides.
TNS_ADMIN	Specifies the location of the network administration directory on the client system if this directory is not in the default location. Consult your Oracle documentation for the default location of the network administration directory on the client system.
Instance Group	Specifies the Oracle database instance group name that this instance is part of. This field is blank if the instance does not belong to an instance group.
Registered	Specifies the date and time when a user registered a set of credentials for this instance. This field is blank if the instance has not been given credentials.
Policies	The names of the policies that the instance has been assigned to.

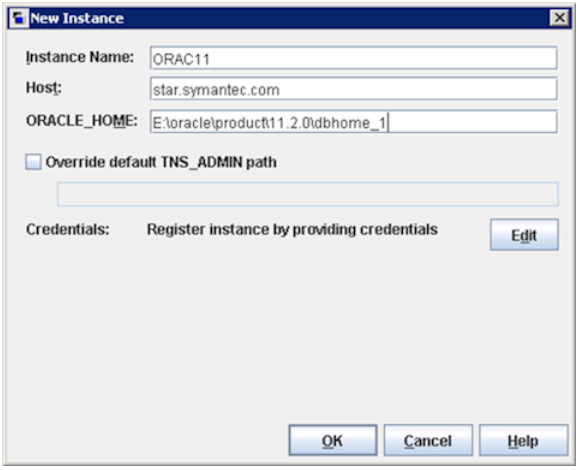
Manually adding an Oracle database instance to the repository

New instances the instance discovery system finds on the clients are automatically added to the repository. However, you may need to add an instance manually. For example, you do not want to wait for the discovery service to discover the new instance.

Note: If necessary, contact the Oracle database administrator for the correct set of credentials. The DBA can also manually add the instance if the DBA is not willing or allowed to share the credentials with the backup administrator. The DBA can manually add the instance using the `nboraadm` command on the client. The Oracle database user is required to have a certain level of credentials. The Oracle database user must have `SYSBACKUP` or `SYSDBA` privileges (based on version of Oracle).

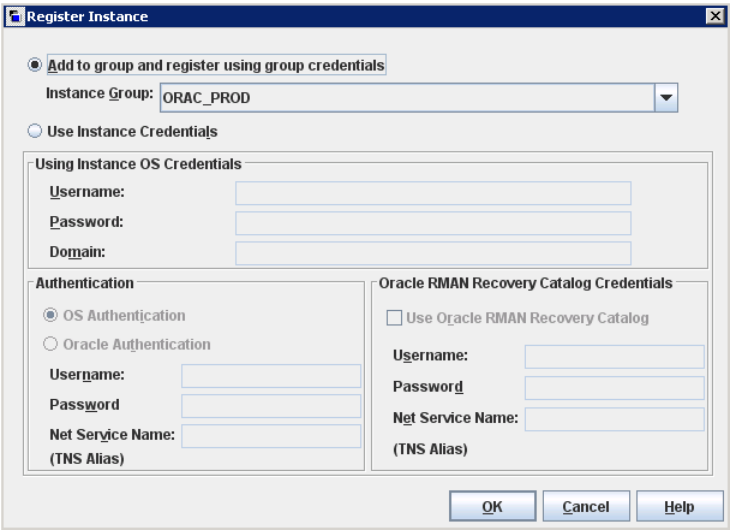
To manually add an Oracle database instance to the repository

1. In the NetBackup Administration Console, in the left pane, expand **NetBackup Management > Applications > Oracle**.
2. Click **All Instances**. All instances in the repository are listed in the right pane.
3. Right-click **All Instances** and select **New instance** to display the following:
4. Fill in the **Instance Name**, **Host**, and **ORACLE_HOME** parameters. Click **Help** to display descriptions of these parameters. For example:



5. (Conditional) Use 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. Click **Help** to display a description of the parameter. Example of the parameter:

6 Click **Provide Credentials**.



7 In the **Register Instance** dialog box, click **Use Instance Credentials**.

8 Enter the **OS Credentials**. You may have to contact the Oracle DBA for the correct credentials.

9 In the **Authentication** area, you can optionally click **Oracle Authentication** to enter specific Oracle credentials. You can also click **Use Oracle RMAN Recovery Catalog** to enter credentials for the RMAN recovery catalog. Then click **OK**.

The system tries to validate the credentials, report its findings, and return you to the **Change Instance** dialog box. Validation can fail for the following reasons:

- If the host name is invalid, the following message appears

  `Could not validate credentials. Failed to connect to client: <client> (40).`

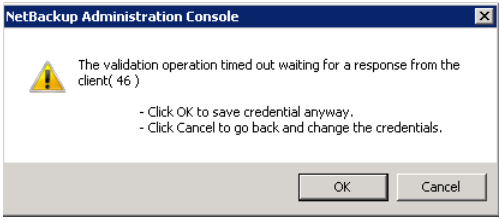
- If the host name is correct but you cannot connect to the host because the host is down, the following message appears:

  `The validation operation timed out waiting for a respond from the client (46)`

- If the host name is correct, but username-password is invalid, the following message appears:

  `Validation of operating system user/password failed for client: <client> (41).`

The error message includes the generated status code which appears in parentheses at the end of the message. The following is an example of an error pop-up window:



Click **OK** to save the credentials, or you can click **Cancel** and re-enter the credentials. If you save the credentials that caused the error, the instance is saved in the repository. You can edit the instance at a later time to correct the validation issue.

Click **OK** in the **Change Instance** dialog box.

You have added the instance to the repository and registered the instance with credentials.

Registering an Oracle database instance

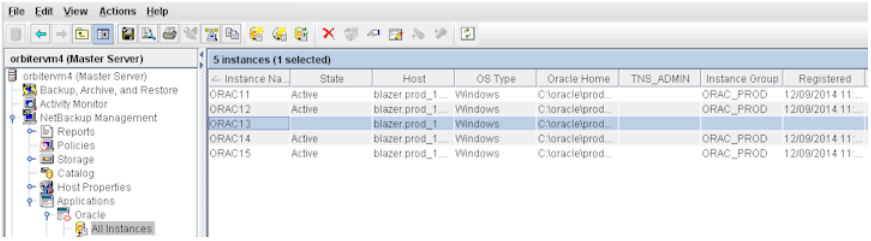
The NetBackup Discovery Service discovers Oracle database instances on the local client host. The service reports to the master server upon startup and every 4 hours thereafter. The master server collects the discovered instances in an instance repository. The user accesses the repository on the **NetBackup Administration Console** or by running the `nboraadm` command.

See the `nboraadm` description in the NetBackup Commands Reference Guide.

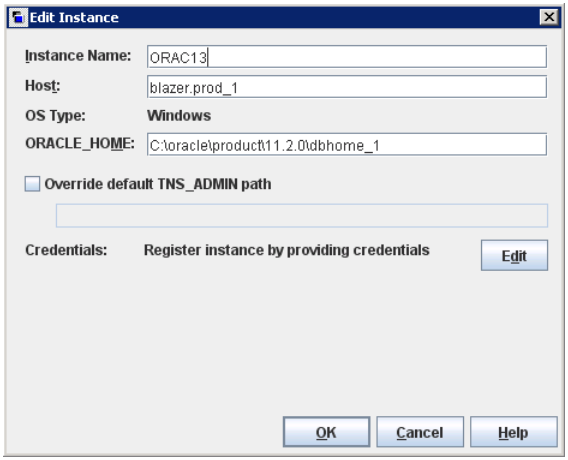
Use the following procedure to register an Oracle database instance that the discovery service adds to the instance list.

To register an Oracle database instance

1. In the NetBackup Administration Console, in the left pane, expand **NetBackup Management > Applications > Oracle**.
2. Click **All Instances**. The right pane displays a list of instances. Instances that have previously been registered show a date and time in the **Registered** column.



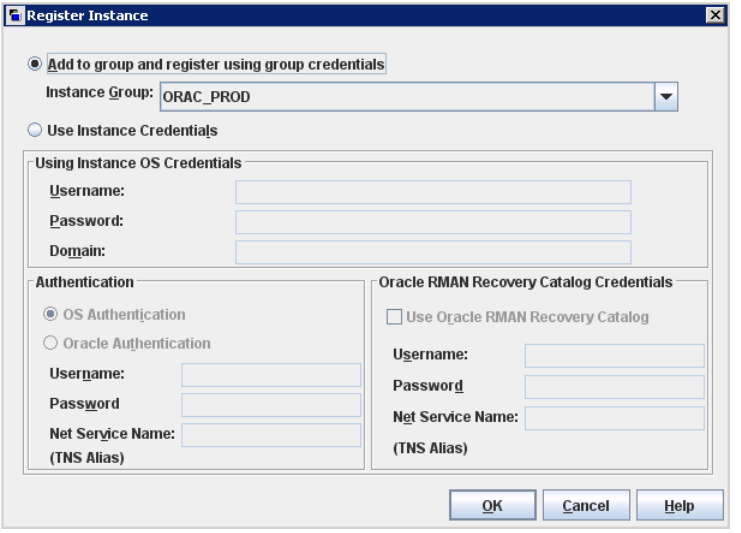
3. Double-click the instance that you want to register. The **Edit Instance** dialog box appears. For example, you can select ORAC13 to display the following:



You can select multiple instances to register at the same time.

4 (Conditional) Use 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. Click **Help** to display a description of the parameter. Example of the parameter:

5 In the **Credential** area, click **Edit** to display the **Register Instance** dialog box. For example:



6 In the **Register Instance** dialog box, click **Use Instance Credentials**.

The Oracle database user is required to have a certain level of credentials. The Oracle database user must have `SYSBACKUP` or `SYSDBA` privileges (based on version of Oracle).

7 Enter the **OS Credentials**.

8 In the **Authentication** area, you can optionally click **Oracle Authentication** to enter specific Oracle credentials. You may need to contact the Oracle DBA for the correct credentials. The system tries to validate the credentials and reports its findings.

You can also click **Use Oracle RMAN Recovery Catalog** to enter credentials for the RMAN recovery catalog. Then click **OK** to save the credentials. The **Edit Instance** dialog box reappears.

Click **OK** in the **Edit Instance** dialog box.

9 In the right pane of the **Applications** dialog, check the **Registered** column to see that the instance is now registered.

10 Repeat for all other instances that you want registered.

About Oracle database instance groups

Instance groups can be a major time saver when you create Oracle policies.

- You can configure an instance group to automatically add newly discovered database instances to the group.
- You need only enter a set of credentials once. The Oracle database user is required to have a certain level of credentials. The Oracle database user must have `SYSBACKUP` or `SYSDBA` privileges (based on version of Oracle). Thereafter, all discovered instances can be automatically assigned the same set of credentials, registering instances on the fly.
- With the selection of an instance group, you can create a single policy that backs up and restores hundreds and even thousands of instances.

See “Creating an Oracle database instance group” on page 30.

Adding an instance to an instance group

You can add an instance to an instance group by using the NetBackup Administration Console or by running the `nboraadm` command.

See the `nboraadm` description in the NetBackup Commands Reference Guide.

Note that you may have already registered an instance individually. When you add it to an instance group, its credentials are automatically changed to the group credentials.

To add an instance to an instance group

1. In the NetBackup Administration Console, in the left pane, expand **NetBackup Management > Applications > Oracle**.
2. Click **All Instances** to display all instances in the right pane.
3. Select the instance that you want to be a member of an instance group. You can select multiple instances from the list.
4. On the **Actions** menu, select **Register**. The **Register Instance** dialog appears. For example:

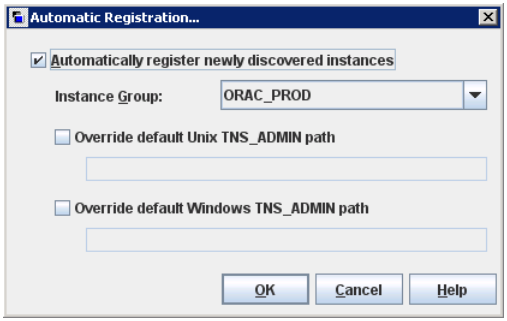
5. On the **Instance Group** pulldown menu, select the desired instance group (InstanceGroup1 in the example).
6. Click **OK**. A **Validation Report** dialog box appears that describes the validation successes and failures.

Automatic Registration of an instance group

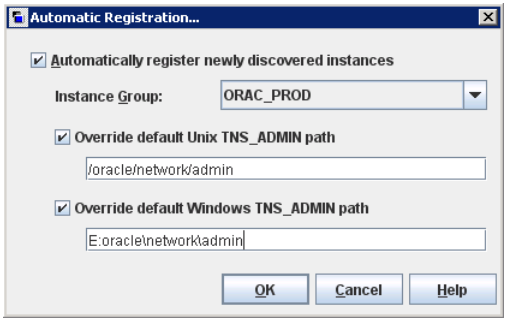
The Oracle Discovery Service brings newly discovered instances into the instance repository. Auto Registration is a mechanism that allows a discovered instance to be brought into the repository as a member of an instance group. The instance assumes the credentials of the group and is automatically registered.

To auto-register an instance group

1. In the NetBackup Administration Console, in the left pane, expand **NetBackup Management > Applications > Oracle**.
2. Click **Instance Groups**, then on the **Actions** menu, select **Auto Registration**. The following dialog box appears:



3. In the **Automatic Registration** dialog box, click the **Automatically register newly discovered instances**. Then select the desired instance group from the pulldown menu.
4. (Conditional) Use the **Override default Unix TNS_ADMIN path** and or the **Override default Windows TNS_ADMIN path** if you need to override the default network administration directory on the client system. Enter the fully qualified path for the correct operating system. You can automatically register instances in Windows, UNIX, or a combination of both operating systems. The following dialog box shows an example of this parameter:



5 Click **OK** to return to the **Instances** display. All newly discovered instances are automatically added to the specified instance group and registered with the group credentials.

6 A validation report shows if the instances passed or failed. Do one of the following:

- Click **OK** to save the credentials anyway. The instance is added to the instance list. However, instances with invalidated credentials cannot be selected as part of an Oracle policy. Their backups fail with a 54xx status error.
- Click **Cancel** to go back and change the credentials.

About instance actions

The **Actions** menu contains several operations that you can perform on the instances in the repository. Another way to perform these actions is to highlight the desired instance or instance group, then right-click and select the operation from the shortcut menu.

Table 4-2 describes the actions or operations that you can perform on Oracle database instances.

Table 4-2 Instance actions

Action	Description
New instance	To create a new instance, select **Actions > New > Instance**. A **New Instance** dialog box appears. Enter the instance properties (instance name, host, ORACLE_HOME, and credentials). See "Manually adding an Oracle database instance to the repository" on page 58.
New Instance Group	To create a new instance group, select **Actions > New > Instance Group**. A **New Instance Group** dialog box appears. See "About Oracle database instance groups" on page 64.
Properties	To display instance or instance group properties, highlight the desired item. Then select **Actions > Properties**. The **Edit Instance** appears where you change the instance properties (instance name, host, ORACLE_HOME, override default TNS_admin path, and credentials).
Register	To register an instance, highlight the instance, then select **Actions > Register**. The **Register Instance** dialog box appears. Change credentials for the selected item. See "Registering an Oracle database instance" on page 61. See "Adding an instance to an instance group" on page 64.

Table 4-2 Instance actions *(continued)*

Action	Description
Delete	To delete an instance or an instance group from the instances repository list, highlight the item to be deleted, then select **Actions > Delete**. You cannot delete an instance or an instance group that is part of a policy. First, use the **Instances and Databases** tab to delete the instance from the policy. Then, in the instances repository list, highlight the instance to be deleted, then select **Actions > Delete**.
Auto Registration	To automatically register newly discovered instances as part of an instance group, highlight **Instances** in the left pane, then select **Actions > Auto Registration**. See "Automatic Registration of an instance group" on page 65.
Clean up instances	This option lets you configure NetBackup to automatically clear orphaned instances from instance management. Orphaned instances are the databases that were discovered at one time but were never registered. To enable instance cleanup, select **Clean up After**. Next, select how often (**days**) that you want NetBackup to perform instance cleanup. **Note:** If instance cleanup is enabled and auto registration activated, cleaned up instances may be rediscovered and added to the auto registration group.

About Oracle Intelligent Policies (OIP)

The Oracle Intelligent Policy (OIP) feature is a method of Oracle policy backup based on Oracle database instances. This method precludes the need to create templates and scripts for your Oracle policies. The OIP feature has the following elements:

- You can create a single policy to protect multiple Oracle database instances that are spread over multiple clients.
- A discovery service discovers Oracle database instances throughout the NetBackup environment. The service polls the clients every five minutes and sends the discovered instances to an instance repository available to you on the NetBackup Administration Console. You manage instances and instance groups through the NetBackup Administration Console or the `nboraadm` command.
- All instances that you want backed up must be registered with credentials. If multiple instances share the same credentials, you can create an instance group for the set of instances with common credentials.

- Multiple instance groups can be created for different sets of instances with different credentials. You can create a default instance group for newly discovered instances to be automatically added to the group, ensuring that new instances are protected.
- The database administrator can control all instances and instance group credentials using the `nboraadm` command on the NetBackup client, which provides improved security throughout the system.
- You are not required to know RMAN or to write and use templates and RMAN scripts. Instead, this feature automatically generates the scripts at run-time.
- The Job Details in the Activity Monitor lets you view the backup summary, database state, RMAN input, and RMAN output for the OIP. Also, the Activity Monitor includes a new Instances column that shows the instance that the associated policy has backed up.
- Enhanced error codes enable faster identification, troubleshooting, and correction of problems. You can easily restart a failed job.
- You no longer need to create an application backup schedule. You only need to create automatic backup schedules for the data movement, which simplifies how retention works on the backup pieces.
- You can manually back up any number of instances or all the instances.
- The OIP automatically selects parameter settings at run-time that enable optimal deduplication.
- You can create a new archived log schedule that backs up the archived redo logs within intervals of minutes.
- The Oracle Intelligent Policy can protect an Oracle database when the Oracle DBA places database backups in the share on a NetBackup appliance.
- The OIP can create and maintain a full set of data file copies in the share on a NetBackup appliance. The Accelerator option is used to update the data file copies using only the changed blocks since the last full backup.
- Oracle 12c has introduced container databases (CDB) and pluggable databases (PDB) and they can be protected using the OIP.

Oracle DBAs can use the `nboraadm` command on the NetBackup client to manage instances, instance groups, and their credentials. This command is particularly useful in environments where the Oracle credentials are known only by the DBAs and not the NetBackup administrators.

The Oracle DBA can use the `nboraadm` command to start an immediate backup from the client if the NetBackup administrator has given the Oracle DBA proper permissions. The `nboraadm` command allows the Oracle DBA to immediately protect

an Oracle database backup instead of waiting for the NetBackup schedule to protect the database backup. Use `nboraadm` command with the `-immediate` option to start a database backup.

You can select Oracle database instances and instance groups to be part of an Oracle backup policy. An Oracle backup policy can be created for the default instance group to ensure that all newly created instances are automatically protected. You can create an OIP in the following ways:

- The Policy Configuration Wizard of the NetBackup Administration Console: The wizard guides you through the setup process by automatically choosing the best values for most configurations.
- The Oracle Policy utility on the NetBackup Administration Console: The Oracle Policy utility is a set of five tabbed panels. The panels contain all the settings and parameters that are needed to create or change an OIP.

See "Creating an Oracle Intelligent Policy (OIP)" on page 70.

See "About policy attributes" on page 90.

See "Instances and Databases tab" on page 77.

See "Backup Selections tab" on page 79.

See "About using Templates and Oracle Intelligent Policy (OIP) with RAC" on page 240.

Creating an Oracle Intelligent Policy (OIP)

This topic guides you through the steps for setting up an Oracle Intelligent Policy (OIP) using the **NetBackup Administration Console**. An OIP is used with Oracle CDB and PDB databases, Copilot, and regular Oracle database instance backups. This method precludes the need to create templates and scripts for your Oracle policies.

Table 4-3 Steps for creating an OIP

Steps	Task	Instructions
Step 1	Register Oracle instances.	NetBackup automatically discovers Oracle instances and displays them in the instance repository. An instance must be registered in order for that instance to be included in an OIP. See "Instance management for an Oracle Intelligent Policy" on page 55. See "About the NetBackup Discovery Service" on page 56. See "Manually adding an Oracle database instance to the repository" on page 58. See "Registering an Oracle database instance" on page 61.
Step 2	(Conditional) Create Oracle instance group.	Instance groups are for instances with common credentials. Add an instance to a group to register that instance. This step is not required to create an OIP. See "About Oracle database instance groups" on page 64. See "Adding an instance to an instance group" on page 64. See "Automatic Registration of an instance group" on page 65.
Step 3	Add new policy and policy name.	In the left pane of the **NetBackup Administration Console**, expand **NetBackup Management > Policies**. Select **Action > New > Policy** or right-click on **All Policies** in the center pane and click **New Policy** on the shortcut menu. Enter a unique name in the **Policy name:** dialog box and click **OK**. See "NetBackup for Oracle backup policy types" on page 48.
Step 4	Configure the **Attributes** tab.	In the **Policy Type** pull-down menu, select **Oracle**. This action causes the tabs along the top of the display to change to a unique Oracle tab set. For information on the **Attributes** tab, see the NetBackup Administrator's Guide, Volume I. The **Use Accelerator** option has a different function when used with an OIP. This option is automatically selected when certain options in the **Backup Selections** tab are set during Copilot configuration. See "About using a NetBackup appliance share for Oracle backups (Copilot)" on page 84.

Table 4-3 Steps for creating an OIP *(continued)*

Steps	Task	Instructions
Step 5	Configure the **Schedules** tab.	The schedules that are defined on the **Schedules** tab determine when backups occur for an OIP. For information on the **Schedules** tab, see the NetBackup Administrator's Guide, Volume I.
Step 6	Configure the **Instances and Databases** tab.	Select the instances or the instance groups that the OIP will back up. An OIP must include either the **Protect Instances and Databases** or the **Protect instance groups** option. See "Instances and Databases tab" on page 77.
Step 7	Configure the **Backup Selections** tab.	You can backup the **Whole database**, **Partial database - Tablespaces**, **Partial database - Datafiles**, **Fast Recovery Area (FRA)**, **Database Backup Shares**, or the **Whole Database - Datafile Copy Share**. See "Backup Selections tab" on page 79. See "Configuring an OIP using a share on the NetBackup appliance (Copilot)" on page 86. See "Configuring the appliance within a RAC environment" on page 257.
Step 8	Configure the **Oracle** tab.	The tab contains setup options for databases, tablespaces, data files, archived redo logs, file name formats, and database backup shares. See "Oracle tab" on page 81.

Oracle database upgrade effect on Oracle Intelligent Policies

Upgrade of an Oracle database causes instance information for the upgraded database to become invalid. If this instance is associated with one or more current NetBackup for Oracle Intelligent Policies, run-time failures can occur. The issue occurs when an Oracle database is upgraded to a new version. The new version is likely to have a different ORACLE_HOME, ORACLE_SID, or Oracle User. If any of these values have changed, the existing instance information in the NetBackup instance repository and in the current Oracle Intelligent Policies becomes invalid. When the discovery service (`nbdisco`) polls the clients again, it discovers the database as a new instance. Consequently, there is no way to associate the new instance to the old instance.

This issue is not version-specific and can affect any valid Oracle upgrade patch, such as:

- Oracle 10 to version 11
- Oracle 10 to version 12
- Oracle 11 to version 12

For more information on valid Oracle upgrade paths, review the following documentation on the Oracle Support website:

http://www.oracle.com/technetwork/database/upgrade/upgrading-oracle-database-wp-12c-1896123.pdf

Therefore, when an existing Oracle database is upgraded and the ORACLE_HOME, ORACLE_SID, or Oracle User are modified, remove the existing instance in the instance repository. After the existing instance is removed, update the instance repository with the new instance information. Make sure to update any policies with the newly-discovered instances.

See "About Oracle Intelligent Policies (OIP)" on page 68.

See "Instance management for an Oracle Intelligent Policy" on page 55.

Configuring NetBackup for Oracle automatic backup schedules

Each policy has an automatic backup schedule. These schedules initiate automatic backups and specify when a user can initiate operations.

To configure an automatic backup schedule

1. On the **Policy** dialog box, click the **Schedules** tab.
2. Click **New**.
3. Specify a unique name for the schedule.
4. Select the **Type of backup**.
5. Specify the other properties for the schedule.

   See "About schedule properties " on page 91.
6. Click **OK**.

About NetBackup for Oracle schedule properties using Oracle Intelligent Policy

This topic describes the schedule properties that have a different meaning for Oracle Intelligent Policy backups than for file system backups. Other schedule properties vary according to your specific backup strategy and system configuration. Additional information about other schedule properties is available.

See the NetBackup Administrator's Guide, Volume I.

Table 4-4 Description of schedule properties

Property	Description
Type of backup	Specifies the type of backup that this schedule can control. The selection list shows only the backup types that apply to the policy you want to configure. See "NetBackup for Oracle backup policy types" on page 48.
Schedule type	You can schedule a backup in one of the following ways: ■ **Frequency** This setting is used only for scheduled backups. It is not used for user-directed backups. **Frequency** specifies the period of time that can elapse until the next backup or archive operation begins on this schedule. For example, assume that the frequency is 7 days and a successful backup occurs on Wednesday. The next full backup does not occur until the following Wednesday. Typically, incremental backups have a shorter frequency than full backups. ■ **Calendar** This setting is used only for scheduled backups. It is not used for user-directed backups. The **Calendar** option lets you schedule the backup operations that are based on specific dates, recurring week days, or recurring days of the month.
Retention	Specifies a retention period to keep backup copies of files before they are deleted. The retention period for an automatic schedule controls how long NetBackup keeps records of when scheduled backups occurred. Set the time period to retain at least two full backups of your database. In this way, if one full backup is lost, you have another full backup to restore. The type of schedule you select affects the retention period as follows: ■ Frequency-based scheduling Set a retention period that is longer than the frequency setting for the schedule. For example, if the frequency setting is set to one week, set the retention period to be at least 2 weeks. The NetBackup scheduler compares the latest record of the automatic backup schedule to the frequency of that automatic backup schedule. This comparison is done to determine whether a backup is due. So if you set the retention period to expire the record too early, the scheduled backup frequency is unpredictable. However, if you set the retention period to be longer than necessary, the NetBackup catalog accumulates unnecessary records. Oracle is not notified when NetBackup expires a backup image. Use Oracle RMAN repository maintenance commands to periodically delete expired backup sets from the Oracle RMAN repository. ■ Calendar-based scheduling The retention period setting is not significant for calendar-based scheduling.
Multiple copies	If you want to specify multiple copies of a backup for the policy, configure **Multiple copies** on the application backup schedule.

Table 4-4 Description of schedule properties *(continued)*

Property	Description
Accelerator forced rescan	This option instructs NetBackup to re-copy all the data files to the share. This option is only available when **Whole Database - Datafile Copy Share** is selected in the **Backup Selections** tab and the **Use Accelerator** option is selected in the **Attributes** tab. This option forces the creation of a new set of database data file copies. When this option is not selected, the data file copies in the share are updated using an incremental backup. The incremental backup contains only the changed blocks since the last full backup.

Oracle Intelligent Policy - Storage and Retention

This topic describes storage and retention properties of the Oracle Intelligent Policy.

See the NetBackup Administrator's Guide, Volume I.

Table 4-5 Storage and retention behavior

Property	Description
Policy is a snapshot type	If the policy is a snapshot type, the following are the possible scenarios of the retention behavior: ■ If the schedule does not override the policy storage unit, and the policy storage unit is a non-snapshot SLP, the SLP determines the retention period and the policy uses the policy storage unit. ■ If the schedule does not override the policy storage unit and the policy storage unit is not an SLP, the schedule determines the retention period, and the policy uses the policy storage unit. ■ If the schedule does override the policy storage unit with an SLP, and it is not a snapshot SLP, the override storage unit takes precedence over the policy storage unit, and the SLP determines the retention period. ■ If the schedule overrides the policy storage unit with a snapshot SLP, the policy storage unit must be a non-snapshot SLP. The SLP on the policy storage unit determines the retention period for the streamed data. Also, the SLP on the schedule determines the retention for the snapshot data.

Table 4-5 Storage and retention behavior *(continued)*

Property	Description
Policy is not a snapshot type	If the policy is not a snapshot type, the following are the possible scenarios of the retention behavior: ■ If the schedule does not override the policy storage unit and the policy storage unit is not an SLP, the schedule determines the retention period. ■ If the schedule does not override the policy storage unit and the policy storage unit is an SLP, the SLP determines the retention period. ■ If the schedule overrides the policy storage unit, and the schedule storage unit is not an SLP, the schedule determines the retention period. ■ If the schedule overrides the policy storage unit and the schedule storage unit is an SLP, the SLP determines the retention period.

The following are examples of the Oracle Intelligent Policy storage and retention behavior for snapshot-based policy types.

Policy storage	Schedule storage	Streamed data retention is derived from:	Snapshot data retention is derived from:
AdvancedDisk	-	Schedule	Schedule
AdvancedDisk	SLP	SLP	SLP
SLP	-	SLP	SLP
Tape library	-	Schedule	Schedule
Non-Snapshot SLP	Snapshot SLP	Non-Snapshot SLP	Snapshot SLP
AdvancedDisk	Snapshot SLP	Invalid configuration	Invalid configuration

The following are examples of the Oracle Intelligent Policy storage and retention behavior for stream-based policy types.

Policy storage	Schedule storage	Streamed data retention is derived from:
AdvancedDisk	-	Schedule
SLP	AdvancedDisk	Schedule
AdvancedDisk	SLP	SLP
SLP	-	SLP

About Oracle Intelligent Policy master server behavior

By default for an Oracle Intelligent Policy, the client uses the first server in the server list to start the Oracle backup or restore operation. However, you may want the operation to recognize the master server name that is passed down from the master server. If so, do one of the following:

- On Windows, enter the USE_REQUESTED_MASTER = TRUE statement into a text file (for example, `new_config.txt`). Then use the following command on the master or the media server to send this newly created configuration file to the client host:

  ```
  # bpsetconfig -h myoracleclient new_config.txt
  ```

- On UNIX, add USE_REQUESTED_MASTER = TRUE to the `bp.conf` file, which enables more than one master server to back up the client.

Instances and Databases tab

Use the **Instances and Databasese** tab to select instances, instance groups, or clients that the Oracle Intelligent Policy is scheduled to back up. Until you select items the first time for this policy, the panel is blank. Click **New** to display another panel that lists all the possible instances, instance groups, or clients.

If you add a new Oracle policy or change an existing Oracle policy, this tab appears along the top of the policy configuration dialog.

You cannot mix instances and instance groups in this list. If you select instances for a policy, then you want to select an instance group, the instances you select are deleted from the list.

The **Instances and Databases** tab displays all the instances or instance groups that the Oracle policy is scheduled to back up. If you add a new Oracle policy or change an existing Oracle policy, this tab is one of several tabs that appear along the top of the dialog. Click **Instances** to display three possible categories of items:

- **Protect Instances and Databases** (OIP option). This panel displays all instances that you have selected to back up for this policy. To add new instances to this list, click **New**. A **Select Instances** panel appears that displays all registered instances. Click the check box next to the instance or instances that you want to add to the list. Instances that are already selected and in the list have their check boxes checked. If an instance does not appear in this panel because it is unregistered, you can register that instance and add it to the policy later. The instance selection does not take effect until you click **OK**.
  Table 4-6 describes all the instance fields for the instances in this list.

- **Protect instance groups** (OIP option). This panel displays all instance groups that you have created. To add new instances to this list, click **New**. A **Select Instance Group** panel appears that displays all instance groups that you have created. All instances that are a part of an instance group at backup time are backed up. To add an instance group to the list of groups that are displayed on this panel, click **New**.

  To see what instances are backed up if the policy is run for an instance group, select the group from the list, then click **Preview Instances**. A panel appears that shows a list of all the registered instances in the group to be backed up.
- **Clients for use with scripts or templates** (Non-OIP option). This option is not for use with OIP. If you want to use the client with scripts or templates method of configuring an Oracle policy instead of the new instance method, select **Clients for use with scripts or templates**. If you select this option, the existing backup selections and instances or instance group are erased. Also, the **Options** tab and the **Instances and Databases** tab are removed, because those options must now be set in the RMAN script that the user supplies.

Table 4-6 Instances and Databases tab fields

Field	Description
Instance Name	The selection at the top of the panel determines the listing in the panel window. ■ **Protect Instances and Databases** displays all individual instances that you have chosen for this Oracle policy. ■ **Protect instance groups** displays all the instance groups that you have created for this policy. ■ **Clients for use with scripts or templates** displays all clients that you have selected for this policy. Click **New** to add more clients to this list.
Database Name	The name of the selection that is referenced for this policy. The **Backup Selections** tab defines what is backed up for the selections. This column only appears when you select **Protect Instances and Databases**. The **Database Name** can reference: ■ An entire instance ■ Single or multiple PDBs
State	Active - DB will be backed up. Done in the host properties application.
Host	Specifies the host where the Oracle database resides.
OS Type	Specifies the operating system of the host. Valid values are Windows and UNIX.

Table 4-6 Instances and Databases tab fields *(continued)*

Field	Description
ORACLE_HOME	The file path of the Oracle home directory where the instance resides.
Instance Group	Specifies the Oracle database instance group name that this instance is part of. This field is blank if the instance does not belong to an instance group.
Registered	Specifies the date and time when a user gave the instance a set of credentials. This field is blank if the instance has not been given credentials.

Backup Selections tab

The **Backup Selections** tab lets you change the type of Oracle backup. You can back up the whole database, only the tablespaces, only the data files, the **Fast Recovery Area (FRA)**, **Database Backup Shares**, or the **Whole Database - Datafile Copy Share**. The following is the selection list:

- **Whole database**
- **Partial database - Tablespaces**
- **Partial database - Datafiles**
- **Fast Recovery Area - (FRA)**. This option backs up the contents of the FRA. For the Oracled atabase instance to be restored and recovered, make sure that the FRA contains a recoverable image set when it is backed up.
- **Database Backup Shares**. This option is used when the Oracle DBA places database backups in the share on a NetBackup appliance (Copilot).

  Note: This feature requires a NetBackup appliance running software version 2.7.1 or later.

- **Whole Database - Datafile Copy Share**. This option is used to create and maintain a full set of data file copies in the share on a NetBackup appliance (Copilot).

  Note: This feature requires a NetBackup appliance running software version 2.7.1 or later.

By default, the **Whole database** option is selected and the backup selections contain the directive `WHOLE_DATABASE`. If you choose one of the partial options (tablespaces or data files), you must click the **New** button to display a new panel. The panel contains a list of instances from which you can select tablespaces or the data files that the new policy can back up.

When you back up tablespaces or data files, this selection applies across all the instances and PDBs that are selected in the policy. If a tablespace is selected for one instance or PDB, that same tablespace is backed up for all instances and PDBs in the policy.

If you set up an OIP and that policy contains a CDB with PDBs, the `CDB$ROOT` is automatically included in the backup. If the policy contains a PDB that is not found when a backup is performed, an error appears in the Activity Monitor. The Administration Console displays a status of either 5421 or 5422.

Note: When the Backup, Archive, and Restore GUI is used, the `CDB$ROOT` is automatically included in a backup of a PDB in a CDB. The `CDB$ROOT` is also automatically included in a tablespace or data file backup. Also, a backup can contain either tablespaces or the data files. A backup cannot contain both of these options.

If you select the **Database Backup Shares** option, the directive `ALL_DATABASE_BACKUP_SHARES` is automatically added to the selection list. Using this directive, the policy backs up all the shares that are used on all appliances per instance. Optionally, you can click **Browse** to display a new panel that contains a list of appliance shares. The appliance shares are where Oracle DBAs have created backups for the instances configured in the policy. Select one or more shares that the new policy should back up. Also, you can click **New** and add an appliance share to the policy manually.

When you back up appliance shares for multiple instances, the **Database Backup Shares** selection applies across all the instances that are selected in the policy. If a share is selected for one instance, the data in that share is backed up for all the instances in that policy.

The **Whole Database - Datafile Copy Share** option allows the NetBackup Administrator to choose an appliance share as the destination for the first backup copy. When the policy runs the first time, an RMAN script is generated that creates a full set of Oracle data file copies. The copies reside in the appliance share. The next time that the full schedule runs, the backup is accelerated if the **Use Accelerator** option is selected. The RMAN script that is generated performs an incremental backup and the changed blocks are merged into the data files. This incremental backup creates an updated full set of Oracle data file copies. After the

new full copy is created in the appliance share, an SLP is used to make additional copies of the full backup. The first copy is always a `remote_vxfs` snapshot.

The **Use Accelerator** feature is automatically selected when you configure an OIP with the **Whole Database - Datafile Copy Share** option. The first time that the full schedule runs it creates a full set of data file copies. After the first full schedule, only the changes are backed up as a backup set and merged with the existing full backup. Basically, an incremental merge is performed and Oracle's Block Change Tracking feature should be enabled for faster incremental backups. Only one share can be set up so if you have two or more instances, all instances reside in the same share.

Note: The **Database Backup Shares** and **Whole Database - Datafile Copy Share** options can only be configured when the media server is a NetBackup appliance. This option does not work with any other type of media server.

Oracle tab

This tab contains options for databases, tablespaces, data files, archived redo logs, file name formats, and database backup shares.

Table 4-7 Oracle tab fields

Field	Description
Tablespace/Datafile Options	**Number of parallel streams** is the number of parallel backup streams that can be used in a backup operation. Select **Specify read-only tablespace options** to enable read-only tablespace options. Possible values are **SKIP** and **FORCE**. **SKIP** means to skip the read-only tablespace during backup. **FORCE** means that RMAN backs up all files. Select **Offline (cold) database backup** to shut down the Oracle database and put it in the mount state. ■ When this option is used with a PDB, the PDB is put in a mounted state for the backup. Once the backup has completed, the PDB is returned to the state it was in before the backup. Select **Skip offline datafiles** to direct the backup operation to not access offline data files.

Table 4-7 Oracle tab fields *(continued)*

Field	Description
Specify maximum limits	Select **Specify maximum limits** to access several I/O and backup set limits. The following parameters should only have to be modified on rare occasions. If these values are not changed, the backup uses the default values defined in RMAN. RMAN default values usually provide the best performance. Maximum I/O Limits parameters: ■ **Read rate (KB/sec)** (RATE) specifies the maximum number of kilobytes (KB) that RMAN reads each second on this channel. This parameter sets an upper limit for bytes read so that RMAN does not consume too much disk bandwidth and degrade performance. ■ **Size of backup piece (KB)** (MAXPIECESIZE) specifies the maximum size of each backup piece that is created on this channel. ■ **Number of open files** (MAXOPENFILES) controls the maximum number of input files that the backup operation can have open at any given time. Maximum backup set limits parameters: ■ **Number of files per backup set** (FILESPERSET) specifies the maximum number of input files to include in each output backup set. ■ **Size of the backup set (KB)** (MAXSETSIZE) specifies a maximum size for a backup set in kilobytes.
Backup Identifier Options	**Backup set identifier:** (**TAG**) specifies a user-specified tag name for a backup set, proxy copy, data file copy, or control file copy. The tag is applied to the output files that the backup generates. **Datafile copy tag:** This option specifies a user-specified tag name when the **Whole Database - Datafile Copy Share** option is used. The tag is associated with the data files that are located on the appliance and is used during the incremental merge process.

Table 4-7 Oracle tab fields *(continued)*

Field	Description
Archived Redo Log Options	Select **Include archived redo logs in full and incremental schedules** to include the archived redo logs in the full and the incremental schedule backups. Select **Delete after making copies** to delete the archived redo logs after the selected number of backups are successful. Uncheck the box or set to 0 to skip the delete operation and retain the logs after backup. **Number of parallel streams** controls the degree of parallelism within a backup. This number specifies the maximum number of connections between RMAN and a database instance. Each connection initiates an Oracle database server session on the target instance. This server session performs the work of backing up backup sets. Specify **Specify maximum limits** to set custom limits for the archive redo logs. ■ **Number of files per backup set** specifies the maximum number of archived redo log files to include in each output backup set. ■ **Size of backup set (KB)** (MAXSETSIZE) specifies a maximum size for a backup set of archived redo logs in kilobytes.
User Specified Backup File Name Formats	Select **Specify backup file name formats** to set up formats for various backup file names for data files, archived redo logs, the control file, and Fast Recovery Area (FRA). Ensure that the format that is specified for all RMAN backup piece names (except for auto-backups of the control file) uses the `_%u` and ends with `_%t`. NetBackup uses this timestamp as part of its search criteria for catalog images. Without this timestamp, performance might degrade as the NetBackup catalog grows. These recommendations help to ensure proper backup, restore, and crosscheck functionality. **Note:** By default OIP uses the following `_d%d_u%u_s%s_p%p_t%t`.

Table 4-7 Oracle tab fields *(continued)*

Field	Description
Database Backup Share Options	These options let you set a time when backup sets and backup copies (data and control file copies) are automatically deleted from the appliance share. However, the files are only deleted if they have been successfully backed up from the share. The two options are **Delete protected backup sets from share after** and **Delete protected backup copies from share after**. The deletion is based on the age of the file in the share. The original dump time or the update time (if an incremental merge is done on the file) determines the age of the file. These options are only available when the **Database Backup Shares** option is selected in the **Backup Selections** tab. Use the drop downs to set the minutes, hours, days, or weeks. **Note:** The **Database Backup Shares** delete options can only be configured when the media server is a NetBackup appliance. This option does not work with any other type of media server. This feature requires a NetBackup appliance running software version 2.7.1 or later.

About using a NetBackup appliance share for Oracle backups (Copilot)

Note: This feature requires a NetBackup appliance running software version 2.7.1 or later.

This feature enhances the Oracle Intelligent Policy by giving you two options for protecting an Oracle database using a share on a NetBackup appliance. The first option gives you better control of backups when Oracle database backups are placed in an appliance share by the DBA. The second option lets you choose an appliance share as the destination for the first backup copy. Now you do not have to rely on the DBA to create backups in the share. You must provision a share on the appliance for these options using the NetBackup Appliance Shell Menu.

The **Database Backup Shares** option provides a share for the DBA on the NetBackup appliance and is protected using the Oracle Intelligent Policy. The backup occurs on the appliance as an off-host backup and all data movement occurs on the appliance and does not affect the Oracle client. Since the OIP protects the appliance share, the backups are visible when the DBA uses RMAN or Oracle Enterprise Manager.

The **Whole Database - Datafile Copy Share** option enhances the OIP to allow the NetBackup Administrator to choose an appliance share as the destination for the first backup copy. When the policy runs the first time, an RMAN script is generated that creates a full set of Oracle data file copies. The data file copies reside in the appliance share. The next time that the full schedule runs, the backup is accelerated if the **Use Accelerator** option is selected. The RMAN script that is generated performs an incremental backup and the changed blocks are merged into the data files. This incremental backup creates an updated full set of Oracle data file copies. After the new full copy is created in the database backup share, an SLP is used to make additional copies of the full backup. The first copy is always a `remote_vxfs` snapshot. The `remote_vxfs` snapshot creates a `vxfs_checkpoint` snapshot of the share on the NetBackup appliance.

On the **Attributes** tab, the **Use Accelerator** feature is automatically selected when you configure an OIP with the **Whole Database - Datafile Copy Share** option selected in the **Backup Selections** tab. The first time that the full schedule runs it creates a full set of data file copies. After the first full schedule, only the changes are backed up as a backup set and merged with the existing full backup. Basically, an incremental merge is performed. Oracle's Block Change Tracking feature should be enabled for faster incremental backups.

When using Copilot to protect your database, NetBackup does not protect extended attributes, extent attributes, or Access Control Lists associated with the database's data files.

Note: These options are available to you but only configurable when you have a NetBackup appliance configured as the media server. Create a share on the appliance using the procedures in the Managing shares section of the Veritas NetBackup 52xx and 5330 Appliance Administrator's Guide. If you enter a share path that is not located on an appliance, nothing is backed up.

See "Configuring an OIP using a share on the NetBackup appliance (Copilot)" on page 86.

See "Backup Selections tab" on page 79.

See "Creating an Oracle Intelligent Policy (OIP)" on page 70.

See "Configuring the appliance within a RAC environment" on page 257.

See "About restoring from a data file copy to ASM storage using RMAN" on page 155.

Configuring an OIP using a share on the NetBackup appliance (Copilot)

Note: This feature requires a NetBackup appliance running software version 2.7.1 or later.

The **Database Backup Shares** option protects the database backups that an Oracle DBA creates on a share on the NetBackup appliance.

The **Whole Database - Datafile Copy Share** option enhances the OIP to allow the NetBackup Administrator to choose an appliance share as the destination for the first backup copy. The backup copy is a full set of data file copies that are maintained by updating only the changed blocks if **Use Accelerator** is selected.

Use the following procedure to set up a backup policy that protects shares on the NetBackup appliance.

To configure an OIP using the Database Backup Shares or Whole Database - Datafile Copy Share options

1. (**Database Backup Shares** option) The Oracle DBA asks NetBackup administrator for the appliance share information.
2. The NetBackup administrator uses the NetBackup Appliance Shell Menu to create a share on the appliance and then sets permissions for the share.
   - For more information about how to set up the share, see Creating a share from the NetBackup Appliance Shell Menu in the Veritas NetBackup 52xx and 5330 Appliance Administrator's Guide
3. The NetBackup administrator sends information about the appliance share to system administrator.
4. The system administrator mounts an appliance share on the Oracle database server using the OS tools.

5 (**Database Backup Shares** option) The Oracle DBA uses RMAN to create a database backup on the appliance share.

6 Configure an OIP.

Attributes tab	On the **Attributes** tab, select **Oracle** as the **Policy Type**. The **Use Accelerator** option is automatically selected when the **Whole Database - Datafile Copy Share** option is selected. If the **Use Accelerator** option is unchecked the full set of data files are copied again (including changed blocks). When the **Use Accelerator** option is used, the Oracle Change Block tracking should be enabled for better performance. For information on the **Attributes** tab, see the NetBackup Administrator's Guide, Volume I.
Schedules tab	On the **Schedules** tab, click **New** and select **Full Backup**. For information on the **Schedules** tab, see the NetBackup Administrator's Guide, Volume I.
Instance tab	Select the Oracle database instance in the **Instance** tab. See "Instances and Databases tab" on page 77.
Backup Selections tab	Select the **Database Backup Shares** option in the **Backup Selections** tab. See "Backup Selections tab" on page 79.
Oracle tab	Set up the deletion of backup sets and data file copies in the **Oracle** tab. See "Oracle tab" on page 81.

Note: The **Database Backup Shares** option can only be configured when the media server is a NetBackup appliance. This option does not work with any other type of media server.

See " Configuring a snapshot policy using a share on the NetBackup appliance (Copilot)" on page 185.

See "About using a NetBackup appliance share for Oracle backups (Copilot)" on page 84.

See “Configuring the appliance within a RAC environment” on page 257.

About script- or template-based Oracle policies

NetBackup users or automatic schedules can start database backups by specifying a template or a shell script in the file list of the Oracle policy. The template or the shell script specifies the backup commands that RMAN performs on the client.

Note: All scripts must be stored and run locally. One recommendation is that scripts should not be world-writable. Scripts are not allowed to be run from network or remote locations. Any script that is created and saved in the NetBackup `db_ext` (UNIX) or `dbext` (Windows) location needs to be protected during a NetBackup uninstall.

For more information about registering authorized locations and scripts, review the knowledge base article:

http://www.veritas.com/docs/000126002

On UNIX, NetBackup for Oracle includes a library of functions that enable RMAN to use NetBackup. You can link to this library

See the instructions for how to link to this library.

See “About linking Oracle RMAN with NetBackup for UNIX” on page 37.

On Windows, NetBackup for Oracle includes a library of functions that enable RMAN to use NetBackup. This library is in `c:\Windows\system32`.

When you use the RMAN `backup` command, each resulting backup set contains at least one backup piece (data file, data file copy, control file, or archive log) from the target database. You must give each backup piece a unique name using the `format` operand. Several substitution variables are available to aid in generating unique names. You can specify the `format` operand in the `backup` command. NetBackup considers the backup piece name as the file being backed up, so this name must be unique in the catalog.

For a backup, the following items apply:

- The `rman` command starts the requested operation on the databases.
- When the process requires media to store backup data, RMAN starts a user-directed backup by issuing a backup request.
- The NetBackup media server connects to NetBackup for Oracle on the client. NetBackup for Oracle on the client sends the database data to the NetBackup media server which saves the data to secondary storage. A restore works in

essentially the same manner except that RMAN issues a restore request. This request causes NetBackup to retrieve the data from secondary storage and send it to NetBackup for Oracle on the client.

- RMAN supports parallel operations, so a single `rman` command can start more than one backup, or restore on the NetBackup system.
- The status for an RMAN operation is stored in the RMAN catalog or in the database control file. This same status appears in the output of the RMAN command that is used to run the backup or restore. This status is the only status that a database administrator must check to verify that a backup or restore has been successful.
- NetBackup also logs status, but only for its own part of the operation. The database administrator cannot use the NetBackup status to determine whether `rman` was successful. Errors can occur in `rman` that do not affect NetBackup and are not recorded in its logs.

Adding a new script- or template-based Oracle policy

This topic describes how to add a new backup policy for a database.

To add a new script- or template-based Oracle policy

1. Log on to the master server as administrator (Windows) or root (UNIX), and start the **NetBackup Administration Console**.
2. If your site has more than one master server, choose the one on which you want to add the policy.
3. In the **NetBackup Administration Console**, select **NetBackup Management** > **Policies**. Then select **Actions > New > New Policy**.
4. In the **Add a New Policy** dialog box, in the **Policy name** box, type a unique name for the new policy. Click **OK**.
5. In the **Add New Policy** dialog box, in the **Policy type** list, select **Oracle**. The tabs along the top of the dialog change to include an **Instances and Databases** tab.

   The database agent policy type does not appear in the drop-down list unless your master server has a license for the database agent.
6. Click the **Instances and Databases** tab and select **Clients for use with scripts or templates**.
7. Click **Yes** on the **Backup Policy Management** dialog box. The tabs along the top of the dialog change again to include a **Clients** tab.

8 Click **OK** to return to the main screen of the **NetBackup Administration Console**. Select **View** > **Refresh** to refresh the GUI so that the appropriate schedule information appears in the **Schedules** tab.

9 In the right pane, double-click the policy that you have added. Another option is to right-click on the policy name in the center pane and select **Change** from the menu.

10 Complete the entries on the **Attributes** tab.

See "About policy attributes" on page 90.

11 Add other policy information as follows:

- Add schedules.
  See "Configuring NetBackup for Oracle automatic backup schedules" on page 73.
- Add clients. On the **Clients** tab, click **Clients for use with Scripts or templates** option. Then click **New** to display a list of all possible clients. Select new clients from this list, then click **OK**.
  See "Adding clients to a policy" on page 95.
- Add templates or scripts to the backup selections list.
  See "About adding backup selections to an Oracle policy" on page 96.
  See "Registering authorized locations used by a NetBackup database script-based policy" on page 337.

12 When you have added all the schedules, clients, and backup selections you need, click **OK**.

About policy attributes

With a few exceptions, NetBackup manages the policy attributes set for a database backup like a file system backup. Other policy attributes vary according to your specific backup strategy and system configuration.

Table 4-8 describes some of the policy attributes available for a NetBackup for Oracle policy. For more information on policy attributes, see the NetBackup Administrator's Guide, Volume I.

Table 4-8 Policy attribute descriptions for NetBackup for Oracle policies

Attribute	Description
Policy type	Determines the types of clients that can be backed up with the policy. For Oracle databases, select the policy type Oracle.

Table 4-8 Policy attribute descriptions for NetBackup for Oracle policies *(continued)*

Attribute	Description
Limit jobs per policy	Sets the maximum number of instances that NetBackup can back up concurrently with this policy.
Follow NFS	This option is available for Oracle policies on UNIX. Select this attribute to back up the files from NFS-mounted file systems. If this option is not selected, NetBackup cannot perform a backup of NFS-mounted files. Also see the NetBackup Administrator's Guide, Volume I. **Note:** This option is not available for snapshot backups.
Keyword phrase	For NetBackup for Oracle, the **Keyword phrase** entry is ignored.
Snapshot Client and Replication Director	This group contains the options that enable backups with Snapshot Client and Replication Director.

About backup schedules, templates, and scripts

Be aware of what may happen if an automatic schedule invokes a script that a user authored. NetBackup does not provide safeguards to prevent an automatic backup schedule, for example, from running a restore or recovery script.

To help guard against such mistakes, use a template instead of a script whenever possible. When a template runs, it detects the backup type on the schedule. You are responsible for specifying a template with the correct operation type (backup or restore) in the policy.

About schedule properties

This topic describes the schedule properties that have a different meaning for database backups than for file system backups. Other schedule properties vary according to your specific backup strategy and system configuration. Additional information about other schedule properties is available. See the NetBackup Administrator's Guide, Volume I.

Table 4-9 Description of schedule properties

Property	Description
Type of backup	Specifies the type of backup that this schedule can control. The selection list shows only the backup types that apply to the policy you want to configure.

Table 4-9 Description of schedule properties *(continued)*

Property	Description
Schedule type	You can schedule an automatic backup in one of the following ways: ■ **Frequency** **Frequency** specifies the period of time that can elapse until the next backup operation begins on this schedule. For example, assume that the frequency is 7 days and a successful backup occurs on Wednesday. The next full backup does not occur until the following Wednesday. Typically, incremental backups have a shorter frequency than full backups. ■ **Calendar** The **Calendar** option lets you schedule the backup operations that are based on specific dates, recurring week days, or recurring days of the month.
Retention	The retention period for an application backup schedule refers to the length of time that NetBackup keeps backup images (stream-based backups). The retention period for an automatic schedule controls how long NetBackup keeps records of when scheduled backups occurred (proxy backups). For example, if your database is backed up once every Sunday morning, you should select a retention period of at least 2 weeks. The type of schedule you select affects the retention period as follows: ■ Frequency-based scheduling Set a retention period that is longer than the frequency setting for the schedule. For example, if the frequency setting is set to one week, set the retention period to be more than one week. The NetBackup scheduler compares the latest record of the automatic backup schedule to the frequency of that automatic backup schedule. This comparison is done to determine whether a backup is due. So if you set the retention period to expire the record too early, the scheduled backup frequency is unpredictable. However, if you set the retention period to be longer than necessary, the NetBackup catalog accumulates unnecessary records. Oracle is not notified when NetBackup expires a backup image. Use Oracle RMAN repository maintenance commands to periodically delete expired backup sets from the Oracle RMAN repository. Oracle XML export operations create archives for long-term storage and recovery. Set the retention level to a period of years or to infinity. ■ Calendar-based scheduling The retention period setting is not significant for calendar-based scheduling.
Multiple copies	If you want to specify multiple copies of a backup for the policy, configure **Multiple copies** on the application backup schedule. If using Snapshot Client, also specify **Multiple copies** on the automatic schedule.

Script- or template-based policy - Storage and Retention

This topic describes storage and retention properties of the script- and template-based policies.

See the NetBackup Administrator's Guide, Volume I.

Table 4-10 Storage and retention behavior

Property	Description
Policy is a snapshot type	If the policy is a snapshot type, the following are the possible scenarios of the retention behavior: ■ If a schedule has overridden the policy storage, the override storage on the schedule takes precedence over the policy storage. ■ If the policy storage is a snapshot SLP, the application schedule must override the policy storage. The storage that is specified on the application schedule may not be a snapshot SLP. ■ If the storage being used is not an SLP, the schedule determines the retention for the snapshot data. ■ If you use the policy storage unit as an SLP, the SLP determines the retention for the snapshot data. Streamed data is processed by using the application schedule. Snapshot data is processed by using the automatic schedule.
Policy is not a snapshot type	If the policy is not a snapshot type, the following are the possible scenarios of the retention behavior: ■ If the application schedule has overridden the policy storage, the override storage on the schedule takes precedence over the policy storage. ■ If the storage being used is not an SLP, the retention is derived from the schedule. ■ If the storage being used is an SLP, the retention is derived from the SLP. Since all data is streamed, the data is processed using the application schedule.

The following are examples of the script- or template-based policy storage and retention behavior for snapshot-based policy types:

Policy storage	Application schedule storage	Full/Incremental schedule storage	Streamed data retention is derived from:	Snapshot data retention is derived from:
AdvancedDisk	-	-	Application Schedule	Full/Incremental Schedule

Policy storage	Application schedule storage	Full/Incremental schedule storage	Streamed data retention is derived from:	Snapshot data retention is derived from:
AdvancedDisk	-	Non-Snapshot SLP	Application Schedule	Non-Snapshot SLP
Non-Snapshot SLP	AdvancedDisk	-	Application Schedule	Non-Snapshot SLP
Tape library	Non-Snapshot SLP	-	Non-Snapshot SLP	Full/Incremental Schedule
Snapshot SLP	AdvancedDisk (must be specified)	Snapshot SLP	Application Schedule	Snapshot SLP on Full/Incremental Schedule
AdvancedDisk	-	Snapshot SLP	Application Schedule	Snapshot SLP
Non-Snapshot SLP	-	-	Non-Snapshot SLP	Non-Snapshot SLP
AdvancedDisk	Non-Snapshot SLP	Snapshot SLP	Non-Snapshot on Application Schedule	Snapshot SLP on Full/Incremental Schedule
Snapshot SLP	Non-Snapshot SLP (must be specified)	Snapshot SLP	Non-Snapshot on Application Schedule	Snapshot SLP on Full/Incremental Schedule

The following are examples of the script- or template-based policy storage and retention behavior for stream-based policy types:

Policy storage	Schedule storage	Application schedule storage	Streamed data retention is derived from:
AdvancedDisk	-	N/A	Application Schedule
Non-Snapshot SLP	AdvancedDisk	N/A	Application Schedule
AdvancedDisk	Non-Snapshot SLP	N/A	Non-Snapshot SLP
Non-Snapshot SLP	-	N/A	Non-Snapshot SLP

Policy storage	Schedule storage	Application schedule storage	Streamed data retention is derived from:
AdvancedDisk	-	Non-Snapshot SLP	Non-Snapshot SLP
Snapshot SLP	-	AdvancedDisk	Application Schedule

Adding clients to a policy

The client list contains a list of the clients on which your scripts are run during an automatic backup or the clients that can send backup requests to the application schedule. A NetBackup client must be in at least one policy but can be in more than one.

NetBackup attempts to run each template in the backup selections list for each client in the client list. If a template is not valid on a particular client, the template is skipped. (For example, if the Oracle home that is specified in the template does not exist on that client.) A policy can contain multiple clients and multiple templates. Only a subset of the templates needs to be valid on each client. If the valid templates are successful, the entire backup is successful.

For a NetBackup for Oracle policy, clients you want to add must have the following items installed or available:

- Oracle
- NetBackup client or server
- The backup shell scripts, unless you use templates

To add clients to a NetBackup for Oracle policy

1. Open the policy you want to edit or create a new policy.

   To access the **Policy** dialog box, double-click the policy name in the **Policies** list in the NetBackup Administration Console.
2. Click the **Clients** tab.
3. Click **New**.
4. Type the name of the client and select the hardware and operating system of the client.
5. Choose one of the following:
   - To add another client, click **Add**.
   - If this client is the last client you want to add, click **OK**.
6. In the **Policy** dialog box, click **OK**.

About adding backup selections to an Oracle policy

The backup selections list in a database policy has a different meaning than for non-database policies. For example, in a Standard or MS-Windows policy, the list contains files and directories to be backed up.

In a database policy, you specify templates or scripts to be run.

Observe the following rules when you use templates or scripts:

- Make sure that the scripts reside on each client in the client list.
- NetBackup installs sample scripts when you install the software; you can modify these scripts for your own use.
- All scripts must be in an authorized location.
  See "Registering authorized locations used by a NetBackup database script-based policy" on page 337.
- If you use NetBackup for Oracle in a NetBackup server cluster, make sure that the scripts reside in a location that is available after a failover.

Note: All scripts must be stored and run locally. One recommendation is that scripts should not be world-writable. Scripts are not allowed to be run from network or remote locations. Any script that is created and saved in the NetBackup `db_ext` (UNIX) or `dbext` (Windows) location needs to be protected during a NetBackup uninstall.

For more information about registering authorized locations and scripts, review the knowledge base article:

http://www.veritas.com/docs/000126002

Add templates or scripts to the backup selections list only if you want to set up a policy for automatic backups. These templates or scripts are run for manual backups and for automatic schedules as specified under the **Schedules** tab. NetBackup runs the templates or scripts in the order that the templates or scripts appear in the backup selections list.

Adding a template to the backup selections list in the NetBackup Administration Console

The following procedure describes how to add a template to the backup selections list in the NetBackup Administration Console.

Note: Be sure to specify the correct template name in the backup selections list to prevent an error or a wrong operation.

To add a template to the backup selections list in the NetBackup Administration Console

1. Open the Policy dialog box.

   To access the Policy dialog box, double-click the policy name in the **Policies** list in the NetBackup Administration Console.
2. Click the **Backup Selections** tab.
3. Click **New**.
4. From the **Template Set** list, choose the template type by operation.
5. From the **Script or Template** list, select a template or type the name of a template.

   Include the `.tpl` extension. Do not include the full path. For example, `weekly_full_backup.tpl`.
6. Click **Add** to add the template to the list.
7. Click **OK**.

Adding a script to the backup selections list in the NetBackup Administration Console

The following procedure describes how to add a script to the backup selections list in the NetBackup Administration Console.

Note: Be sure to specify the correct script name in the backup selections list to prevent an error or a wrong operation.

To add a script to the backup selections list in the NetBackup Administration Console

1. Open the Policy dialog box.

   To access the Policy dialog box, double-click the policy name in the **Policies** list in the NetBackup Administration Console.
2. Click the **Backup Selections** tab.
3. Click **New**.

4 In the **Script or Template** box, type the full path name of a script on the client.

For example:

```
/backup_scripts/db/cold_backup.sh
C:\backup_scripts\db\cold_backup.cmd
```

See "Registering authorized locations used by a NetBackup database script-based policy" on page 337.

5 Click **Add** to add the script to the list.

6 Click **OK**.

About configuring the run-time environment

When the Oracle Intelligent Policy is not used, there are many user configurable variables that can affect the operation of NetBackup for Oracle. Most can be set only in the NetBackup for Oracle Template Wizard or in the RMAN script. A few can be set in multiple places, most notably those that specify the master server, client name, policy, and schedule.

When these variables are configured in multiple places, the following order of precedence is used (the list is ranked highest to lowest):

- RMAN SEND command variables, if specified in the backup script.
- RMAN ENV parameter variables, if specified in the backup script.
  See "About the RMAN SEND command variables" on page 101.
- The template fields for Client name and Schedule name, if specified in the backup template.
- The template fields for Server name and Backup policy name, if specified in the backup template and initiated from the client.
- Environment variables that are inherited from the Oracle listener process startup environment, if RMAN connects to the database using TNS SQL*Net.
- Environment variables that are set in the backup script before `bpdbsbora`or RMAN is started.
- The environment variables that the login or shell inherits.
  See "About the Oracle RMAN environment" on page 99.
- The environment variables that the master server initiation of an automatic schedule sets.
  See "About the environment variables set by NetBackup for Oracle" on page 101.
- On UNIX, the Oracle user's configuration file; `$HOME/bp.conf`.

- The NetBackup configuration:
  - Windows: The `HKEY_LOCAL_MACHINE\Software\Veritas\NetBackup\CurrentVersion\Config` registry keys.
  - UNIX: The `/usr/openv/netbackup/bp.conf` file.
  - Both: The NetBackup GUI settings for server, client name, optional default policy, and optional default schedule.

  See "About the bp.conf file on UNIX systems" on page 104.
- The following defaults apply:
  - A server must be specified, there is no default.
  - The client name defaults to the host name.
  - The master server selects the first policy of type Oracle for the client name.
  - The master server selects the first schedule of type Application Backup (stream-based) or Automatic Full Backup (proxy) from the policy.

Note: The Server name and Backup policy name that is configured within a backup template are only used when initiated from the client.

If the backup is initiated from an automatic schedule on the master server the operation is different. The backup uses the name of the master server and policy that was used to initiate the template. This operation allows a template to be used with multiple policies, with different automatic schedules, and even different master servers.

About the Oracle RMAN environment

The Oracle RMAN program inherits the environment of the program or shell from which it was started. The environment may come from a number of places:

- The global environment or profile for the host
- The profile of the user
- The NetBackup master server
- A non-NetBackup scheduler
- A backup script
- An interactive terminal session

Additionally, once RMAN is started it connects to the database instance and starts the Oracle database server processes that perform the backup. If the connection

is by local logon and password (without a TNS alias), the Oracle database server process is a child of the RMAN program. The Oracle database server process inherits the environment from RMAN. Because the NetBackup for Oracle agent is a shared library loaded into the Oracle database server process it too inherits that environment.

However, if RMAN connects to the database instance by SQL*Net (logon and password@TNSalias) the Oracle database server process is a child of the SQL*Net listener service. This SQL*Net listener service was started previously and independently of RMAN. As a result, the NetBackup for Oracle agent does not inherit the environment from RMAN. Instead, the agent inherits the environment from which the listener service was started

To avoid unexpected results, it is recommended to configure RMAN to always use the `send` command to pass the desired variables and values to NetBackup explicitly. Alternatively the RMAN ENV parameter can be used to make the variables and values available to NetBackup.

Example 1. Use the `send` command to specify the policy and server to use for a database backup. As this example shows, specify the variables in the string in the RMAN script after all channels have been allocated and before the `backup` command.

```
run {
    allocate channel t1 type 'SBT_TAPE';
    allocate channel t2 type 'SBT_TAPE';
    send 'NB_ORA_POLICY=your_policy,NB_ORA_SERV=your_server';
    backup (database format 'bk_%U_%t');
    release channel t1;
    release channel t2;
 }
```

Example 2. Use the `parms` operand to specify the policy and server to use for a database backup. The `parms` operand is set with each `allocate channel` command in the shell script.

```
run {
    allocate channel t1 DEVICE TYPE 'SBT_TAPE'
     PARMS "SBT_LIBRARY=/usr/openv/netbackup/bin/libobk.so,
     ENV=(NB_ORA_POLICY=your_policy,NB_ORA_SERV=your_server)";
    allocate channel t2 DEVICE TYPE 'SBT_TAPE'
     PARMS "SBT_LIBRARY=/usr/openv/netbackup/bin/libobk.so,
     ENV=(NB_ORA_POLICY=your_policy,NB_ORA_SERV=your_server)";
    backup (database format 'bk_%s_%p_%t');
    release channel t1;
```

```
    release channel t2;
}
```

About the environment variables set by NetBackup for Oracle

When an automatic schedule runs, NetBackup sets environment variables for shell scripts to use. These variables are set only if the backup is started from the server, either automatically by the NetBackup scheduler or manually through the administrator interface.

On UNIX and Windows, these variables can be used to perform conditional operations within the backup script.

Table 4-11 shows the variables.

Table 4-11 Variables that NetBackup for Oracle sets

Environment variable	Purpose
NB_ORA_SERV	Name of the NetBackup server that initiated the automatic schedule.
NB_ORA_POLICY	Name of the Oracle policy that contained the automatic schedule.
NB_ORA_CLIENT	Name of the NetBackup client in the policy.
NB_ORA_FULL	Set to 1 for a Full schedule.
NB_ORA_INCR	Set to 1 for a Differential incremental schedule.
NB_ORA_CINC	Set to 1 for a Cumulative incremental schedule.
NB_ORA_PC_SCHED	Name of the automatic schedule.

About the RMAN SEND command variables

The Oracle SEND command and ENV parameter support several options that are used with NetBackup for Oracle. The variables that the SEND command specifies supersede those specified by the ENV parameter. Also, spaces are not permitted when the variables and values are specified.

Table 4-12 describes the options you can set for the RMAN SEND command.

Table 4-12 Options for the SEND command

Option	Purpose
BKUP_IMAGE_PERM	Lets you set the permissions on a backup image at backup time. Possible values are the following: **USER** - set the permissions to 600. Only the original user who backed up the data has access to the backup images. **GROUP** - set the permissions to 660. Anyone from the same group as the original user who backed up the data has access to the backup images. **ANY** - set the permissions to 664. Anyone has access to the backup images. If this keyword is not specified, the permissions default to 660. To specify this keyword, use the send command to set the variable. For example: `SEND 'BKUP_IMAGE_PERM=ANY';` **Note:** The BKUP_IMAGE_PERM option does not affect the permissions for the physical files that are included in an RMAN Proxy copy backup. Ensure the physical file owner, group, and permissions are set correctly before the backup. For more information, review the following document: http://www.veritas.com/docs/TECH213927
NB_ORA_CLIENT	Specifies the name of the Oracle client.
NB_ORA_COPY_NUMBER	Specifies which copy of the backup image to use for the restore.
NB_ORA_METADATA	Enables (YES) and disables (NO) metadata collection for Guided Recovery operations.
NB_ORA_PARENT_JOBID	Enables the parent ID of the job ID to be displayed in the Activity Monitor (only valid if it is a scheduled job).
NB_ORA_PC_RESTORE	Specifies a snapshot rollback restore using a script or RMAN command.

Table 4-12 Options for the SEND command *(continued)*

Option	Purpose
NB_ORA_PC_SCHED	Specifies the NetBackup for the Oracle schedule that NetBackup uses for a proxy copy file-based backup. (This schedule can be Full, Differential Incremental, or Cumulative Incremental backup type). For scheduled backups, this variable is passed from the scheduler. When you create an RMAN template with the NetBackup for Oracle RMAN template generation wizard, this variable is automatically created in the template.
NB_ORA_PC_STREAMS	Specifies the number of backup streams that NetBackup starts simultaneously in each proxy copy session. When a backup is started, NetBackup groups all data files into a specified number of backup streams that are based on the file sizes. NetBackup tries to create streams of equal size. The default value for NB_ORA_PC_STREAMS is 1. Only a user can set this variable. When you create an RMAN template using the NetBackup for Oracle RMAN template generation wizard, it is automatically created in the template. In order for this variable to be automatically created, you must provide a value for the number of parallel streams. This also can be used to specify the number of restore streams that start simultaneously. For more information about restores, refer to: See "About Oracle multistream restore for proxy backup" on page 133.
NB_ORA_POLICY	Specifies the name of the policy to use for the Oracle backup.
NB_ORA_RESTORE_PRIORITY	Specifies the restore priority in NetBackup.
NB_ORA_SCHED	Specifies the name of the Application Backup schedule to use for the Oracle backup.
NB_ORA_SERV	Specifies the name of the NetBackup master server.

Table 4-12 Options for the SEND command *(continued)*

Option	Purpose
NB_ORA_SERVER_READ_TIMEOUT	Configured to instruct the dbclient to lengthen or shorten the timeout on the media server. The media server uses this timeout when it waits for a progress status update from the client during transfer of the backup image. Typically, this setting should not be adjusted. To review setting information and delay examples, refer to the following article: http://www.veritas.com/docs/TECH227741
NB_ORA_DISK_MEDIA_SERVER	Specifies which media server to use when more than one has access to the image to be restored. Supersedes any FORCE_RESTORE_MEDIA_SERVER setting on the master server.
CPF1_POLICY	Policy to be used for duplex copy number 1.
CPF1_SCHED	Application backup schedule for duplex copy number 1.
CPF2_POLICY	Policy to be used for duplex copy number 2.
CPF2_SCHED	Application backup schedule for duplex copy number 2.
CPF3_POLICY	Policy to be used for duplex copy number 3.
CPF3_SCHED	Application backup schedule for duplex copy number 3.
CPF4_POLICY	Policy to be used for duplex copy number 4.
CPF4_SCHED	Application backup schedule for duplex copy number 4.

For more information, see the NetBackup System Administrator's Guide, Volume I.

About the bp.conf file on UNIX systems

A NetBackup for Oracle user can create a bp.conf file in the Oracle user's home directory on the NetBackup for Oracle client host. When a NetBackup for Oracle operation is started, the user's bp.conf file is searched before the master configuration file (/usr/openv/netbackup/bp.conf). Any option that is found at the user level overrides the same option's setting at the master level.

Table 4-13 shows the options you can set in the user's bp.conf file.

Table 4-13 Options for the user bp.conf file

Option	Purpose
BPBACKUP_POLICY	This option specifies the name of the policy to use for the backup.
BPBACKUP_SCHED	This option specifies the name of the Application Backup type of schedule to use for the backup.
CLIENT_NAME	This option specifies the name of the Oracle client. This name is especially useful for a redirected restore operation.
CLIENT_READ_TIMEOUT	Use this option to increase the number of seconds that the Oracle client initially waits for a response from the NetBackup server. The default is the greater of 900 or CLIENT_READ_TIMEOUT.
ORACLE_METADATA	Set to YES to enable metadata collection for Guided Recovery.
SERVER	This option specifies the name of the NetBackup master server. There can only be one SERVER option in the user bp.conf file.
VERBOSE	This option causes NetBackup to include more information in its debug logs.

For more information, see the NetBackup System Administrator's Guide, Volume I.

The following shows example bp.conf entries for an Oracle user:

```
SERVER=jupiter
CLIENT_READ_TIMEOUT=900
VERBOSE=1
```

About creating templates and shell scripts

RMAN templates and scripts contain the commands that run NetBackup RMAN backup and recovery jobs. Templates and scripts must be created before NetBackup can perform scheduled backups. These are the template files or shell scripts that are specified in policy configuration on the NetBackup server.

Starting the NetBackup Backup, Archive, and Restore interface

To start the NetBackup Backup, Archive, and Restore interface

1. Use operating system methods to log into the client upon which NetBackup for Oracle is installed.
2. Make sure that the Oracle database is in the `mount` or `open` state.
3. Start the NetBackup Backup, Archive, and Restore interface on the NetBackup client.
   - From the Windows Start menu, choose **All Programs > Veritas NetBackup > Backup, Archive, and Restore**.
   - On UNIX, run the following command:

     ```
     /usr/openv/java/jbpSA &
     ```
4. Provide the information that the logon dialog box requests.

   On Windows, you do not have to logon as the administrator or as the Oracle administrator.

   On UNIX systems, how you log onto NetBackup depends on how your Oracle authentication is configured:

   - OS authentication for Oracle:
     Log on to NetBackup as an Oracle DBA UNIX account that includes `sysdba` privileges.
   - Oracle authentication by password file:
     Log on to NetBackup using any UNIX account, including root. You need to provide additional Oracle logon information later in the backup process.

   For the host name, type the name of the client upon which the Oracle database and NetBackup for Oracle reside. Type your user name and password in the other fields. You can log on as a regular user.

RMAN templates and shell scripts

You can use templates or shell scripts with the NetBackup for Oracle agent.

The NetBackup for Oracle backup wizard creates backup templates. You can launch this wizard from the NetBackup Backup, Archive, and Restore interface.

See "Creating RMAN templates using the NetBackup for Oracle RMAN template generation wizard" on page 107.

The NetBackup for Oracle backup wizard does not support all of the RMAN commands and options that Oracle provides. Write a shell script if a template does not provide all the functionality you require.

Shell scripts that the user writes must conform to RMAN and operating system shell syntax. Sample backup and recovery shell scripts are installed on the client with the NetBackup for Oracle agent. Modify these scripts to meet your individual requirements.

See "About creating RMAN scripts manually" on page 109.

NetBackup for Oracle also provides a utility, `bpdbsbora`, that can generate a shell script from a backup wizard template. A user can create a template with the wizard and then generate a shell script from the template. The script should be reviewed to make sure the `TARGET_CONNECT_STR` has the correct credentials before execution.

See "Creating an RMAN script from a template" on page 109.

Creating RMAN templates using the NetBackup for Oracle RMAN template generation wizard

The NetBackup for Oracle backup wizard stores information about desired RMAN backup operations. The wizard uses the information to create a template that you can run immediately. Or you can save in a NetBackup location on the master server for later use. Before you can save on the master server, the client must be in a policy or have images in the NetBackup catalog.

For more information on backup strategies and RMAN functionality, see your Oracle documentation.

If Oracle is installed on a Windows system, the Backup, Archive, and Restore interface on the client displays an Oracle node in the left pane. From the client, expand the Oracle node in the left pane to view an Oracle database instance hierarchy. Select a node in the left pane to view details in the right pane.

If your current logon does not have Oracle SYSDBA or SYSBACKUP privileges, the system prompts you to enter your Oracle database logon information. You need to enter your user name and password with SYSDBA or SYSBACKUP privileges to continue. Optionally, you can also enter your net service name (TNS alias).

To create RMAN templates using the NetBackup for Oracle RMAN template generation wizard

1. Log on to NetBackup for Oracle client and start the NetBackup Backup, Archive, and Restore interface.

   See "Starting the NetBackup Backup, Archive, and Restore interface" on page 106.

2. In the Backup, Archive, and Restore interface, expand an Oracle database instance and select the database object(s) (data files, tablespaces, archived redo logs) to back up.

   When you select the Oracle database instance, you back up the whole database using RMAN.

3. Choose **Actions > Backup**.

   The NetBackup for Oracle RMAN template generation wizard displays the following screens for you to enter information about the backup operation you want to perform:

   - Welcome (UNIX only)
   - Target Database Logon Credentials (SYSDBA only)
   - Recovery Catalog Logon Credentials
   - Archived redo logs
   - Configuration Options
   - Backup Options
   - Database State
   - NetBackup for Oracle Configuration Variables
   - Backup Limits

   If you need an explanation of any of the fields on the wizard screens or more details, click **Help** on the wizard screen.

4. After you complete the wizard, the Template Summary screen displays the summary of the backup template:

   You can run the template immediately after the wizard finishes, save the template to the master server, or both. Select **Perform backup immediately** and or **Save Template** then click **Finish**.

   See "About storing templates" on page 112.

See "About using Templates and Oracle Intelligent Policy (OIP) with RAC" on page 240.

Creating an RMAN script from a template

You can use the `bpdbsbora` command to create a script from a backup template. This command generates RMAN shell scripts from the templates that the backup wizard creates.

At the command prompt, type this command in the following format:

```
bpdbsbora -backup -g script_file -t templ_name.tpl -S server_name
```

Where:

`-backup`	Specifies the template type.
`-g script_file`	Specifies the name of the file to which you want `bpdbsbora` to write the script. Enclose *script_file* in quotation marks if it contains blanks. This option cannot be used with the `-r` (run) option.
`-t templ_name.tpl`	Specifies the name of the template that you want to use as the basis for the script. Make sure that the template exists. `bpdbsbora` retrieves backup templates from a known location on the master server, so specify only the template file name.
`-S server_name`	Specifies the master server upon which the template resides. When you specify the `bpdbsbora` command, it retrieves backup templates from the specified master server.

See "Registering authorized locations used by a NetBackup database script-based policy" on page 337.

About creating RMAN scripts manually

You can create RMAN scripts manually instead of using the template wizard. When you create a script, you need to specify the type of backup and assign a name to the output file. Keep in mind the following considerations:

Backup type

RMAN supports the following different types of backups (In the examples, *n* must be 1 or higher):

- **BACKUP FULL**
- **BACKUP INCREMNTAL LEVEL 0** (Full backup base for incremental backups)
- **BACKUP INCREMENTAL LEVEL** *n* (Differential incremental backup)
- **BACKUP INCREMENTAL LEVEL** *n* **CUMULATIVE** (Cumulative incremental backup)

When generating a data file backup set, you can make either an incremental backup or a full backup. Both a full backup and an incremental level 0 perform a complete backup of the data file. However, an incremental level 0 backup can be used as the base for incremental level *n* and or incremental level *n* cumulative backups.

File names

Observe the following with regard to file names:

- Each output file must have a unique name. Use the `%U` format specifier to satisfy this restriction. `%U` is equivalent to `%u_%p_%c`, and it guarantees the uniqueness of the backup set name in all circumstances.
- Put `%t` at the end of the backup file name format. NetBackup uses the timestamp as part of its search criteria for catalog images. Without this timestamp, performance might degrade as the NetBackup catalog grows.
- Ensure that the format that is specified for all RMAN backup piece names does not contain any space characters.

See "Registering authorized locations used by a NetBackup database script-based policy" on page 337.

About the NetBackup for Oracle sample scripts

When you install NetBackup for Oracle, there are some sample scripts that can be used as examples. You must modify any sample script you use to work within your environment. The NetBackup installation writes example scripts to the following directory:

Windows:

```
install_path\NetBackup\dbext\Oracle\samples\rman
```

UNIX:

```
/usr/openv/netbackup/ext/db_ext/oracle/samples/rman
```

The Oracle example scripts are as follows:

Windows:

```
cold_duplex_cluster_database_backup_full.cmd
cold_cluster_database_backup.cmd
cold_database_backup.cmd
cold_pdb_backup.cmd
cluster_database_restore.cmd
complete_database_restore.cmd
complete_pdb_restore.cmd
hot_database_tablespace_backup_proxy.cmd
hot_pdb_backup.cmd
hot_database_backup.cmd
hot_pdb_tablespace_backup_proxy.cmd
pit_database_restore.cmd
pit_cluster_database_restore.cmd
pit_pdb_restore.cmd
```

UNIX:

```
cold_database_backup.sh
cold_pdb_backup.sh
hot_database_backup.sh
hot_database_tablespace_backup_proxy.sh
hot_pdb_backup.sh
hot_pdb_tablespace_backup_proxy.sh
complete_database_restore.sh
complete_pdb_restore.sh
pit_database_restore.sh
pit_pdb_restore.sh
```

Using the NetBackup for Oracle sample scripts

The following procedure describes how to use the sample scripts to manually create your own script.

To use sample scripts provided by NetBackup for Oracle

1. Copy the example scripts to a different directory on your client. Oracle scripts can be located anywhere on the client.
2. Modify each script for your environment.
3. On UNIX, make sure the `su` command logs into the correct user.

   If you do not include an `su - user` (*user* is Oracle administrator account) in your Oracle scripts, they do not run with the proper permissions and environment variables. Problems with your database backups and restores can arise.

About the set duplex command

RMAN provides an API that lets you make up to four backup sets simultaneously, each an exact duplicate of the others. Using NetBackup, for example, you can back up each copy to a different tape to protect against disaster, media damage, or human error. Use the `set duplex` and the `send` commands to take advantage of this feature.

The `set duplex` command specifies the number of copies of each backup piece to create. The `set duplex` command affects all channels that are allocated after you issue the command. It remains in effect until explicitly disabled or changed during the session. You cannot issue the `set duplex` command after allocating a channel.

The command syntax is:

```
set duplex = {ON | OFF | 1 | 2 | 3 | 4}
```

By default, duplex is `OFF` (a single backup set is produced). If you specify `ON`, it produces two identical backup sets.

Note that you must enable the `BACKUP_TAPE_IO_SLAVES` initialization parameter to perform duplexed backups. RMAN configures all media as needed for the number of backup copies you request. For more information on `BACKUP_TAPE_IO_SLAVES`, see your Oracle documentation.

Use the `send` command to specify the policy and schedule to use with each backup. Because NetBackup uses the policy or schedule to determine what media to use, this information is required for each copy, or an error occurs.

The command syntax is as follows:

```
send 'keyword=value [, keyword=value,...]';
```

The keywords that are used to specify a policy are `CPF1_POLICY`, `CPF2_POLICY`, `CPF3_POLICY`, and `CPF4_POLICY`, which specify the backup policy for duplexed file 1 through duplexed file 4.

The keywords that are used to specify a schedule are `CPF1_SCHED`, `CPF2_SCHED`, `CPF3_SCHED`, and `CPF4_SCHED`, which specify the Application Backup schedule for duplexed file 1 through duplexed file 4.

About storing templates

NetBackup for Oracle saves backup templates on the master server and restore templates on the client. A backup template is retrieved from the master server as part of a backup (server-directed, scheduled, or user-directed) and is run on the client. Backup templates are associated with a policy by specifying its name in the

policy backup selections list. Because backup templates are stored on the server in a known location, server-directed and scheduled backups use the same copy of the template. The server-directed and scheduled backups use the same copy of the template for each client in the policy client list.

When templates are saved, if the template does not end with `'.tpl'`, the extension is appended to the file name before the template is saved.

Before you run a template on a NetBackup for Oracle client, NetBackup verifies the validity of the template for that client. The verification is done by checking the Oracle installation information that is stored in that template. Only valid templates are run on each client.

The NetBackup for Oracle Recovery saves a template to a user-specified location on the client. The location that is specified should include a fully qualified path to a directory where the user has write access.

Templates store the encrypted passwords that are decrypted at run-time.

About storing shell scripts

Shell scripts must reside on the NetBackup client. Backup shell scripts are associated with a policy by specifying the file name (including path) in the policy backup selections list. For server-directed or scheduled backups, each client in the policy's client list must have a copy of the script with the same name in the same location.

See “About adding backup selections to an Oracle policy” on page 96.

The backup and the recovery process sometimes require passwords for Oracle database access or system user accounts. Because a shell interprets the shell scripts, store the passwords in clear text.

See “Registering authorized locations used by a NetBackup database script-based policy” on page 337.

Configuring the logon account for the NetBackup Client Service for NetBackup for Oracle

This topic applies to those that are running NetBackup for Oracle on a Windows platform.

Because the NetBackup Client Service is started by default under the `SYSTEM` account, you must also give special attention to database user authentication. The `SYSTEM` account does not have permission to connect to the target database if you use OS authentication instead of passwords.

If you use OS authentication, run the NetBackup client service under an account that has SYSDBA privileges.

For more information on OS authentication, see your Oracle documentation.

Note: In a cluster environment, perform the steps on each database node in the cluster. For an off-host backup, perform the steps on the alternate client.

To configure the logon account for the NetBackup Client Service for NetBackup for Oracle

1. Open the Windows Services application.
2. Double-click the **NetBackup Client Service** entry.
3. Click the **Log On** tab.
4. Type the account name with SYSDBA privileges.
5. Type the password.
6. Click **OK**.
7. Stop and start the NetBackup Client Service.
8. Close the Services control panel application.

Testing configuration settings for NetBackup for Oracle

After you configure the servers and clients in your environment, test the configuration settings. Perform a manual backup (or backups) with the automatic backup schedules you created. A description of status codes and other troubleshooting information is available.

See the NetBackup Status Codes Reference Guide.

See the NetBackup Troubleshooting Guide.

To test the configuration settings

1. Log onto the master server as administrator (Windows) or root (UNIX).
2. Start the NetBackup Administration Console.
3. In the left pane, click **Policies**.
4. Click the policy you want to test.

5 Select **Actions > Manual Backup**.

The **Schedules** pane contains the name of possible schedule or schedules that are configured for the policy that you want to test.

For an Oracle Intelligent Policy, an **Instances** pane contains a list of instances that are configured for the policy. Select one or more of the instances to start the backup.

For a script- or template-based policy, the **Clients** pane contains the name of the client or clients that are listed in the policy. Select one or more of the clients to start the backup.

6 Follow the directions in the **Manual Backup** dialog box. Then click **OK**.

7 To check the status of the backup, click **Activity Monitor** in the **NetBackup Administration Console**.

The Activity Monitor and the script output indicate the status of the backup operation.

Chapter 5

Performing backups and restores of Oracle

This chapter includes the following topics:

Overview of using NetBackup for Oracle

The NetBackup graphical user interfaces and command line interfaces let you perform Oracle backup and recovery operations using Oracle RMAN utilities. You

can also use the Oracle Enterprise Manager to perform Oracle backup and recovery operations. The Oracle RMAN command line interface is also used to maintain and query the RMAN repository.

Maintaining the RMAN repository

The RMAN repository is the collection of metadata about your target databases that RMAN uses to conduct its backup, recovery, and maintenance operations. You can either create a recovery catalog in which to store this information or let RMAN store it exclusively in the target database control file. Although RMAN can conduct all major backup and recovery operations using only the control file, some RMAN commands function only when you use a recovery catalog.

Table 5-1 shows the tasks that are required to maintain the RMAN repository and a subset of the repository maintenance commands that perform the tasks. Some of these commands might not be available with all versions of RMAN.

Table 5-1 Tasks and commands

Task	Commands that perform the task
Register a database with the recovery catalog	Before using RMAN with a recovery catalog, register the target database in the recovery catalog. To register, start and mount the target database but do not open it. At the RMAN prompt, issue a `register database` command.
Reset the incarnation in the recovery catalog	The `reset database` command directs RMAN to create a new database incarnation record in the recovery catalog.

Table 5-1 Tasks and commands *(continued)*

Task	Commands that perform the task

Crosscheck the information in the RMAN repository	Because NetBackup can expire images independently from Oracle, the RMAN repository can contain outdated information. Run an RMAN crosscheck to ensure that data in the recovery catalog or control file is in sync with data in the backup image catalog. The crosscheck queries NetBackup for the existence of each backup piece and then marks it as available or expired in the RMAN repository. Use one of the following commands to check the specified files. You need to run separate commands to delete images or repository records.
	■ The `change...crosscheck` command queries NetBackup to determine if a backup piece is available. If not, RMAN marks the backup piece as expired. If it was expired but is now available, RMAN marks the backup piece as available. The command syntax is as follows:
	`change backuppiece {primary_keylist | filename_list | tag} crosscheck;`
	`change backupset {primary_keylist} crosscheck;`
	■ The `crosscheck backupset` command operates on available and expired backup pieces. RMAN updates their status with the result (available or expired).
	■ To crosscheck a database, start RMAN and connect to the target database and to the recovery catalog (if used). At the `rman` command prompt, enter the following:
	`allocate channel for maintenance type 'SBT_TAPE';`
	`crosscheck backupset of database;`
	The length of time to perform an RMAN crosscheck depends on several factors:
	■ Number of RMAN backup pieces being crosschecked.
	■ Number of RMAN backup pieces past their NetBackup retention period when NetBackup expires them, not RMAN.
	■ Format of the RMAN backup piece name and if the Veritas recommended _%t appears at the end of the format statement.
	■ Number of Oracle clients.
	■ Number of NetBackup policies of any kind.
	■ Length of time NetBackup retains backups and the number of backup images for the client in the NetBackup catalog.
	■ Scheduling time and the length of time between RMAN catalog maintenance operations.
	■ Speed and accuracy of host name and reverse host name resolution on the NetBackup master server.
	■ Number and complexity of the operations that the NetBackup master server performs during each crosscheck request.
	■ Normal performance.

Table 5-1 Tasks and commands *(continued)*

Task	Commands that perform the task

Crosscheck using the Copilot share	If files on a Copilot share are deleted outside of RMAN, the subsequent incremental merge backups that are done to the share fail. An RMAN crosscheck of the share must be done before the next backup to prevent more failures. This version of the RMAN crosscheck is slightly different from the other crosscheck examples because of the need to specify `type disk` instead of `type SBT_TAPE`. When running the RMAN crosscheck, the default is the *NetBackup_policyname*. However, if the **Datafile copy tag** is changed in the **Oracle** tab, then that tag name must be used in place of *NetBackup_policyname*. An example of the command syntax follows (using the default *NetBackup_policyname*):
	
	`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;`
	`}`

Delete obsolete backups	The `DELETE OBSOLETE` command deletes the backups that are no longer needed to satisfy specified recoverability requirements. You can delete obsolete pieces according to the configured default retention policy, or another retention policy that a `DELETE OBSOLETE` option specifies. As with other forms of the `DELETE` command, the deleted files are removed from the backup media (i.e. expired from NetBackup). Then they are deleted from the recovery catalog, and marked as `DELETED` in the control file.
	
	If you specify the `DELETE OBSOLETE` command with no arguments, then RMAN deletes all the obsolete backups that the currently configured retention policy defines. For example:
	
	`Allocate channel for maintenance type 'SBT_TAPE';`
	`DELETE OBSOLETE;`
	
	You can also use the `REDUNDANCY` or `RECOVERY WINDOW` clauses with `DELETE` to delete the backups that are obsolete under a specific retention policy instead of the configured default:
	
	`DELETE OBSOLETE REDUNDANCY = 3;`
	`DELETE OBSOLETE RECOVERY WINDOW OR 7 DAYS;`

Table 5-1 Tasks and commands *(continued)*

Task	Commands that perform the task

Delete expired backups	The `delete expired backupset` command operates only on the expired backup pieces that are found in the recovery catalog. RMAN removes them from the recovery catalog and also from the backup media (i.e. expires them from NetBackup).
	
	To delete expired backup sets of a database from the recovery catalog, start RMAN and connect to the target and the recovery catalog databases. At the RMAN command prompt, type the following commands:
	
	`allocate channel for maintenance type 'SBT_TAPE';`
	`delete expired backupset of database;`
	
	The `crosscheck` and `delete backupset` commands restrict the list of objects to only those that are operated on. The restrictions are placed on the specified Oracle device type (disk or SBT tape), object type (archived logs or database files), and date range.

Resynchronize the recovery catalog	RMAN compares the recovery catalog to either the current control file of the target database or a backup control file. It subsequently updates the catalog with the missing information or changed information. If you are running in `ARCHIVELOG` mode, do the following: Resynchronize the recovery catalog regularly because the recovery catalog is not updated automatically when a log switch occurs or when a redo log is archived. You must also resynchronize the recovery catalog after making any change to the physical structure of the target database. As with log archive operations, the recovery catalog is not automatically updated when a physical schema change is made. The RMAN `backup`, `copy`, `restore`, and `switch` commands update the recovery catalog automatically when the target database control file is available. The recovery catalog database is available when one of these commands is executed. If the recovery catalog is unavailable when you issue `backup` or `copy` commands, you should resynchronize it manually. To resynchronize the recovery catalog, start RMAN and issue the `resync catalog` command.

Table 5-1 Tasks and commands *(continued)*

Task	Commands that perform the task
Change the availability of a backup set or file copy	Periodically, you might need to notify RMAN that the status of a backup set, backup piece, data file copy, or archived redo log has changed. The RMAN `change` command enables you to make a variety of useful record changes. The `change ... uncatalog` command removes references to a backup piece, data file copy, or archive log from the recovery catalog. This command works only with a recovery catalog. The `change ... delete` command removes references to a backup piece, data file copy, or archive log from the control file and recovery catalog. It physically deletes the file. This command works with or without a recovery catalog. The `change ... crosscheck` command removes references to a backup piece, data file copy, or archive log from the control file and recovery catalog. The references are removed when that file no longer exists. This command works with or without a recovery catalog. The `change ... unavailable` command marks a backup piece, data file copy, or archive log as unavailable. This command works only with a recovery catalog.
Validate the restore of backups	A restore validation retrieves the backup pieces from storage (NetBackup) and checks that the retrieved pieces are intact. But the restore validation discards the backup pieces without saving the contents into the database. Use `restore ... validate` when you want RMAN to choose the backups to test. Use `validate backupset` when you want to specify the backup sets to test.

Querying the RMAN repository

RMAN lets you generate a number of reports relevant for backup and recovery using the `report` and `list` commands. The `list` command lists the contents of the recovery catalog or control file, and the `report` command performs a more detailed analysis.

Use the `report` and `list` commands to determine what you have backed up and what you need to back up. The information is available whether or not you use a recovery catalog.

You can use the `report` command to answer many different questions.

Some examples are as follows:

- Which files need a backup?
- Which files have not had been backed up in awhile?
- Which files are not recoverable due to unrecoverable operations?
- Which backup files can be deleted?

- What was the physical schema of the database at some previous point in time?

The `list` command queries the recovery catalog and control file and produces a listing of its contents. The primary purpose of the `list` command is to determine the backups that are available.

You can list the following information:

- Backup sets containing a backup of a specified list of data files.
- Backup sets containing a backup of any data file that is a member of a specified list of tablespaces.
- All backup sets or copies of all data files in the database.
- Backup sets containing a backup of any archive logs with a specified name or within a specified range.
- Incarnations of a specified database or of all databases that are known to the recovery catalog.

For more information on querying the RMAN repository, see your Oracle documentation.

About NetBackup for Oracle backups

You can perform different types of backups using NetBackup. Backups can be run automatically by using the schedules that you determine, or you can run a backup manually. The following table describes these methods of running a backup.

Automatic backups	When the NetBackup scheduler invokes a schedule for an automatic backup, the NetBackup for Oracle backup templates or shell scripts run as follows: ■ In the same order as they appear in the file list ■ On all clients in the client list The NetBackup for Oracle backup templates or shell scripts start the database backup by running the `rman` command. When the backup is started through NetBackup, RMAN performs error checking. The `rman` command generates an error if it considers a command invalid, but it allows any of the commands it typically considers valid to proceed. When you specify the wrong script file name, you can start an unintended operation.

Manual backups	You can use the NetBackup server software to manually run an automatic backup schedule for the Oracle policy. For more information, see the NetBackup Administrator's Guide, Volume I. See "Testing configuration settings for NetBackup for Oracle" on page 114.

Running NetBackup for Oracle templates

The Oracle template administration interface is available in the NetBackup Backup, Archive, and Restore interface.

Use this dialog to run, edit, delete, rename, and view existing backup templates. These are the templates created by the NetBackup for Oracle RMAN template generation wizard. Before you can run, edit, delete, or rename templates on the master server, the client must exist in a policy or in the NetBackup image catalog.

See "Creating RMAN templates using the NetBackup for Oracle RMAN template generation wizard" on page 107.

To use Oracle template administration

1. In the Backup, Archive, and Restore interface, choose Actions > **Administer Database Templates > Oracle**.

   The **Select Template** list shows the names and descriptions of the RMAN backup templates that are stored on the current master server.

2. Select the name of the backup template you want to run.

3. Click **Run**.

   You can use the View Status tool to see the status of the backup. Click Actions > **View Status**.

   The Oracle template administration window provides the following functions:

Run	Runs the selected template.
Edit	Changes the contents of an existing template. The selected backup template is loaded into the NetBackup for Oracle RMAN template generation wizard.
Delete	Removes the selected template. On Windows, you must be a system administrator or the template creator to delete a template. On UNIX, you must be the root user or the template creator to delete a template.
Rename	Changes the name of the selected template. On Windows, you must be a system administrator or the template creator to rename a template. On UNIX, you must be the root user or the template creator to rename a template.
View	Displays a summary of the selected template.

Using bpdbsbora to run a backup template

The `bpdbsbora` command lets you run a backup template that the NetBackup for Oracle RMAN template generation wizard creates.

At the command prompt, type this command using the following options:

```
bpdbsbora -backup -r -t templ_name.tpl [-S srvr_name] [-L prog_file]
```

Where:

`-backup`	Specifies the template type.
`-r`	Runs the template.
`-t` *`templ_name`*`.tpl`	Specifies the file name of the template that you want to use. `bpdbsbora` retrieves backup templates from a known location on the master server, so specify only the template file name.
`-S` *`server_name`*	Optional. Specifies the master server upon which the templates reside. When it is specified, the `bpdbsbora` command retrieves backup templates from the specified master server.
`-L` *`prog_file`*	Optional. Specifies a run-time progress log. Enclose *prog_file* in quotation marks (" ") if it contains space characters.

For example:

```
bpdbsbora -backup -r -t ORCLMonfull.tpl -S my_mast -L my_prog_log
```

Running the NetBackup for Oracle shell script

When you run a NetBackup for Oracle shell script on a client to initiate a backup from the command prompt, specify the full path name to the file that contains the script. For example:

Windows:

```
install_path\oracle\scripts\db_full_backup.cmd
```

UNIX:

```
/oracle/scripts/db_full_backup.sh
```

The shell starts the database backup by running the Oracle shell script. The Oracle shell script contains commands to run `rman`.

The NetBackup installation script installs sample scripts in the following location:

Windows:

```
install_path\NetBackup\dbext\oracle\samples\rman
```

UNIX:

```
/usr/openv/netbackup/ext/db_ext/oracle/samples/rman
```

Running RMAN

As an Oracle user, you can run the `rman` command from the command prompt with the RMAN command file as a parameter. This topic describes how to set the master server to `hag` and the Oracle policy to `obk` before you start the backup.

On Windows, RMAN functionality runs as a service, so use the `send` operand to set up the run-time environment. To start a backup using the `rman` command from the command prompt, type the following:

```
# send "'NB_ORA_POLICY=obk,NB_ORA_SERV=hag'" cmdfile    \
"install_path\oracle\scripts\db_full_backup.rcv"
```

On UNIX, type the following at the command prompt:

```
# rman target 'internal/oracle@ORCL' rcvcat 'rman/rman@RCAT'
# send "'NB_ORA_POLICY=obk,NB_ORA_SERV=hag'" cmdfile    \
'/oracle/scripts/db_full_backup.rcv"
```

If you intend to connect to a database using a TNS alias, the RMAN `send` command specifies the environment variables. The example sets the master server to `hag` and the Oracle policy to `obk` before you start the backup.

See "About the bp.conf file on UNIX systems" on page 104.

Note: To run script files for database operations other than backups or restores, Veritas recommends that you run the `rman` command directly rather than using NetBackup.

For `rman` command script syntax and examples, see your Oracle documentation.

Browsing backups using the bplist command

You can use the `bplist` command to browse Oracle backups. The command returns a list of backup file names.

Before using this command, log onto the master server or the client:

- On Windows, log on as administrator to the master server and to the client with the appropriate *altnames* entry.
- On UNIX, log on as root to the master server and to the client with the appropriate *altnames* entry.

The following example uses the command to search all Oracle backups for a client named `jupiter`:

```
# bplist -C jupiter -t 4 -R /

/exb_n2bm5bco_1_1392342936
/exb_mabm02ko_1_1392170136
/exb_lqbltds6_1_1392083334
```

The `-t 4` on this command specifies the Oracle backups. The `-R` specifies the default number (999) of directory levels to search.

For more information on the `bplist` command, see the NetBackup Commands Reference Guide.

You can also use the RMAN `report` and `list` commands to browse Oracle backups.

See "Querying the RMAN repository" on page 121.

Managing expired backup images

NetBackup and Oracle each maintain a repository of RMAN-initiated backup image information. The retention setting in the Application Backup schedule for RMAN stream-based backups determines the NetBackup image retention. But for RMAN proxy backups and OIP backups, the retention setting on the Automatic Backup schedule determines retention of the NetBackup image.

To manage expired backup images from the NetBackup repository, access the Retention setting of the Application backup schedule. Specify the length of time before NetBackup expires a backup image.

See "About schedule properties " on page 91.

You can also manage the expired backup images from the Oracle repository. This method sets the backup retention as an RMAN attribute, rather than a NetBackup attribute. RMAN deletes the obsolete but not the unexpired backups from NetBackup. The following items are also part of this process:

- Set the NetBackup backup retention for Oracle backups to be either infinite or significantly longer than the RMAN retention.
- Set the RMAN retention to the number or duration to keep the backup sets in the RMAN catalog. If no RMAN catalog exists, then use SQL to set an appropriate value for "control_file_record_keep_time". The minimum appropriate time is the catalog backup retention time plus the maximum time between catalog maintenance operations.
- On a regular basis, run the RMAN `delete obsolete` command to expire obsolete images from the RMAN catalog, the control file, and from NetBackup.
- If a cross-check of the catalog is required, perform the cross-check after RAMN deletes the obsolete backups.

- Stagger the initiation of RMAN catalog maintenance functions. Staggering is done to limit the number of concurrent checks or deletion requests that RMAN makes of the NetBackup master server.
- Perform the RMAN catalog maintenance functions on a more frequent basis to limit the number of NetBackup catalog requests in a single session.
- Ensure that the format that is specified for all RMAN backup piece names (except for autobackups of the control file) ends with `_%t`.
- Ensure that the format that is specified for all RMAN backup piece names does not contain any space characters.
- Avoid the creation of excessive, small backup pieces of database files or archive logs.

You can manually remove references to backup images from the Oracle RMAN repository. Use RMAN repository maintenance commands to remove references to backup files. You can use these commands to delete backup image information from both the Oracle RMAN repository and the NetBackup repository.

More information is available on the RMAN repository maintenance commands.

See "Maintaining the RMAN repository" on page 117.

When a request is issued to delete a backup file from the RMAN repository, RMAN sends the request to NetBackup. The request tells NetBackup to delete the corresponding image from the NetBackup repository, regardless of the retention level.

About NetBackup for Oracle restores

Make sure that a backup has completed successfully before you attempt a restore. An error occurs if a backup history does not exist.

NetBackup for Oracle includes a recovery wizard that solicits information from the user about the desired RMAN restore and recovery operations. The wizard uses the information to create a template.

The recovery wizard saves a recovery template locally in a user-specified location on the NetBackup client. Recovery templates are not stored on the master server because recovery is always user directed, not scheduled. Typically, you run the recovery template immediately and then delete it.

The recovery process sometimes requires passwords for Oracle database access and system user accounts. Templates store the encrypted passwords that are decrypted at run-time.

Because recovery can be a complex process, it might be necessary to perform manual steps as part of the operation. For more information, see your Oracle documentation.

The restore browser is used to display database objects. A hierarchical display is provided where objects can be selected for recovery. The top database node expands to show all of the installed databases.

On Windows, Oracle services are searched for in the Registry to get the names and location of each database.

On UNIX, the `oratab` file is read to get the names and location of each database.

The objects (tablespaces, data files, PDBs, and users) that make up an Oracle database are displayed by expanding an individual database node. This information is gathered from various database tables and views. Since you must be connected to the database before you can access its tables or views, logon criteria must be provided. When a user selects or expands a database node the wizard first tries to logon to the database using OS authentication. If the authentication fails the user is solicited for a user name and password. Optionally, the user is prompted for the `Net Service Name` if the connection is through SQL-Net, which is then used to log on to the database. This user must have SYSDBA or SYSBACKUP privileges since the logon credentials are also used to perform the RMAN restore. The logon fails if the database is not in a mount state or an open state.

On Windows, NetBackup uses an API to browse the database. Logging is recorded in the `nbwin` folder.

On UNIX, the GUI uses the `bpubsora` utility to access and query the database. If a problem occurs when NetBackup attempts to connect or browse a database, run this utility from the command line to debug the issue.

The recovery wizard has several limitations:

- The database is displayed only in its current state. If objects have been deleted from the database since the last backup, these objects do not appear among the objects you can select for restore. To restore the objects that have been deleted, you need to restore the entire database to a point in time before the objects were deleted.
- Data is restored to the original location. The wizard does not provide a way for the user to specify alternate file names.
- The wizard does not restore control files.

Starting the recovery wizard

This topic describes how to start the recovery wizard.

To start the recovery wizard

1. Start the Backup, Archive, and Restore interface.
2. (Conditional) Change the policy type.

   Perform this step if the Oracle node is not visible.

   From the File menu (Windows) or Actions menu (UNIX), choose **Specify NetBackup Machines and Policy Type**.
3. Select files for Restore:
   - On Windows, click **Select for Restore**.
   - On UNIX, click the **Restore Files** tab.
4. Expand the Oracle node in the left pane to view an Oracle database instance hierarchy.
5. Select a node in the left pane to view details in the right pane.

Using the recovery wizard

When you are ready to perform a recovery, follow these steps to create and run a template with the recovery wizard.

To use the recovery wizard

1. Open the Backup, Archive, and Restore interface.
2. Select the Restore operation:
   - On Windows, click **Select for Restore**
   - On UNIX, click on the **Restore Files** tab. In the **Restore Type** list, select **Normal Backups**.
3. In the left pane, select the Oracle database instance.
4. In the right pane, select the database object(s) (databases, tablespaces, data files, and users) you want to recover.

   If you select the Oracle database instance, the wizard recovers the entire database using RMAN.
5. Click Actions > **Restore**.

   Enter information about the recovery operation you want to perform in the screens that the NetBackup for Oracle recovery wizard displays.

   The screens are as follows:
   - Welcome
   - Target Database Logon Credentials

- Recovery Catalog Logon Credentials
- Recovery Options
- Restore Options
- Recover Limits
- Database State

If you need an explanation of any of the fields on the wizard screens, click **Help** on the wizard screen.

6 When you have completed the wizard, the Selection Summary screen displays the summary of the recovery template. Review this summary. You can choose to run the template immediately after the wizard finishes or save the template locally, or both.

If you need an explanation of any of the fields on the wizard panels, click **Help** on the wizard panel.

7 Click **Finish** to run, to save, or to run and save the recovery template.

Using bpdbsbora to run a recovery template

The `bpdbsbora` command lets you run a recovery template that the NetBackup Recovery Wizard creates.

At the command prompt, type this command and the following options:

```
bpdbsbora -restore -r -t [/path/]templ_name.tpl [-L progress_file]
```

Where:

`-restore`	Specifies the template type.
`-r`	Runs the template.
`-t templ_name.tpl`	Specifies the full-path name of the template file that you want to use. Unlike backup templates, restore templates do not reside in a predetermined location on the master server. They are considered to be temporary in nature and should reside on the client. If the full path is not specified as part of the restore template name, the file might not be found.
`-L progress_file`	Optional. Specifies a run-time process log. Enclose *progress_file* in quotation marks (" ") if they contain space characters.

For example:

For Windows:

```
bpdbsbora -restore -r -t install_path\oracle\restore_templs\ORCL_MON_Full.tpl
```

For UNIX:

```
bpdbsbora -restore -r -t /oracle/restore_templs/ORCL_MON_Full.tpl
```

About an Oracle recovery shell script on the client

You can initiate a database recovery from the command prompt by typing the full path to the shell script that performs an Oracle recovery. For example:

Windows:

```
install_path\oracle\scripts\database_restore.cmd
```

UNIX:

```
/oracle/scripts/database_restore.sh
```

The operating system shell starts the database restore by running the Oracle shell script file. The Oracle shell script file contains commands to run RMAN.

The NetBackup installation script writes sample scripts to the following location:

Windows:

```
install_path\Netbackup\dbext\oracle\samples\rman\
```

UNIX:

```
/usr/openv/netbackup/ext/db_ext/oracle/samples/rman
```

Running RMAN on the client

You can run the `rman` command from a command prompt on the client. Use the appropriate RMAN command file as a parameter.

On UNIX, the following example assumes that you are logged on as an Oracle administrator.

To run the RMAN command on the client:

- At the command prompt, type the following:

  Windows: `rman target 'internal/oracle@ORCL' rcvcat 'rman\rman@RCAT' cmdfile 'install_path\oracle\scripts\database_restore.rcv'`

  UNIX: `rman target 'internal/oracle@ORCL' rcvcat 'rman/rman@RCAT' cmdfile '/oracle/scripts/database_restore.rcv'`

About Oracle multistream restore for proxy backup

NetBackup lets you specify the number of restore streams that start simultaneously when the RMAN command is used. You can use the SEND command variable `NB_ORA_PC_STREAMS` or the RMAN `ENV` parameter to specify the number of restore streams. When you send the request to NetBackup, there may not be the same number of streams or jobs running during restore. NetBackup adjusts the stream count based on the count that is specified when you use the `NB_ORA_PC_STREAMS` variable. Or, NetBackup uses the number of images the requested restore job needs if the restore job needs more than one image. NetBackup selects whichever is the minimum number needed to complete the restore job.

When the restore job needs only one image and it is a snapshot, the stream count is based on the count that you specify in `NB_ORA_PC_STREAMS`. Or, NetBackup uses the number of files the requested restore job needs to complete. NetBackup selects whichever is the minimum number needed to complete the restore job. Also, the files are evenly distributed across the streams based on the file size.

When the restore needs only one image and that image is not a snapshot, then NetBackup does not attempt to perform a multistream restore.

See "About the RMAN SEND command variables" on page 101.

When the multistream restore is started, a parent job is created that initiates a child job for each stream. If you cancel the parent job, all incomplete child jobs are canceled and the job exits with a status of 150. If one of the child jobs is successful before parent cancelation, then the parent job exits with a status of 1. If you cancel one of the running child jobs, the child exits with status 150 and the parent job exits with a status of 1.

Note: Multistream restore only works when using Oracle backup images and is only accessible using command-line inputs.

Multistream restore supports the following snapshot method images:

- remote_vxfs
- VxFS_Checkpoint
- VxVM

Multistream restore is not supported when using the following types of images:

- Block level incremental images
- Off-host supported snapshot method images

It is recommended to configure RMAN to always use the SEND command to pass the desired variables and values to NetBackup explicitly. Alternatively the RMAN

ENV parameter can be used to make the variables and values available to NetBackup. The following are examples of running the multistream restore:

Example 1. Use the SEND command to specify the NB_ORA_PC_STREAMS variable.

```
RUN {
ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';
SEND 'NB_ORA_PC_STREAMS=<number of restore streams>';
RESTORE DATABASE; RECOVER DATABASE;
RELEASE CHANNEL ch00;
}
```

Example 2. Use the PARMS operand to specify the NB_ORA_PC_STREAMS variable.

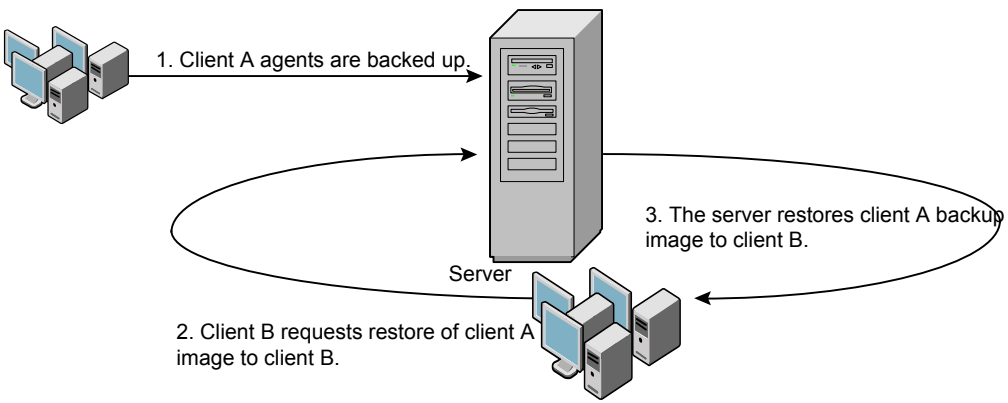
```
RUN {
ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE'
PARMS "ENV=(NB_ORA_PC_STREAMS= <number of restore streams>)";
RESTORE DATABASE; RECOVER DATABASE;
RELEASE CHANNEL ch00;
}
```

Redirecting a restore to a different client

With NetBackup for Oracle you have the option to restore a database to a client other than the one that originally performed the backup. The process of restoring data to another client is called a redirected restore.

Figure 5-1 shows a redirected restore.

Figure 5-1 Redirected restore



The user on client A cannot initiate a redirected restore to client B. Only the user on client B, which is the client receiving the backup image, can initiate the redirected restore. Any user who belongs to the database group that performed the backup can restore it, unless the BKUP_IMAGE_PERM variable is set to USER.

Preparing the master server for an alternate restore

The examples in the following procedure assume that the database instance `ORAC11` was backed up by `client2`, and you want to restore `ORAC11` to `client1`.

For more information on how to manage client restores, see the NetBackup Administrator's Guide, Volume I.

To prepare the NetBackup master server for alternate restores

1. Log onto the NetBackup master server that hosts the policy that backed up database instance `ORAC11`.
2. Create a *dest_client_name* file on the NetBackup master server.
   - Windows: *install_path*\NetBackup\db\altnames*dest_client_name*
   - UNIX: /usr/openv/netbackup/db/altnames/*dest_client_name*

   Where *dest_client_name* is the name of a client that is allowed to be a destination client for alternate restores. For example, `client1`.
3. After creating a *dest_client_name* file, add the name of the NetBackup for Oracle source client to the *dest_client_name* file. For example, add the following line to this file:

   ```
   client2
   ```

For more information on managing a client restore, see the NetBackup Administrator's Guide, Volume I.

About performing a redirected restore with RMAN

Perform the following procedure on the destination client host if you want to restore any RMAN backups that another client owns.

The user on client A cannot initiate a redirected restore to client B. Only the user on client B, which is the client receiving the backup image, can initiate the redirected restore. Any user who belongs to the database group that performed the backup can restore it, unless the BKUP_IMAGE_PERM variable is set to USER.

Note: If the RMAN catalog database has been lost, restore the catalog database first before continuing with the redirected restore.

To perform a redirected restore

1. Enable a network connection to the RMAN catalog database that the source client used.
2. Do one of the following:
   - On Windows, use the `rman parms` option to set the `NB_ORA_CLIENT` environment variable to the source client.
   - On UNIX, set the `NB_ORA_CLIENT` environment variable to the source client.
3. On UNIX, check the `bp.conf` files on the source client. Make sure that the `CLIENT_NAME` variable either is not set or is set to the host name of the source client.
4. Make the `init.ora` file of the source client available to the destination client.

   Copy the file to the destination client or modify the file on the destination client. Change all location-specific parameters.
5. Create a folder or set the permissions for a directory to restore the data files:
   - On Windows, create and start an Oracle service for the previously set `ORACLE_SID`. Create the folder to which you want to restore the data files.
   - On UNIX, grant write permission to the directory to which you want to restore the data files.
6. Set up a password file for the destination client database.
7. Start the database in the `nomount` state.
8. Start RMAN, connecting to the catalog. On Windows, also connect to the target database.
9. On UNIX, set *dbid* to be the DBID of the source client database. Connect to the target database without using a user ID and password.
10. Run an RMAN restore script. On UNIX, you can alternatively type the RMAN commands for the restore.

Example - Performing a redirected restore of Oracle

For example, assume the following:

- Source client is `camel`
- Destination client is `giraffe`
- Master server is `lion`
- `ORACLE_SID` is `test`

- The user is connected to the Oracle database using a local connection, not SQL*Net
- UNIX user is `ora` on both `camel` and `giraffe`

To perform a redirected restore (example)

1. Create the following file on server `lion`:

   Windows: *`install_path`*`\NetBackup\db\altnames\giraffe`

   UNIX: `/usr/openv/netbackup/db/altnames/giraffe`

   Edit `giraffe` to contain the name `camel`:

2. Do one of the following:
   - Windows: Use the BAR GUI to set `lion` as the master server.
   - UNIX: Log onto `giraffe` as `ora`. Set `SERVER=lion` in `$ORACLE_HOME/bp.conf`. This server must be the first server that is listed in the `bp.conf` file.
3. Modify the network `tnsnames.ora` file to enable the RMAN catalog connection.
4. Create `inittest.ora.file`.
5. Windows: Using Oracle administration, create and start `ORACLESERVICETEST`.
6. Set the environment variable `ORACLE_SID` to `test`. On UNIX, also set `NB_ORA_CLIENT` to `camel`.

7 Make sure that the destination database directory exists and has appropriate access permissions.

The data files are restored to the directory path with the same name they had when they were backed up.

8 Start the database in a `nomount` state.

On UNIX, the following is the output:

```
SQL> startup nomount pfile=$ORACLE_HOME/dbs/inittest.ora
%rman catalog rman/rman@rcat
RMAN> set dbid=<dbid of source database on camel
RMAN> connect target/
RMAN> run {
RMAN>        ALLOCATE CHANNEL CH00 TYPE 'SBT_TAPE';
RMAN>        SEND 'NB_ORA_SERV=lion, NB_ORA_CLIENT=camel';
RMAN>        restore controlfile;
RMAN>     }

SQL> alter database mount;
%orapwd file=$ORACLE_HOME/dbs/orapwtest password=<oracle>
%rman catalog rman/rman@RCVCAT

RMAN>set dbid=<Saved dbID of Source Target>
RMAN>connect target/
RMAN>run {
RMAN>        ALLOCATE CHANNEL CH00 TYPE 'SBT_TAPE';
RMAN>        ALLOCATE CHANNEL CH01 TYPE 'SBT_TAPE';
RMAN>        SEND 'NB_ORA_SERV=lion, NB_ORA_CLIENT=camel';
RMAN>        restore database;
RMAN>        restore archivelog all;
RMAN>     }

SQL>recover database until cancel using backup controlfile;
```

Now apply the archived logs. Type `cancel` when you decide to stop recovery.

Using NetBackup for Oracle in a Microsoft Windows cluster environment

To use NetBackup for Oracle in a Microsoft Cluster environment, the following must be installed in the cluster nodes:

- NetBackup client or server (7.5 or greater)

- NetBackup for Oracle on Windows (7.5 or greater)
- Oracle Database version 10g or greater
- Oracle Failsafe 3.11 for Oracle 10g or greater
  - Review the Oracle compatibility list for complete information.

NetBackup for Oracle users in a Microsoft Cluster environment must take some additional steps to prepare for server-directed backups, user-directed backups, and user-directed restores.

About backups of an Oracle clustered database on Windows

The most convenient way to back up your clustered databases is to set up schedules for automatic backups. NetBackup for Oracle comes with sample scripts for clustered Oracle databases. The NetBackup for Oracle installation process installs the sample scripts in the following location:

install_path\NetBackup\dbext\oracle\samples\rman\

Modify the scripts to give values to the following variables:

- Oracle SID
- Oracle Home
- Cluster Name, Domain
- Failsafe Home
- Failsafe user ID
- Failsafe Password
- Failsafe Database Resource Name
- Virtual Oracle Database Name

You can also manually back up an Oracle policy. Refer to the following procedure:

See "Testing configuration settings for NetBackup for Oracle" on page 114.

For more information on how to back up or restore Microsoft Cluster using NetBackup, see the NetBackup Administrator's Guide, Volume I.

Bringing the database instance offline on Windows

Before you can perform a user-directed backup or restore from the client, you must take the database instance offline. You can use the Failsafe graphical user interface or the Failsafe command line (FSCMD).

To take the database instance offline with Failsafe graphical user interface

1. Select the Oracle database resource in the Failsafe graphical user interface.
2. Choose to bring it offline.

To take the database instance offline with Failsafe command line (FSCMD), type the following command:

- `fscmd offlineresource salesdb /cluster=curly /offline=immediate /domain=`*`domainname`* `/user=`*`user`* `/pwd=`*`pwd`*

To bring the resource offline, the preceding command sets `offline=immediate`.

Alternately, based on your need you can specify one of the following as the argument:

`abort`	Shuts down the database instantaneously by aborting the database instance.
`immediate`	Shuts down the database immediately by terminating SQL statements in progress, rolling back uncommitted transactions and disconnecting users.
`normal`	Shuts down the database and doesn't allow new connections after the command was issued. This command waits for the connected users to disconnect before the database is shut down.
`transactional`	Shuts down the database only after all of the current transactions have completed.

Because the `offlineresource` operation shuts down the Oracle database service, enter the following command to start the Oracle database service:

`net start` *`OracleService`*

Bringing the database instance online on Windows

After you perform a user-directed backup or restore from the client, you must bring the database instance online. You can use the Failsafe graphical user interface or the Failsafe command line (FSCMD).

To bring the database instance online with Failsafe graphical user interface

1. Select the resource in the Failsafe graphical user interface.
2. Choose to bring it online.

To bring the database instance online with Failsafe command line (FSCMD), type the following command:

- `fscmd online resource salesdb /cluster=curly /offline=immediate /domain=`*`domainname`* `/user=`*`user`* `/pwd=`*`pwd`*

User-directed backup or restore from the Windows client

This section explains the process to prepare a Microsoft Cluster environment for a user-directed backup or restore operation.

Note: When performing user-directed backups, make sure that you are on the node that owns the shared drive where the Oracle database is installed.

Note: When user-directed client restores are performed with different configuration options of NetBackup failover media servers and a UNIX or Windows master server, see the NetBackup Administrator's Guide, Volume I.

To perform a user-directed backup or restore from the client

1. Take the clustered Oracle database instance offline.

   See "Bringing the database instance offline on Windows" on page 139.

2. Shut down and then startup the database in `mount` state.

   The sequence is necessary to perform administrative tasks like backup and recovery. Use the `svrmgrl` or `sqlplus` utility from Oracle. At the command line, type the following:

   ```
   Shutdown option [normal, abort, immediate]
   startup mount
   ```

3. Perform the backup or recovery.

   See "Using the recovery wizard" on page 130.

4. Bring the Oracle database online with failsafe after the desired backup or restore is complete. The database is then enabled to fail over between the configured cluster of nodes.

   See "Bringing the database instance online on Windows" on page 140.

Creating an instant recovery point from an Oracle Copilot image

The `nborair` command can determine if an image is available for Oracle Copilot instant recovery.

Note: The functionality for creating an instant recovery point is not in the GUI. This feature is command line option only.

Refer to the NetBackup Commands Reference Guide for more usage options using the `nborair` command.

To create an instant recovery point

1. Determine if there are any images available for instant recovery by running the `nborair -list_images [-client name] [-server master]` command.

   The NetBackup administrator or the DBA can run this command from the NetBackup client or master server.

   Example output:

```
# nborair -list_images -client orachost1.demo.com -server mastsrv123
Time: 08/30/2016 15:51:17  ID: orachost1.demo.com_1472590277 Full Backup     policy1
Time: 08/31/2016 11:20:17  ID: orachost1.demo.com_1472660417 Full Backup     policy1
Time: 09/02/2016 10:42:45  ID: orachost1.demo.com_1472830965 Full Backup     policy1
```

2. List the files that are included in the backup image by running the `nborair -list_files -backupid backup_id` command.

   The NetBackup administrator or the DBA can run this command from the NetBackup client or master server. The DBA sees only the files they can access when this command is run.

   Example output:

```
# nborair -list_files -backupid orachost1.demo.com_1472590277
-rw-r----- orac112 dba 807411712 Sep 02 10:42 /backup/data_D-ORAC112_I-3955369132_TS-SYSAUX...
-rw-r----- orac112 dba 744497152 Sep 02 10:42 /backup/data_D-ORAC112_I-3955369132_TS-SYSTEM...
-rw-r----- orac112 dba 52436992 Sep 02 10:42 /backup/data_D-ORAC112_I-3955369132_TS-UNDOTBS...
-rw-r----- orac112 dba 5251072 Sep 02 10:42 /backup/data_D-ORAC112_I-3955369132_TS-USERS_FN...
-rw-r----- orac112 dba 163328 Sep 02 10:42 /backup/arch_D-ORAC112_I-3955369132_SCN-3744354_...
-rw-r----- orac112 dba 2560 Sep 02 10:42 /backup/arch_D-ORAC112_I-3955369132_SCN-3744354_5i...
-rw-r----- orac112 dba 98304 Sep 02 10:42 /backup/spfile_D-ORAC112_I-3955369132_T-20160902_...
-rw-r----- orac112 dba 1425408 Sep 02 10:42 /backup/cf_D-ORAC112_I-3955369132_T-20160902_5k...
```

3 Create the instance recovery point by running the `nborair -create_recovery_point -backupid` *backup_id* `-dest_client` *name* command. The *backup_id* is the same *backup_id* found in step 1.

The NetBackup administrator must run this command from the NetBackup master server.

For this example, the destination client is **oracdest**.

Example output:

```
# nborair -create_recovery_point -backupid orachost1.demo.com_1472590277
 -dest_client oracdest
Appliance: appl5330
Export path: /shares/share1_orachost1.demo.com_1472590277_rp1
Export options: oracdest(rw,no_root_squash,insecure)
```

4 Mount the recovery point on the destination client using the OS tools and with the required mount options per Oracle documentation.

Example:

```
mount -t nfs
appl5330:/shares/share1_orachost1.demo.com_1472590277_rp1 /mnt
```

For Windows, Oracle's DNFS needs to be configured. The recovery point has to be exported with the insecure option.

5 (Conditional) On the destination host, verify the mount point is from the backup ID that was requested by running the `nborair -validate -backupid` *backup_id* `-mount_path` *mount_path* command.

The NetBackup administrator or the DBA can run this command on the destination host.

Example output:

```
# nborair -validate -backupid orachost1.demo.com_1472590277 -mount_path /mnt
Validation successful - Recovery point mounted on /mnt was
created from backup ID orachost1.demo.com_1472590277
```

See "Single-step restore to ASM storage from a Copilot recovery point" on page 151.

Deleting an instant recovery point for Oracle Copilot instant recovery

The `nborair` command can delete an instant recovery point that is available for Oracle Copilot instant recovery.

Note: The functionality for deleting an instant recovery point is not in the GUI. This feature is command line option only.

Refer to the NetBackup Commands Reference Guide for more usage options using the `nborair` command.

To delete an instant recovery point

1. (Conditional) Verify the recovery point is unmounted from the destination client using the OS tools.

   UNIX: `umount /mnt`

2. List the recovery point on the NetBackup appliance by running the `nborair -list_recovery_points -appliance` *`appliance_name`* command.

   The NetBackup administrator must run this command from the NetBackup master server.

   Example output:

   ```
   # nborair -list_recovery_points -appliance appl5330
   Total 1 recovery points found.

   Export path: /shares/share1_orachost1.demo.com_1472590277_rp1
   Share name: share1
   Export options: oracdest(rw,no_root_squash,insecure)
   ```

3. Delete the recovery point on the NetBackup appliance by running the `nborair -delete_recovery_point -appliance` *`appliance_name`* `-export_path` *`export_path`* command.

   The NetBackup administrator must run this command from the NetBackup master server.

   Example output:

   ```
   # nborair -delete_recovery_point -appliance appl5330
   -export_path /shares/share1_orachost1.demo.com_1472590277_rp1
   ```

Cleaning up the Copilot share after point in time restore of database

After a point in time restore of an Oracle database, RMAN can leave files from the previous database incarnations on a Copilot share. NetBackup does not automatically clean up the files from the previous database incarnation. This procedure describes how to manually clean up the share using RMAN.

Note: The functionality for cleaning up a Copilot share is not in the GUI. This feature is command line option only.

To clean up the Copilot share

1. Open a command prompt on the NetBackup client.
2. Set the `NLS_DATE_FORMAT` to display hours, minutes, and seconds.

   UNIX:

   ```
   NLS_DATE_FORMAT=DD-MON-YY_HH24:MI:SS
   export NLS_DATE_FORMAT
   ```

   Windows:

   ```
   set NLS_DATE_FORMAT=DD-MON-YY_HH24:MI:SS
   ```

3. Log into RMAN and if NetBackup uses the RMAN catalog, it is required to log in to the catalog.
4. Use the `RMAN> list incarnation of database;` command to find the `Reset Time` for the current incarnation.

   Example:

```
List of Database Incarnations
DB Key  Inc Key DB Name  DB ID            STATUS  Reset SCN  Reset Time
------- ------- -------- ---------------- --- ---------- ----------
10046   10054   ORACLEC2 3019371157       PARENT  1          11-SEP-14_08:40:48
10046   10047   ORACLEC2 3019371157       PARENT  2233668    27-APR-17_10:23:22
10046   11551   ORACLEC2 3019371157       CURRENT 2323198    28-APR-17_10:41:37
```

5. Use the `list backup summary completed before "to_date()" device type disk;` command to find all the backup pieces from the previous incarnation by using the reset time (`"to_date()"` must match `NLS_DATE_FORMAT`).

   Example:

```
RMAN> list backup summary completed before "to_date('28-APR-17_10:41:37',
'DD-MON-YY_HH24:MI:SS')" device type disk;

List of Backups
===============
Key     TY LV S Device Type Completion Time    #Pieces #Copies Compressed Tag
------- -- -- - ----------- ------------------ ------- ------- ---------- ---
10192   B  F  A DISK        27-APR-17_10:42:59 1       1       NO         TAG20170427T104257
10193   B  F  A DISK        27-APR-17_13:16:37 1       1       NO         TAG20170427T131636
10194   B  F  A DISK        27-APR-17_13:16:55 1       1       NO         TAG20170427T131654
10195   B  F  A DISK        27-APR-17_13:28:52 1       1       NO         TAG20170427T132851
10196   B  F  A DISK        27-APR-17_13:29:08 1       1       NO         TAG20170427T132906
10197   B  F  A DISK        27-APR-17_14:00:31 1       1       NO         TAG20170427T140031
10198   B  F  A DISK        27-APR-17_14:00:43 1       1       NO         TAG20170427T140043
10199   B  F  A DISK        27-APR-17_14:07:31 1       1       NO         TAG20170427T140730
10200   B  F  A DISK        27-APR-17_14:07:48 1       1       NO         TAG20170427T140747
10759   B  A  A DISK        28-APR-17_10:28:46 1       1       NO         DCS_CDB
10786   B  F  A DISK        28-APR-17_10:28:56 1       1       NO         DCS_CDB
10814   B  F  A DISK        28-APR-17_10:29:08 1       1       NO         DCS_CDB
```

6. Use the `list backup summary completed before "to_date()" device type disk tag '';` command to find the backup pieces on the share by using the `tag` (by default, the `tag` is the NetBackup policy name).

   Example:

```
RMAN> list backup summary completed before "to_date('28-APR-17_10:41:37',
'DD-MON-YY_HH24:MI:SS')" device type disk tag 'DCS_CDB';

List of Backups
===============
Key     TY LV S Device Type Completion Time    #Pieces #Copies Compressed Tag
------- -- -- - ----------- ------------------ ------- ------- ---------- ---
10759   B  A  A DISK        28-APR-17_10:28:46 1       1       NO         DCS_CDB
10786   B  F  A DISK        28-APR-17_10:28:56 1       1       NO         DCS_CDB
10814   B  F  A DISK        28-APR-17_10:29:08 1       1       NO         DCS_CDB
```

7 Use the `list backup completed before "to_date()" device type disk tag '';` command to remove the summary option to see what files need deleting.

Example:

```
RMAN> list backup completed before "to_date('28-APR-17_10:41:37',
'DD-MON-YY_HH24:MI:SS')" device type disk tag 'DCS_CDB';

List of Backup Sets
===================
BS Key  Size       Device Type Elapsed Time Completion Time
------- ---------- ----------- ------------ -------------------
10759   40.00K     DISK        00:02:55     28-APR-17_10:28:46
        BP Key: 10762   Status: AVAILABLE  Compressed: NO  Tag: DCS_CDB
        Piece Name: C:\HA_NBA_SHARE\ARCH_D-ORACLEC2_I-3019371157_SCN-2323355_26S2QF5F_DCS_CDB

  List of Archived Logs in backup set 10759
  Thrd Seq     Low SCN    Low Time            Next SCN   Next Time
  ---- ------- ---------- ------------------- ---------- ---------
  1    19      2322734    28-APR-17_10:16:54 2323527    28-APR-17_10:25:48
  1    20      2323527    28-APR-17_10:25:48 2323546    28-APR-17_10:25:49

BS Key  Type LV Size       Device Type Elapsed Time Completion Time
------- ---- -- ---------- ----------- ------------ -------------------
10786   Full    80.00K     DISK        00:03:02     28-APR-17_10:28:56
        BP Key: 10789   Status: AVAILABLE  Compressed: NO  Tag: DCS_CDB
        Piece Name: C:\HA_NBA_SHARE\SPFILE_D-ORACLEC2_I-3019371157_T-20170428_27S2QF5I_DCS_CDB
  SPFILE Included: Modification time: 27-APR-17_14:57:53
  SPFILE db_unique_name: ORACLEC2

BS Key  Type LV Size       Device Type Elapsed Time Completion Time
------- ---- -- ---------- ----------- ------------ -------------------
10814   Full    17.17M     DISK        00:03:11     28-APR-17_10:29:08
        BP Key: 10816   Status: AVAILABLE  Compressed: NO  Tag: DCS_CDB
        Piece Name: C:\HA_NBA_SHARE\CF_D-ORACLEC2_I-3019371157_T-20170428_28S2QF5L_DCS_CDB
  Control File Included: Ckp SCN: 2323603      Ckp time: 28-APR-17_10:25:57
```

8 Use the `delete backup completed before "to_date()" device type disk tag '';` command to delete the unwanted backup pieces.

Example:

```
RMAN> delete backup  completed before  "to_date('28-APR-17_10:41:37',
'DD-MON-YY_HH24:MI:SS')" device type disk tag 'DCS_CDB';

allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=242 device type=DISK

List of Backup Pieces
BP Key  BS Key  Pc# Cp# Status      Device Type Piece Name
------- ------- --- --- ----------- ----------- ----------
10762   10759   1   1   AVAILABLE   DISK        C:\HA_NBA_SHARE\ARCH_D-ORACLEC2_I-3019371157_
SCN-2323355_26S2QF5F_DCS_CDB
10789   10786   1   1   AVAILABLE   DISK        C:\HA_NBA_SHARE\SPFILE_D-ORACLEC2_I-3019371157_
T-20170428_27S2QF5I_DCS_CDB
10816   10814   1   1   AVAILABLE   DISK        C:\HA_NBA_SHARE\CF_D-ORACLEC2_I-3019371157_
T-20170428_28S2QF5L_DCS_CDB

Do you really want to delete the above objects (enter YES or NO)? YES
deleted backup piece
backup piece handle=C:\HA_NBA_SHARE\ARCH_D-ORACLEC2_I-3019371157_SCN-2323355_26S2QF5F_DCS_CDB
RECID=50 STAMP=942488751
deleted backup piece
backup piece handle=C:\HA_NBA_SHARE\SPFILE_D-ORACLEC2_I-3019371157_T-20170428_27S2QF5I_DCS_CDB
RECID=51 STAMP=942488754
deleted backup piece
backup piece handle=C:\HA_NBA_SHARE\CF_D-ORACLEC2_I-3019371157_T-20170428_28S2QF5L_DCS_CDB
RECID=52 STAMP=942488758
Deleted 3 objects
```

9 Use the `list copy completed before "to_date()" tag '';` command to find the data file copies on the share using the same reset time and `tag`.

Example:

```
RMAN> list copy completed before  "to_date('28-APR-17_10:41:37',
'DD-MON-YY_HH24:MI:SS')" tag 'DCS_CDB';

specification does not match any control file copy in the repository
List of Datafile Copies
=======================
Key     File S Completion Time    Ckp SCN    Ckp Time
------- ---- - ------------------ ---------- ------------------
10649   1    A 28-APR-17_10:25:39 2323417    28-APR-17_10:25:15
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSTEM_FNO-1_1GS2QE1J_S-48_
I-3019371157_DCS_CDB
        Tag: DCS_CDB

10251   2    A 28-APR-17_10:15:32 2243146    27-APR-17_10:31:51
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSTEM_FNO-2_1LS2QEGQ_S-53_
I-3019371157_DCS_CDB
        Tag: DCS_CDB
        Container ID: 2, PDB Name: PDB$SEED

10648   3    A 28-APR-17_10:25:39 2323417    28-APR-17_10:25:15
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSAUX_FNO-3_1IS2QE8G_S-50_
I-3019371157_DCS_CDB
        Tag: DCS_CDB

10249   4    A 28-APR-17_10:13:19 2243146    27-APR-17_10:31:51
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSAUX_FNO-4_1JS2QEBG_S-51_
I-3019371157_DCS_CDB
        Tag: DCS_CDB
        Container ID: 2, PDB Name: PDB$SEED

10647   5    A 28-APR-17_10:25:38 2323417    28-APR-17_10:25:15
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-UNDOTBS1_FNO-5_1HS2QE57_S-49_
I-3019371157_DCS_CDB
        Tag: DCS_CDB

10646   6    A 28-APR-17_10:25:37 2323417    28-APR-17_10:25:15
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-USERS_FNO-6_1NS2QEJV_S-55_
I-3019371157_DCS_CDB
        Tag: DCS_CDB
```

10 Use the `delete copy completed before "to_date()" tag '';` command to delete the data file copies on the selected share.

Example:

```
RMAN> delete copy completed before  "to_date('28-APR-17_10:41:37',
'DD-MON-YY_HH24:MI:SS')" tag 'DCS_CDB';

released channel: ORA_DISK_1
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=242 device type=DISK
specification does not match any control file copy in the repository
List of Datafile Copies
=======================

Key     File S Completion Time    Ckp SCN    Ckp Time
------- ---- - ------------------ ---------- ------------------
10649   1    A 28-APR-17_10:25:39 2323417    28-APR-17_10:25:15
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSTEM_FNO-1_1GS2QE1J_S-48_
I-3019371157_DCS_CDB
        Tag: DCS_CDB

10251   2    A 28-APR-17_10:15:32 2243146    27-APR-17_10:31:51
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSTEM_FNO-2_1LS2QEGQ_S-53_
I-3019371157_DCS_CDB
        Tag: DCS_CDB
        Container ID: 2, PDB Name: PDB$SEED

10648   3    A 28-APR-17_10:25:39 2323417    28-APR-17_10:25:15
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSAUX_FNO-3_1IS2QE8G_S-50_
I-3019371157_DCS_CDB
        Tag: DCS_CDB

10249   4    A 28-APR-17_10:13:19 2243146    27-APR-17_10:31:51
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSAUX_FNO-4_1JS2QEBG_S-51_
I-3019371157_DCS_CDB
        Tag: DCS_CDB
        Container ID: 2, PDB Name: PDB$SEED

10647   5    A 28-APR-17_10:25:38 2323417    28-APR-17_10:25:15
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-UNDOTBS1_FNO-5_1HS2QE57_S-49_
I-3019371157_DCS_CDB
        Tag: DCS_CDB
```

```
10646   6    A 28-APR-17_10:25:37 2323417    28-APR-17_10:25:15
        Name: C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-USERS_FNO-6_1NS2QEJV_S-55_
I-3019371157_DCS_CDB
        Tag: DCS_CDB


Do you really want to delete the above objects (enter YES or NO)? YES
deleted datafile copy
datafile copy file name=C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSTEM_FNO-1_1GS2QE1J_
S-48_I-3019371157_DCS_CDB RECID=36 STAMP=942488739
deleted datafile copy
datafile copy file name=C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSTEM_FNO-2_1LS2QEGQ_
S-53_I-3019371157_DCS_CDB RECID=29 STAMP=942488132
deleted datafile copy
datafile copy file name=C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSAUX_FNO-3_1IS2QE8G_
S-50_I-3019371157_DCS_CDB RECID=35 STAMP=942488739
deleted datafile copy
datafile copy file name=C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-SYSAUX_FNO-4_1JS2QEBG_
S-51_I-3019371157_DCS_CDB RECID=27 STAMP=942487999
deleted datafile copy
datafile copy file name=C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-UNDOTBS1_FNO-5_1HS2QE57_
S-49_I-3019371157_DCS_CDB RECID=34 STAMP=942488738
deleted datafile copy
datafile copy file name=C:\HA_NBA_SHARE\DATA_D-ORACLEC2_I-3019371157_TS-USERS_FNO-6_1NS2QEJV_
S-55_I-3019371157_DCS_CDB RECID=33 STAMP=942488737
Deleted 6 objects
```

Single-step restore to ASM storage from a Copilot recovery point

The following procedure shows how to use RMAN to restore from a recovery point. This procedure is only viable after the command `nborair -create_recovery_point` is run and the recovery point is mounted on a target client.

Note: The functionality for single-step restore to ASM storage is not in the GUI. This feature is run with RMAN only.

The procedure example assumes that a recovery point is already mounted and uses the mount point of `/db_mp` as the example. All RMAN commands must run from the target host.

To perform a single-step restore to ASM storage from a recovery point

1 Catalog the backups from the recovery point.

```
RMAN> catalog start with '/db_mp/';

searching for all files that match the pattern /db_mp/

List of Files Unknown to the Database
=====================================
File Name: /db_mp/data_D-ORAC112_I-3955369132_TS-SYSAUX_FNO-2_8hrgu3qd_s-1297_I-3955369132
File Name: /db_mp/data_D-ORAC112_I-3955369132_TS-SYSTEM_FNO-1_8irgu3qk_s-1298_I-3955369132
File Name: /db_mp/data_D-ORAC112_I-3955369132_TS-UNDOTBS1_FNO-3_8jrgu3qr_s-1299_I-3955369132
File Name: /db_mp/data_D-ORAC112_I-3955369132_TS-USERS_FNO-4_8krgu3qt_s-1300_I-3955369132
File Name: /db_mp/arch_D-ORAC112_I-3955369132_SCN-5248163_a8rh0s3b
File Name: /db_mp/spfile_D-ORAC112_I-3955369132_T-20160929_a9rh0s3c
File Name: /db_mp/cf_D-ORAC112_I-3955369132_T-20160929_aarh0s3d

Do you really want to catalog the above files (enter YES or NO)? YES
cataloging files...
cataloging done

List of Cataloged Files
=======================
File Name: /db_mp/data_D-ORAC112_I-3955369132_TS-SYSAUX_FNO-2_8hrgu3qd_s-1297_I-3955369132
File Name: /db_mp/data_D-ORAC112_I-3955369132_TS-SYSTEM_FNO-1_8irgu3qk_s-1298_I-3955369132
File Name: /db_mp/data_D-ORAC112_I-3955369132_TS-UNDOTBS1_FNO-3_8jrgu3qr_s-1299_I-3955369132
File Name: /db_mp/data_D-ORAC112_I-3955369132_TS-USERS_FNO-4_8krgu3qt_s-1300_I-3955369132
File Name: /db_mp/arch_D-ORAC112_I-3955369132_SCN-5248163_a8rh0s3b
File Name: /db_mp/spfile_D-ORAC112_I-3955369132_T-20160929_a9rh0s3c
File Name: /db_mp/cf_D-ORAC112_I-3955369132_T-20160929_aarh0s3d
```

2 Restore the datafiles from the point in time of the recovery point.

The following RMAN restore is from disk (`DISK`). Also, this example uses the `NLS_DATE_FORMAT="DD-MM-YYYY-HH24:MI:SS"` command that was set in the environment before RMAN was run. Use the date format for your environment.

```
RMAN> restore until time '2016-09-29-10:00:00' database;

Starting restore at 2016-10-12:15:51:22
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=193 device type=DISK

channel ORA_DISK_1: restoring datafile 00001
input datafile copy RECID=461 STAMP=925055096
file name=/demo_2/data_D-ORAC112_I-3955369132_TS-SYSTEM_FNO-1_8irgu3qk_s-1298_I-3955369132
destination for restore of datafile 00001: /db/orac112/app/oradata/orac112/system01.dbf
channel ORA_DISK_1: copied datafile copy of datafile 00001
output file name=/db/orac112/app/oradata/orac112/system01.dbf RECID=0 STAMP=0
Finished restore at 2016-10-12:15:51:34
```

3 Recover the database.

If the restore of archive logs is not available on disk, then the logs are restored from NetBackup (`sbt_tape`).

```
RMAN> run
{
allocate channel ch00 type sbt_Tape;
recover database;
release channel ch00;
}

released channel: ORA_DISK_1
allocated channel: ch00
channel ch00: SID=193 device type=SBT_TAPE
channel ch00: Veritas NetBackup for Oracle - Release 8.0 (2016091418)

Starting recover at 2016-10-12:15:54:13

starting media recovery

archived log for thread 1 with sequence 508 is already on disk as file
/db/orac112/app/fast_recovery_area/ORAC112/archivelog/2016_09_29/o1_mf_1_508_cytbkv22_.arc
archived log for thread 1 with sequence 509 is already on disk as file
/db/orac112/app/fast_recovery_area/ORAC112/archivelog/2016_09_29/o1_mf_1_509_cytbkv36_.arc
....
archived log file name=
/db/orac112/app/fast_recovery_area/ORAC112/archivelog/2016_09_29/o1_mf_1_508_cytbkv22_.arc
thread=1 sequence=508
archived log file name=
/db/orac112/app/fast_recovery_area/ORAC112/archivelog/2016_09_29/o1_mf_1_509_cytbkv36_.arc
thread=1 sequence=509
....
media recovery complete, elapsed time: 00:00:55
Finished recover at 2016-10-12:15:55:09

released channel: ch00

RMAN>
```

See "Creating an instant recovery point from an Oracle Copilot image" on page 142.

See "About using a NetBackup appliance share for Oracle backups (Copilot)" on page 84.

See “Configuring an OIP using a share on the NetBackup appliance (Copilot)” on page 86.

About restoring from a data file copy to ASM storage using RMAN

When you use a proxy method for data file copies, NetBackup cannot place the file directly back in ASM storage. You need to do a two-step restore for the data file copies.

If the backups are stream-based then restore directly from NetBackup.

When you restore back to the appliance share, make sure that the share on the appliance is configured with the `no_root_squash` NFS export option enabled.

For more information, refer to the Managing shares chapter in the Veritas NetBackup Appliance Administrator’s Guide.

The first step is to stage the files to a file system. The second step is to use RMAN to restore the files into ASM storage.

The following is an example RMAN script to stage the files to a file system:

```
RUN {
ALLOCATE CHANNEL ch00
   TYPE 'SBT_TAPE';
SEND 'NB_ORA_CLIENT=clientname,NB_ORA_SERV=servername';
SET NEWNAME FOR TABLESPACE USERS TO '/dump/%U';
RESTORE TABLESPACE USERS;
RELEASE CHANNEL ch00;
}
```

Once the file is on a file system, then you can restore to ASM storage by running the following:

```
RUN {
ALLOCATE CHANNEL dc00 DEVICE TYPE DISK;
RESTORE TABLESPACE USERS;
RECOVER DATABASE;
RELEASE CHANNEL dc00;
}
```

Chapter 6

Guided Recovery

This chapter includes the following topics:

About OpsCenter Guided Recovery

The use of the OpsCenter web-based user interface to guide a user through the Oracle cloning operation offers several benefits:

- The process is more automated, making the operation easier to perform.

- OpsCenter retrieves information for you such as databases and control files, shortening the Oracle clone setup time.
- A validation process increases the rate of successfully completing the cloning operation.
- You do not need access to the original database to perform the cloning operation.

Setting up for Guided Recovery cloning

Guided Recovery cloning requires metadata cataloging, which enables database information to display in OpsCenter. Metadata cataloging must occur during the backup from the Oracle database to be cloned. The collected metadata displays within the OpsCenter interface to guide the Clone operation. Cloning also requires that the Oracle destination file paths exist before the operation begins.

Do the following before you perform a Guided Recovery cloning operation:

- Configure metadata cataloging before taking the backup, that is used for the cloning operation, using one of these methods.
  - Place the following text into a text file (for example:*new_config.txt*) on the master or the media server that has access to the client:

    ```
    ORACLE_METADATA=YES
    ```

    Then send this configuration to the client host by using the following `bpsetconfig` command:

    ```
    bpsetconfig -h myoracleclient new_config.txt
    ```

    The `bpsetconfig` command is located in the `admincmd` directory.
    Windows: *`install_path`*`\NetBackup\bin\admincmd`
    UNIX: `/usr/openv/netbackup/bin/admincmd`
  - Alternatively on UNIX and Linux, ensure that the Oracle metadata parameter in the client's `bp.conf` is set at backup time as follows:

    ```
    ORACLE_METADATA=YES
    ```

  - Alternatively, the RMAN commands can include a SEND statement at the time of the backup.

    ```
    ... allocate channels ...
    SEND 'NB_ORA_METADATA=YES';
    ... backup command ...
    ```

- Set up all destination file paths before you run the cloning operation because the operation does not create new file paths during the process. Ensure that the Oracle user has write access to these paths.

Guided Recovery cloning pre-operation checks

Check the following items before you begin the cloning process:

- Ensure that the source and the destination systems and the source and the destination databases are compatible. Examples are Solaris 9 to Solaris 10 and Oracle 11 to Oracle 11.
- The cloning operation does not support offline tablespaces or raw tablespaces.
- The cloning operation does not support Oracle Automatic Storage Management (ASM).
- To use a different user or a different group for the clone, change the permissions of the backup image at backup time. Add the 'BKUP_IMAGE_PERM=ANY' to the send commands during the backup of the source database.
  See "About the environment variables set by NetBackup for Oracle" on page 101.
- If the destination client is different than the source client, perform an alternate restore procedure.
  See "Redirecting a restore to a different client" on page 134.
- On Windows systems, if the NetBackup Legacy Network Service runs as the Oracle user, that user needs the right to "Replace a process level token".
- On Oracle 9 for Windows, run the Oracle service under the Oracle user account. By default, it runs under the local system. On Oracle 10G systems and later, you can run under the local system.
- On Windows systems, if you clone to the same system, shut down the source database to successfully complete the operation. Otherwise, an error indicating the database cannot be mounted in exclusive mode appears.
- On UNIX and Linux systems, if the cloning user shares an existing Oracle home, the user must have write access to some directories such as `DBS`.
- On UNIX and Linux systems, shut down the source database before you clone in the following situation: You clone to the same system and you either use the same user or use the same home as the source database.

Performing a Guided Recovery cloning operation

You need to log onto OpsCenter, to perform a cloning operation. OpsCenter is the web GUI that you use to perform all guided recovery operations.

To perform a cloning operation on an Oracle database in OpsCenter

1. When you log onto OpsCenter, the first screen that appears is the **Monitor Overview** screen. Along the top of the screen, click **Manage > Restore**.
2. On the **What do you want to restore?** screen, click **Clone Oracle Database**.
3. On the small **Select a Master Server** dialog box, use the drop-down menu to select the master server that you want to work with, then click **OK**.

   See "Select a Master Server dialog" on page 160.
4. The **Select Source Database** screen lets you filter the list of databases by database name, host name, database version, platform, and date. The default condition is to display all databases that are backed up in the default date range. Click **Show Databases**.

   More information is available on this screen.

   See "Select Source Database panel" on page 161.
5. The databases appear under the filtering part of the same screen. Click **option** at the left side of the desired database entry to select the database on which you want to perform a cloning operation. Then click **Next>**.
6. The **Select Control File Backup** screen shows a timeline view of the control file backups. Select the icon for the desired control file backup from the timeline view. You can hover over the icon to display the control file details. If the icon represents multiple backups, you can hover over the icon to display all versions of the backup for that time periods.

   Additional information is available to verify that you have selected the correct control file. The lower left corner of the screen lists three links. More information is available about these links.

   See "Select Control File Backup panel" on page 161.

   Click on the icon of the control file backup you want to restore for the clone of the selected database. The default is the latest backup selected. Then click **Next>**.
7. The **Destination Host and Login** screen contains parameters for the destination of the clone to be created. Enter the destination host name in the text box that is provided or click **Browse** and select from a list of available hosts. Note the following prerequisites concerning the destination host:

   - The platform type of the source and destination must be the same.

- A NetBackup client must be installed.
- A compatible version of Oracle must be installed.

See "Destination host and login panel" on page 162.

For operating system authentication, enter a user name, password (Windows), and domain (Windows). Then click **Next>**.

8 The **Define Destination Parameters** screen appears. The five tabs on this screen are used to change database attributes, the destination paths of control files, data files, redo logs, and restore options. After you have changed the destination parameters, click **Next>**.

See "Destination Parameters panel" on page 162.

9 The **Selection Summary** screen lets you scan the information you have entered on the previous screens. Links to the recovery sets and destination database attributes let you view and verify any changes you have made. When you are satisfied with the summary information, click **Next>**.

See "Selection summary panel" on page 163.

10 The **Pre-clone Check** screen lets you validate the database attributes and the file paths. To validate, click the underlined word **here**. If a directory path does not already exist, the validation check flags the error. If a file already exists, the validation check also flags the error, so that the cloning operation does not overwrite the file.

See "Pre-clone check panel" on page 163.

When you are ready to launch the cloning operation, click **Launch Cloning Process**. A display appears that is similar to the NetBackup Activity Monitor.

Note: In NetBackup (7.1 or greater), validation of the data files that reside in raw devices may fail even though the Clone operation was successful. You may receive an error that states the validation for specific paths failed.

Select a Master Server dialog

From the pulldown menu, select the NetBackup master server that collected the backup information to be used for the cloning operation.

Select Source Database panel

When the **Select Source Database** screen first appears, the lowest portion of the screen shows a list of the latest backups for all the databases that the master server knows about for the default date range.

The upper portion of the screen shows parameters for filtering the list of databases. If the list is long, you can filter what databases appear by database name, host name, database version, and date range. Multiple filter parameters can be used at the same time.

For example, to show only the Solaris databases that are backed up between 11/05/2011 and 11/12/2011, select Solaris from the Platform: pulldown menu. Then select the dates from the calendar icons. Then click **Show Databases** to display the new filtered list of databases.

Select Control File Backup panel

The Guided Recovery **Select Control File Backup** screen is a timeline view of all the control files that are backed up for the selected database. The timeline displays an icon for each control file that is associated with the backed up database. When you first enter this screen, the latest backup control file is already selected.

Hover over the icon on the timeline to display a popup that shows information about that file: backup name, type of media, the size of the backup, etc.

Multiple control files may be displayed on the timeline. To view all the instances of control files, you may need to increase the scope of the timeline. You can display the timeline in days, weeks, months, or years. If multiple control files were backed up during a single timeline unit, a different icon appears representing more than one control file (for example, if the database was backed up twice in an hour). To select from among these files, hover over the icon. A popup lists each control file in table format. It shows several items including the backup name and the type of media. Click **option** next to the desired control file.

You can also click one of the links in the lower left of the screen to verify that you have selected the proper control file.

- **View Database Schema** shows the schema of the selected control file. It shows how the database is laid out by listing each data file name, tablespace name, and its size.
- **View Datafiles Recovery Set** shows the data file backups to be used for the restore process. It also shows the backup and image information that is displayed for each data file. The data file recovery set is generated only for the files that are backed up as part of an incremental strategy. Even though files that are

backed up as part of a full backup do not appear in this list, the clone still completes successfully.

If the image spans media, only the first media is shown in the list.

- **View Archived Log Recovery Set** shows the archive log backups that may be used to recover the database to the latest point in time of that control file. This set is generated only for the files that are backed up as part of an incremental strategy. Even though files that are backed up as part of a full backup do not appear in this list, the clone still completes successfully.

Destination host and login panel

The Select Destination Parameters screen lets you enter the destination host and the Oracle logon information. For Windows, you are asked for the domain name, user name, and password. For UNIX and Linux, you are asked only for the user name.

The following rules apply to the selection of the destination host:

- The destination must be of the same platform type as the source of the clone.
- A NetBackup client must be installed.
- A compatible version of Oracle must be installed.

Destination Parameters panel

Guided Recovery uses many values from the source database as default values for the destination database. You can modify these values if not appropriate for the destination database.

Note: The Windows information you enter on this screen is case-sensitive. Be sure to enter the Windows information appropriately.

The **Destination Parameters** screen contains the following tabs:

- **Database Attributes**. This pane appears when you first enter the Database Attributes screen. Each attribute name has identical source and destination attributes. You can change the destination attribute of the instance name, database name, and database home. Note that the instance name is case-sensitive while the database name is not case-sensitive.

  If you use a temporary tablespace or data files, and you plan to write the data files back to the same location, do not modify the path. If you must modify the path, make sure that it is identical to the source path including case (upper,

lower, mixed). Otherwise, the clone fails with an error that indicates the temporary file already exists. This limitation does not affect UNIX and Linux systems.

- **Control File Paths**. This pane displays the source path and the destination path for each control file. You can change a control file destination path by clicking in the associated text window and entering the new path. You can also click Browse to navigate to the desired path. When you change a path, a highlight bar appears around the text window as a visual indicator that this path has changed.
- **Data File Paths**. This pane lets you change the destination path for one or more data files. Enter the path in the text window provided, then select the data files on which to apply it, and press the Apply option.
- **Redo Log Paths**. This pane displays the source path and the destination path for all redo logs. You can type in a new destination path or click Browse to navigate to the desired path. When you change a path, a highlight bar appears around the text window as a visual indicator that this path has changed.
- **Restore Options**. This pane displays restore options. The option that is displayed on this pane is **Number of parallel streams for restore and recover**.

When you are done making changes on this screen, click **Next>**. All the information from the previous screen is saved in preparation for the cloning operation. All the changes that are made in this screen are temporary and are active only for the cloning session.

Selection summary panel

The following information appears on this screen:

- The selected master server and the source database attributes.
- The date and time of the selected control file backup, and the backup media type.
- The database recovery set and the archived log recovery set.
- The destination database attributes selected in the previous screen and the database initialization parameters to be used for the cloning operation.

Pre-clone check panel

The Guided Recovery **Pre-clone Check** screen lets you validate the database attributes and the file paths. To validate, click the underlined word **here**. If a file path does not already exist, the validation check flags the error. If a file already

exists, the validation check also flags the error, so that the cloning operation does not overwrite the file.

You can also specify an email address, so when the cloning process completes, an email is sent to you that gives you the status of the cloning operation along with other pertinent information.

Job Details panel

The Job Details screen is intended to reflect the NetBackup Activity Monitor. More information is available on the Activity Monitor.

For more information, see the NetBackup Administrator's Guide, Volume I.

Guided Recovery post-clone operations

Perform the following after the cloning operation has completed:

- On Windows systems, if the cloning operation fails, use the `dbca` utility to delete the database. `dbca` sometimes removes directories, so verify before retrying the operation.
- On UNIX systems, update the `oratab` file with the appropriate instance information.
- On UNIX systems, if the cloning operation fails, do the following cleanup:
  - If the database is active, shut down the database.
  - Remove init<SID>.ora, spfile<SID>.ora, and any other files that are associated with the SID being used, from the <$ORACLE_HOME>/DBS directory.
  - Remove all data files.
- If a cloned Oracle database contains read-only tablespaces or data files, you must make them read-write before RMAN backs them up, or RMAN cannot restore them. After the backup (cloning operation), you can return the items to read-only.
  The following shows an example of the sequence of steps in the process:
  - Back up Oracle database A which contains read-only tablespace TABLE1.
  - Clone database A to database B.
  - Use the Oracle `alter tablespace` command to make tablespace TABLE1 read-write. You may revert to read-only if you want.
  - Back up database B.

- Use RMAN to restore database B.

Troubleshooting Guided Recovery

Guided Recovery operations are in addition to the normal NetBackup for Oracle operations.

On UNIX and Linux systems, gather all legacy logs at VERBOSE=5. On Windows systems, gather them at General=2, Verbose=5, and Database=5. All unified logs should be gathered at DebugLevel=6 and DiagnosticlLevel=6.

In addition to the troubleshooting methods and evidence that you use for resolving NetBackup for Oracle operations, there is also information that is required specifically for troubleshooting Guided Recovery when it fails.

For more information about NetBackup debug logs and reports, refer to the NetBackup Administrator's Guide, Volume I.

Troubleshooting files for metadata collection operations at the time of the backup

The information in the following log files can be helpful when you troubleshoot Guided Recovery metadata collection operations.

From the Oracle client host:

- netbackup/logs/bphdb legacy logs
- netbackup/logs/dbclient legacy logs (The directory must be writable by the Oracle users.)
- ncf unified logs, OID 309, New Client Framework
- ncforautil unified logs, OID 360, New Client Framework Oracle Utility
- ncforaclepi, OID 348, New Client Framework Oracle Plugin

From the NetBackup media server: netbackup/logs/bpbrm legacy logs

From the NetBackup master server:

- netbackup/logs/bprd legacy logs
- nbars unified logs, OID 362, NetBackup Agent Request Service
- dars unified logs, OID 363, Database Agent Request Service

For more information about NetBackup debug logs and reports, refer to the NetBackup Administrator's Guide, Volume I.

Troubleshooting files for Guided Recovery validation operations

The information in the following log files can be helpful when you troubleshoot Guided Recovery validation operations.

From the Oracle client host:

- netbackup/logs/vnetd legacy logs
- ncf unified logs, OID 309, New Client Framework
- ncfnbcs unified logs, OID 366, New Client Framework NetBackup Client Services

From the NetBackup master server:

- netbackup/logs/vnetd legacy logs
- nbars unified logs, OID 362, NetBackup Agent Request Service
- dars unified logs, OID 363, Database Agent Request Service

From the Veritas OpsCenter server:

- <SYMCOpsCenterServer>/config/log.conf file
- opscenterserver unified logs, OID 148 (The default location is <SYMCOpsCenterServer >/logs)
- opscentergui unified log, OID 147 (The default location is <SYMCOpsCenterGUI>/logs)

For more information about NetBackup debug logs and reports, refer to the NetBackup Administrator's Guide, Volume I.

Troubleshooting files for Guided Recovery cloning operations

The information in the following log files can helpful when you troubleshoot Guided Recovery cloning operations.

From the Oracle client host:

- netbackup/logs/bphdb legacy logs (Includes the obk_stdout and obk_stderr logs.)
- netbackup/logs/bpdbsbora legacy logs
- netbackup/logs/dbclient legacy logs (The directory must be writable by the Oracle users.)
- A tar of netbackup/logs/user_ops (UNIX/Linux)
- A compress of NetBackup\Logs\user_ops (Windows)

From the NetBackup master server:

- netbackup/logs/vnetd legacy logs

- netbackup/logs/bprd legacy logs
- nbars unified logs, OID 362, NetBackup Agent Request Service
- dars unified logs, OID 363, Database Agent Request Service

From the Veritas OpsCenter server:

- <SYMCOpsCenterServer>/config/log.conf file
- opscenterserver unified logs, OID 148 (The default location is <SYMCOpsCenterServer >/logs)
- opscentergui unified log, OID 147 (The default location is <SYMCOpsCenterGUI>/logs)

Chapter 7

NetBackup for Oracle with Snapshot Client

This chapter includes the following topics:

About NetBackup for Oracle with Snapshot Client

To use NetBackup for Oracle with Snapshot Client, NetBackup Snapshot Client and NetBackup for Oracle must both be licensed and installed.

Before you use NetBackup for Oracle with Snapshot Client, confirm that your platform is supported.

See "Verifying the operating system and platform compatibility" on page 35.

A snapshot is a disk image of the client's data that is made almost instantaneously. When it is used with NetBackup Snapshot Client, NetBackup for Oracle can back up Oracle objects by taking snapshot images of the component files. Later, it backs up the snapshot version to the storage unit.

Snapshot backup captures the data at a particular instant without having caused significant client downtime. Client operations and user access continue without interruption during the backup. The resulting capture or snapshot can be backed up without affecting the performance or availability of the database.

The following NetBackup Snapshot Client features are available for use with NetBackup for Oracle.

Table 7-1 Snapshot Client features used with NetBackup for Oracle

Feature	Description
Instant recovery	This feature enables instant recovery of backups from disk. It combines snapshot technology with the ability to do rapid disk-based restores. NetBackup creates the image without interrupting user access to data. Optionally, the image is retained on disk as well as backed up to storage. Instant recovery enables block-level restores. The maximum number of instant recovery snapshots to be retained at one time is calculated per client and database name. With the `remote_vxfs` method, the number of snapshots to be retained at one time is calculated per client, database name, and NetBackup appliance.
Off-host backup	An off-host backup shifts the burden of backup processing onto a separate backup agent, such as an alternate client. This shift reduces the effect on the client's computing resources ordinarily caused by a local backup. The backup agent reads the data from the client disk and writes it to storage. On UNIX, an off-host backup can also be directed to a NetBackup media server, or third-party copy device.
Block-level incremental backup	On UNIX, a Block-Level Incremental (BLI) Backup uses the change tracking capabilities of the Veritas File System (VxFS) Storage Checkpoint feature. In a BLI backup, only the changed blocks of data are backed up, not the entire file or file system. A BLI backup saves time, decreases the amount of backup media that is required, and significantly reduces CPU and network overhead during backups. You can perform a BLI backup with or without RMAN.

Table 7-1 Snapshot Client features used with NetBackup for Oracle *(continued)*

Feature	Description
Proxy copy	A proxy copy is a special type of backup in which the NetBackup for Oracle agent manages the control of the data transfer. During the backup and restore operations, the proxy copy enables the agent to manage the entire data movement between the disks that contain the data files and the storage devices that NetBackup manages. Backups and restores remain tightly integrated with Oracle and its catalog, greatly simplifying administration tasks.
File-based operations	Oracle provides the list of files that require backup or restore to NetBackup for Oracle with Snapshot Client. More information is available. See "NetBackup for Oracle file-based operations" on page 171.
Stream-based operations	Stream-based operations are the standard NetBackup implementation of conventional NetBackup for Oracle backup and restore. More information is available. See "NetBackup for Oracle stream-based operations" on page 170.

Proxy copy

A proxy copy is a special type of backup in which the NetBackup for Oracle agent manages the control of the data transfer. During the backup and restore operations, proxy copy enables the agent to manage the entire data movement between the disks that contain the data files and the storage devices that NetBackup manages.

With proxy copy, RMAN provides a list of files that require backup or restore to the NetBackup for Oracle agent. The agent determines how the data is moved and when to move the data. Proxy copy is an extension to Oracle's Media Management API.

Backups and restores remain tightly integrated with RMAN and its catalog, which greatly simplifies administration tasks.

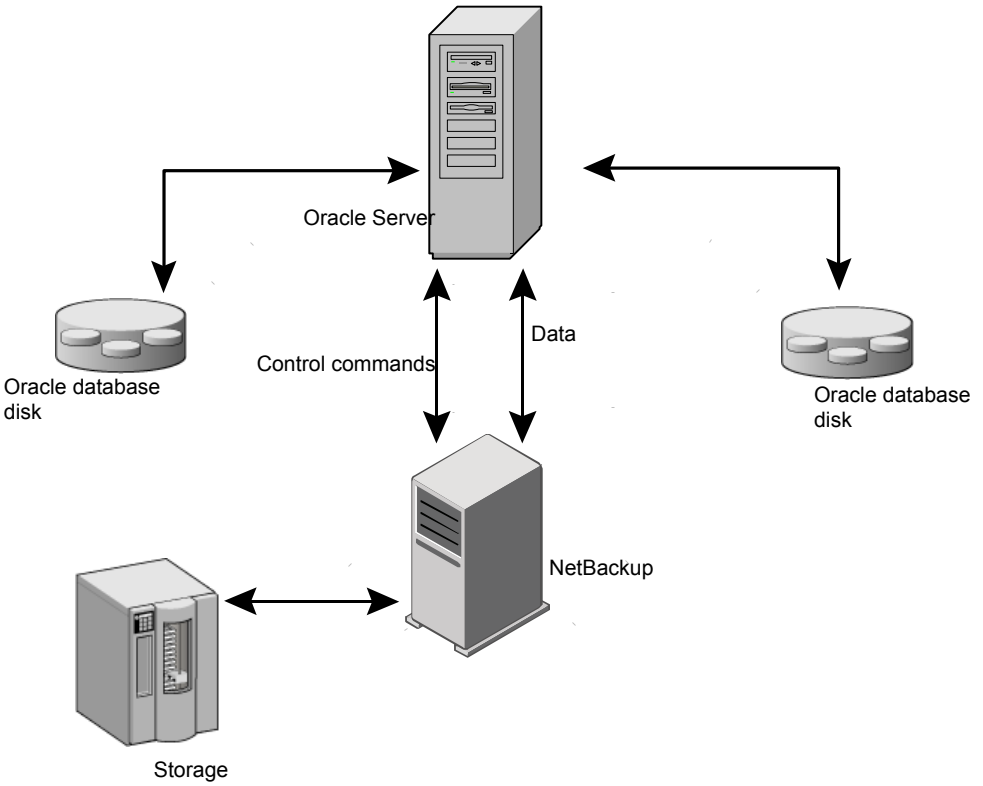
NetBackup for Oracle stream-based operations

Stream-based operations are the standard NetBackup implementation of conventional RMAN backup and restore. In a stream-based backup, NetBackup

moves the data that the server process provides. NetBackup captures the data stream content that RMAN provides. If the user has specified multiple streams, then RMAN opens multiple streams and NetBackup catalogs them as separate images.

Figure 7-1 represents a stream-based backup or restore.

Figure 7-1 NetBackup for Oracle RMAN stream-based backup or restore

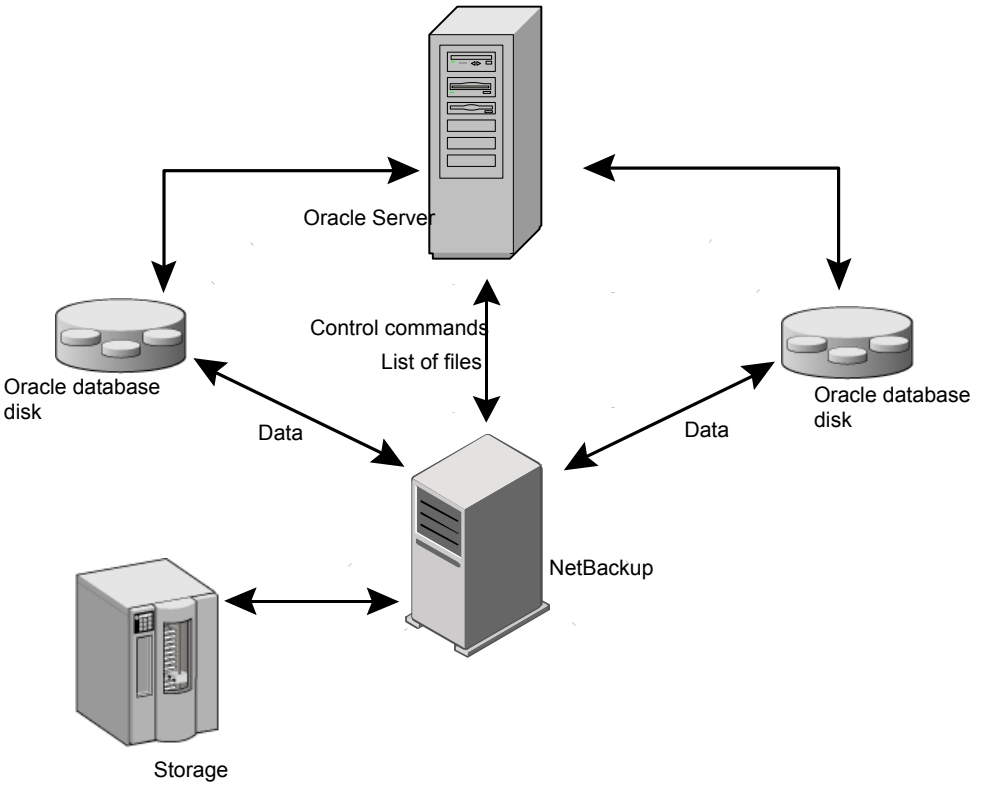


NetBackup for Oracle file-based operations

File-based operations are the NetBackup for Oracle with Snapshot Client implementation of Oracle proxy copy backups and restores. In a file-based operation, RMAN provides the list of files that require backup or restore to NetBackup for Oracle with Snapshot Client. NetBackup for Oracle with Snapshot Client performs the data movement.

Figure 7-2 represents a file-based backup or restore.

Figure 7-2 NetBackup for Oracle with Snapshot Client file-based backup or restore



How NetBackup for Oracle with Snapshot Client works

NetBackup users or schedules start database backups or restores. The Oracle Intelligent Policy automatically generates an RMAN script. The script- or template-based policy uses a template or a shell script in the backup selections list of the Oracle policy. A template-based policy uses the template to generate the RMAN script. The template or the shell script specifies backup or restore commands for the Oracle Recovery Manager (RMAN) to use when you perform the backup or restore on the client.

The RMAN `backup proxy` command initiates a proxy copy backup of the specified objects. The objects that can be backed up using the proxy copy functionality depend

on the Oracle version. RMAN translates the objects into the physical file names and provides a list of file names to NetBackup for Oracle.

See "Database objects supported by advanced backup methods" on page 173.

The agent checks that the policy it uses for the backup is configured with the appropriate Snapshot Client attributes. The agent then initiates file-based backups of the Oracle files and uses the NetBackup Snapshot Client interface to perform the data movement.

When Oracle performs proxy copy backups, it puts the data files being backed up into backup mode. NetBackup then creates a snapshot of the files. After the snapshot has been created, the NetBackup for Oracle agent signals back to Oracle to take the data files out of backup mode. The data files being backed up are in backup mode only for the period of time necessary to capture a snapshot of the data.

About the NetBackup for Oracle backup and restore operations

For a backup operation, the NetBackup for Oracle agent performs the following steps:

- Receives a list of files to back up from RMAN.
- A unique backup file name identifies each file in the NetBackup catalog. To ensure that this procedure occurs, use the `format` operand to give each data file a unique name.
- Queries the policy to check whether the Snapshot Client policy attributes are specified.
- Initiates a configured number of Snapshot Client backups and waits until the jobs are completed.
  See "About NetBackup multistreaming" on page 174.

For a restore operation, the NetBackup for Oracle agent performs the following steps:

- Receives a list of files to restore from RMAN.
- Sends a restore request to the NetBackup server for all files in the list.
- Waits for NetBackup to restore all files in the file list.

Database objects supported by advanced backup methods

Oracle controls the kinds of database objects that can be backed up by proxy copy and, therefore, what NetBackup can back up using Snapshot Client backup methods. Oracle allows proxy copy backups of databases, tablespaces, and data files. With Oracle 10g releases and later, Oracle also allows proxy copy backups of archived

redo logs. As a result, NetBackup can use file-based Snapshot Client backup methods to back up these objects.

For control files, Oracle RMAN performs conventional stream-based backups only. NetBackup for Oracle must use stream-based backups for control files even when you use Snapshot Client methods for the other database objects.

The Oracle Intelligent Policy handles both stream-based and file-based components. File-based and stream-based backups require different configurations. When configuring your NetBackup for Oracle with Snapshot Client backups, be sure to configure a policy that allows both stream-based and file-based backups.

About NetBackup multistreaming

On the initial call, NetBackup for Oracle with Snapshot Client returns a special entry to RMAN indicating that it supports proxy copy. It also indicates to RMAN that it supports an unlimited number of files to be proxy-copied in a single proxy copy session. The number of channels that are allocated for the RMAN `backup proxy` command does not control the degree of parallelism for proxy backups. RMAN uses only one channel for proxy copy backups except when a specific configuration is used.

The `NB_ORA_PC_STREAMS` variable controls the number of proxy copy backup streams to be started. By default, the agent initiates one backup job for all files. If the RMAN `send` command passes `NB_ORA_PC_STREAMS`, NetBackup for Oracle splits the files into the number of groups that the variable specifies based on the file size. The agent attempts to create streams of equal size and determines the number of processes that run to perform the backup.

RMAN multiple channels

If you allocate multiple channels for an RMAN proxy copy backup session, RMAN uses only one channel to perform a proxy backup of all objects. All other channels can be used for a stream-based (non-proxy) backup of the control file or archived redo logs.

See “Proxy backup examples” on page 177.

Restoring data files to a new location

NetBackup for Oracle with Snapshot Client can restore the data files that are backed up by proxy to a new location. The new location can be specified by using the RMAN `set newname` command or `ALTER DATABASE RENAME DATAFILE` statement before a restore is initiated. For example, to restore a data file for tablespace `TEST` to a new location, you can use the following RMAN commands:

```
RUN
 {
 allocate channel t1 'SBT_TAPE';
 sql 'alter tablespace TEST offline immediate'
 # restore the datafile to a new location
 set newname for datafile '/oradata/test.f' to
 '/oradata_new/test.f';
 restore tablespace TEST;
 # make the control file recognize the restored file as current
 switch datafile all;
 recover tablespace TEST;
 release channel t1;
 }
```

The RMAN procedure for the data files that are backed up by proxy is the same as for conventionally backed up data files. RMAN knows that the data files were backed up by proxy, and it issues a proxy restore request to NetBackup for Oracle, which restores the data files to the new location. For more information on the required procedure, see your Oracle documentation.

Redirecting a restore to a different client

The procedure for restoring a proxy backup to a different destination client is the same as the procedure for stream-based, non-proxy backups.

Symbolic links and raw data files (UNIX)

NetBackup for Oracle with Snapshot Client backs up and restores the data files that consist of symbolic links and regular files. Both the symbolic link and the file are backed up and restored. However, if you selected **Retain snapshots for instant recovery** then the symbolic link must reside on the same file system as the data file. When you use instant recovery, if the symbolic link resides on a different file system than the data file it points to, the restore fails.

NetBackup for Oracle with Snapshot Client backs up and restores data files created on raw partitions.

Quick I/O data files (UNIX)

NetBackup for Oracle with Snapshot Client backs up and restores Quick I/O Oracle data files. A Quick I/O file consists of two components: a hidden file with space allocated for it and a link that points to the Quick I/O interface of the hidden file.

On the backup, NetBackup for Oracle with Snapshot Client follows the symbolic link and backs up both components of the Quick I/O file: the symbolic link and the hidden file.

On the restore, NetBackup for Oracle with Snapshot Client restores both components from the backup image. If one or both of the components are missing, NetBackup for Oracle with Snapshot Client creates the missing component(s).

RMAN incremental backups

You can use proxy copy backups as a part of the incremental strategy with conventional non-proxy RMAN backups. RMAN lets you create a proxy copy incremental level 0 backup. This backup can be the base for subsequent RMAN traditional incremental backups (level 1-*n*). To accomplish this backup, perform a snapshot proxy copy (file-based) level 0 incremental backup and follow with an RMAN traditional (stream-based) level 1-*n* incremental backup.

In Oracle 10g it is possible to track changed blocks using a change tracking file. Enabling change tracking does produce a small amount of database overhead, but it greatly improves the performance of incremental backups. Use the `ALTER DATABASE ENABLE BLOCK CHANGE TRACKING; sqlplus` command to enable block change tracking on the database.

In the following example, the first `run` command initiates a proxy copy backup of tablespace `tbs1`. NetBackup for Oracle uses a snapshot file-based backup to perform a full tablespace backup. RMAN designates this backup as eligible for incremental level 1-*n* backups. The second `run` command initiates a traditional non-proxy level 1 incremental backup of the same tablespace `tbs1`. In this case, NetBackup for Oracle performs a stream-based backup.

```
run {
allocate channel t1 type 'SBT_TAPE';
backup
    incremental level 0
    proxy
    format 'bk_%U_%t'
    tablespace tbs1;
release channel t1;
}

run {
allocate channel t1 type 'SBT_TAPE';
backup
    incremental level 1
    format 'bk_%U_%t'
```

```
    tablespace tbs1;
release channel t1;
}
```

Proxy backup examples

The Oracle Intelligent Policy automatically creates the RMAN proxy script. In some instances, you need to create a custom script specific to your environment.

The following examples show how to use multiple channels in RMAN scripts with proxy backups.

Table 7-2 Proxy backup examples

Backup example	Sample script

This RMAN sample script initiates a whole database backup, which includes the control file. RMAN starts one proxy copy backup session by sending a list of all data files to the NetBackup for Oracle agent on channel `t1`.	`run {`
	`allocate channel t1 type 'SBT_TAPE';`
	`send 'NB_ORA_PC_STREAMS=3';`
	`backup proxy`
	`format 'bk_%U_%t'`
	`(database);`
	`release channel t1;`
	`}`
	
	The agent splits the files into three streams and initiates a file-based backup for each stream. After the proxy backup is done, RMAN starts a non-proxy conventional backup of the control file on channel `t1`.

Table 7-2 Proxy backup examples *(continued)*

Backup example	Sample script

This RMAN sample script initiates a whole database backup, which includes the control file. RMAN starts one proxy copy backup session by sending a list of all data files to the NetBackup for Oracle agent on channel `t1`. The agent splits the files into three streams and initiates a file-based backup for each stream. At the same time, RMAN starts a non-proxy conventional backup of the control file on channel `t2`.	`run {`
	`allocate channel t1 type 'SBT_TAPE';`
	`allocate channel t2 type 'SBT_TAPE';`
	`send 'NB_ORA_PC_STREAMS=3';`
	`backup proxy`
	`format 'bk_%U_%t'`
	`(database);`
	`release channel t1;`
	`release channel t2;`
	`}`
	
	If the RMAN recovery catalog is not used, the version of the control file being backed up does not contain information about the current backup. To include the information about the current backup, back up the control file as the last step in the backup operation. This step is not necessary if the recovery catalog is used.
	
	`Run {`
	`allocate channel t1 type 'SBT_TAPE';`
	`backup`
	`format 'cntrl_%s_%p_%t'`
	`current controlfile;`
	`release channel t1;`
	`}`

Table 7-2 Proxy backup examples *(continued)*

Backup example	Sample script

In this sample script, RMAN initiates two proxy copy backups sequentially on channel `t1`. It starts a proxy backup of tablespace `tbs1` data files. After the backup is done, it starts another proxy backup of tablespace `tbs2` data files.	`run {`
	`allocate channel t1 type 'SBT_TAPE';`
	`backup proxy`
	`format 'bk_%U_%t'`
	`(tablespace tbs1);`
	`backup proxy`
	`format 'bk_%U_%t'`
	`(tablespace tbs2);`
	`release channel t1;`
	`}`
	
	This configuration can cause problems if the sequential backups create snapshots on the same or a separate volume that share a snapshot resource specification. In such a situation, issue a single `backup` command such as the following which specifies both tablespaces rather than two separate `backup` commands:
	
	`run {`
	`allocate channel t1 type 'SBT_TAPE';`
	`backup proxy`
	`format 'bk_%U_%t'`
	`(tablespace tbs1, tbs2);`
	`release channel t1;`
	`}`

In this example, RMAN distributes proxy copy backups over two channels. It creates two proxy copy backup sessions sending `tbs1` data files on channel `t1` and `tbs2` data files on channel `t2`. Such a method is useful if you want to specify different NetBackup configurations for each channel. In this example, each `send` command specifies a different policy that is sent to the proxy backups. Each of the proxy backups uses this policy.	`run {`
	`allocate channel t1 type 'SBT_TAPE';`
	`send 'NB_ORA_POLICY=policy1';`
	`allocate channel t2 type 'SBT_TAPE';`
	`send 'NB_ORA_POLICY=policy2';`
	`backup proxy`
	`format 'bk_%U_%t'`
	`(tablespace tbs1 channel t1);`
	`(tablespace tbs2 channel t2);`
	`release channel t1;`
	`release channel t2;`
	`}`

About configuring Snapshot Client with NetBackup for Oracle

This topic explains how to configure snapshot and instant recovery backups for the Oracle policy. For information on how a snapshot method is automatically selected and details on the types of backup methods, see the NetBackup Snapshot Client Administrator's Guide.

Snapshot backups do not back up all database objects. Your backup configuration must include one or more automatic schedules to perform snapshot backups and one or more application schedules to perform stream-based backups. This configuration ensures that the entire database can be restored successfully.

For snapshot or instant recovery backups, configure the following policies and schedules as follows:

- A Oracle policy with the following attributes:
  - Snapshot methods for the file systems in which the database files reside.
  - A backup method on the policy attributes dialog box.
  - An Automatic Full Backup schedule to perform snapshot and off-host backups of the database.
  - (Conditional) For script- or template-based policies: An Application Backup schedule to back up the transaction logs.

To use NAS snapshot with NetBackup for Oracle, the Oracle database must be installed and configured to work in a NAS environment.

If you want to use a SnapVault storage unit, make sure that the storage unit is configured before you start configuring the NAS snapshot policy.

For more information about NAS snapshot and SnapVault, see the NetBackup Snapshot Client Administrator's Guide.

Configuration requirements for snapshot backups with NetBackup for Oracle

Each agent has its own hardware requirements, software requirements, compatibility with certain features, and the snapshot methods that are supported. Special requirements apply for specific types of backups. See the NetBackup Snapshot Client Administrator's Guide and the Veritas Support website for more information. Familiarize yourself with this information before you configure any snapshot backups.

The following list highlights some of the requirements that pertain to database agents:

- Snapshot Client backups do not back up all database objects. Your backup configuration must include schedules to perform snapshot and stream-based backups. This configuration ensures that the entire database can be restored successfully.
- On UNIX, the user identification and group identification numbers (UIDs and GIDs) associated with the files to be backed up must be available. The UID and GID must be available to both the primary client and the alternate backup client. The UID on the primary client and the alternate backup client must be the same. Similarly, the GID on the primary client and the alternate backup client must be the same.

  Note: The UID number can be different than the GID number.

- Allocate different areas for data files, archived redo logs, and the control file for database activities. Write the data files to their own repository because it is required for an instant recovery point-in-time rollback. Only data files can exist on the volume or the file system that you want to restore.
- The hardware and software that is required for the appropriate snapshot method must be installed and configured correctly.
- NetBackup Snapshot Client must be installed and configured correctly, and the license for this option must be registered.
- To perform off-host backups, perform any special configuration that is required.

Configuring a snapshot policy for NetBackup for Oracle

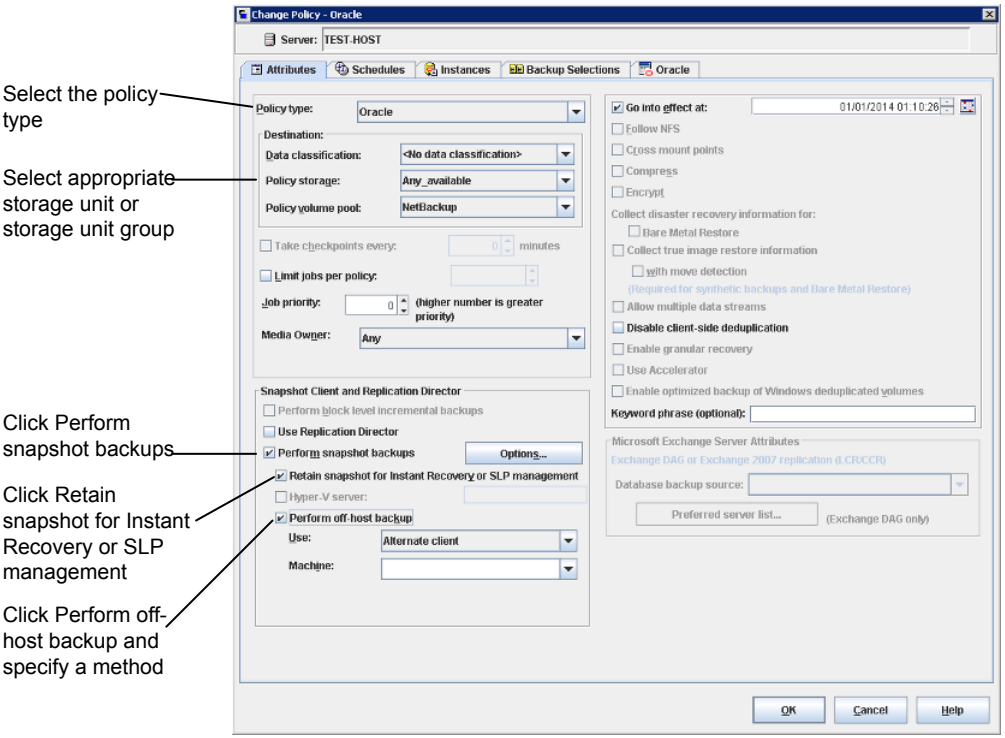
The following procedure shows how to configure a snapshot policy with optional instant recovery, snapshot retention, and off-host backup.

This procedure does not detail how to configure a snapshot policy when using a NetBackup appliance.

See “ Configuring a snapshot policy using a share on the NetBackup appliance (Copilot)” on page 185.

To configure a snapshot policy

1. Open the policy you want to configure.
2. Click on the **Attributes** tab. The following screen appears.



3. Select the Oracle policy type.
4. Select a policy storage unit from the **Policy storage** list.

   Select a policy storage unit in this step even if you plan to select **Instant Recovery Snapshots Only** later in this procedure.

   NetBackup uses this storage unit for the stream-based backups of the control files and the archived redo logs that are included in this policy.

   On UNIX, NetBackup also uses this storage unit if you select **Third Party Copy Device** when you configure the schedule.

   On UNIX, **Any_available** is not supported for the following data movers: **NetBackup Media Server** or **Third-party Copy Device**.
5. Click **Perform snapshot backups**.

6 (Optional) Click **Options** to choose a snapshot method.

By default NetBackup chooses a snapshot method for you. To choose a snapshot method, click **auto** (the default) or click one of the methods that are presented in the list.

The snapshot method that you can use depends on your hardware environment and software environment. Only certain snapshot methods are supported in certain environments. See the NetBackup Snapshot Client Administrator's Guide or the supported platforms matrix on the Veritas Support website for more information.

You can configure only one snapshot method per policy. For example, assume that you want one snapshot method for clients a, b, and c, and a different method for clients d, e, and f. Then you need to create two policies for each group of clients and select one method for each policy.

7 (Optional) Select **Retain snapshot for Instant Recovery or SLP management**.

When this option is selected, NetBackup retains the snapshot backup image on disk for later use in recovery.

8 (Optional) Select **Perform off-host backup**.

By default, the client that hosts the database performs the backup. If you want to reduce the I/O processing load on the client that hosts the database, specify an alternate client to perform the backup.

9 (Conditional) Select an off-host backup method.

The following off-host backup methods are available:

Use Alternate client (UNIX and Windows clients)	If you select **Alternate client**, also specify the name of the client to perform the backup. This option may require additional configuration. The alternate client must be a client that shares the disk array.
Use Data mover (UNIX clients only).	If you click **Data mover**, also select one of the following possible data movers: **NetBackup Media Server** **Third-Party Copy Device** **Network Attached Storage**

10 Click the **Schedules** tab.

11 Click **New**.

12 Configure a schedule for the database files.

13 (Conditional) To create only disk images, in the **Destination** panel, under **Instant Recovery**, select **Snapshots only**.

This setting suppresses NetBackup's default behavior, which is to copy the snapshot to a storage unit. When you select **Snapshots only**, NetBackup creates the on-disk snapshot copy of the database, but it does not copy the snapshot to a storage unit. The on-disk snapshot becomes the only backup copy. Note that the on-disk snapshot is not considered to be a replacement for a traditional backup.

14 (Conditional) On the **Schedules** tab, configure a backup schedule for the control files or archived redo logs.

- Oracle Intelligent Policy backup policy. Configure an **Archived Redo Log Backup** schedule for this policy.
- Script- or template-based backup policy. Configure an **Application Backup** schedule for this policy.

NetBackup uses this storage unit for the stream-based backups of the control files and the logs that are included in this policy. NetBackup copies the database's control files and archived redo logs to the storage unit you select.

For UNIX clients, if you selected **Third-Party Copy Device** as an off-host backup method, click **Override policy storage unit**. Then select a non-SAN Media Manager or other storage unit type that is appropriate to back up the control files and archived redo logs.

15 Configure the Clients, instances, or instance groups.

- Oracle Intelligent Policy backup policy. On the **Instances and Databases** tab, specify the instances or instance group, to be included in this policy.
- Script- or template-based backup policy. On the **Clients** tab, specify the clients to be included in this policy.

16 On the **Backup Selections** tab, specify the correct setup depending on policy setup.

- Oracle Intelligent Policy backup policy. Use the radio button to select **Whole Database**, **Partial database – Tablespaces**, **Partial database – Datafiles**, **Fast Recovery Area**, **Database Backup Shares**, or **Whole Database - Datafile Copy Share** when using this type of policy.
- Script- or template-based backup policy. Specify the backup template or backup script when you use this type of policy.

More information is available about how to use templates and scripts for a NetBackup for Oracle policy with Snapshot Client.

See "About Snapshot Client effects" on page 194.

17 Configure other attributes and add any additional schedules and backup selections.

Configuring a snapshot policy using a share on the NetBackup appliance (Copilot)

Note: This feature requires a NetBackup appliance running software version 2.7.1 or later.

Use the following procedure to configure an Oracle snapshot policy that uses **Database Backup Shares** or **Whole Database - Datafile Copy Share** options. This procedure uses the Oracle Intelligent Policy, which makes configuration easier.

To configure a snapshot policy using a NetBackup appliance share

1 Open the policy you want to configure or create a new policy.

Do not use the **Policy Configuration Wizard** when performing this procedure.

2 Select the **Attributes** tab.

3 Select **Oracle** as the policy type if this policy is new.

4 Select a policy storage unit from the **Policy storage** list.

- **Policy storage**

Oracle combines snapshots (proxy) and stream-based backups as part of the same backup. The storage that is indicated here is used for the stream-based part of the **Database Backup Shares** or **Whole Database - Datafile Copy Share** backup.

Select a storage lifecycle policy that is configured to contain the stream-based (non-snapshot) part of the database backup. The storage must use a storage lifecycle policy that is configured for non-snapshot backups.

5 Select **Perform snapshot backups**.

6 Click **Options** to choose a snapshot method.

When you use the **Database Backup Shares** or **Whole Database - Datafile Copy Share** options, `remote_vxfs` is the only valid snapshot method.

Note: If there is more than one backup share that is associated with the database instance, then **Maximum Snapshots** should be set to number of recovery points you want multiplied with number of backup shares. Example: If you want three recovery snapshot points and the database instance is associated with two backup shares then **Maximum Snapshots** should be set to 6.

---

7 Select **Retain snapshot for Instant Recovery or SLP management**.

8 Select the **Schedules** tab.

9 Click **New**.

10 Configure a **Full** schedule for the database backup shares.

- **Type of backup**: Select **Full Backup**. The **Full Backup** is used for both the snapshot part of the database and the non-snapshot (stream-based) part of the Oracle database.
- **Override policy storage selection**: Enable and select the SLP that is configured for a snapshot. (A snapshot SLP is one in which the first operation is a snapshot operation.) This option must be enabled so that the schedule storage overrides the policy storage with a snapshot SLP.
- **Retention**: The retention for the streamed data is based on the non-snapshot SLP that was indicated as the **Policy storage** in Step 4.
  - The non-snapshot SLP specified on the policy storage in Step 4 determines the retention for the streamed data.
  - The snapshot SLP that is specified as the schedule storage (**Override policy storage selection**) determines the retention for the snapshot data.

When **Database Backup Shares** or **Whole Database - Datafile Copy Share** is selected, it is recommended that an SLP is set up to backup from the snapshots and copy snapshots to a storage unit. NetBackup retains the snapshot backup image on disk for later use in SLP management.

Click **OK** to save the schedule.

11 (Optional) On the **Schedules** tab, configure an **Archived Redo Log Backup** schedule for the archived redo logs.

12 Select the **Instances and Databases** tab and specify the instances to back up. The policy must include at least one instance. To continue to use the Oracle Intelligent Policy method, select either **Protect instances** or **Protect instance groups**.

13 On the **Backup Selections** tab, use the radio button to select **Database Backup Shares** or **Whole Database - Datafile Copy Share** options.

14 (Optional) Configure other attributes and add any additional schedules.

See "Configuring a snapshot policy for NetBackup for Oracle" on page 181.

See "About Snapshot Client effects" on page 194.

See "Configuring an OIP using a share on the NetBackup appliance (Copilot)" on page 86.

Restoring NetBackup for Oracle from a snapshot backup

The following topics describe how to restore files, volumes, and file systems from a snapshot backup:

- See "About restoring individual files from a NetBackup for Oracle snapshot backup" on page 187.
- See "About NetBackup for Oracle restores of volumes and file systems using snapshot rollback" on page 188.
- See "Performing a NetBackup for Oracle point-in-time rollback restore from a SnapVault backup (UNIX)" on page 189.
- See "Performing a snapshot rollback restore from the Java or Windows interface" on page 188.

About restoring individual files from a NetBackup for Oracle snapshot backup

Data that is backed up with Snapshot Client methods is restored in the same way as data that is backed up without Snapshot Client methods.

Use this procedure for the files that were backed up with, or without, instant recovery enabled. In all cases, Oracle determines the files that were backed up, and it initiates a corresponding restore request to the database agent.

If instant recovery is enabled, NetBackup attempts to restore the file by using the unique restore methods available with the instant recovery feature. The type of restore method that NetBackup uses depends on your environment and the type

of backup performed. If NetBackup is unable to use any of the instant recovery methods, it restores the file in the typical manner. Data is copied from the snapshot to the primary file system. Information on the instant recovery methods that NetBackup uses is available.

See the NetBackup Snapshot Client Administrator's Guide.

About NetBackup for Oracle restores of volumes and file systems using snapshot rollback

You can request that an entire volume or an entire file system be restored from an instant recovery Snapshot backup. This type of a restore is called a point in time rollback. All the data in the snapshot is restored; single file restore is not available in a rollback.

See the NetBackup Snapshot Client Administrator's Guide.

The following considerations are relevant for NetBackup for Oracle restores:

- Snapshot rollback overwrites the entire volume.
- With NetBackup for Oracle, snapshot rollback always performs file verification. The agent checks for the following:
  - The requested files (number and names) are identical to those in the snapshot
  - The primary volume does not contain any files that were created after the snapshot was made

  If verification fails, the rollback aborts with status 249.

Performing a snapshot rollback restore from the Java or Windows interface

This topic describes how to perform a snapshot rollback restore from the Java or Windows interface.

To perform a snapshot rollback restore from the Java or Windows interface

1. Open the Backup, Archive, and Restore interface.
2. Select one of the following:
   - In the Java interface, click the **Restore Files** tab.
   - In the Windows interface, select **File > Select Files and Folders to Restore**.

     If the data file you want to restore has not changes since it was backed up, the rollback may fail. Initiate the restore from a script and use the FORCE option.

3 Select **Actions > Select Restore Type > Point in Time Rollback**.

4 Use the NetBackup for Oracle recovery wizard for the restore.

See "About NetBackup for Oracle restores" on page 128.

Performing a snapshot rollback restore using a script or RMAN command

This topic describes how to perform a snapshot rollback restore using a script or RMAN command.

Note: If the data file you want to restore has not changed since it was backed up, the rollback may fail. Initiate the restore from a script and use the Oracle FORCE option.

To specify a snapshot rollback restore using a script or RMAN command, follow this example:

- If you want to use a shell script or RMAN command, set a new variable, `NB_PC_ORA_RESTORE=rollback`
  - Example:

```
RUN {
     allocate channel t1 'SBT_TAPE';
     send 'NB_ORA_PC_RESTORE=rollback';
     sql 'alter tablespace TEST offline immediate'
     restore tablespace TEST;
     recover tablespace TEST;
     release channel t1;
}
```

Performing a NetBackup for Oracle point-in-time rollback restore from a SnapVault backup (UNIX)

When you select a point-in-time rollback restore from a SnapVault backup, NetBackup restores the entire subvolume (qtree) to a new subvolume (qtree) on the primary host. The restore does not overwrite the existing subvolume. File verification is not performed.

The format of the new subvolume name is as follows:

mountpointname`_restore.`*timestamp*

For example: `subvol1_restore.2005.05.19.10h49m04s`

To perform a NetBackup for Oracle point-in-time rollback restore from a SnapVault backup (UNIX)

1. Unmount the original subvolume, which is the subvolume that the restore process did not overwrite.
2. Rename the original subvolume.
3. Rename the new subvolume with the name of the original.
4. Mount the new subvolume on the client. Use the `ALTER DATABASE RENAME DATAFILE` command to point to the restored data file on the newly created subvolume.

About configuring NetBackup for Oracle block-level incremental backups on UNIX

If only a small portion of a database changes on a daily basis, full database backups are costly in terms of time and media. The Block-Level Incremental (BLI) Backup interface extends the capabilities of NetBackup to back up only the file system blocks that contain changed data blocks.

A database BLI backup is done at the file system block level, which means only changed file blocks are backed up. Unchanged blocks within the files are not backed up. The VxFS Storage Checkpoint facility tracks changed blocks in real time. Accordingly, a BLI backup does not need to search the entire volume for the modified blocks at backup time. BLI backup saves time, decreases the amount of backup media that is required, and significantly reduces CPU and network overhead during backups. In addition, BLI backup allows more frequent backups, so backup images are more up to date.

BLI backup is particularly useful for any large databases that are sized in terms of hundreds of gigabytes or terabytes. Most traditional methods for database backup require that any change in the database—no matter how small—requires that the entire database is backed up. With BLI backup, only modified blocks (or file) need to be backed up.

The recommended method for performing BLI backups is the proxy BLI agent with RMAN. This method supports the other features of NetBackup for Oracle, including the policy types and schedules and the convenience of the template generation wizard. It also remains tightly integrated with RMAN and its catalog, which greatly simplifies administration tasks.

You can also perform backups with the script-based BLI method without RMAN.

See “About script-based block-level incremental (BLI) backups without RMAN” on page 274.

Note: Veritas recommends that Snapshot Client users who want to perform BLI backups use BLI with RMAN.

NetBackup for Oracle also provides a method for BLI backup without RMAN that uses scripts to put tablespaces into, and take them out of, backup mode. This method is not recommended, and it requires a significantly different configuration. But for Oracle 12c, using script-based BLI backups without the use of RMAN are not supported.

How BLI works with NetBackup for Oracle (UNIX)

NetBackup supports BLI full backups and BLI incremental backups of Oracle databases.

BLI backup supports two types of incremental backups: differential and cumulative. Full, differential incremental, and cumulative incremental backups are specified as part of the policy schedule configuration. When a restore is performed, NetBackup restores an appropriate full backup. Then it applies the changed blocks from the incremental backups.

Restoring any of the incremental backup images requires NetBackup to restore the last full backup image and all the subsequent incremental backups. The restore process continues until the specified incremental backup image is restored. NetBackup performs this restore process automatically, and it is completely transparent. The media that stored the last full backup and the subsequent incremental backups must be available, or the restore cannot proceed.

Note that restoring a file rewrites all blocks in that file. The first subsequent differential incremental backup and or all subsequent cumulative incremental backups back up all the blocks in the restored file. After an entire database is restored, the first subsequent backup results in a full backup.

The restore destination can be a VxFS, UFS (Solaris), JFS (AIX), or HFS (HP-UX) file system. The destination VxFS file system does not need to support the Storage Checkpoint feature to restore files. However, a VxFS file system with the Storage Checkpoint feature is needed to perform BLI backups of the restored data.

This topic uses the following terms to describe BLI backups:

- Full Backup.
  A backup in which NetBackup backs up each database file completely, not just data blocks that have changed since the last full or incremental backup.
- Cumulative BLI Backup.
  This type of backup is a backup of all the changed blocks in the database files since the last full backup. A cumulative BLI backup image contains only the data blocks of database files that changed since the last full backup. A cumulative

BLI backup can reduce the number of incremental backup images that must be applied during a restore operation. This speeds up the restore process.

- Differential BLI backup.
  A backup in which NetBackup performs a backup of only those data blocks (within the database files) that changed since the last backup. The previous backup can be of type full, cumulative incremental, or differential incremental.

When NetBackup initiates BLI backups, it creates, manages, and uses the appropriate Storage Checkpoints of the filesystem(s) hosting the Oracle data file systems. These Storage Checkpoints identify and maintain a list of modified blocks.

About the Storage Checkpoint facility and NetBackup for Oracle

The BLI backup methodology uses the Storage Checkpoint facility in the Veritas File System (VxFS). This facility is available through the Storage Foundation for Oracle.

The VxFS Storage Checkpoint facility keeps track of the file blocks modified by the database since the last backup. NetBackup with BLI backup leverages this facility to back up only changed blocks for an incremental backup. The entire volume or file is not backed up.

VxFS Storage Checkpoint is a disk-efficient and I/O-efficient snapshot of file systems. A Storage Checkpoint provides a consistent, stable view of a file system at the instant when the file system was snapped or checkpointed. Instead of making a physically separate copy of the file system, a Storage Checkpoint tracks changed file system blocks. Disk space is saved and I/O overhead is significantly reduced.

Because the changed blocks are tracked, the VxFS Storage Checkpoint enables BLI backups. VxFS Storage Checkpoint facility provides a consistent view of file systems, which allows BLI backup to freeze the database image during database backups.

The Storage Checkpoint operation is similar to the snapshot file system mechanism. However, the Storage Checkpoint persists after a system restart which is unlike a snapshot. Also, the Storage Checkpoint operation is totally transparent to backup administrators. The Checkpoint image is managed and available only through NetBackup or through the VxDBA utility for database backup available with the Veritas Storage Foundation.

For more information on Storage Checkpoints, see the Veritas Storage Foundation Administrator's Guide.

You can take a Storage Checkpoint while the database is online or offline. To take a Storage Checkpoint while the database is online, you must enable archive log mode. During the creation of the Storage Checkpoint, all tablespaces are placed in backup mode.

Configuration requirements for BLI backups with NetBackup for Oracle

Before you configure BLI backups, make sure that your configuration meets the following requirements:

- NetBackup for Oracle is installed, licensed, and configured.
- NetBackup Snapshot Client is installed and configured, and the master server must have a valid license for this option.
- Veritas Storage Foundation for Oracle must be installed and configured.
- Veritas File System must have Storage Checkpoint licensed.

For more information on requirements, see the NetBackup Snapshot Client Administrator's Guide.

Configuring policies for BLI backups with NetBackup for Oracle

This topic explains how to configure BLI backups for Oracle policies. BLI backups do not back up all database objects. Include schedules to perform stream-based backups.

Your backup configuration must ensure that the entire database can be successfully restored.

See "Configuration requirements for BLI backups with NetBackup for Oracle" on page 193.

To configure a policy for BLI backups, configure the following:

- The BLI backup method on the policy attributes dialog box.
- An **Automatic Backup** schedule to perform full and incremental snapshot backups of the data files.
- An **Application Backup** schedule to perform a stream-based backup of control files and archived redo logs. These files are backed up with standard RMAN operations.

To configure a policy for BLI backups

1. Open the policy you want to configure.
2. Click the **Attributes** tab.
3. From the **Policy Type** list, choose **Oracle**.
4. Select a **Policy storage**.
5. Select **Perform block level incremental backups**.
6. To configure schedules, click the **Schedules** tab.

Oracle does not support proxy backups of database control files and archived redo logs. To perform a whole database proxy backup, which automatically includes a backup of the control file, configure the following:

- One or more automatic backup schedules to perform proxy BLI backups of the data files.
- An Application Backup schedule type to back up the control files and archived redo logs.

7 On the **Clients** tab, specify clients to be backed up with this policy.

8 On the **Backup Selections** tab, specify the template or script.

About the types of NetBackup for Oracle BLI backups

NetBackup performs BLI backups with Automatic Full Backup, Automatic Differential Incremental Backup, and Automatic Cumulative Incremental Backup schedules.

If a user initiates a backup and the proxy schedule name is not specified on the request with the `NB_ORA_PC_SCHED` environment variable, the NetBackup server starts an Full Backup schedule by default.

NetBackup for Oracle checks that a full backup was performed before it proceeds with an incremental backup. If the NetBackup scheduler or user initiates an incremental backup, and NetBackup for Oracle finds no record of a full backup using the same policy, it performs a full backup.

To ensure that it has a proper set of images to restore, NetBackup performs a full backup when it encounters the following situations:

- If the number of backup streams that is specified changed from the previous backup. This change can be made in the `NB_ORA_PC_STREAMS` environment variable.
- If NetBackup does not have a valid full backup image for the same policy in its database. For example, this situation can occur if images were expired.
- If a new file was added to or deleted from the list of files for an incremental backup.

NetBackup for Oracle always initiates a full backup under these conditions, even if you want to perform an incremental backup.

About Snapshot Client effects

The following topics describe how the Snapshot Client software affects backup types, schedule properties, and templates. Snapshot Client also affects scripts and environment variables.

How Snapshot Client software affects backup types

The backup types available on the **Schedules** tab of the policy play a different role for NetBackup for Oracle with Snapshot Client backups.

See Table 7-3 on page 195.

Table 7-3 Backup types for Oracle policies

Backup type	Description
Application Backup	An application backup applies only to template- or script-based policies not the Oracle Intelligent Policies. The Application Backup schedule stores stream-based backups. The Default-Application-Backup schedule is automatically configured as an Application Backup schedule.
Full backup Differential incremental backup, Cumulative incremental backup	The full and incremental backup schedule types automatically start the backups by running the NetBackup for Oracle RMAN scripts or templates. They also store the snapshot backups. **Note:** For most snapshot types, any automatic backup schedule (full, cumulative, or differential) results in a full volume snapshot. BLI is the only snapshot method that can perform an incremental backup.

How Snapshot Client software affects schedule properties

Some schedule properties have a different meaning for Snapshot Client database backups than for a regular database backup. For a description of other schedule properties, see the information that is specific to standard database agent backups.

See “About schedule properties ” on page 91.

Table 7-4 explains the properties for Snapshot Client backups.

Table 7-4 Schedule properties

Property	Description
Retention	Automatic Schedules: Determines how long to retain history of the backups that the master server schedules and also how long to retain snapshot backups. Application Schedules: Determines how long to retain stream-based backups.

Table 7-4 Schedule properties *(continued)*

Property	Description
Multiple Copies	For snapshot backup, configure **Multiple copies** on the automatic backup schedule. For stream-based backups, configure **Multiple copies** on the Application backup schedule.
Frequency	Determines how often an Automatic schedule executes a backup. Does not apply to Application backup schedules.

How Snapshot Client software affects templates and scripts

You can use a template that the NetBackup for Oracle wizard creates to perform backups with Snapshot Client. After they are created, templates reside on the NetBackup master server and are available for use by other NetBackup for Oracle clients.

See "About creating templates and shell scripts" on page 105.

In the RMAN template generation wizard, the **Specify Maximum Limits** selection options on the backup limits screen are not applicable for snapshot backups. RMAN uses these options only for conventional stream-based backups. If the template includes archived redo logs, NetBackup does use this option to back up the logs.

Whether you use a template or script, you must enable the advanced backup method for your clients. Configure this method on the **Attributes** tab of the policy. At run time, the agent checks the policy attributes to determine if a Snapshot Client backup method is configured and performs a proxy file-based backup. A template defaults to a single session for proxy backups.

If you use a script, the script must reside on each client that is included in the policy. Include the RMAN `backup proxy` command in the script to perform the advanced backup method. Sample scripts are included with the installation.

NetBackup for Oracle with Snapshot Client environment variables

You can use environment variables to change the number of streams the proxy copy session uses or to specify an alternate backup schedule.

The following list shows the variables that you can to set that are specific to NetBackup for Oracle with Snapshot Client:

NB_ORA_PC_SCHED	The NetBackup for Oracle schedule NetBackup uses for a proxy copy file-based backup. (This schedule can be Full, Differential Incremental, or Cumulative Incremental backup type). For scheduled backups, this variable is passed from the scheduler. When you create an RMAN template with the NetBackup for Oracle RMAN template generation wizard, this variable is automatically created in the template.
NB_ORA_PC_STREAMS	Specifies the number of backup streams that NetBackup starts simultaneously in each proxy copy session. When a backup starts, NetBackup groups all data files into a specified number of backup streams that are based on the file sizes. NetBackup tries to create streams of equal size. The default value for NB_ORA_PC_STREAMS is 1. Only a user can set this variable. When you create an RMAN template using the NetBackup for Oracle RMAN template generation wizard, this variable is automatically created in the template when you provide a value for the **Number of parallel streams**.

For NetBackup for Oracle with Snapshot Client, the order of precedence for environment variables is the same as for standard NetBackup for Oracle. Refer to the instructions for how to configure the NetBackup and the user variables.

See "About configuring the run-time environment" on page 98.

NetBackup for Oracle installs sample scripts in the following location:

Windows:

install_path\NetBackup\dbext\oracle\samples\rman

UNIX:

/usr/openv/netbackup/ext/db_ext/oracle/samples/rman

The following are the scripts for NetBackup for Oracle with Snapshot Client that show how to configure the required variables:

Windows:
`hot_database_backup_proxy.cmd`
UNIX:
`hot_database_backup_proxy.sh`
	This script sets the environment and calls RMAN with the appropriate command to perform a whole database proxy backup. When NetBackup runs a schedule, it sets the environment variables that NetBackup for Oracle with Snapshot Client uses. The script shows how to use the RMAN `send` command to pass the NetBackup for Oracle with Snapshot Client variables with a vendor-specific quoted string.

Windows:
`hot_tablespace_backup_proxy.cmd`
UNIX:
`hot_tablespace_backup_proxy.sh`
	This script sets the environment and calls RMAN with the appropriate command to perform a tablespace proxy backup.

If you use scripts, use the `send` command to pass the environment variables to the agent. The following example uses the `send` command to specify the values for `NB_ORA_PC_SCHED` and `NB_ORA_PC_STREAMS`:

```
run {
 allocate channel t1 type 'SBT_TAPE';
 send 'NB_ORA_PC_SCHED= sched, NB_ORA_PC_STREAMS= number';
 backup proxy
 (database format 'bk_%U_%t');
 }
```

For more information, see the sample scripts that are provided with the agent.

See "Proxy backup examples" on page 177.

About Oracle support for Replication Director

Replication Director can be used to create snapshots of the Oracle database and replicate the snapshots to other NetApp disk arrays. To use Replication Director, the Oracle database must exist on a NetApp NAS disk array. (It is not supported on SAN storage at this time.)

Oracle snapshot backups that use Replication Director are supported on UNIX platforms only.

The administrator can create an Oracle policy to use Replication Director by using either the following methods:

- The Oracle Intelligent Policy (recommended).
  See "Configuring an Oracle Intelligent Policy using Replication Director" on page 199.

- Create a script- or template-based Oracle policy.
  See "Configuring a script- or template-based Oracle policy" on page 205.

Table 7-5 describes the differences between the two methods:

Table 7-5 Differences in Oracle snapshot policy setup

Configuration	Oracle Intelligent Policy	Script- or template-based Oracle policy
Scripts	■ All scripts that are necessary to protect all parts of the database are automatically generated at run-time. ■ The administrator does not need to know how to configure RMAN scripts. ■ The retention levels for the different parts of the database are automatically assigned	■ NetBackup can continue to use custom scripts to perform database backups. ■ The administrator must know how to configure RMAN scripts. ■ The administrator must set the retention levels for the different parts of the database correctly. ■ The administrator must ensure that a snapshot of the proxy data is created.
Schedules	The administrator configures only one schedule that backs up all parts of the database and sets the correct retention automatically. The **Archived Redo Log** schedule is not supported with a snapshot backup.	The administrator must configure two schedules with two retentions: ■ One **Full Backup** schedule to back up the snapshot (proxy) data part of the database. ■ One **Application Backup** schedule to back up the stream-based part of the Oracle database. The **Archived Redo Log** schedule is available with a configured script.
Backups	User-directed backups are not supported. To attempt a user-directed backup (results in a status 240 (no schedules of the correct type exist in this policy).	User-directed backups are supported.
Load balancing	RAC load balancing is not supported.	RAC load balancing is supported.

Configuring an Oracle Intelligent Policy using Replication Director

Use the following procedure to configure an Oracle snapshot policy that uses Replication Director. This procedure uses the Oracle Intelligent Policy, which makes configuration easier.

To create an Oracle Intelligent Policy

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Policies**.
2. On the **Actions** menu, click **New > New Policy**.
3. Type a unique name for the new policy in the **Add a New Policy** dialog box and click **OK**.

   Do not use the **Policy Configuration Wizard** to configure a policy for Replication Director.

4. Select the **Attributes** tab. The following items are specific to creating an Oracle policy for snapshots with Replication Director:

   - **Policy type**
     For NetBackup to perform Oracle backups, select **Oracle**. An **Oracle** tab appears.
   - **Policy storage**
     Oracle combines snapshots (proxy) and stream-based backups as part of the same backup. The storage that is indicated here is used for the stream-based part of the Replication Director backup.
     Select a storage lifecycle policy that is configured to contain the stream-based (non-snapshot) part of the database backup. The storage must use a storage lifecycle policy that is configured for non-snapshot backups.
   - **Use Replication Director**
     Enable **Use Replication Director** to automatically select other options that Replication Director requires:
     - **Perform snapshot backups**: Ensures that the policy creates snapshots of the disk array.
     - **Retain snapshots for Instant Recovery or SLP management**: Ensures that the policy retains the snapshot after the backup completes.
     - **Options** button

Snapshot Type

- **Auto** (default): The OpenStorage partner uses the best snapshot technology available to that partner to create the snapshot.
- **Differential**: The OpenStorage partner creates a snapshot that is completely dependent on the source. This parameter is based on copy-on-write technology. The device creates a cache object to maintain the original blocks of the snapshot when the blocks are modified.
- **Plex**: The OpenStorage Partner creates a snapshot that is completely independent of the source snapshot. This option is based on mirror-break-off technology. When a mirror device is attached to the source, the contents of the mirror device is exactly the same as the source device. When the relationship is broken between the two, the mirror device is separated from the source. The mirror device acts as a point-in-time copy.
- **Clone**: The OpenStorage Partner creates an independent copy of the volume. The copy process can take some time as the entire copy must be complete. The snapshot that is created is independent of the source.

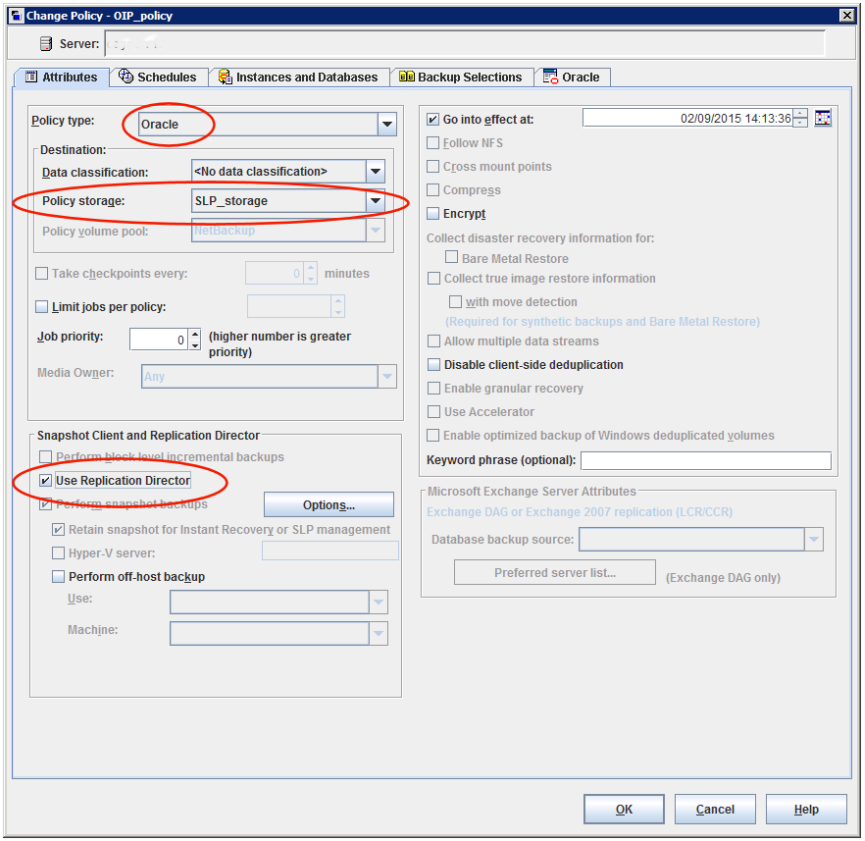
Maximum Snapshots

Sets the maximum number of snapshots to be retained at one time.

The default setting is one. Choose the number of snapshots that is appropriate for your environment. Note that the maximum number of snapshots on a NetApp volume is 255.

When the maximum is reached, snapshot rotation occurs: The next snapshot causes the oldest to be deleted.

Managed by SLP retention is automatically selected if the **Fixed** or the **Expire after Copy** retention is currently selected in the SLP.



5 Select the **Schedules** tab. Create one schedule:

- **Type of backup**: Select **Full Backup**. The **Full Backup** is used for both the snapshot (proxy) part of the database and the non-snapshot (stream-based) part of the Oracle database.
  The Oracle Intelligent Policy does not support the snapshot of an **Archived Redo Log Backup**. To take a snapshot of the archived redo logs, use the script- or template-based Oracle policy method.

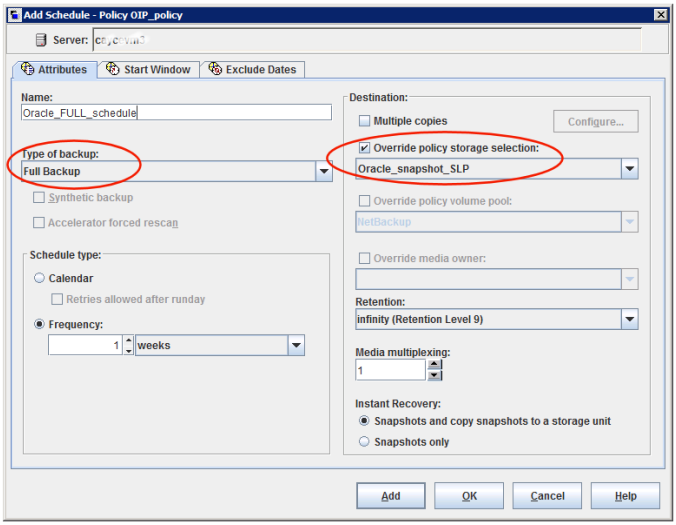
  Note: Unless creating Block Level Incremental (BLI) backups, always select **Full Backup** to create snapshots of the Oracle database.

- **Override policy storage selection**: Enable and select the SLP that is configured for snapshot replication. (A snapshot SLP is one in which the

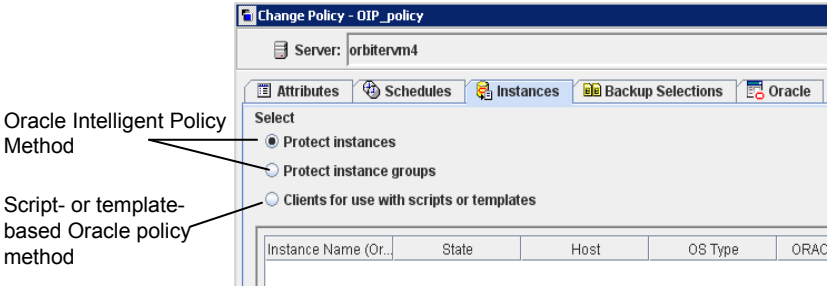
first operation is a snapshot operation.) This option must be enabled so that the schedule storage overrides the policy storage with a snapshot SLP.

- **Retention**: The retention for the streamed data is based on the non-snapshot SLP that was indicated as the **Policy storage** in Step 4.
  - The non-snapshot SLP specified on the policy storage in Step 4 determines the retention for the streamed data.
  - The snapshot SLP that is specified as the schedule storage (**Override policy storage selection**) determines the retention for the snapshot data.

Click **OK** to save the schedule.



6 Select the **Instances and Databases** tab and specify the instances to back up. The policy must include at least one instance. To continue to use the Oracle Intelligent Policy method, select either **Protect instances** or **Protect instance groups**.



7 Select the **Backup Selections** tab. Select the parts of the database to back up. Note that the selection applies to all listed instances.

The following can be selected for the policies that use Replication Director:

- **Whole database**: Backs up the entire database (default).
- **Partial database - Tablespaces**: Backs up the tablespaces.
- **Partial database - Datafiles**: Backs up the data files.
- **Fast Recovery Area (FRA)**: Do not select for a policy that uses Replication Director.
- **Database Backup Shares**: Do not select for a policy that uses Replication Director.
- **Whole Database - Datafile Copy Share**: Do not select for a policy that uses Replication Director.

Note: If you back up the partial database, and later want to perform a Point-in-time rollback restore, make sure that you select all of the tablespaces or data files from a partition in the **Backup Selections**.

For copy-back restores, this is not a requirement.

---

8 Select the **Oracle** tab to configure Oracle RMAN properties.

9 When the policy configuration is complete, click **OK**.

Configuring a script- or template-based Oracle policy

Use the following procedure to configure an Oracle snapshot policy that uses Replication Director. This procedure uses an Oracle policy type, but does not automatically generate the necessary scripts. It allows the administrator to use custom scripts and templates.

To create a script- or template-based Oracle policy

1. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Policies**.
2. On the **Actions** menu, click **New > New Policy**.
3. Type a unique name for the new policy in the **Add a New Policy** dialog box and click **OK**.

   Do not use the **Policy Configuration Wizard** to configure a policy for Replication Director.

4. Select the **Attributes** tab. The following items are specific to creating an Oracle policy for snapshots with Replication Director:

   - **Policy type**
     For NetBackup to perform Oracle backups, select **Oracle**. An **Oracle** tab appears.
   - **Policy storage**
     Oracle combines snapshots (proxy) and stream-based backups as part of the same backup. The storage that is indicated here is used for the stream-based part of the Replication Director backup.
     Select the storage that is configured to contain the stream-based (non-snapshot) part of the database backup. The storage can be either a storage lifecycle policy that is configured for non-snapshot backups, or a disk or Media Manager unit.
   - **Use Replication Director**
     Enable **Use Replication Director** to automatically select other options that Replication Director requires:
     - **Perform snapshot backups**: Ensures that the policy creates snapshots of the disk array.
     - **Retain snapshots for Instant Recovery or SLP management**: Ensures that the policy retains the snapshot after the backup completes.
     - **Options** button

Snapshot Type

- **Auto** (default): The OpenStorage partner uses the best snapshot technology available to that partner to create the snapshot.
- **Differential**: The OpenStorage partner creates a snapshot that is completely dependent on the source. This parameter is based on copy-on-write technology. The device creates a cache object to maintain the original blocks of the snapshot when the blocks are modified.
- **Plex**: The OpenStorage Partner creates a snapshot that is completely independent of the source snapshot. This option is based on mirror-break-off technology. When a mirror device is attached to the source, the contents of the mirror device is exactly the same as the source device. When the relationship is broken between the two, the mirror device is separated from the source. The mirror device acts as a point-in-time copy.
- **Clone**: The OpenStorage Partner creates an independent copy of the volume. The copy process can take some time as the entire copy must be complete. The snapshot that is created is independent of the source.

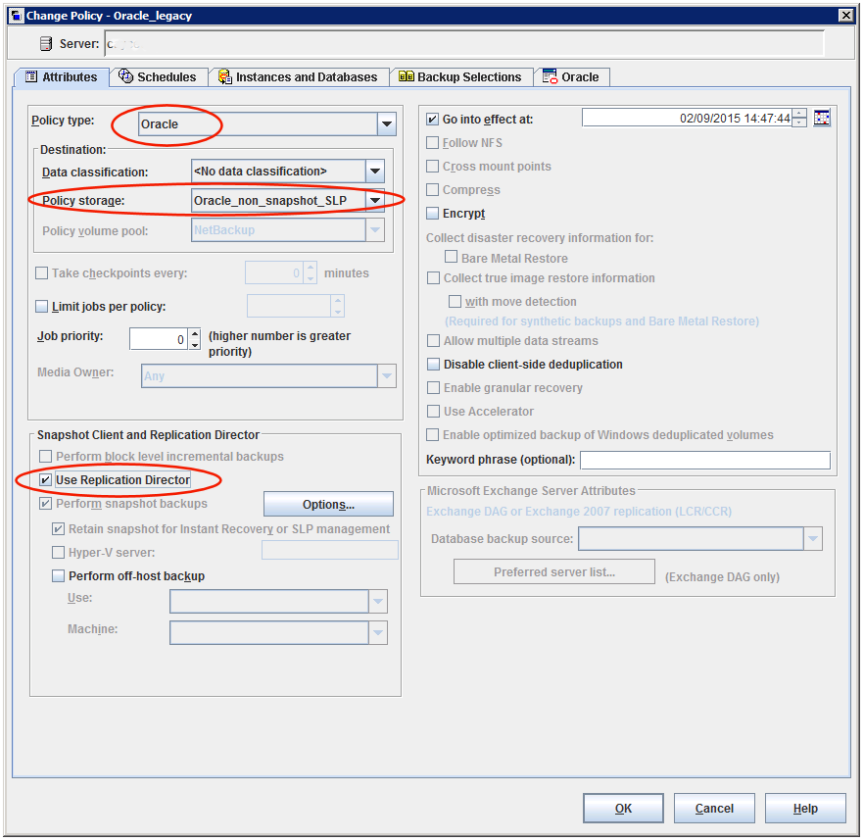
Maximum Snapshots

Sets the maximum number of snapshots to be retained at one time.

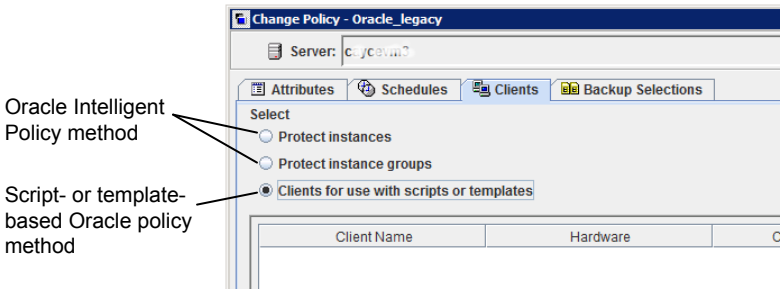
The default setting is one. Choose the number of snapshots that is appropriate for your environment. Note that the maximum number of snapshots on a NetApp volume is 255.

When the maximum is reached, snapshot rotation occurs: The next snapshot causes the oldest to be deleted.

Managed by SLP retention is automatically selected if the **Fixed** or the **Expire after Copy** retention is currently selected in the SLP.



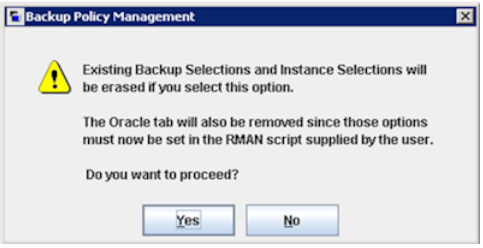
5 Select the **Instances and Databases** tab and specify the instances to back up. Select **Clients for use with scripts and templates**. If either of the other two are selected, the Oracle Intelligent Policy is used and the scripts are created automatically.



After selecting the **Clients for use with scripts and templates** option, a message appears that describes the effect of this choice:

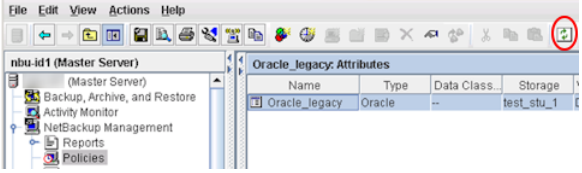
- Existing selections (if any) for this policy are erased.
- The **Oracle** tab is removed from this policy.
- Another effect is that the **Selections** tab turns into the **Clients** tab.

Click **Yes** to continue Oracle policy configuration.



6 Click **Yes** to save and close the entire policy.

7 In the **NetBackup Administration Console**, select the policy and click the refresh button in the toolbar.

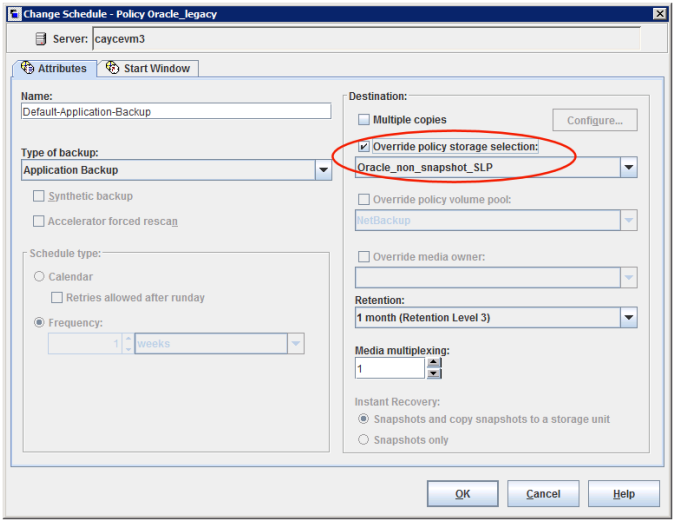


8 Re-open the policy and select the **Schedules** tab.

Modify the **Default-Application-Backup** schedule:

- **Override policy storage selection**: Enable and select a non-snapshot storage unit or a non-snapshot SLP. This is most likely the storage unit that is specified on the **Attributes** tab. Indicating it here makes the selection explicit.
- **Retention**: The policy or SLP indicates the retention for the backup:
  - When the storage is an SLP, the SLP determines the retention and no selection is possible here.
  - When the storage is not an SLP, the schedule determines the retention and a selection is possible here.

Click **OK** to save the schedule.

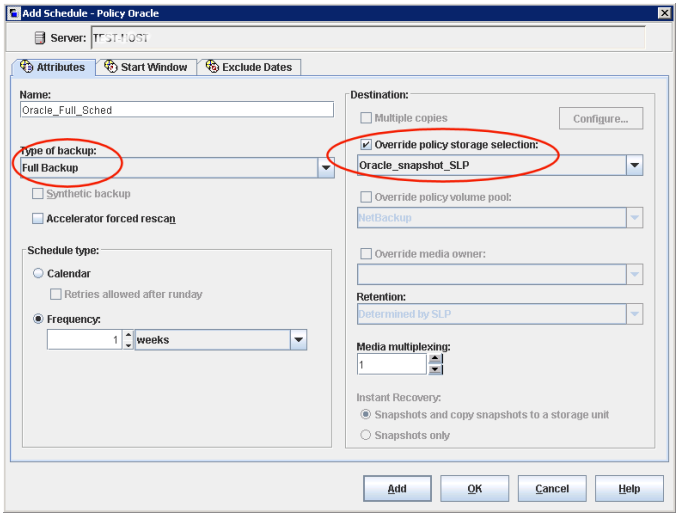


Create one **Full Backup** schedule:

- Name the schedule.
- **Type of backup**: Select **Full Backup**.

  Note: Unless creating Block Level Incremental (BLI) backups, always select **Full Backup** to create snapshots of the Oracle database.

- **Override policy storage selection**: Enable and select the SLP that is configured for snapshot replication.
- **Retention**: The SLP indicates the retention for the backup.



9 Configure the schedule in the **Start Window** tab and the **Exclude Days** tab.

Click **OK** to save and close the schedule.

10 Select the **Clients** tab. By default, the **Clients for use with scripts or templates** option is selected for this script- or template-based Oracle policy.

11 Add the client name(s) that contain the Oracle database and indicate the operating system of each.

12 Select the **Backup Selections** tab. Specify the script or the template that NetBackup should use. Indicate only one script or one template.

13 When the policy configuration is complete, click **OK**.

Chapter 8

Troubleshooting

This chapter includes the following topics:

About troubleshooting NetBackup for Oracle

NetBackup, NetBackup for Oracle, and the Oracle Recovery Manager (RMAN) all provide reports on database backup, archive, and restore operations. These reports are useful for finding the errors that are associated with those applications.

For more information about debug logs and reports, refer to the NetBackup Administrator's Guide, Volume I.

About NetBackup for Oracle troubleshooting steps

When troubleshooting NetBackup for Oracle problems, the following items are referred to as the API:

- On Windows, `orasbt.dll` is called the API.
- On UNIX, the `libobk` module is called the API. Many media manager vendors also call the `libobk` module DMO (Database Module).

To perform this procedure, ensure that NetBackup is properly installed and configured:

To perform general troubleshooting steps

1. When verifying your installation, ensure that the NetBackup for Oracle binaries exist.

   On UNIX, these are located in `/usr/openv/netbackup/bin`.

   The binaries are as follows:

On Windows: *install_path*\NetBackup\bin\bphdb.exe On UNIX: `bphdb`	The binary resides on the client and both the NetBackup scheduler and the graphical interface uses the binary to start backups. The main purpose of `bphdb` is to run an Oracle Intelligent Policy or a template or a shell script that calls `rman`, `bporaexp`, or `bporaimp`.
On Windows: `c:\Windows\System32\orasbt.dll`	Provides the functions that RMAN can call.
On UNIX: `libobk`	A shared library module that contains the functions that RMAN can call. This library is loaded when RMAN is started. The name of this binary depends on the operating system. See "About linking Oracle RMAN with NetBackup for UNIX" on page 37.

2. For the Backup, Archive, and Restore interface and the Oracle Intelligent Policy, verify that the following binaries exist.

   On Windows: *install_path*\NetBackup\bin\bpdbsbora.exe

   On Windows: *install_path*\NetBackup\bin\bpubsora.exe

   On Windows: *install_path*\NetBackup\bin\dbsbrman.dll

   On UNIX: `/usr/openv/netbackup/bin/bpdbsbora`

   On UNIX: `/usr/openv/netbackup/bin/bpubsora`

   On UNIX: `/usr/openv/lib/libdbsbrman.so` (`libdbsbrman.sl` on HP-UX)

3. Check that both the NetBackup server and client software work properly. That is, check that normal operating system files can be backed up and restored from the client. The NetBackup client must be running the same version of software as the NetBackup server.

4. The logs can become very large, especially `bpdbm`. Ensure that enough free disk space exists in the log directory disk partition.

5 Check that the following NetBackup log directories exist:

- On the Windows client: `bpdbsbora`, `bporaexp`, `bporaimp`, `bpubsora`, `dbclient`, `bphdb`, `bpfis`, `bplist`, and `bpcd`.
- On the UNIX client: `bpdbsbora`, `bporaexp` (or `boraexp64`), `bporaimp` (or `boraimp64`), `bpubsora`, `dbclient`, `bphdb`, `bpfis`, and `bpcd`. These directories must have `777` permissions.
- On the master server: `bprd` and `bpdbm`.
- On the host with the storage unit: `bpbrm` and `bptm`.

The `VERBOSE` level must be 5.

6 On UNIX, confirm the `/usr/openv/netbackup/logs/user_ops` directory and the subdirectories have 777 permissions. They must exist and be accessible for the applications to operate correctly.

See "Permissions for NetBackup for Oracle log directories" on page 47.

NetBackup debug logs and reports

The NetBackup server and client software let you enable detailed debugging logs. The information in these log files can help you troubleshoot the problems that occur outside of either the database agent or RMAN.

Note the following with regard to these logs:

- These logs do not reveal the errors that occur when RMAN is running unless those errors also affect NetBackup. Oracle may (or may not) write errors in the application to the NetBackup logs. Your best sources for Oracle error information are the logs provided by Oracle.
- Generally, each debug log corresponds to a NetBackup process and executable. However, for an RMAN backup, the debug log is created in the `dbclient` directory, which has no corresponding executable.

More detailed information about the debug log files is available.

See the NetBackup Troubleshooting Guide.

Also refer to the following file:

Windows:

install_path\NetBackup\logs\README.debug file

UNIX:

/usr/openv/netbackup/logs/README.debug file

NetBackup provides other reports that are useful in isolating problems. One such report is All Logs Entries on the server. Information on server reports is available.

See the NetBackup Administrator's Guide, Volume I.

Enabling the debug logs manually (Windows)

To create the NetBackup for Oracle for Windows database agent logs manually

1 Create the following directories on the client:

- `bpubsora`
  For any Oracle database instance browse problems when a template is created for backup or restore.

  install_path\NetBackup\logs\bpubsora

- `bphdb`
  For any backup that is initiated from an automated schedule on the master server.

  install_path\NetBackup\logs\bphdb

- `bpdbsbora`
  For any template-based backup or restore, including OIP and Guided Recovery.

  install_path\NetBackup\logs\bpdbsbora

- `dbclient`
  For any backup or restore using RMAN.

  install_path\NetBackup\logs\dbclient

- `bpbkar`
  For any snapshot backup.

  install_path\NetBackup\logs\bpbkar

- `tar`
  For any snapshot restore.

install_path\NetBackup\logs\tar

2 Verify the user or group that the Oracle process (process that loads orasbt.dll) has appropriate permissions to write to the following directories if they exist. If the following directories do not exist, the directories are created automatically with the correct permissions.

install_path\NetBackup\logs\user_ops

install_path\NetBackup\logs\user_ops\dbext

install_path\NetBackup\logs\user_ops\dbext\logs

Also verify that the user or group that the Oracle process runs as has appropriate permissions to write to the log directories in step 1.

3 On the NetBackup server or servers, create the debug log directories for the legacy processes that interact with the Oracle agent.

On the master server:

install_path\NetBackup\logs\bprd

On the media server or servers:

install_path\NetBackup\logs\bpbrm

install_path\NetBackup\logs\bptm

4 The debug logs for unified processes on the server and the client hosts are created automatically by NetBackup.

NetBackup writes unified logs to install_path\NetBackup\logs.

For information on how to use logs and reports, see the NetBackup Troubleshooting Guide.

Enabling the debug logs manually (UNIX)

To create the NetBackup for Oracle for UNIX database agent logs manually

1 Create the following directories on the client:

- bpubsora
  For any Oracle database instance browse problems when a template is created for backup or restore.

  /usr/openv/netbackup/logs/bpubsora

- bphdb

For any backup that is initiated from an automated schedule on the master server.

```
/usr/openv/netbackup/logs/bphdb
```

- `bpdbsbora`

  For any template-based backup or restore, including OIP and Guided Recovery.

  ```
  /usr/openv/netbackup/logs/bpdbsbora
  ```

- `dbclient`

  For any backup or restore using RMAN.

  ```
  /usr/openv/netbackup/logs/dbclient
  ```

- `bpbkar`

  For any snapshot backup.

  ```
  /usr/openv/netbackup/logs/bpbkar
  ```

- `nbtar`

  For any snapshot restore.

  ```
  /usr/openv/netbackup/logs/tar
  ```

2 Verify the user or group that the Oracle process (process that loads `libobk`) has appropriate permissions to write to the following directories if they exist. If the following directories do not exist, the directories are created automatically with the correct permissions.

```
/usr/openv/logs/user_ops
```

```
/usr/openv/logs/user_ops/dbext
```

```
/usr/openv/logs/user_ops/dbext/logs
```

Also verify that the user or group that the Oracle process runs as has appropriate permissions to write to the log directories in step 1.

3 On the NetBackup server or servers, create the debug log directories for the legacy processes that interact with the Oracle agent.

On the master server:

`/usr/openv/logs/bprd`

On the media server or servers:

`/usr/openv/logs/bpbrm`

`/usr/openv/logs/bptm`

4 The debug logs for unified processes on the server and the client hosts are created automatically by NetBackup.

NetBackup writes unified logs to `/usr/openv/logs`.

For information on how to use logs and reports, see the NetBackup Troubleshooting Guide.

About the NetBackup for Oracle log files

Table 8-1 describes the logs that are created when you create the log directories. Use a text editor to view the contents of the logs.

The log are located in the following directories:

Windows: *install_path*`\NetBackup\logs\<cmd>`

UNIX: `/usr/openv/netbackup/logs/<cmd>`

For example, the logs for `bphdb` all appear in the *install_path*`\NetBackup\logs\bphdb` directory (Windows) or the `/usr/openv/netbackup/logs/bphdb` directory (UNIX).

Table 8-1 Log files

Log directory	Description
bphdb	The bphdb directory contains the following types of logs: ■ Windows: obk_stdout.*mmddyy*.*hhmmss*.txt UNIX: obk_stdout.*mmddyy* Unless it is redirected elsewhere, NetBackup writes template or shell script output to this file. ■ Windows: obk_stderr.*mmddyy*.*hhmmss*.txt UNIX: obk_stderr.*mmddyy* Unless it is redirected elsewhere, NetBackup writes template or shell script errors to this file. ■ Windows: *mmddyy*.log UNIX: log.*mmddyy* This log contains debugging information for the bphdb process. bphdb is the NetBackup database backup binary. It is invoked when an automatic backup schedule is run. NetBackup for Oracle uses this client process for template or shell script execution.
dbclient	The dbclient directory contains the following execution log: ■ Windows: *mmddyy*.log ■ UNIX: log.*mmddyy* This log contains debugging information and execution status for the Oracle for NetBackup client processes. On Windows, the processes are linked to the library program that is provided with NetBackup for Oracle. On UNIX, this library program is libobk.
bpdbsbora	The bpdbsbora directory contains the following execution log: ■ Windows: *mmddyy*.log ■ UNIX: log.*mmddyy* This log contains debugging information and execution status for the NetBackup for Oracle backup and recovery wizards and for the bpdbsbora command line utility. This log also contains the debugging information and execution status information that is generated when an Oracle template is run from an automatic schedule (when bphdb invokes bpdbsbora to run the template).
bporaexp64	The bporaexp (or bporaexp64 on UNIX) directory contains the following execution log: ■ Windows: *mmddyy*.log ■ UNIX: log.*mmddyy*.log

Table 8-1 Log files *(continued)*

Log directory	Description
bporaimp64	The `bporaimp` (or `bporaimp64` on UNIX) directory contains the following execution log: ■ Windows: *`mmddyy`*`.log` ■ UNIX: `log.`*`mmddyy`*

Setting the debug level on a Windows client

To control the amount of information that is written to the debug logs, change the Database debug level. Typically, the default value of 0 is sufficient. However, technical support may ask you to set the value higher to analyze a problem.

The debug logs are located in *`install_path`*`\NetBackup\logs`.

To change the amount of debug information in other log directories, set the other debug levels. For instance, Verbose.

To set the debug level on a Windows client

1. Open the **Backup, Archive, and Restore** interface.
2. Select **File > NetBackup Client Properties**.
3. Click the **Troubleshooting** tab.
4. Set the **General** debug level.
5. Set the **Verbose** debug level.
6. Set the **Database** debug level.
7. Click **OK** to save your changes.
8. Stop and start the Oracle database services. This action is necessary for `orasbt.dll` to pick up the new debug level.

Setting the debug level on a UNIX client

To control the amount of information that is written to the debug logs, change the “Database” debug level. Typically, the default value of 0 is sufficient. However, Technical Support may ask you to set the value higher to analyze a problem.

The debug logs are located in `/usr/openv/netbackup/logs`.

To set the debug level on a UNIX client

- Enter the following line in the `bp.conf` file.

  ```
  VERBOSE = X
  ```

  Where *X* is the debug level you want.

About RMAN utility logs

RMAN uses a command language interpreter, and it can be run in interactive or batch mode. You can use the following syntax to specify a log file on the command line to record significant RMAN actions:

```
msglog 'logfile_name'
```

Troubleshooting RMAN backup or restore errors

An RMAN backup error can originate from NetBackup or from Oracle, as follows:

- On the NetBackup side, an error can be from the API, from the NetBackup server or client, or from Media Manager.
- On the Oracle side, an error can be from RMAN or from the target database instance.

Veritas suggests that you use the following steps when troubleshooting a failed operation:

- Check the logs to determine the source of the error.
- Troubleshoot each stage of the backup or restore.

Verifying the RMAN script on UNIX

The following procedure describes how to verify that the RMAN script works correctly.

To verify the RMAN script

1. Use RMAN to make a backup directly to disk. Do not use NetBackup.
2. Use RMAN with NetBackup to create a backup.

3 Check the `/usr/openv/netbackup/logs/dbclient` directory permissions. They should be set to `777`.

4 Look for a log file in `/usr/openv/netbackup/logs/dbclient`.

If no log file exists, `libobk` is not linked into Oracle properly.

See "Testing configuration settings for NetBackup for Oracle" on page 114.

Troubleshooting each stage of the backup or restore

The following explains the sequence of events for an action initiated by RMAN and suggests solutions for the problems that can occur at each point in the sequence:

- `rman` starts.

  A backup or restore can be started in any of the following ways:

  - From an RMAN backup or restore initiated from the operating system prompt such as:

    ```
    rman target user/pwd[@TNS_alias] \
    rcvcat user/pwd[@TNS_alias]\
    cmdfile RMAN_script_file_name
    ```

    Where the *RMAN_script_file_name* is fully qualified.

  - Using a template that runs from the NetBackup client interface or from `bpdbsbora`.
  - Manually from the administrator interface on the master server.
  - Automatically by an automatic backup schedule.
    If an error occurs now, check the RMAN log.

- RMAN verifies its environment and then issues requests to the API.
  On Windows, some information, such as the NetBackup version, API versions, and trace file name, is registered with RMAN. An error now is usually due to a problem with client and server communication. Check the messages in the `bprd` and the `bpcd` logs for clues.
  On UNIX, some information, such as the NetBackup version, API versions, trace file name, and NetBackup signal handlers, is registered with RMAN. An error now is usually due to a problem with client and server communication. Check the messages in the `bprd`and the `bpcd` logs for clues. Also verify the `bp.conf` entries on the client.
- RMAN issues a backup or restore request.

The API gathers necessary parameters and sends the `backup` or `restore` request to the NetBackup server. The API waits until both the server and client are ready to transfer data before it returns to the request.

The API then sends this information to the master server's `bprd` process.

To troubleshoot a problem in this part of the first sequence, examine the following file:

Windows:

install_path\NetBackup\logs\dbclient*mmddyy*.log

UNIX:

/usr/openv/netbackup/logs/dbclient/log.*mmddyy*

If the `bprd` process failed, check the logs for `bprd` and `bpbrm`.

A failure now is frequently due to bad NetBackup server or Oracle policy configuration parameters.

NetBackup can usually select the correct Oracle policy and schedules. But NetBackup can select a policy or schedule in error if there are several Oracle policies in its database.

On Windows, try setting the `SERVER` and `NB_ORA_POLICY` values in the client environment.

On UNIX, try setting the `SERVER` and `POLICY` values in the `bp.conf` file on the client or by setting environment variables.

For example, the following C Shell `setenv` commands specify the Oracle policy, schedule, and server for NetBackup to use:

```
setenv NB_ORA_POLICY policyname
setenv NB_ORA_SCHED application_backup_schedule_name
setenv NB_ORA_SERV NetBackup_server
```

- RMAN issues read or write requests to the API, which then transfers data to or from the NetBackup server.

  A failure here is probably due to NetBackup media, network, or timeout errors.

- RMAN tells the API to close the session.

  The API waits for the server to complete its necessary actions (for example, it verifies the backup image) and then exits.

  An error can originate from either NetBackup or RMAN, as follows:

  - RMAN aborts if it encounters an error while it reads a data file during the backup (for example, if Oracle blocks are out of sequence). It also aborts if NetBackup sends a bad backup image during the restore.

- NetBackup might return an error code to the API if for some reason it could not complete the backup successfully.

Troubleshooting the UNIX browser interface and wizards

If you do not see the Oracle database instance in your Backup, Archive, and Restore interface, verify the following:

- A NetBackup for Oracle license is installed on the master server.
- For browsing in the restore window, the policy type must be set to Oracle.

  Perform the following actions to change the client policy type:

  - On the **Actions** menu, select **Specify NetBackup Machines and Policy type**.
  - In the **Policy type** drop-down list, select **Oracle**.
  - Click **OK**.

  On Windows, to change the client policy type:

  - On the **File** menu, select **Specify NetBackup Machines and Policy Type**.
  - On the **Specify NetBackup Machines** dialog, click the **Clients/Policy Type** tab.
  - In the **Policy Type** drop-down list, select **Oracle**.
  - Click **OK**.
- On UNIX, the `oratab` file is in the correct location (`/etc/oratab` or `/var/opt/oracle/oratab`) and contains all of the available Oracle SIDs. Although Oracle allows the use of wild cards in the `oratab` file, the NetBackup BAR GUI requires that each SID be specified.

If you have trouble connecting to the Oracle database, verify the following:

- Make sure that the database is in a mount state or an open state.
- Make sure that your login ID and password have Oracle SYSDBA or SYSBACKUP privileges. Initially, NetBackup for Oracle attempts OS Authentication to log on. If that fails, you are prompted for a user name, password, and an optional Transparent Network Substrate (TNS) alias. The user name and password you enter must have SYSDBA or SYSBACKUP privileges.
- In a clustered environment, failure to connect to the database can mean a problem with the network configuration. The browser must connect locally.

However, in some environments, all connections are considered to be remote connections, even a connection to a local database. This behavior is true for example in an Oracle Real Application Clusters (RAC) environment. In such cases, you must make the connection using a TNS alias.

In a Linux environment, Oracle backups and restores fail if the Linux logon is not the Oracle user. In such cases, Oracle generates the following message:

```
INF - ORA-19554: error allocating device, device type: SBT_TAPE, device name:
INF - ORA-27211: Failed to load Media Management Library
```

If you want to start an Oracle job as someone other than an Oracle user, augment the default shared library search path. Use the Linux `ldconfig`(8) command to add `$ORACLE_HOME/lib` to the search path.

Troubleshooting NetBackup for Oracle with Snapshot Client

Debug logs used for troubleshooting the problems that occur with NetBackup and NetBackup for Oracle have been discussed in previous areas. In addition to those logs, there are debug logs used for troubleshooting NetBackup for Oracle with Snapshot Client.

Snapshot Client backup and debug messages are written to the following subdirectories of:

Windows:

install_path\NetBackup\logs

UNIX:

/usr/openv/netbackup/logs/

The logs are as follows:

- The `bpbrm` log is on the NetBackup media server.
- The `bptm/bpdm` log is on the NetBackup media server.
- The `bpbkar` log is on the NetBackup client and alternate client.
- The `bpfis` log is on the NetBackup client and alternate client.
- The `bppfi` log is on the NetBackup client or alternate client.

Snapshot Client restore and debug messages are written to the following subdirectories on the NetBackup master server:

- The `bprestore` is almost always a client log on the NetBackup host that initiated the restore by using the `bprestore` command.
- The `bprd` is on the NetBackup master server.
- The `bpbrm` is on the NetBackup master server.
- The `bptm/bpdm` is on the NetBackup media server. Both the tape and the disk backup log to `bptm`, disk backups also log to `bpdm`.
- The `tar` is on the NetBackup client or redirected client.

Additional help for troubleshooting most installation and other issues is available in the NetBackup Snapshot Client Administrator's Guide.

See "About NetBackup for Oracle troubleshooting steps" on page 212.

Minimizing timeout failures on large database restores

Large database restores sometimes fail when multiple restore sessions compete for resources. In this situation, a restore session can be delayed while waiting for media or device access. If the delay is too long, the restore session times out. Use the following procedure to minimize session timeouts and to allow the restores to complete successfully.

To minimize timeout failures on large database restores

1. In the NetBackup Administration Console, expand **NetBackup Management > Host Properties > Clients**.
2. Double-click the client.
3. Select the **Timeouts** properties.
4. Set the **Client read timeout** property to a large value.

   The default for the **Client read timeout** setting is 300 seconds (5 minutes). For database agent clients, increase the value significantly from the recommended value.

   See the NetBackup Administrator's Guide, Volume 1.

   For example, change this setting to 30-60 minutes to minimize timeout errors.
5. Click **OK** for each client.

Note: This change may delay detecting problems during subsequent backups. Consider putting the original value back in place once any restore that requires a change is complete.

Minimizing the loading and unloading of tapes for database backups

You can minimize excessive unloading and reloading of tapes between multistreamed database backups by changing the media settings for the master or the media server.

See the NetBackup Administration Guide, Volume 1 for details.

To minimize loading and unloading of tapes

1. Open the NetBackup Administration Console.
2. Choose **Host Properties**.
3. Choose **Master Servers** or **Media Servers**.
4. Double-click on the name of the server.
5. In the left pane, click **Media**.
6. Configure the following settings:
   - **Media unmount delay**
   - **Media request delay**
     Use this variable only with non-robotic drives, such as tape stackers.

Delays in backup job transfer and completion

Sometimes you may see a Oracle backup job pause for an extended time during the data transfer. Also, the backup job may appear to hang after the transfer completes but before the job completes. The delay may be due to one of the following:

- Oracle delays
- Network issues
- Storage unit delays
- Oracle database server post-backup processing

The delays during the transfer can be especially pronounced if using large data files. Lengthy delays make it difficult for NetBackup to know if Oracle is hung or

delayed. To review setting information and delay examples, refer to the following article:

http://www.veritas.com/docs/TECH227741

To determine the cause of delays after the transfer, refer to the following article:

http://www.veritas.com/docs/TECH198864

Appendix A

Real Application Clusters

This appendix includes the following topics:

About Real Application Clusters

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.

About virtual names and NetBackup for Oracle

Users of a RAC can typically access the database by a virtual network host name. This access is dependent on the configuration of a RAC and any cluster software on which it is running.

The virtual network host name may be associated with an IP address in the following ways:

- With an IP address for a host in the cluster
- A virtual IP address for an Oracle database instance running on a host in the cluster
- A failover virtual IP address that may move between the hosts in the cluster

Backup operations may use the various virtual network host names, or the network host name of the hosts in the cluster.

To differentiate between the various network names, the following terms and definitions are used:

Host name	The network host name that is associated with a specific host in the cluster.
VIP name	The network host name that is associated with a virtual IP address specific to an instance in the cluster.
Failover name	The network host name that is associated with an IP address that is active on a running node. This network host name is the network host name that can perform a backup at this time.

Warning: Do not use a single client name if the backup is load balanced across more than one node. In a load-balanced configuration, the node that hosts the IP address to which the client name resolves, generates successful backups. However, the jobs originating from the other nodes fail with status code 54.

Oracle 11g R2 Grid Infrastructure (CRS) includes the Single Client Access Name (SCAN) feature. A single SCAN can resolve to multiple IP addresses each assigned to a different physical node in the cluster.

A SCAN can be used in a NetBackup policy that receives the Application Backup request. However, this abstraction of the client name causes backup and restore jobs to fail with status code 54. Also, the client side fails with status code 6 (backup) or status code 5 (restore).

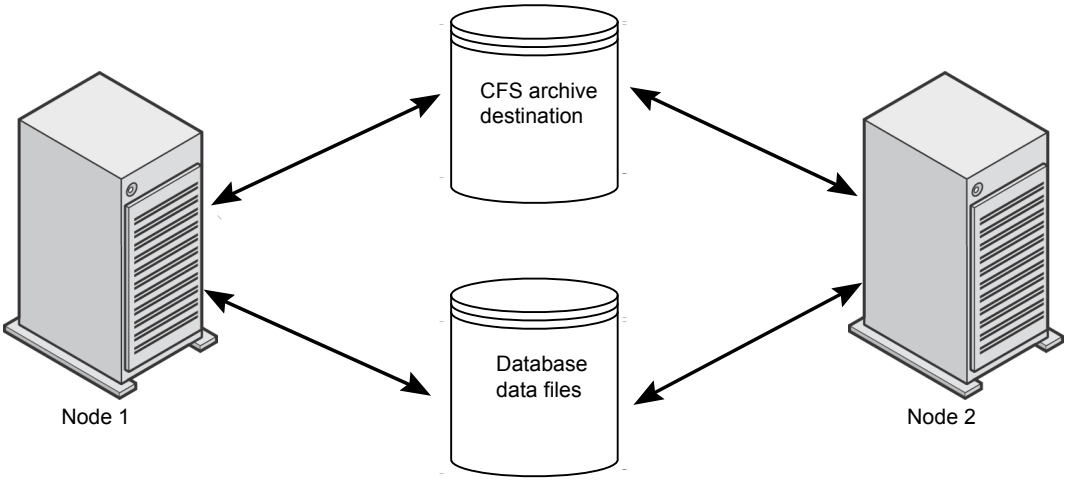
Accordingly, ensure that the client that appears in the NetBackup Oracle policy is not a SCAN. Also, ensure that any NB_ORA_CLIENT or CLIENT_NAME that the node provides in the backup request is not a SCAN. These names must reliably resolve on both the master server and the media server to an IP address. This IP address allows the server processes to connect to the node from which the backup request originated.

About RAC archiving schemes

The preferred RAC configuration uses a cluster file system archiving scheme. In this scheme, each node writes to a single Cluster File System (CFS) archived log destination and can read the archived log files of the other nodes.

Figure A-1 depicts a CFS archiving scheme.

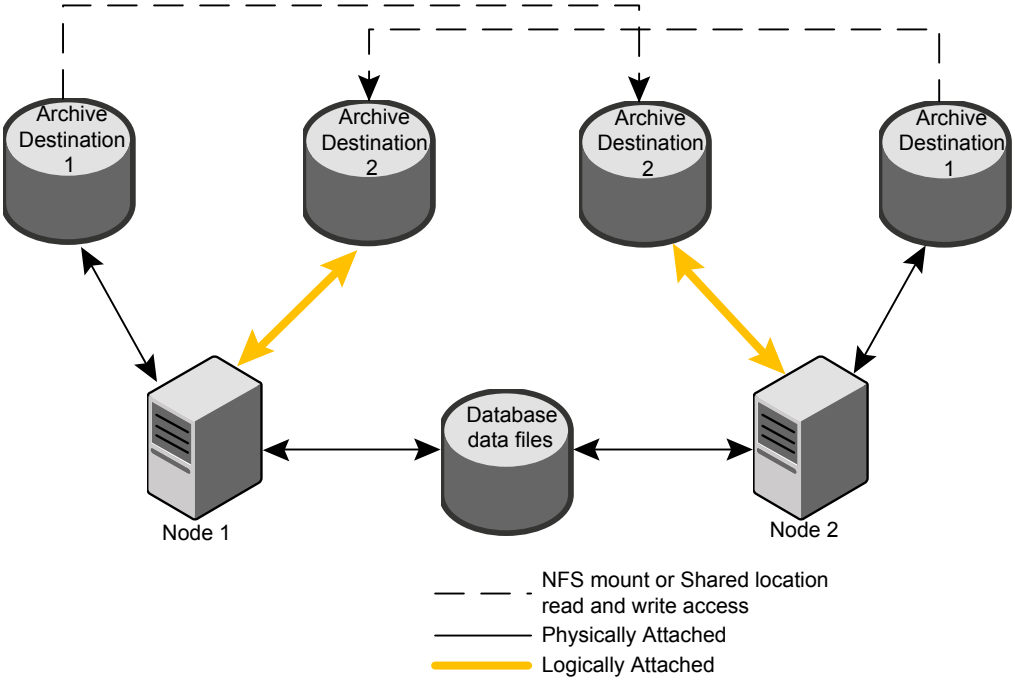
Figure A-1 CFS archiving scheme



If the CFS solution is not available, Oracle recommends a scheme like that in Figure A-2. In Figure A-2, each node archives to a local directory and writes a copy to each of the other nodes' archive directories. The locations are shared between the nodes (with read and write permissions) by NFS mounting the directory (UNIX) or sharing the locations (Windows).

Figure A-2 describes non-CFS local archiving scheme with archive sharing.

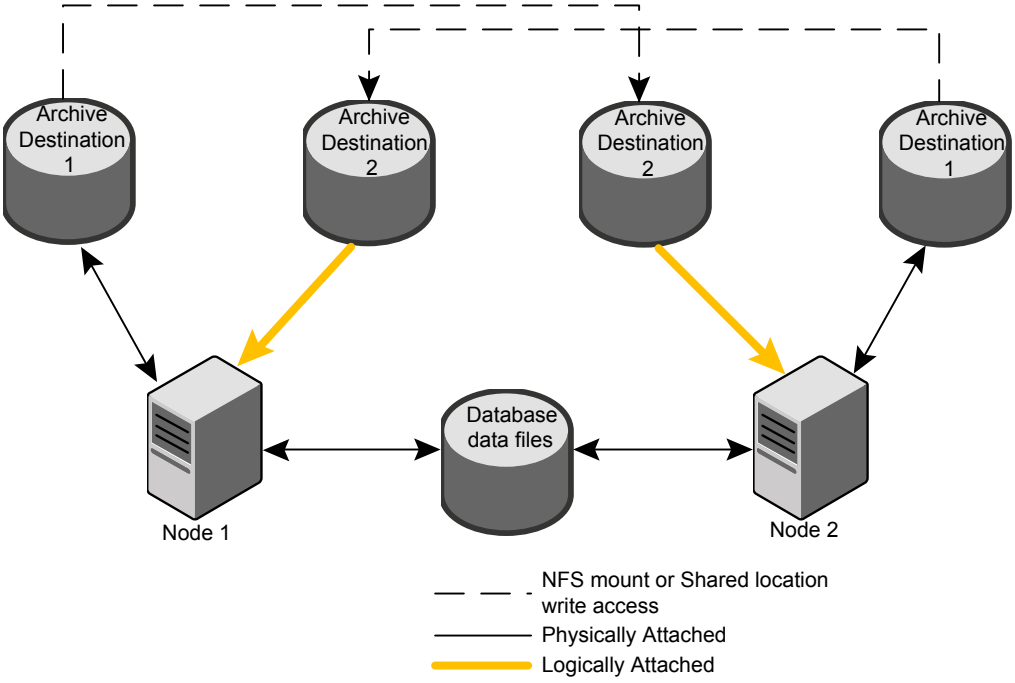
Figure A-2 Non-CFS local archiving scheme with archive sharing



A scheme similar to the previous one exists if each node archives to a local directory, and the locations are shared (read-only) with the other nodes in the cluster. These locations are shared among the nodes by NFS-mounting the directory (UNIX) or sharing the locations (Windows). Therefore, each node can read each archive destination.

Figure A-3 describes non-CFS local archiving scheme with archive read-only sharing.

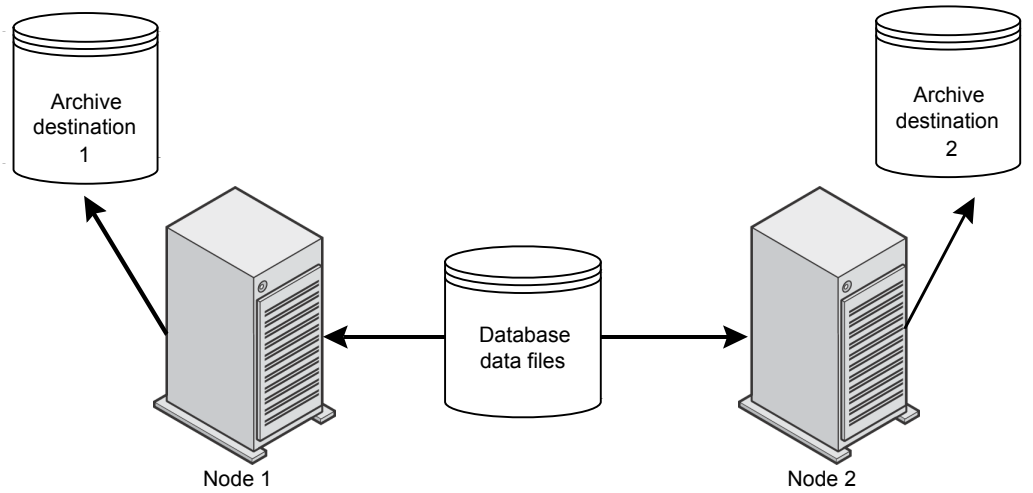
Figure A-3 Non-CFS local archiving scheme with archive read-only sharing



The simplest archiving scheme is local archiving with no sharing. Each node writes only to the local destination, and no access is given to the other nodes in the cluster.

Figure A-4 describes non-CFS local archiving scheme with no archive sharing.

Figure A-4 Non-CFS local archiving scheme with no archive sharing



For more information about configuration and additional archiving scheme examples see your Oracle documentation.

About backing up a database

If you are in a RAC environment and you chose one of the archive log schemes that are described in the previous topic, you can perform a backup with typical RMAN scripts.

In the following example, RMAN backs up the database, including all of the archive logs. This example assumes that the archive logs are accessible by each node in the cluster. If they are not, then the archive logs need to be backed up separately on each node.

Note: This example works only if the backup is not load balanced across multiple nodes, because NB_ORA_CLIENT=$NB_ORA_CLIENT evaluates only to the node on which the RMAN script is executed.

```
RUN
{
ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';

SEND 'NB_ORA_CLIENT=$NB_ORA_CLIENT,NB_ORA_SERV=$NB_ORA_SERV';

BACKUP
      DATABASE;
sql 'alter system archive log current';
RELEASE CHANNEL ch00;
ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';

SEND 'NB_ORA_CLIENT=$NB_ORA_CLIENT,NB_ORA_SERV=$NB_ORA_SERV';

BACKUP
      ARCHIVELOG ALL ;
RELEASE CHANNEL ch00;
}
```

Example of restoring a database

Restoring the database from the nodes where the backup was performed is straightforward and identical to a typical RMAN restore.

In this example, the backup images to be restored must all be accessible by the client name `saturn` in the image database on the master server `jupiter`.

Note: This example works only if the backup is not load balanced across multiple nodes. The reason is because NB_ORA_CLIENT=$NB_ORA_CLIENT evaluates only to the node on which the RMAN script is executed.

The following example restores the entire database from any node:

```
RUN {
ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';
SEND 'NB_ORA_CLIENT=saturn,NB_ORA_SERV=jupiter';
RESTORE
      DATABASE;
RECOVER
      DATABASE;
RELEASE CHANNEL ch00;
}
```

Troubleshooting database restores (UNIX and Windows)

An RMAN restore to one node of a cluster can fail with a status code 39 when the following situation is present:

- The `NB_ORA_CLIENT` is set to the virtual name of the cluster.
- The client name is set to the virtual name of the cluster.

To remedy this problem, use the hostname.

More information is available on restores and redirected restores.

See "About NetBackup for Oracle restores" on page 128.

See "Example of restoring a database" on page 236.

About restoring archive logs

You can use the typical RMAN script to restore the archive logs under the following circumstances:

- If the remote archived log destinations allow write access.
  See Figure A-2 on page 232.
- If the archive logs reside on a CFS.
  See Figure A-1 on page 231.

In the examples that follow, the client is *saturn* and the server is *jupiter*. The backups are stored under the client name *saturn*.

The following example restores all of the archive logs:

```
RUN {
ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';
SEND 'NB_ORA_CLIENT=saturn,NB_ORA_SERV=jupiter';
RESTORE
      ARCHIVELOG ALL;
RELEASE CHANNEL ch00;
}
```

If the remote archive logs destinations do not allow write access, use a script such as the following to restore the archive logs:

```
RUN {
ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';
SEND 'NB_ORA_CLIENT=saturn,NB_ORA_SERV=jupiter';
```

```
SET ARCHIVELOG DESTINATION TO <directory>;
RESTORE
      ARCHIVELOG ALL;
RELEASE CHANNEL ch00;
}
```

Where <directory> is the directory into which the archive logs are restored.

Use a script like the preceding one if your configuration is a configuration shown in one of the following topics:

- See Figure A-3 on page 234.
- See Figure A-4 on page 235.

Appendix B

Best practices for protecting Oracle RAC with NetBackup

This appendix includes the following topics:

Oracle RAC with NetBackup best practices

The Real Application Clusters (RAC) option allows multiple concurrent instances to share a single physical database.

Oracle database backup and recovery is more difficult as databases grow in size and greater demands on database availability limit the time to perform backups. Often the backup time window is too short to accommodate a complete backup process by using only one backup node in the cluster. Database administrators need more efficient methods to complete these large backups in the allotted time. For the Oracle RAC database, Oracle can split the backups into pieces and send them in parallel from multiple nodes, which shortens the processing time.

This section describes the methods that can be used to backup the Oracle RAC database. You can use one node to backup the database or balance the backup load across multiple nodes of an Oracle RAC database.

About using Templates and Oracle Intelligent Policy (OIP) with RAC

The NetBackup for Oracle Template Wizard and Oracle Intelligent Policy both work well for backing up Oracle database instances. They can be used to backup Oracle RAC when only a single host name or client name is needed to affect the backup. They cannot be used to backup Oracle RAC when more than one client name must be used.

The following are the two situations when the Template Wizard or the OIP cannot be used to backup Oracle RAC:

- The channels are load balanced across the hosts in the cluster.
- One client name is used to determine the host on which to execute RMAN, and the channels are allocated using a different client name.

Note: Using a separate template or OIP for each instance in a RAC may be successful. However, using these methods may result in multiple backups of the same shared application data.

Backup scripts or Oracle launch mechanisms provides greater flexibility for complex configurations and are preferred for use with RAC.

About NetBackup for Oracle operations

The following lists what occurs when you initiate RMAN:

- The NetBackup Oracle policy can contain one or more client names and one or more backup scripts to execute.

  Note: Oracle 11g R2 Grid Infrastructure (CRS) includes the Single Client Access Name (SCAN) feature. This feature allows a single host name to resolve to multiple IP addresses each assigned to a different physical node in a cluster. Ensure that the client that appears in the NetBackup Oracle policy is not a SCAN. Also, ensure that any NB_ORA_CLIENT or CLIENT_NAME provided by the client host in the backup request is not a SCAN. These names must reliably resolve on both the master server and the media server to a client host IP address. This IP address allows the server processes to connect to the client host from which the backup request originated. If the SCAN is used in a NetBackup policy, this abstraction of the client name leads to backup and restore jobs failing. The backup and restore jobs may fail with a status 54. The client side fails with status 6 (backup) or status 5 (restore).

- The NetBackup master server uses the automatic schedules in the Oracle policy to determine when the scripts in the backup selections are run on clients.
- The NetBackup scheduler starts one Automatic Backup job for each client in the policy. The jobs for multiple clients can run concurrently. The scheduler executes each script on each client in the specified sequence. All the scripts for one client are run in the same automatic job.
- The backup scripts start RMAN.
- If an automatic schedule and script do not exist in the policy, a process on the client can still initiate RMAN when necessary.

The following lists what occurs when RMAN requests the backup:

- RMAN connects to the appropriate Oracle database instance(s) for the backup. Hence, the script may execute on one host, but the backup may take place on a different host.
- RMAN allocates one or more channels according to the backup script.
- RMAN sends one or more backup pieces on each channel, in sequence.
- Each channel interacts with NetBackup for Oracle and sends a user-directed backup request to the NetBackup master server for each backup piece.

- Each request becomes a separate NetBackup Application Backup job. Hence there can be one Application Backup job queued or active, concurrently, per allocated channel.
- RMAN can send one or more of the variables NB_ORA_CLIENT, NB_ORA_POLICY, and NB_ORA_SCHED to the NetBackup master server.
- If RMAN does not send NB_ORA_CLIENT, the client name is used.
- If RMAN does not send NB_ORA_POLICY, the master server selects the first Oracle policy it finds for the client.
- If RMAN does not send NB_ORA_SCHED, the master server selects the first Application Backup schedule in the policy.
- The NetBackup master server must be able to match any requested client name, Oracle policy and Application Backup schedule, or the job fails.

The following lists how NetBackup receives the data from RMAN:

- The Application Backup jobs activate and the NetBackup media server processes which connect to the provided client name to receive the data. Hence, the client name that is sent in the user-directed request must bring the data connection back to the requesting host.
- RMAN sends the appropriate data on the appropriate channel, and the data is transferred to storage.

Example RAC configuration: Failover name exists and backup is not load balanced

In this configuration, a failover name exists such that the NetBackup media server can always reach an available host to execute the backup script. Further, since load balancing is disabled, RMAN allocates the channels on a single host, typically the same host where the script executes.

The configuration is as follows:

- Configure the policy to specify the failover name as the client name. The automatic schedule then runs the backup script on a host that is currently operational.
- The backup script or an identical copy must be accessible to all hosts in the cluster. The clustered file system is a good location.
- Configure the backup script so that RMAN provides to NetBackup the failover name from the policy. It floats to the active instance-host and ensures successful data transfer, and all the backups are stored under that single client name.

```
ALLOCATE CHANNEL ... ;
SEND 'NB_ORA_CLIENT=$NB_ORA_CLIENT';
BACKUP ... ;
```

- The NetBackup master server configuration must allow the physical host names access to all of the backup images.

  ```
  cd /usr/openv/netbackup/db/altnames
  echo "hostname1" >> hostname1
  echo "vipname1" >> hostname1
  echo "hostname2" >> hostname1
  echo "vipname2" >> hostname1
  echo "failover_vipname" >> hostname1
  cp hostname1 hostname2
  ```

- You can use Preferred Network on the client to specify the outbound interface for user-directed requests to the master server. This method is not recommended. However, if you use this method then you must allow the VIP names to access all of the backup images.

  ```
  cd /usr/openv/netbackup/db/altnames
  cp hostname1 vipname1
  cp hostname1 vipname2
  ```

  Note: This method may not be desirable because it affects the source IP for user-directed file system backup, list, and restore requests.

The backup script then runs on the active host that currently hosts the failover name. RMAN allocates the channels on that host to perform the backup. The Application Backup jobs queue to the failover name, and the NetBackup media server connects back to the failover name for the data transfer. The backup images are stored under the failover name regardless of which host performed the backup. Restores can take place from either host as long as the restore request is configured to SEND 'NB_ORA_CLIENT=failover name';

Example RAC configuration: Failover name exists and backup is load balanced

In this configuration, the NetBackup master server can always use the failover name to reach an active host to run the backup script. However, because RMAN allocates channels on both hosts, the NetBackup media server must connect back to the

correct host to obtain the data for each request. Hence, the backup images are stored under two different client names which must differ from the failover name that is used to execute the script.

- Set up the policy to specify the failover name as the client name. Thus, the Automatic schedule executes the backup script on a host that is currently operational.
- The backup script or an identical copy must be accessible to all hosts in the cluster. The clustered file system is a good location.
- Do not configure the backup script to send a single value for NB_ORA_CLIENT. The NetBackup media server must connect back to the correct host, which depends on which host originated the user-directed backup request. Select one of the following three methods to accomplish this task:
- Configure the backup to provide a host-specific client name with each backup request using one of the following three options:
  - Configure RMAN to bind specific channels to specific instances and provide the associated client names on each channel for backup image storage. Also, configure RMAN for connect-back to the requesting host for the data transfer. Do not use the failover name, because it is active on only one of the hosts.

```
ALLOCATE CHANNEL 1 ... PARMS='ENV=(NB_ORA_CLIENT=vipname1)' CONNECT='sys/passwd@vipname1';
ALLOCATE CHANNEL 2 ... PARMS='ENV=(NB_ORA_CLIENT=vipname2)' CONNECT='sys/passwd@vipname2';
ALLOCATE CHANNEL 3 ... PARMS='ENV=(NB_ORA_CLIENT=vipname1)' CONNECT='sys/passwd@vipname1';
ALLOCATE CHANNEL 4 ... PARMS='ENV=(NB_ORA_CLIENT=vipname2)' CONNECT='sys/passwd@vipname2';
```

Note: If one or more of these nodes are down, these allocation operations fail which causes the backup to fail.

  - Alternatively, configure Oracle to bind specific channels to specific hosts.

```
CONFIGURE CHANNEL 1 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname1' PARMS
   "ENV=(NB_ORA_CLIENT=vipname1)";
CONFIGURE CHANNEL 2 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname2' PARMS
   "ENV=(NB_ORA_CLIENT=vipname2)";
CONFIGURE CHANNEL 3 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname1' PARMS
   "ENV=(NB_ORA_CLIENT=vipname1)";
CONFIGURE CHANNEL 4 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname2' PARMS
   "ENV=(NB_ORA_CLIENT=vipname2)";
```

- Alternatively and by default, the backup uses the client names which should be distinct for each host and is typically the physical host name.

- Because CLIENT_NAME or NB_ORA_CLIENT values must differ from the failover name in the policy, the NetBackup master server cannot accept the user-directed backup request. You must implement one of the following options.
  - **Option A**: Modify the existing policy and the backup script to handle multiple client names.
    - Add both VIP names or both host names to the policy, in addition to the failover name.
    - Modify the script so that it exits with status 0 if the client name is not the failover name.
  - **Option B**: Alternatively, use a separate policy to accept the backup requests.
    - Create a second policy to receive the backup requests from RMAN.
    - Set the policy type to be Oracle.
    - Set the policy to contain the NB_ORA_CLIENT or client names as configured in the previous information.
    - The Application Backup schedule must have an open window to accept the backups.
    - The policy does not need a backup script or an automatic schedule.
    - Configure the backup script to provide the name of this policy with each user-directed backup request:
    - ```
      ALLOCATE CHANNEL...PARMS='ENV=(NB_ORA_POLICY=<second_policy_name>)';
      or
      SEND 'NB_ORA_POLICY=<second_policy_name>';
      ```

- The NetBackup master server configuration must allow the physical host names access to the backup images. The images are stored under the VIP names or host names as follows:

```
cd /usr/openv/netbackup/db/altnames
echo "failover_name" >> hostname1
echo "hostname1" >> hostname1
echo "vipname1" >> hostname1
echo "hostname2" >> hostname1
echo "vipname2" >> hostname1
cp hostname1 hostname2
```
```

- You can use Preferred Network or another means to force NetBackup to use the IP addresses associated with the VIP names for outbound user-directed requests. If you use this method then you must allow the VIP names to access all of the backup images.

```
cd /usr/openv/netbackup/db/altnames
cp hostname1 vipname1
cp hostname1 vipname2
```

Option A: The NetBackup scheduler starts three automatic jobs, and each runs the backup script (two of them on the host that currently hosts the failover name). The two executions of the backup script that receive the VIP names or host names exit immediately with status 0. The reason immediate exit is done is to avoid a redundant backup and any retries. The third execution of the backup script that receives the failover name, starts RMAN. RMAN then sends the data for backup by using the appropriate client name for the instance or host for the channel. NetBackup stores the backup images under the initiating policy using both client names.

Option B: The first policy runs the backup script by using the failover name. RMAN sends the name of the second policy and the configured client names for each channel with the user-directed request from each host. The second policy stores the backup images using both client names.

Either client can initiate a restore. RMAN must be configured with 'SET AUTOLOCATE ON;' to request the backup pieces from the appropriate instance-host that performed the backup. Alternatively, you can restore from either host or instance if you configure each restore request to include the correct client name. This name is the client name used at the time the backup piece was transferred to storage.

```
SEND 'NB_ORA_CLIENT=client_name_used_by_backup'
```

Example RAC configuration: Failover name is not available and backup is not load balanced

In this configuration, VIP names or host names allow connections to the respective hosts in the cluster. You need a special configuration to ensure that the backup script executes on at least one of the hosts but not on both hosts. Otherwise, a backup may not occur if the specified instance is down, or a redundant backup occurs if both of the specified instances are active.

For ease of discussion, the term primary refers to the instance on which the backup normally occurs. The term secondary refers to the other instance which may be used if the primary is unavailable. In addition, because the backup may occur on

either host, the backup images have the potential to be stored under both client names. The image storage name is dependent on which host is active at the time of the backup. The configuration is as follows:

- The policy specifies client names for both hosts, either hostname1 and hostname2, or vipname1 and vipname2. The specification of client name ensures that the backup is attempted on a host which is currently operational.
- The backup script must be accessible to both hosts in the cluster, the clustered file system makes a good location.
- The backup script should be customized so that it starts RMAN on exactly one of the clients. If the script is executed on the primary, then start RMAN and perform the backup. If the script is executed on the secondary and the primary is up, then exit with status 0 so the NetBackup scheduler doesn't retry this client. If the script is executed on the secondary and the primary is down, then start RMAN and perform the backup. You can build the script customization around a `tnsping` to the primary or even a query of the database. Use this customization to see if the other instance is open and able to perform the backup.

  ```
  $ select INST_ID, STATUS, STARTUP_TIME, HOST_NAME from gv$instance;

      INST_ID STATUS STARTUP_T HOST_NAM
      ---------- ------------ --------- ----------
      1 OPEN 13-JAN-09 vipname1
      2 OPEN 13-JAN-09 vipname2
  ```

- Each user-directed backup request must use a client name which allows the NetBackup media server to connect back to the correct host for the data transfer. By default, the backup uses the CLIENT_NAME from the bp.conf file which is distinct for each host. A better solution is to configure RMAN to provide the appropriate client name from the policy as follows:

  ```
  SEND 'NB_ORA_CLIENT=$NB_ORA_CLIENT';
  ```

- Configure the NetBackup master server to give the physical host names access to all of the backup images.

  ```
  cd /usr/openv/netbackup/db/altnames
  echo "hostname1" >> hostname1
  echo "vipname1" >> hostname1
  echo "hostname2" >> hostname1
  echo "vipname2" >> hostname1
  cp hostname1 hostname2
  ```

- You can use Preferred Network or another means to force NetBackup to use the IP addresses associated with the VIP names for outbound user-directed requests. If you use this method then you must allow the VIP names to access all of the backup images.

```
cd /usr/openv/netbackup/db/altnames
cp hostname1 vipname1
cp hostname1 vipname2
```

Either client can initiate a restore. RMAN must be configured with 'SET AUTOLOCATE ON;' to request the backup set pieces from the appropriate instance or host that performed the backup. Alternatively, you can restore from either host or instance if you configure each restore request to include the correct client name. This client name is the one that is used at the time the backup set piece was transferred to storage.

```
SEND 'NB_ORA_CLIENT=client_name_used_by_backup'
```

Example RAC configuration: Failover name is not available, and backup is load balanced, one policy with custom script

A load-balanced backup without a failover name must overcome the combined challenges of the preceding configurations. Because a failover name does not exist, the NetBackup scheduler must attempt to execute the backup script on both hosts. In this case, the script must start RMAN on only one of the hosts. Because RMAN may allocate channels on both instances, the user-directed requests must present host specific names. The requirement is that the connect-back from the NetBackup media server must be able to retrieve the data from the correct host.

- The policy should specify both client names, either hostname1 and hostname2 or vipname1 and vipname2. The specification of client names is to ensure that the backup script is executed on at least one host which is currently operational.
- The backup script must be accessible to both hosts in the cluster. The clustered file system makes a good location.
- The backup script should be customized so that it starts RMAN on exactly one of the clients. If the backup script is executed on the primary, then start RMAN and perform the backup. If the backup script is executed on the secondary and the primary is up, then exit with status 0 so that the NetBackup scheduler doesn’t retry this client. If the backup script is executed on the secondary and the primary is down, then start RMAN and perform the backup. The script customization

can be built around a `tnsping` to the primary or even a query of the database. Use this customization to see if the other instance is open and able to perform the backup.

```
$ select INST_ID, STATUS, STARTUP_TIME, HOST_NAME from gv$instance;

    INST_ID STATUS STARTUP_T HOST_NAM
    ---------- ------------ --------- ----------
    1 OPEN 13-JAN-09 vipname1
    2 OPEN 13-JAN-09 vipname2
```

- The backup script must not be configured to send a single value for NB_ORA_CLIENT. This configuration is because the NetBackup media server needs to connect back to the correct host depending on which host originated the user-directed backup request.
- Configure the backup to provide a host-specific client name with each backup request using one of the following three options:
  - Configure RMAN to bind specific channels to specific instances and provide the associated client names on each channel for backup image storage. Also, configure RMAN for connect-back to the requesting host for the data transfer.

```
ALLOCATE CHANNEL 1 ... PARMS='ENV=(NB_ORA_CLIENT=vipname1)' CONNECT='sys/passwd@vipname1';
ALLOCATE CHANNEL 2 ... PARMS='ENV=(NB_ORA_CLIENT=vipname2)' CONNECT='sys/passwd@vipname2';
ALLOCATE CHANNEL 3 ... PARMS='ENV=(NB_ORA_CLIENT=vipname1)' CONNECT='sys/passwd@vipname1';
ALLOCATE CHANNEL 4 ... PARMS='ENV=(NB_ORA_CLIENT=vipname2)' CONNECT='sys/passwd@vipname2';
```

Note: If one or more of these nodes are down, these allocation operations fail which causes the backup to fail.

  - Alternatively, configure Oracle to bind specific channels to specific hosts.

```
CONFIGURE CHANNEL 1 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname1' PARMS
   "ENV=(NB_ORA_CLIENT=vipname1)";
CONFIGURE CHANNEL 2 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname2' PARMS
   "ENV=(NB_ORA_CLIENT=vipname2)";
CONFIGURE CHANNEL 3 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname1' PARMS
   "ENV=(NB_ORA_CLIENT=vipname1)";
CONFIGURE CHANNEL 4 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname2' PARMS
   "ENV=(NB_ORA_CLIENT=vipname2)";
```

- Alternatively by default, the backup uses the client names which should be distinct for each host and is typically the physical host name.

- Configure the NetBackup master server to allow the physical host names access to all of the backup images.

```
cd /usr/opnv/netbackup/db/altnames
echo "hostname1" >> hostname1
echo "vipname1" >> hostname1
echo "hostname2" >> hostname1
echo "vipname2" >> hostname1
cp hostname1 hostname2
```

- You can use Preferred Network or another means to force NetBackup to use the IP addresses associated with the VIP names for outbound user-directed requests. If you use this method then you must allow the VIP names to access all of the backup images.

```
cd /usr/openv/netbackup/db/altnames
cp hostname1 vipname1
cp hostname1 vipname2
```

The net result is that the backup script runs on all of the currently active hosts but only starts RMAN on one host. RMAN allocates channels across the hosts for load balancing. The user-directed backup requests include a NB_ORA_CLIENT or CLIENT_NAME specific to the requesting host and which matches the policy. The connect-back for data transfer and the backup image are stored under that name.

Either client can initiate a restore. RMAN must be configured with 'SET AUTOLOCATE ON;' to request the backup pieces from the appropriate instance-host that performed the backup. Alternatively, you can restore from either host or instance if you configure each restore request to include the correct client name. This name is the client name used at the time the backup piece was transferred to storage.

```
SEND 'NB_ORA_CLIENT=client_name_used_by_backup';
```

Example RAC configuration: Failover name is not available and backup is load balanced, simple script with manual policy failover

Some implementations of RAC (Linux/Windows) do not include a failover name. Also, some sites do not need a robust backup script that determines the active

instance in real time. If this scenario is the case, use the following configuration to manually initiate a backup from the secondary host when the primary host is down.

- Create a first Oracle policy with an Application Backup schedule to receive the backup images from both hosts. Configure both VIP names or the host names as clients in the policy. Do not configure an Automatic Backup schedule or a backup selection (script).
- Create a second Oracle policy to execute the backup script on the primary host. Configure the VIP name or host name of the primary host in the policy. Configure the pathname to the backup script in the policy. Create an Automatic Backup schedule with an open window in the policy.
- Create a third Oracle policy that can be used to manually execute the backup script on the secondary host when the primary host is unavailable. Configure the VIP name or host name of the secondary host in the policy. Configure the pathname to the backup script in the policy. Create an Automatic Backup schedule without an open window in the policy.
- The backup script must be accessible to both hosts in the cluster, the clustered file system makes a good location.
- Configure the backup to provide a host-specific client name with each backup request using one of the following three options:
  - Configure RMAN to bind specific channels to specific instances and provide the associated client names on each channel for backup image storage. Also, configure RMAN for connect-back to the requesting host for the data transfer.

```
ALLOCATE CHANNEL 1 ... PARMS='ENV=(NB_ORA_CLIENT=vipname1)' CONNECT='sys/passwd@vipname1';
ALLOCATE CHANNEL 2 ... PARMS='ENV=(NB_ORA_CLIENT=vipname2)' CONNECT='sys/passwd@vipname2';
ALLOCATE CHANNEL 3 ... PARMS='ENV=(NB_ORA_CLIENT=vipname1)' CONNECT='sys/passwd@vipname1';
ALLOCATE CHANNEL 4 ... PARMS='ENV=(NB_ORA_CLIENT=vipname2)' CONNECT='sys/passwd@vipname2';
```

Note: If one or more of these nodes are down, these allocation operations fail which causes the backup to fail.

  - Alternatively, configure Oracle to bind specific channels to specific hosts.

```
CONFIGURE CHANNEL 1 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname1' PARMS
   "ENV=(NB_ORA_CLIENT=vipname1)";
CONFIGURE CHANNEL 2 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname2' PARMS
   "ENV=(NB_ORA_CLIENT=vipname2)";
CONFIGURE CHANNEL 3 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname1' PARMS
   "ENV=(NB_ORA_CLIENT=vipname1)";
```

```
CONFIGURE CHANNEL 4 DEVICE TYPE 'SBT_TAPE' CONNECT 'sys/passwd@vipname2' PARMS
   "ENV=(NB_ORA_CLIENT=vipname2)";
```

- Alternatively and by default, the backup uses the client names which should be distinct for each host and is typically the physical host name.

- Configure the NetBackup master server to allow the physical host names access to all of the backup images.

```
cd /usr/opnv/netbackup/db/altnames
echo "hostname1" >> hostname1
echo "vipname1" >> hostname1
echo "hostname2" >> hostname1
echo "vipname2" >> hostname1
cp hostname1 hostname2
```

- Although not recommended, you can use preferred network or another means to force NetBackup to use the IP addresses associated with the VIP names for outbound user-directed requests. If you use this method then you must allow the VIP names to access all of the backup images.

```
cd /usr/openv/netbackup/db/altnames
cp hostname1 vipname1
cp hostname1 vipname2
```

The second policy executes the backup script on the primary host when it is scheduled. RMAN starts the backup process on all of the hosts, and they send back the appropriate NB_ORA_CLIENT or CLIENT_NAME for that host. If the primary is down, initiate the third policy manually from the NetBackup master server and perform a similar backup.

Either client can initiate a restore. RMAN must be configured with 'SET AUTOLOCATE ON;' to request the backup pieces from the appropriate instance-host that performed the backup. Alternatively, you can restore from either host or instance if you configure each restore request to include the correct client name. This name is the client name used at the time the backup piece was transferred to storage.

```
SEND 'NB_ORA_CLIENT=client_name_used_by_backup';
```

Image catalog configuration for RAC

If the RAC backup used a failover name as the NB_ORA_CLIENT, then the backup images from all nodes are stored under that single client name. Because the backup

images are stored under a single client name, the image catalog does not need any special configuration.

However, if a failover name was not used, then the backup images for individual clients are stored in uniquely named image directories. This configuration can cause complications when an operation such as crosscheck or restore are performed from an alternate cluster or an alternate node within the cluster

---

Note: This technique works best when you use the VIP names for the instances as the *racclient* names. If you use physical host names, the backup images from file system backups are stored with the Oracle backup images within a single image directory. This situation can result in two potential problems. First, if the same file name exists on both hosts but with different content, care must be used to select the correct backup image from which to restore. The selection confusion can be eliminated by configuring the file system backup to specify a policy keyword. The keyword is specific to the host from which each file system backup is taken. Then use the host-specific keyword to constrain the image search when performing browse and restore. Second, either host can restore the files that were backed up from the other host. Being part of the same cluster, this restore technique is normally not a concern. But be aware in case there are special considerations for permissions and security restrictions at your site.

The following procedure can be used to centralize storage of the backup images from all nodes in the cluster under one client name. That single client name can then be used for maintenance and restore operations.

In the following procedure, all steps are performed on the master server unless otherwise noted. Also, the procedure uses two examples of network host names that are routable:

- *racclient1*
- *racclient2*

In this procedure, the logical name for the cluster is *racname*. If there is a failover name that is always active on a node in the cluster, then it could be used as the *racname*. Alternatively, the *racname* can temporarily be added as a host name alias for *racclient1* or *racclient2* to complete the initial configuration and then be removed.

To centralize storage of the backup images from all nodes in the cluster under one client name

1 On both the master and the media server, confirm that the RAC client names are resolvable, network routable, and reverse resolve accurately:

```
bpclntcmd –hn racclient1
bpclntcmd –hn racclient2
ping racclient1
ping racclient2
bpclntcmd –ip <ip_address_for_racclient1>
bpclntcmd –ip <ip_address_for_racclient2>
```

Fix any host name forward and reverse resolution inconsistencies, and any network routing problems. Be sure to clear the NetBackup host cache and wait 10 seconds after making any name resolution changes:

```
bpclntcmd –clear_host_cache
```

2 On the master server, check if image directories or client aliases already exist for either of the *racclients* or the logical name for the cluster:

Windows:

```
dir install_path\Veritas\NetBackup\db\images\racclient1
dir install_path\Veritas\NetBackup\db\images\racclient2
dir install_path\Veritas\NetBackup\db\images\racname
```

UNIX:

```
ls -ld /usr/openv/netbackup/db/images/racclient1
ls -ld /usr/openv/netbackup/db/images/racclient2
ls -ld /usr/openv/netbackup/db/images/racname
```

Windows or UNIX:

```
bpclient -client racclient1 -list_all_aliases
bpclient -client racclient2 -list_all_aliases
bpclient -client racname -list_all_aliases
```

Note: Do not continue this procedure if either of the client names already have image directories or are aliases to a client name other than the *racname*.

Instead of using this procedure, consider merging the existing image directories and client names per the following Veritas knowledge base article.

https://www.veritas.com/docs/000018409

Alternatively, create new network resolvable and network routable host names for the RAC clients and return to step 1.

---

3 If the logical cluster name already had an image directory and is an alias for itself, then skip to step 5.

4 Run a backup using the logical cluster name as a NetBackup client name.

- If the *racname* is not a resolvable host name, temporarily make it a host name alias for the host name of one of the RAC client names. Changing the host name alias is most easily done my modifying the hosts file.
- The backup should be a file system backup using a new or an existing policy, it can be a backup of only one file.
- Afterward, make sure the *racname* has an image directory and client alias per the checks in step 2. Then remove any temporary host name alias or policy that was created.

5 Direct future backups and image searches for *racclient1* and *racclient2* to the logical cluster name.

Create the client aliases for the cluster and confirm:

```
bpclient -client racname -add_alias racclient1
bpclient -client racname -add_alias racclient2

bpclient -client racname -list_all_aliases
bpclient -client racclient1 -list_all_aliases
bpclient -client racclient2 -list_all_aliases
```

If problems are encountered, refer to the following tech note:

https://www.veritas.com/docs/000018409

6 Create or modify an Oracle policy for the RAC, specify *racclient1* and *racclient2* as the clients.

For more information on policy and RMAN configuration techniques, See "Oracle RAC with NetBackup best practices" on page 240.

7 Ensure that the policy is active and run a backup of the RAC using the policy.

8 Allow the client hosts to use NB_ORA_CLIENT=*racname* during crosscheck and restore operations. These *altname* files are created on the master server. The *peername* is the host name to which the master server resolves the source IP address from which each client connects to the master. The *peername* is easily determined when you run `bpclntcmd -pn` on each client host.

Windows:

```
cd install_path\Veritas\NetBackup\db\altnames
echo racname >> peername_racclient1
echo racname >> peername_racclient2
```

UNIX:

```
cd /usr/openv/netbackup/db/altnames
echo racname >> peername_racclient1
echo racname >> peername_racclient2
```

From *racclient1*, the *peername* is 'racclient1.com':

```
$ bpclntcmd -pn
expecting response from server mymaster
racclient1.com racclient1 192.168.0.11 60108
```

For more information about client alias best practices, refer to the following tech note:

http://www.veritas.com/docs/TECH208362

See "Oracle RAC with NetBackup best practices" on page 240.

See "About NetBackup for Oracle operations" on page 241.

Configuring the appliance within a RAC environment

Note: This feature requires a NetBackup appliance running software version 2.7.1 or later.

RAC may be used with the OIP and the appliance. You can use either the **Database Backup Shares** or **Whole Database - Datafile Copy Share** option in the OIP configuration. Both options only use a single node when a share is used on the appliance.

When the **Database Backup Shares** option is used, the DBAs have the ability to load balance the backups to the appliance share. Once the DBAs have placed a backup on the appliance share, NetBackup uses a single node of the cluster to protect the share. It does not matter which nodes are used to backup to the appliance share. NetBackup only uses a single node to protect the data on the share.

The **Whole Database - Datafile Copy Share** option uses a single node of the RAC cluster to move the data to the appliance share and protect the share.

Use the following procedure to configure the RAC environment to use OIP and the appliance to protect the share.

To configure the RAC environment with OIP and the appliance NFS share

1. Mount the appliance share at the same mount point on each node.
2. Configure all backups images so that they are cataloged under one client name.
   - See "Image catalog configuration for RAC" on page 252.
3. Configure the master server to allow physical host name access to the backup images.

```
cd /usr/openv/netbackup/db/altnames
echo "failover_name" >> hostname1
echo "hostname1" >> hostname1
echo "vipname1" >> hostname1
echo "hostname2" >> hostname1
echo "vipname2" >> hostname1
cp hostname1 hostname2
```

4 Add a database instance from one RAC node to the Oracle database instance repository.

5 Create an OIP (using the **Database Backup Shares** or **Whole Database - Datafile Copy Share** option) and only put one instance from the RAC cluster into the policy.

See "Configuring an OIP using a share on the NetBackup appliance (Copilot)" on page 86.

See "About using Templates and Oracle Intelligent Policy (OIP) with RAC" on page 240.

See "Oracle RAC with NetBackup best practices" on page 240.

Appendix C

Deduplication best practices

This appendix includes the following topics:

Optimizing and deduplicating stream-based and proxy copy Oracle backups

NetBackup enables you to perform optimized deduplication of Oracle databases. You can perform either a stream-based backup or a proxy copy backup.

Veritas recommends that you perform a proxy copy if the database consists of many small tablespaces. A proxy copy is also recommended if the DBA or the backup administrator does not want to set `FILESPERSET=1`.

To configure a proxy copy Oracle backup, you need to edit the RMAN script and configure NetBackup for Oracle.

See "Editing the RMAN script and configuring NetBackup for Oracle for a proxy copy backup" on page 265.

For stream-based backups, Veritas recommends that you specify `FILESPERSET=1` for all Oracle database backups. When `FILESPERSET=1` is specified, Oracle

generates the backup set identically each time. The backup set is generated with the same data from the same files in the same sequence each time the database is backed up. This uniformity ensures better deduplication. In addition, when `FILESPERSET=1` is in effect, Oracle does not perform multiplexing, so Oracle includes only one file in each backup set. If `FILESPERSET` is specified with a number other than `1`, Oracle groups files together unpredictably and deduplication rates suffer. You may also want to increase the number of channels that are allocated to the backup, if possible.

Veritas recommends that you test your database backups by running both stream-based backups and proxy copy backups. Measure the deduplication rates and the backup times, and see which method fits best in your environment. The Oracle database files themselves benefit the most from deduplication. Typically, the archive logs and the control files are unique, so they benefit less from deduplication.

Deduplication performs best when used in the following ways:

Stream deduplication	The Oracle Intelligent Policy detects both ASM and non-ASM environments to generate the correct backup scripts ensuring good deduplication rates. In a non-ASM environment, scripts are generated that are a non-snapshot proxy backup. In an ASM environment, scripts are generated that set `FILESPERSET=1` if this command has not been modified in a backup policy. You may need to create a custom script for your environment. However, in most situations, the Oracle Intelligent Policy creates the script that is needed for your environment.
Snapshot deduplication	When you use snapshot deduplication, nothing changes and NetBackup proxy snapshot backup is performed. If ASM is detected, an error is displayed. Snapshot backup is not allowed in an ASM environment.

Note: In OIP when deduplication storage is used and a stream-based backup is selected, the policy overrides and attempts to perform a proxy backup. The override is attempted if `NO ASM` storage is found in the database. The `ORACLE_OVERRIDE_DATA_MOVEMENT` setting in the `bp.conf` file can be used to override this behavior.

Set `ORACLE_OVERRIDE_DATA_MOVEMENT=1` to always do streaming.

Set `ORACLE_OVERRIDE_DATA_MOVEMENT=2` to always do proxy.

Set `ORACLE_OVERRIDE_DATA_MOVEMENT=>2` to maintain standard behavior.

On UNIX you can edit the `/usr/openv/netbackup/bp.conf` file.

On Windows you can use the `bpsetconfig` command (`install_path\NetBackup\bin\admincmd\bpsetconfig`) on the server to set the client's configuration. See the following example:

```
bpsetconfig -h myoracleclient

ORACLE_OVERRIDE_DATA_MOVEMENT = 1
```

For information about the backup methods, see the following:

- See "Configuring a stream-based Oracle backup" on page 261.
- See "Editing the RMAN script and configuring NetBackup for Oracle for a proxy copy backup" on page 265.

Configuring a stream-based Oracle backup

The following procedure explains how to reconfigure an existing Oracle RMAN specification to achieve a stream-based, optimized, deduplicated Oracle backup.

To configure a stream-based Oracle backup

1. On the client computer that hosts the Oracle database, open the RMAN backup script in a text editor, and make the following edits:
   - Add the `FILESPERSET=1` parameter to the part of the RMAN script that specifies how you want to back up the database.
     Do not add `FILESPERSET=1` to the section of the RMAN script that specifies how to back up the control files or archive logs. Typically, these other data objects are unique to each backup, so there is very little potential gain from optimizing the control file and archive log backups for deduplication.
     Example RMAN script after editing:

```
BACKUP
FILESPERSET=1
%BACKUP_TYPE%
FORMAT 'bk_u%%u_s%%s_p%%p_t%%t'
DATABASE;
```

The addition of `FILESPERSET=1` suppresses Oracle multiplexing of more than one data file into a backup set. When you suppress Oracle multiplexing, Oracle creates the backup set identically each time the backup runs. NetBackup can deduplicate these identical backup sets.

- Specify parallel backup streams for the database backup.
  Specify appropriate `ALLOCATE CHANNEL` and `RELEASE CHANNEL` parameters in the backup script.

For an example that shows an edited backup script, see the following:

See "Example RMAN script for a stream-based backup" on page 263.

2 Disable Oracle's optimization and encryption for the duration of the database backup.

By default, Oracle disables optimization and encryption. If optimization and encryption are enabled, run the following RMAN commands from the command line to disable optimization and encryption:

```
RMAN> CONFIGURE BACKUP OPTIMIZATION OFF;
RMAN> CONFIGURE ENCRYPTION FOR DATABASE OFF;
```

If your site requires encryption, you can specify encryption in the NetBackup for Oracle backup policy.

3 Disable Oracle's compression for the duration of the database backup.

By default, Oracle disables compression. If compression is enabled, Oracle compresses unused sections in streams, and the result is unpredictable deduplication rates. If compression is enabled, run the following RMAN command from the command line to disable compression:

```
RMAN> CONFIGURE DEVICE TYPE SBT_TAPE BACKUP TYPE TO BACKUPSET;
```

If your site requires compression, you can specify compression in the NetBackup for Oracle backup policy.

4 Configure a NetBackup for Oracle policy.

If you want to compress or encrypt the backup, enable compression and encryption in the NetBackup `pd.conf` file.

Run a full database backup as soon as you can. The policy can perform incremental backups until the full backup can be run.

Note: Make sure that Oracle optimization, encryption, and compression are disabled for the entirety of the database backup. Make sure to check specifications outside of the RMAN backup script, too.

Example RMAN script for a stream-based backup

The following is an example fragment from an RMAN script that performs an optimized, deduplicated, stream-based backup of an Oracle database.

```
RUN {

# Back up the database.
# Use 4 channels as 4 parallel backup streams.

ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';
ALLOCATE CHANNEL ch01 TYPE 'SBT_TAPE';
ALLOCATE CHANNEL ch02 TYPE 'SBT_TAPE';
ALLOCATE CHANNEL ch03 TYPE 'SBT_TAPE';
SEND ' NB_ORA_SERV=$NB_ORA_SERV’;

BACKUP
    $BACKUP_TYPE
    SKIP INACCESSIBLE
    TAG hot_db_bk_level0
```

```
    # The following line sets FILESPERSET to 1 and facilitates database deduplication.
    FILESPERSET 1
    FORMAT 'bk_%s_%p_%t'
    DATABASE;
    sql 'alter system archive log current';
RELEASE CHANNEL ch00;
RELEASE CHANNEL ch01;
RELEASE CHANNEL ch02;
RELEASE CHANNEL ch03;


# Back up the archive logs
# The FILESPERSET parameter setting depends on the number of archive logs you have.

ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';
ALLOCATE CHANNEL ch01 TYPE 'SBT_TAPE';
SEND ' NB_ORA_SERV=$NB_ORA_SERV';
BACKUP
   FILESPERSET 20
   FORMAT 'al_%s_%p_%t'
   ARCHIVELOG ALL DELETE INPUT;
RELEASE CHANNEL ch00;
RELEASE CHANNEL ch01;
#
# Note: During the process of backing up the database, RMAN also backs up the
# control file.  This version of the control file does not contain the
# information about the current backup because "nocatalog" has been specified.
# To include the information about the current backup, the control file should
# be backed up as the last step of the RMAN section.  This step would not be
# necessary if we were using a recovery catalog or auto control file backups.
#
ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';
SEND ' NB_ORA_SERV=$NB_ORA_SERV';
BACKUP
    FORMAT 'cntrl_%s_%p_%t'
    CURRENT CONTROLFILE;
RELEASE CHANNEL ch00;
}
```

Editing the RMAN script and configuring NetBackup for Oracle for a proxy copy backup

The following procedure explains how to edit the RMAN script on the client.

To edit the RMAN script

1. On the client computer that hosts the Oracle database, open the RMAN backup script in a text editor, and make the following edits:

   - Add `PROXY` to the list of commands that backs up the data files.

     Example RMAN script after editing:

     ```
     BACKUP
     FORMAT 'bk_u%u_s%s_p%p_t%t'
     PROXY
     DATABASE;
     ```

   - Specify the `NB_ORA_PC_STREAMS` parameter in the database backup script. The `NB_ORA_PC_STREAMS` variable controls the number of proxy copy backup streams to be started. By default, the agent initiates one backup job for all files. If the RMAN `send` command passes `NB_ORA_PC_STREAMS`, NetBackup for Oracle splits the files into the number of groups that are specified by the variable based on the file size. The agent attempts to create streams of equal size and determines the number of processes that run to perform the backup.

   For an example that shows an edited backup script, see the following:

   See "Example RMAN script for a proxy copy backup" on page 266.

2. Disable Oracle's optimization and encryption for the duration of the database backup.

   By default, Oracle disables optimization and encryption. If the optimization and encryption are enabled, run the following RMAN commands from the command line to disable optimization and encryption:

   ```
   RMAN> CONFIGURE BACKUP OPTIMIZATION OFF;
   RMAN> CONFIGURE ENCRYPTION FOR DATABASE OFF;
   ```

   If your site requires encryption, you can specify encryption in the NetBackup for Oracle backup policy.

3 Disable Oracle's compression for the duration of the database backup.

By default, Oracle disables compression. If compression is enabled, Oracle compresses unused sections in streams, and the result is unpredictable deduplication rates. If compression is enabled, run the following RMAN command from the command line to disable compression:

```
RMAN> CONFIGURE DEVICE TYPE SBT_TAPE BACKUP TYPE TO BACKUPSET;
```

If your site requires compression, you can specify compression in the NetBackup for Oracle backup policy.

4 Configure a NetBackup for Oracle policy.

If you want to compress or encrypt the backup, enable compression and encryption in the NetBackup `pd.conf` file.

Run a full database backup as soon as you can. You can perform incremental backups until the full backup can be run.

Note: Make sure that Oracle optimization, encryption, and compression are disabled for the entirety of the database backup. Also, make sure to check specifications outside of the RMAN backup script.

Example RMAN script for a proxy copy backup

The following is an example of an RMAN script that performs an optimized, deduplicated, proxy copy backup of an Oracle database.

```
RUN {

# Back up the database.

ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';

# Specify 2 streams.

SEND 'NB_ORA_PC_STREAMS=2';
BACKUP
    PROXY
    SKIP INACCESSIBLE
    TAG hot_db_bk_proxy
    FORMAT 'bk_%s_%p_%t'
```

```
    DATABASE;
    sql 'alter system archive log current';
RELEASE CHANNEL ch00;

# Back up the archive logs.
# The FILESPERSET parameter setting depends on the number of archive logs you have.

ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';
ALLOCATE CHANNEL ch01 TYPE 'SBT_TAPE';
SEND ' NB_ORA_SERV=$NB_ORA_SERV';
BACKUP
   FILESPERSET 20
   FORMAT 'al_%s_%p_%t'
   ARCHIVELOG ALL DELETE INPUT;
RELEASE CHANNEL ch00;
RELEASE CHANNEL ch01;

#
# Note: During the process of backing up the database, RMAN also backs up the
# control file.  This version of the control file does not contain the
# information about the current backup because "nocatalog" has been specified.
# To include the information about the current backup, the control file should
# be backed up as the last step of the RMAN section.  This step would not be
# necessary if we were using a recovery catalog or auto control file backups.
#
ALLOCATE CHANNEL ch00 TYPE 'SBT_TAPE';
SEND ' NB_ORA_SERV=$NB_ORA_SERV';

BACKUP
    FORMAT 'cntrl_%s_%p_%t'
    CURRENT CONTROLFILE;
RELEASE CHANNEL ch00;
}
```

Appendix D

Snapshot Client support of SFRAC

This appendix includes the following topics:

About Snapshot Client support of SFRAC

Veritas Storage Foundation for the Oracle Real Application Clusters (RAC) environment leverages storage management and high availability technologies for deployment of Oracle RAC on UNIX environments.

Storage Foundation is a complete solution for heterogeneous online storage management. Based on VxVM and VxFS, it provides a standard set of integrated tools to centrally manage data growth, maximize storage hardware usage, and provide data protection.

NetBackup configuration for an SFRAC environment

To perform the offhost snapshot backup of Oracle database in the SFRAC environment, the NetBackup client software must be installed on each node of the cluster.

You need to configure the following:

- On the master server or media server that resides outside of the cluster, you must configure the policy to back up the Oracle RAC database.
- Configure the alternate client so that the snapshot is taken using that offhost. The alternate client should not be part of the cluster.

Note: IPv6 is not supported for SFRAC.

Configuring the SFRAC environment for a backup operation

The backup and rollback operations involve the Oracle Agent and the hardware array. The configuration steps required for both of these operations should also be done before taking the snapshot.

The following lists the prerequisites before you perform a backup in the SFRAC environment.

To configure the SFRAC environment for a backup operation

1. Configure a virtual IP or virtual name over the cluster. NetBackup refers to the client by using this virtual name.
2. The NetBackup client name on each node of the cluster must match the virtual name that is configured on the cluster. Do one of the following:
   - If you have already installed the client, change the CLIENT_NAME entry in the `bp.conf` file of the NetBackup directory to the following:

     ```
     CLIENT_NAME = <virtual_name>
     ```

   - Alternatively, add the following parameter to the RMAN script file that you are using for backup and restore, and keep the default CLIENT_NAME as the hostname:

     ```
     NB_ORA_CLIENT = <host_name>
     ```

3. Specify the required host mode options in the storage array that provides the storage LUNs. For example, in the Host group options of an Hitachi array, enter the type of host (for example, Solaris) and enable the VERITAS Database Edition/Advanced Cluster for Oracle RAC (Solaris) option.

4 Add the following line to the `bp.conf` file, on each node in the cluster.

```
PREFERRED_NETWORK = <virtual-host-name>
```

This entry is required when running a rollback operation.

5 If the CFS version that you run does not support group quiescence, enable serial quiescence by adding the following lines to the `/usr/openv/lib/vxfi/configfiles/vxfsfi.conf` file.

```
[QUIESCENCE_INFO]
"QUIESCENCE_SERIAL_QUIESCENCE"=dword:00000001
```

6 Ensure that the database is in open (read-write) mode.

7 Ensure that the service group for the database in VCS is in the online state.

8 Because only the master node of the cluster supports the rollback restore, change the virtual IP before a rollback operation so that it points to the master node.

9 Configure a snapshot backup policy for the SFRAC environment. In the backup selection tab of the policy, make sure that you provide a path name to the RMAN script. Make sure that the script resides on all the nodes of the cluster. Parameters like ORACLE_SID can differ on each of the nodes. For example, on node 1, the ORACLE_SID can be symc1 and on node 2, the ORACLE_SID can be symc2.

Performing a rollback restore in an SFRAC environment

The following procedure describes the manual steps that are needed to restore volumes and file systems by using the snapshot rollback method in an SFRAC environment.

A typical host deployment for running NetBackup for Oracle in an SFRAC environment is as follows: Host A and Host B are in the cluster and Host C is used as an alternate client. The instant recovery snapshot is taken using the Oracle policy and the Hardware Snapshot FIM (frozen image method).

The application I/O stack is built upon the hardware array of VxVM (CVM) and VxFS (CFS).

The Veritas Cluster Server (VCS) controls the Oracle RAC database and other required essential resources such as shared storage. VCS defines and manages its resources as a single unit called a service group. A service group contains all the necessary components and resources of an application.

The following are entities in the VCS that monitor the application I/O stack:

- CFSMount contains the mount points (cfs) where data files, archive logs, and control files are stored.
- CVMVolDg contains all the Volume Groups (cvm) configured on top of the various array LUNs that participate in the hardware snapshot.
- The Database Resource Group contains the database instance and assists in failover.

To perform a rollback restore in the SFRAC environment

1. Ensure that you previously created a virtual IP for the clustered node. Point that virtual IP to the master node of the cluster.
2. On all the clustered nodes, take the VCS database service group (Oracle, CFSMount, and CVMVolDg resources) offline by using the following command:

   ```
   # hagrp -offline <DB_Service_Group> -any
   ```

3. Freeze the database service group.

   ```
   # hagrp -freeze <DB_Service_Group>
   ```

4. Mount the CFSMount points manually outside VCS on the master node. This action helps when you start the database in mount state.

   ```
   # mount -F vxfs -o cluster <mntPt>
   ```

5. Start the database with mount option on the clustered master node using one of these options:

   Option 1:

   ```
   # sqlplus /as sysdba
   # startup mount;
   ```

   Option 2:

   ```
   # sqlplus /as sysbackup
   # startup mount;
   ```

6 Run the rollback restore operation from the RMAN script or the client GUI. A sample RMAN script file (`hot_database_backup_proc`) is located in the following directory path:

```
/usr/openv/netbackup/ext/db_ext/oracle/samples/rman
```

To perform PIT rollback, add the following parameter to the script:

```
NB_ORA_PC_RESTORE=rollback
```

7 Unmount the CFS on the master node.

```
# umount <mntPt>
```

8 Unfreeze the VCS database service group.

```
# hagrp -unfreeze <DB_Service_Group>
```

9 On all the clustered nodes, take the VCS database service group (Oracle, CFSMount, and CVMVolDg resources) back online:

```
# hagrp -online <DB_Service_Group> -any
```

Troubleshooting NetBackup in an SFRAC environment

The following describes some common errors and how to troubleshoot them:

- Problem: The backup failed with error code 6 displayed in the GUI. The `rman_script.out` file shows the following error:

```
RMAN-06403: could not obtain a fully authorized session
 ORA-01034: ORACLE not available
 ORA-27101: shared memory realm does not exist
 SVR4 Error: 2: No such file or directory
```

Resolution: Check the ORACLE_HOME and ORACLE_SID values. ORACLE_HOME should not have an extra '/' at the end.

- Problem: The backup failed with error code 239. The `dbclient` logs show the following log statement:

```
serverResponse: ERR - server exited with status 239: the specified
client does not exist in the specified policy
01:02:23.844 [4000] <16> CreateNewImage: ERR - serverResponse() fail
```

Resolution: The client name mentioned in the policy and in the `bp.conf` file at the client are different.

- Problem: The backup failed with error 156. The `bpfis` logs show the following error.

```
CVxFSPlugin::vxFreezeAll : ioctl VX_FREEZE_ALL failed with errno : 16
CVxFSPlugin::quiesce - Could not quiesce as VX_FREEZE_ALL failed and
VX_FREEZE is not allowed
```

Resolution: Add the following lines to the `/usr/openv/lib/vxfi/configfiles/vxfsfi.conf`file:

```
file:[QUIESCENCE_INFO]
"QUIESCENCE_SERIAL_QUIESCENCE"=dword:00000001
```

- Problem: The rollback failed with the following error displayed in the GUI:

```
Failed to process backup file <bk_113_1_728619266>
```

The `dbclient` logs show the following error:

```
xbsa_ProcessError: INF - leaving
xbsa_QueryObject: ERR - VxBSAQueryObject: Failed with error: Server
Status: client is not validated to use the server
xbsa_QueryObject: INF - leaving (3)
int_FindBackupImage: INF - leaving
int_AddToFileList: ERR - Failed to process backup file
<bk_113_1_728619266>
```

Resolution : Add the following line in the `bp.conf` file on the master node of the cluster PREFERRED_NETWORK = <virtual_name>

Appendix E

Script-based block-level incremental (BLI) backups without RMAN on UNIX and Linux systems

This appendix includes the following topics:

About script-based block-level incremental (BLI) backups without RMAN

NetBackup for Oracle with Snapshot Client extends the capabilities of NetBackup to back up only changed data blocks of Oracle database files. NetBackup recommends using RMAN-based BLI backups, which allow the use of templates and remain tightly integrated with Oracle administration.

If you choose to use script-based BLI backups without RMAN, you can configure NetBackup for BLI support. A BLI backup backs up only the changed data blocks

of Oracle database files. NetBackup for Oracle script-based BLI performs backups using the Storage Checkpoint facility in the Veritas File System (VxFS) available through the Veritas Storage Foundation for Oracle.

About BLI backup and restore operations

A BLI backup performs database backups by obtaining the changed blocks identified by the Storage Checkpoints. BLI backups can also be performed while the database is online or offline. As with Storage Checkpoints, you must enable archive log mode to perform online BLI backups.

A BLI backup places the tablespaces in backup mode, takes a Storage Checkpoint, and then performs the backup. You specify how and when to back up the database when configuring the NetBackup notify scripts.

For example, suppose at 4:00 p.m. you lost a disk drive and its mirrored drive. A number of user tablespaces reside on the disk drive, and you want to recover all committed transactions up to the time you lost the drive. Because the BLI backup facility lets you perform more frequent backups, you did an online differential incremental backup at 1:00 p.m.

You recover by shutting down the database, installing new replacement disk drives, and restoring all the data files with NetBackup. Then you apply the archive logs to recover the tablespaces on the failed drive. If you used Fulldata Storage Checkpoints, the extra redo logs generated during an online backup are small, the media recovery part of the database recovery takes very little time. Moreover, because you have a recent backup, the entire recovery is accomplished quickly.

Verifying installation requirements for BLI backups without RMAN

Verify the following requirements before you begin the installation.

To verify the installation requirements

1. Make sure that the following products are properly installed and configured:
   - NetBackup
   - A supported level of Oracle
   - NetBackup for Oracle

- Veritas Storage Foundation for Oracle

2 Verify licensing.

The products must have valid licenses. To check for licenses, enter the following commands based on your version:

For VxFS versions earlier than 3.5:

```
# vxlicense -p
```

For VxFS versions 3.5 or later:

```
# vxlicrep
```

The command displays all the valid licenses that are installed on the system. If you have valid licenses, the Storage Checkpoint feature and the Veritas Storage Foundation for Oracle appear in the list.

3 Verify that both the NetBackup server (master and media) and client software work properly.

Particularly, verify that you can back up and restore typical operating system files from the client.

File system and Storage Checkpoint space management

To support BLI backups, the VxFS file systems need extra disk space to keep track of the block change information. The space that is required depends on the type of checkpoint that is used and the database change rate while the backup is running.

Using Storage Checkpoints has an effect on space in the following ways:

Nodata Storage Checkpoint	If the database is offline during the entire backup window (a cold database backup) or you use this checkpoint type, the additional space is minimal. Each file system requires about 1% of free space. This checkpoint sets a bit to indicate if a file block changed. When you use this checkpoint type, the data files are left in quiesce (write suspend) mode for the duration of the backup.

Fulldata Storage Checkpoint	If the database is online during the backup and using this checkpoint type, then more free space is needed in the file system. NetBackup for Oracle keeps the Oracle containers in quiesce (write suspend) mode only for the time that is needed to create a Storage Checkpoint. During the backup, the checkpoint creates copies of any file blocks immediately before they are changed. The backup up contains only the unchanged blocks and the original copies of the changed blocks. After the backup completes, the Fulldata Storage Checkpoint is converted to a Nodata Storage checkpoint and the copied blocks are returned to the free list. If the workload change rate is light during backup or the backup window is short, 10% free space is usually sufficient for the workload. If the database has a heavy change rate while the backup is running, the file systems may require more than 10% of free space.

Note: The default option that NetBackup uses for backups is Fulldata Storage Checkpoint.

To use Nodata Storage Checkpoint instead of the default option, a user must create the following empty touch file:

```
/usr/openv/netbackup/ext/db_ext/NODATA_CKPT_PROXY
```

Creating NetBackup policies for script-based BLI backup

To allow full and incremental backups, you must add at least one Standard type policy to NetBackup and define the appropriate schedules for that policy. Use the NetBackup Administration Console to add policies. NetBackup policies define the criteria for the backup.

These criteria include the following:

- Policy attributes
- Clients and the files or directories to be backed up on the client
- Storage unit to use
- Backup schedules

While most database NetBackup BLI backup policy requirements are the same as for file system backups, the following items have special requirements:

- The number of policies that are required
  See "Number of policies required for BLI backup" on page 278.
- Policy attribute values
  See "About BLI policy attributes" on page 280.
- The BLI client list
  See "About the BLI client list" on page 280.
- The list of directories and files to back up
  See "Backup selections list for BLI backups" on page 281.
- Schedules
  See "About schedules for BLI backup policies" on page 281.

Number of policies required for BLI backup

A database BLI backup requires at least one Standard type policy.

This policy usually includes the following:

- One full backup schedule
- One incremental backup schedule
- One user-directed backup schedule for control files and archive logs

Only one backup stream is initiated for each backup policy during automatic backups. To enable multiple backup streams, define multiple policies for the same database. If you have more than one database SID, configure policies for each SID. If you intend to do simultaneous backups of more than one SID on the same file system, use Nodata Storage Checkpoints. Set the `METHOD` to `NODATA_CKPT_HOT`.

For example, to back up file systems `F1`, `F2`, `F3`, and `F4` with two streams, you need to define two policies (`P1` and `P2`) with `F1` and `F2` backed up in `P1`, and `F3` and `F4` backed up in `P2`. If you have one large file system that needs to be backed up with multiple streams, divide the files in the file system between different policies. After a file is added to a policy, it should stay in that policy. If you must rearrange the file list, do so only prior to a full backup.

If you have more than one policy defined for an Oracle database instance, NetBackup groups the database instance by the NetBackup keyword phrase. Identify one of the policies as the `POLICY_IN_CONTROL` in the NetBackup notify scripts. This policy performs database shutdowns and restarts. All policies with the same keyword phrase need to be configured to start simultaneously.

Warning: Care must be taken when specifying the keyword phrase. A multistream backup is attempted if the backup process finds more than one policy with the following characteristics: Each policy has the BLI attribute set, each policy is active, each policy contains the same client, and each policy has an identical keyword phrase.

Typical failure status is: “74 - timeout waiting for bpstart_notify to complete.”

"See “NetBackup restore and backup status codes” on page 295.

You can check the file systems on the backup client to see if they are included in one of the NetBackup policies on the server. To see if you need to add any new file systems to the NetBackup policies, run the following commands from the server on a regular basis, perhaps as a `cron`(1) job:

```
# cd /usr/openv/netbackup/bin/goodies/
# ./check_coverage -coverage -client mars -mailid \nbadmin
```

The preceding command generates the following output and mails it to the specified `mailid`:

```
File System Backup Coverage Report (UNIX only)
-----------------------------------------------
Key:      * - Policy is not active
  UNCOVERED - Mount Point not covered by an active policy
  MULTIPLE  - Mount Point covered by multiple active policies

CLIENT: mars
Mount Point  Device             Backed Up By Policy  Notes
-----------  ------             -------------------  -----
/            /dev/vg00/lvol3    production_servers
/home        /dev/vg00/lvol5    production_servers
/oradata1    /dev/dsk/c1t0d0    block_incr1
/oradata2    /dev/dsk/c1t0d0    block_incr1
/oradata3    /dev/nbuvg/nbuvol  UNCOVERED
/opt         /dev/vg00/lvol6    production_servers
/oracle      /dev/vg00/oracle   production_servers
/stand       /dev/vg00/lvol1    production_servers
/usr         /dev/vg00/lvol7    production_servers
/var         /dev/vg00/lvol8    production_servers
```

If there is an `UNCOVERED` file system that is used by Oracle, add it to one of the NetBackup policies so that all the necessary file systems are backed up at the same time.

Note: After a file system is added to a policy, it is a good idea to keep the file system in that policy. If you change the policy, NetBackup performs a full backup the next time backups are run even if an incremental backup is requested.

About BLI policy attributes

NetBackup applies policy attribute values when it backs up files.

The following attributes must be set for BLI backup:

Policy Type	Set to Standard.
Perform block level incremental backups	Select to enable BLI backups. If the BLI attribute is not enabled, NetBackup uses the standard method to back up the files in the file list.
Job Priority	Set so that the BLI backup policies run before other policies.
Keyword phrase	Define as the Oracle database instance name (`$ORACLE_SID`) in each of the policies for the same instance. Multistream backups start when all the policies with a particular keyword phrase complete their respective startup scripts. If you have multiple Oracle database instances (SIDs) use a separate set of policies for each SID. If the SIDs are backed up simultaneously and any share a common file system for data files, use Nodata Storage Checkpoints. Set the `METHOD` to `NODATA_CKPT_HOT`.

Note: Do not change a keyword phrase after it is set in a policy. The keyword phrase is used in naming Storage Checkpoints. Changing the keyword phrase necessitates a full backup even if an incremental backup is requested.

The NetBackup Administrator's Guide, Volume I describes other policy attributes and how to configure them.

About the BLI client list

The client list specifies the clients upon which you configured a BLI backup. For a database backup, specify the name of the machine upon which the database resides. Specify the virtual hostname if clustered.

Backup selections list for BLI backups

The backup selections list specifies a list of directories and files to back up. The list must contain all the database files or their directory names. Using directory names, rather than file names, ensures that new database files added to an existing configuration are backed up without having to update the file list. Use the `check_coverage` script to make sure all file systems are backed up.

If you are using the Quick I/O interface, you need to specify both the Quick I/O file name and the associated hidden file in the file list (for example, `dbfile` and `.dbfile`), or you need to specify the directory that contains both files. NetBackup does not follow the symbolic links to automatically back up the hidden file if you enumerate only the `dbfile` explicitly in the backup selections list. They are both included if you enumerate their common directory.

When the NetBackup scheduler invokes an automatic backup schedule, it backs up the files one at a time, in the same order they appear in the backup selection list.

Oracle does not recommend backing up the online redo log, so it is recommended that you place online redo log files in a different file system than datafiles, archive log files, or database control files. Do not include the online redo log files in the file list.

About schedules for BLI backup policies

The NetBackup server starts these schedule types:

- Full Backup
- Differential Incremental Backup
- Cumulative Incremental Backup

Each BLI backup policy must include one full backup schedule and at least one incremental backup schedule. In addition, you must designate one of the BLI backup policies as the `POLICY_IN_CONTROL`. The policies for each stream must have the same types of schedules.

The NetBackup Administrator's Guide, Volume I describes other schedule attributes and how to configure them.

You can configure the following types of schedules:

- User-directed backup schedule. The user-directed backup schedule encompasses all the days and times when user-directed backups are allowed to occur. Set the backup window as described.
  The policies for each stream must have the same types of schedules.

- Automatically initiated backup schedules. Include server-initiated backup schedules to specify the days and times for NetBackup to automatically start backups of the files specified in the policy file list. Set the backup window as described.

For server-initiated full and incremental backup schedules, set the start times and durations to define the appropriate windows for the backups. Follow the same procedure used to define backup schedules for other policies. For more information on these procedures, see the NetBackup Administrator's Guide, Volume I.

The backups are started by the scheduler only within the backup window specified. For the `POLICY_IN_CONTROL`, include in the user-directed backup schedule the time periods when the BLI backup policies complete.

Set the retention level and periods to meet user requirements.

Example Oracle BLI backup policy

The following example shows attributes and schedules for an Oracle BLI backup policy. Use the NetBackup Administration Console to add policies.

```
Policy Name: oracle_backup1
  Policy Type:  Standard
  Active:  yes
  Block level incremental:  yes
  Job Priority:  0
  Max Jobs/Policy:  1
  Residence:  oracle_tapes
  Volume Pool:  NetBackup
  Keyword:  ORA1
Client List: Sun4 Solaris2.6 mars
             HP9000-800 HP-UX11.00 mars
Backup Selections List: /oradata/oradata1
Schedule:             full
    Type:             Full Backup
    Frequency:        1 week
    Retention Level: 3 (one month)
    Daily Windows:
          Sunday     18:00:00  -->  Monday     06:00:00
          Monday     18:00:00  -->  Tuesday    06:00:00
          Tuesday    18:00:00  -->  Wednesday  06:00:00
          Wednesday  18:00:00  -->  Thursday   06:00:00
          Thursday   18:00:00  -->  Friday     06:00:00
          Friday     18:00:00  -->  Saturday   06:00:00
          Saturday   18:00:00  -->  Sunday     06:00:00
```

```
Schedule:             incr
    Type:             Differential Incremental Backup
    Frequency:        1 day
    Retention Level: 3 (one month)
    Daily Windows:
          Sunday      18:00:00  -->  Monday     06:00:00
          Monday      18:00:00  -->  Tuesday    06:00:00
          Tuesday     18:00:00  -->  Wednesday  06:00:00
          Wednesday   18:00:00  -->  Thursday   06:00:00
          Thursday    18:00:00  -->  Friday     06:00:00
          Friday      18:00:00  -->  Saturday   06:00:00
          Saturday    18:00:00  -->  Sunday     06:00:00
Schedule:             userbkup
    Type:             User Backup
    Retention Level: 3 (one month)
    Daily Windows:
          Sunday      00:00:00  -->  Sunday     24:00:00
          Monday      00:00:00  -->  Monday     24:00:00
          Tuesday     00:00:00  -->  Tuesday    24:00:00
          Wednesday   00:00:00  -->  Wednesday  24:00:00
          Thursday    00:00:00  -->  Thursday   24:00:00
          Friday      00:00:00  -->  Friday     24:00:00
          Saturday    00:00:00  -->  Saturday   24:00:00
```

In this example, the `oracle_backup1` policy backs up all the files in `/oradata/oradata1`. The policy specifies a weekly full backup, a daily differential incremental backup, and a user-directed backup schedule. The archive logs and the control file are backed up using the user-directed schedule at the completion of the full or incremental backup.

Setting the maximum jobs per client global attribute

Set the **Maximum Jobs per Client** to the number of policies that have the same keyword phrase. This number can be greater than one when multiple job policies are defined to back up multiple file systems.

About BLI backup methods

You can choose from the following backup methods when configuring BLI notify scripts:

Table E-1 BLI backup terminology

Term	Definition
cold database backup	A cold database backup is taken while the database is offline or closed. BLI backup shuts down the database and performs either full or block-level incremental backups. This backup method is also referred to in Oracle documentation as a "consistent whole database backup" or a "closed backup." The data from a cold backup is consistent, resulting in easier recovery procedures. To select this backup method, set `METHOD` to `SHUTDOWN_BKUP_RESTART`. In an offline backup, all database files are consistent to the same point in time (for example, when the database was last shutdown using typical methods). The database must stay shut down while the backup runs.
hot database backup	A hot database backup allows the database to be online and open while the backup is performed. With the Storage Checkpoint facility, this backup method runs database backups in parallel so a database does not need to be in backup mode for a long time. To select this backup method, set `METHOD` to `ALTER_TABLESPACE`. Hot backups are required if the database must be up and running 24 hours a day, 7 days a week. To use hot backups, the database must be in `ARCHIVELOG` mode. BLI backup uses the `alter tablespace begin backup` command and the `alter tablespace end backup` command to put the database into and take it out of backup mode. Oracle documentation refers to this method as an inconsistent whole database backup or open backup. Unlike the cold database backup method, the data in hot backups is fuzzy or inconsistent until the appropriate redo log files (online and archived) are applied after the restore operation to make the data consistent.
Nodata storage checkpoint hot	A Nodata storage checkpoint hot backup puts the tablespaces in backup mode for the duration of the backup. It uses a Nodata Storage Checkpoint to reduce the amount of file system space consumed. To select this backup method, set `METHOD` to `NODATA_CKPT_HOT`. Use this method if all of the following conditions are present: ■ You are backing up multiple Oracle database instances. ■ More than one instance shares the file system. ■ The backup of the instances can overlap in time.

Table E-1 BLI backup terminology *(continued)*

Term	Definition
quick freeze database backup	The quick freeze database backup is different than an online database backup, because it requires the database to be brought down briefly to take a snapshot or Fulldata Storage Checkpoint of the database image. The Fulldata Storage Checkpoint is created in a few seconds and the database can be restarted immediately. A backup image from a quick freeze database backup is equivalent to a backup image from a cold database backup. You can choose this backup method when you configure BLI notify scripts. To select this backup method, set `METHOD` to `SHUTDOWN_CKPT_RESTART`. See "Creating notify scripts for BLI backups" on page 285.

If the database is in `ARCHIVELOG` mode, you can use all four methods to back up the database. If the database is in `NOARCHIVELOG` mode, you can only select the cold backup or quick freeze backup.

When you use the cold and quick freeze database backups, the default shutdown command that you use in the `bpstart_notify.oracle_bli` script is `shutdown` or `shutdown normal`. These commands wait for all users to log off before it initiates the shutdown. In some circumstances, even after all interactive users are logged off, processes such as the Oracle Intelligent Agent (Oracle `dbsnmp` account) can still be connected to the database, preventing the database shutdown. Attempt to use the default shutdown commands to shut down the database cleanly. Alternatively, you can use `shutdown immediate` to initiate the database shutdown immediately.

Creating notify scripts for BLI backups

Create notify scripts that run on the clients to synchronize the backup operation and the database operation. You need a set of three notify scripts for each policy that is performing BLI backups. The scripts must be in the `/usr/openv/netbackup/bin` directory on the NetBackup client.

The scripts are named as follows:

- `bpstart_notify.`*`POLICY`*
- `post_checkpoint_notify.`*`POLICY`*
- `bpend_notify.`*`POLICY`*

To create the notify scripts, run the following script as root:

```
/usr/openv/netbackup/ext/db_ext/oracle/bin/setup_bli_scripts
```

This script copies the sample notify script templates to `/usr/openv/netbackup/bin` and makes the necessary changes based on the information you provide.

The notify script templates are located on the local machine in the following location:

```
/usr/openv/netbackup/ext/db_ext/oracle/samples
```

When you run `setup_bli_scripts` you need to supply the following information:

- Identify the POLICY_IN_CONTROL
  See "Identify the POLICY_IN_CONTROL for BLI backups" on page 286.
- Provide the Oracle environment variables
  See "Oracle environment variables for BLI scripts" on page 286.
- Select a backup method
- Notify scripts for other policies
  See "About BLI notify scripts for other policies" on page 287.

See the information about how to use the notify scripts to back up your Oracle database.

Identify the POLICY_IN_CONTROL for BLI backups

If you have more than one policy defined on the server for one Oracle database instance, identify one of the policies as the `POLICY_IN_CONTROL`. This is the policy that initiates the database `shutdown`, `startup`, or `alter tablespace` commands. The `POLICY_IN_CONTROL` can be any policy (for example, the first policy defined). This variable is stored in the notify scripts.

Oracle environment variables for BLI scripts

If you create notify scripts, or if you run `setup_bli_scripts`, you need to provide values for the Oracle environment variables.

These variables are as follows:

`ORACLE_DBA`	User name of the Oracle database administrator. Typically, `oracle`.
`ORACLE_BASE`	`$ORACLE_BASE` of the Oracle database instance.
`ORACLE_HOME`	`$ORACLE_HOME` of the Oracle database instance.
`ORACLE_SID`	Oracle database instance ID (`$ORACLE_SID`) if it is different from the keyword.

ORACLE_LOGS	Directory in which the Oracle archive logs reside.
ORACLE_CNTRL	Location to which a copy of the Oracle control file is written so that it can be backed up.
SQLCMD	sqldba, svrmgrl, or sqlplus command to start up or shut down the database.
ORACLE_INIT	Path name for the Oracle startup parameter file (INIT.ORA). If you are using an Oracle SPFILE as your parameter file, do not set the ORACLE_INIT environment variable.
ORACLE_CONFIG	Path name for the Oracle configuration file (CONFIG.ORA). Some database configurations use the CONFIG.ORA file to specify values for the database parameters that usually do not change. The CONFIG.ORA file can be called by the INIT.ORA file using an include statement.

About BLI notify scripts for other policies

If you have more than one policy defined to support multiple backup streams, create a copy of the notify scripts for each policy defined.

For example, assume that you have two policies defined, oracle_backup1 and oracle_backup2. Also assume that POLICY_IN_CONTROL is set to oracle_backup1. You also need to create notify scripts for policy oracle_backup2. The setup_bli_scripts script performs this step automatically.

Sample setup_bli_scripts session

The following sample session shows how to use setup_bli_scripts to create the notify scripts.

```
#/usr/openv/netbackup/ext/db_ext/oracle/bin/setup_bli_scripts

Please enter the user name of your Oracle administrator? orac901

ORACLE_BASE is the Oracle environment variable that identifies
the directory at the top of the Oracle software and administrative
file structure. The value of this variable is typically
/MOUNTPOINT/app/oracle

Please enter your ORACLE_BASE? /dbhome/oracle/orac901

ORACLE_HOME is the Oracle environment variable that identifies the
directory containing the Oracle software for a given Oracle server
```

```
release. The value of this variable is typically
/dbhome/oracle/orac901/product/RELEASE

Please enter your ORACLE_HOME? /dbhome/oracle/orac901

sqlplus will be used.

The default "connect" statement that will be used to connect to the database is:
                            "connect / as sysdba"

Would you like to modify the connect and use a specific login? (y/n) n

"connect / as sysdba" will be used.


Please enter the Oracle instance (ORACLE_SID) you want to back up? orac901

If you are using a CONFIG.ORA file, you need to specify where
it is, so that it can be backed up. If this does not apply
apply to your configuration, hit ENTER to go on. If this does
apply to your configuration, specify the file path.
Typically this would be:
/dbhome/oracle/orac901/admin/orac901/pfile/configorac901.ora
but this file could not be found.

Enter your Oracle config file path or hit ENTER:

To back up a copy of the Oracle control file, you need to specify a file
path where Oracle can write a copy of the control file.

Please enter the file path where Oracle is to write a copy of your
control file? /dbhome/oracle/orac901/admin/orac901/pfile/cntrlorac901.ora

To back up the Oracle archive logs, you need to specify their location.


Enter the directory path to your Oracle archive logs?
/dbhome/oracle/orac901/admin/orac901/arch

Do you have more archive log locations? (y/n): n

Do you want the output of successful executions of the NetBackup
scripts mailed to you? y
```

```
Please enter the mail address to send it to? jdoe@company.com

Do you want the output of unsuccessful executions of the NetBackup
scripts mailed to you? y
Please enter the mail address to send it to? jdoe@company.com

There are 4 backup methods to choose from:
   ALTER_TABLESPACE      - Use alter tablespace begin backup method
   NODATA_CKPT_HOT       - Use alter tablespace begin backup with nodata ckpts
   SHUTDOWN_CKPT_RESTART - Shutdown, create the ckpt clones, and restart
   SHUTDOWN_BKUP_RESTART - Shutdown the DB, backup, and then restart
If one of the methods requiring DB shutdown are selected, you may experience
problems with timeouts if the database can't be shut down in a timely
manner. You may want to change the shutdown command in the notify scripts to
shutdown immediate, or you may have to increase the BPSTART_TIMEOUT value in the
bp.conf file on the master server, or you may want to change the backup
method to ALTER_TABLESPACE or NODATA_CKPT_HOT.
Note: the default BPSTART_TIMEOUT value is 300 seconds.

Do you want to use the ALTER_TABLESPACE method? y

You now need to decide on how many NetBackup policies you will have
backing up simultaneously. The first one you enter will be known
as the POLICY_IN_CONTROL in the scripts and will perform any needed
DB operations. When you create the policies on the NetBackup server,
you will have to divide the filesystems between these policies.

Please enter the name of the policy that will be the POLICY_IN_CONTROL? BLI_1
Please enter the name of another policy or DONE to stop? BLI_2
Please enter the name of another policy or DONE to stop? BLI_3
Please enter the name of another policy or DONE to stop? BLI_4
Please enter the name of another policy or DONE to stop? BLI_5
Please enter the name of another policy or DONE to stop? BLI_6
Please enter the name of another policy or DONE to stop? DONE
```

Performing backups and restores

After the installation and configuration are complete, you can use the NetBackup interfaces to start Oracle backups and restores. You can run backups manually by using schedules that you determine. You can also run a schedule manually.

Note: You must be the root user to perform all operations using the BLI backup software.

About NetBackup for Oracle agent automatic backups

The best way to back up databases is to set up schedules for automatic backups.

Note: You must be the root user to perform all operations using the BLI backup software.

Note: For HP-UX PA-RISC checkpoints to unmount and be cleaned up, create touch file `/usr/openv/netbackup/AIO_READS_MAX` that contains the value 1.

HP-UX PA-RISC checkpoints may not be unmounted on Oracle database agents.

About NetBackup for Oracle manual backups

You can also run an Automatic Backup schedule manually using the NetBackup Administration Console. For information about performing manual backups of schedules, see the NetBackup Administrator's Guide, Volume I.

Note: You must be the root user to perform all operations using the BLI backup software.

Note: For HP-UX PA-RISC checkpoints to unmount and be cleaned up, create touch file `/usr/openv/netbackup/AIO_READS_MAX` that contains the value 1.

To perform a cold (offline) backup, set the environment variable `METHOD` in the `bpstart_notify script` on the client to `SHUTDOWN_BKUP_RESTART`. The `bpstart_notify script` shuts down the database before the backup begins and the `bpend_notify script` restarts the database after the backup completes.

To perform a hot (online) backup using Fulldata Storage Checkpoints, make sure the database is running in `ARCHIVELOG` mode and set the variable `METHOD` to `ALTER_TABLESPACE`. The `bpstart_notify` script changes the tablespaces to online backup mode before the backup begins, and the `post_checkpoint_notify` script changes the tablespaces back to normal mode after the Fulldata Storage Checkpoints are created.

To perform a Nodata Storage Checkpoint Hot (online) backup, make sure the database is running in `ARCHIVELOG` mode and set the environment variable `METHOD`

in the `bpstart_notify` script to `NODATA_CKPT_HOT`. The `bpstart_notify` script changes the tablespaces to online backup mode before the backup begins. The `bpend_notify` script changes the tablespaces back to normal mode after the backup completes.

To perform a quick freeze backup, set the environment variable `METHOD` in the `bpstart_notify` script to `SHUTDOWN_CKPT_RESTART`. The `bpstart_notify` script shuts down the database and the `post_checkpoint_notify` script restarts it immediately after the Fulldata Storage Checkpoints are created. Taking VxFS Fulldata Storage Checkpoints is very fast (within a minute), and with the NetBackup queuing delay for scheduling the backup jobs, the database down time is typically only a few minutes.

Backing up Quick I/O files

A Quick I/O file consists of two components: a hidden file with the space allocated for it, and a link that points to the Quick I/O interface of the hidden file. Because NetBackup does not follow symbolic links, you must specify both the Quick I/O link and its hidden file in the list of files to be backed up.

Note: You must be the root user to perform all operations using the BLI backup software.

For example:

```
ls -la /db02
total 2192
drwxr-xr-x 2 root   root      96 Jan 20 17:39 .
drwxr-xr-x 9 root   root    8192 Jan 20 17:39 ..
-rw-r--r-- 1 oracle dba  1048576 Jan 20 17:39 .cust.dbf
lrwxrwxrwx 1 oracle dba       22 Jan 20 17:39 cust.dbf ->\
           .cust.dbf::cdev:vxfs:
```

The preceding example shows that you must include both the symbolic link `cust.dbf` and the hidden file `.cust.dbf` in the backup file list.

If you want to back up all Quick I/O files in a directory, you can simplify the process by only specifying the directory to be backed up. In this case, both components of each Quick I/O file is properly backed up. In general, you should specify directories to be backed up unless you only want to back up some, files in those directories.

Note: For HP-UX PA-RISC checkpoints to unmount and be cleaned up, create touch file `/usr/openv/netbackup/AIO_READS_MAX` that contains the value 1.

Restoring BLI backup images

Restoring the backup images that a BLI backup creates is no different than restoring the backup images that are created using the default NetBackup configuration. Restoring to any of the incremental backup images requires NetBackup to restore the last full backup image and all the subsequent incremental backups until the specified incremental backup image is restored. NetBackup does this automatically. The media that stored the last full and the subsequent incrementals must be available, or the restore cannot proceed.

You can start the restore operations from the NetBackup client by using the Backup, Archive, and Restore interface. To restore the latest copy of each file, select either the files or parent directories with the latest backup date, and click **Restore**. For more information on restoring, see the NetBackup Backup, Archive, and Restore Getting Started Guide.

If the operation is to restore files from an incremental backup image, NetBackup issues multiple restore operations beginning from the last full backup image and the subsequent incremental backup images until the selected date. The activity of multiple restores is logged in the Progress Log.

If you plan to restore files backed up by another client or to direct a restore to another client, start the restore from the NetBackup server using the Backup, Archive, and Restore interface. Before you initiate a restore, a backup must have successfully completed or an error occurs during the execution.

For Solaris, the restore destination can be a VxFS or UFS file system. The destination file system does not need to support the Storage Checkpoint feature, but to be able to perform BLI backups of the restored data, a VxFS file system with the Storage Checkpoint feature is required.

For HP-UX, the restore destination can be a VxFS or HFS file system. The destination file system does not need to support the Storage Checkpoint feature to restore files. However, a VxFS file system with the Storage Checkpoint feature is required to perform BLI backups of the restored data.

For AIX, the restore destination can be a VxFS or JFS file system. The destination file system does not need to support the Storage Checkpoint feature to restore files. However, a VxFS file system with the Storage Checkpoint feature is required to perform BLI backups of the restored data.

Note that restoring a file causes all blocks in that file to be rewritten. Thus, all the blocks in the file are considered to have been modified. Thus, the first subsequent differential incremental backup and all subsequent cumulative incremental backups back up all of the blocks in the restored file. If you are restoring an entire database or a file system, the first subsequent backup backs up all blocks that are restored.

To restore a Quick I/O file, if both the symbolic link and the hidden file already exist, NetBackup restores both components from the backup image. If either one of the two components is missing, or both components are missing, NetBackup creates or overwrites as needed.

Oracle database recovery might be necessary after restoring the files. See the Oracle documentation for more information on doing database recovery.

About NetBackup backup and restore logs

NetBackup provides logs on the database backup and restore operations. These logs are useful for finding problems that are associated with those operations. The following table describes the most useful logs and reports for troubleshooting backup and restore operations.

Table E-2 NetBackup backup and restore logs

Log file type	Description
NetBackup progress logs	For user-directed backups and restores performed with Backup, Archive, and Restore interface, the most convenient log to use for NetBackup is the progress log. The progress log file is written to the user's home directory, by default in `/usr/openv/netbackup/logs/user_ops/`*`username`*`/logs`. This log indicates whether NetBackup was able to complete its part of the operation. You can view the progress log from the Backup, Archive, and Restore interface, or you can use a file editor such as `vi`(1).
NetBackup debug logs	The NetBackup server and client software provide debug logs for troubleshooting problems that occur outside of BLI backups. To enable these debug logs on the server or client, create the appropriate directories under the following directory: `/usr/openv/netbackup/logs` For more information on debug logs, see the NetBackup Troubleshooting Guide or see the `/usr/openv/netbackup/logs/README.debug` file.
NetBackup reports	In addition to logs, NetBackup provides a set of reports that help isolate problems. One report is `All Log Entries` on the server. For a description of all reports, see the NetBackup Administrator's Guide, Volume I.

About troubleshooting backup or restore errors

A backup or restore error can originate from NetBackup for Oracle, from the NetBackup server or client, from the Media Manager, or from VxFS. In addition to examining log files and reports, you should determine at which stage of the backup or restore operation the problem occurred. You can also use NetBackup status codes to determine the cause of the problem.

Troubleshooting stages of backup and restore operations

Refer to the following list to determine the source of a backup or restore error:

- A backup or restore can be started in either of the following ways:
  - Manually from the administrator interface on the master server
  - Automatically by a NetBackup server using a full schedule or incremental schedule

  If an error occurs during the start operation, examine the Java reports window for the possible cause of the error.
- If the backup or restore starts successfully but eventually fails, one of the following can be the cause:
  - Server/Client communication problem
  - Schedule error
  - Media-related error
  - VxFS errors

  For more information, see the NetBackup Troubleshooting Guide.
- There can be insufficient disk space for the VxFS Fulldata Storage Checkpoints to keep track of changed block information. Check the `All Log Entries` report for errors.
  If there is a file system out-of-space condition, increase the size of the file system so it is large enough for Fulldata Storage Checkpoints or use the Nodata Storage Checkpoint Hot backup method. This error does not affect the integrity of the backup images because a full backup of the affected file system occurs after the condition is fixed.
- If an incremental backup is intended, but the whole file system is backed up instead, one of the following conditions might be present:
  - Storage Checkpoints that keep track of changes have been removed
  - The **Block level incremental** attribute is not selected
  - Other errors with a nonzero status code

  The most common cause of this problem is the file system removed the Storage Checkpoint that keeps track of the block changes. This action might occur if the file system runs out of space, and there are no volumes available to allocate to the file system. The integrity of the backup images is not affected, because a full backup of the file system occurs at the next backup opportunity after NetBackup detects that a Storage Checkpoint is missing.

NetBackup restore and backup status codes

The status codes and their meanings are as follows:

- Status Code 9. An extension package is needed but was not installed.
  The client does not have the NetBackup binaries required to do BLI backups. Use `update_clients` on the server to push out new binaries. Also, use `vxlicense -p` to verify that the Storage Checkpoint feature [83] and the Veritas Storage Foundation for Oracle [100] are installed.
- Status Code 69. Invalid file list specification.
  Look for a message such as the following in the error log on the server:

  ```
  FTL - /oradata is not in a VxFS file system. A block incremental
  backup of it is not possible.
  ```

  This indicates that there was an attempt to back up a file system that is not a VxFS file system with the **Block level incremental** attribute. This error can also occur if the file system is not mounted.
- Status Code 73. `bpstart_notify` failed.
  When running the notify scripts, the `bpstart_notify` script exited with a nonzero status code, or the permission bits are set wrong on the `bpstart_notify` script. The script must have execute permission. If the permission bits are set, check the `bpstart_notify_output.`*`ORACLE_SID`* file in the `/usr/openv/netbackup/bin/BLOCK_INCR` directory.
- Status Code 74. Client timed out waiting for `bpstart_notify` to complete.
  Check the `BPSTART_TIMEOUT` setting on the NetBackup server. The `BPSTART_TIMEOUT` specified did not allow enough time for the script to complete. The shutdown database operation might be taking too long, or the script might be waiting for other streams to start. Check the `bpstart_notify_output.`*`ORACLE_SID`* file and the `post_checkpoint_notify_output.`*`ORACLE_SID`* file in the `/usr/openv/netbackup/bin/BLOCK_INCR` directory. Make sure that the policies and schedules are configured with appropriate multiplexing factors and that the required storage units that allow all streams to start at the same time are configured. Check to see if all needed tape drives are working and available. Make sure that the database is not processing transactions so that the instance cannot be shut down immediately (if you are using one of the backup methods where the database is shut down).
  Finally, make sure that the priority on the BLI policies is higher than other policies, so they get access to the tape drives before the other policies.
- Status Code 75. Client timed out waiting for `bpend_notify` to complete.

Check the `BPEND_TIMEOUT` setting on the NetBackup server. The `BPEND_TIMEOUT` specified did not allow enough time for the script to complete. The restart database operation might be taking too long, or the script might be waiting for other streams to call the `bpend_notify` script. Check the `bpend_notify_output.`*`ORACLE_SID`* file and the `post_checkpoint_notify_output.`*`ORACLE_SID`* file in the `/usr/openv/netbackup/bin/BLOCK_INCR` directory. Make sure that the policies and schedules are configured with appropriate multiplexing factors and that the required storage units that can allow all streams to be started at the same time are configured. Verify that all needed tape drives are working and available during backup.

- Status Code 77. Execution of the specified system command returned a nonzero status code.
  Check the `post_checkpoint_notify_output.`*`KEYWORD`* file in the `/usr/openv/netbackup/bin/BLOCK_INCR` directory for the possible cause. The `post_checkpoint_notify` script exited with a nonzero status code.
- Status Code 143. Invalid command protocol.
  Check to see if the **Block level incremental** policy attribute is selected without a keyword specified. Set the **Keyword phrase** in the policies to the Oracle database instance name (`$ORACLE_SID`).

Improving NetBackup backup performance

If backups are running slowly, check to see if the database has an excessive workload. BLI backups allow hot database backups and quick freeze database backups. Because the database is running during both of these backup methods while NetBackup is backing up the database files, Oracle I/O can affect the backup performance.

If the database is not running with a high transaction volume, troubleshoot NetBackup. If the incremental backup takes a long time to finish, it could mean that there are more changed blocks since the last incremental backup. Verify whether the size of the incremental backup image has increased, and consider increasing the frequency of incremental backups.

Finally, you can improve the speed at which backup is performed by using multiplexed backups. Assigning multiple policies to the same backup device is helpful when devices are not writing at their maximum capacity.

About BLI backup and database recovery

A BLI backup does not perform automatic database recovery. This process includes restoring the database files from NetBackup images and applying the Oracle redo

log files to the database files. Follow the Oracle documentation to perform database recovery after a restore.

Appendix F

XML Archiver

This appendix includes the following topics:

NetBackup for Oracle XML export and XML import

While Oracle RMAN performs backup, restore, and recovery of physical Oracle database objects (data files, tablespaces, control files, and archived redo logs), the NetBackup for Oracle XML export and XML import utilities provide backup and restore of logical database objects (tables, users, and rows).

The XML format is used to provide a self-identifying and system-independent format ideal for database archiving.

NetBackup for Oracle XML export and import archiving features

Table F-1 describes NetBackup for Oracle XML export and XML import archiving features.

Table F-1 NetBackup for Oracle XML export and XML import archiving features

Feature	Description
System- and database-independent archive format	NetBackup for Oracle uses the eXtensible Markup Language (XML) standard to represent relational database table data that is extracted from an Oracle database. The eXtensible Markup Language (XML) is a universal format for structured documents and data. The XML 1.0 standards are produced by the World Wide Web Consortium and include the XML Schema standard. Unicode UTF-8 is the character set encoding generated by NetBackup for Oracle. Standard XML processors support UTF-8. US7ASCII is a strict subset of UTF-8.
Self-identifying archive format	The XML Schema standard is used to describe the table data that is included in an archive. In this way, the archive contains the key to understanding the format of the data as well as the data itself.
Command line interfaces that allow export and import at row-level granularity	Parameter files specify the table data to include in an archive and the table data to extract from an archive for import into an Oracle database.
Restore destination option	NetBackup for Oracle can either restore XML data to an operating system directory or import the data back into the Oracle database.
Flexible archive image searches	The NetBackup catalog contains information on the contents of the archive that can be searched by using flexible search criteria, such as tablename or user.

XML export archive process

Figure F-1 shows the XML export archive process.

Figure F-1 XML export archives

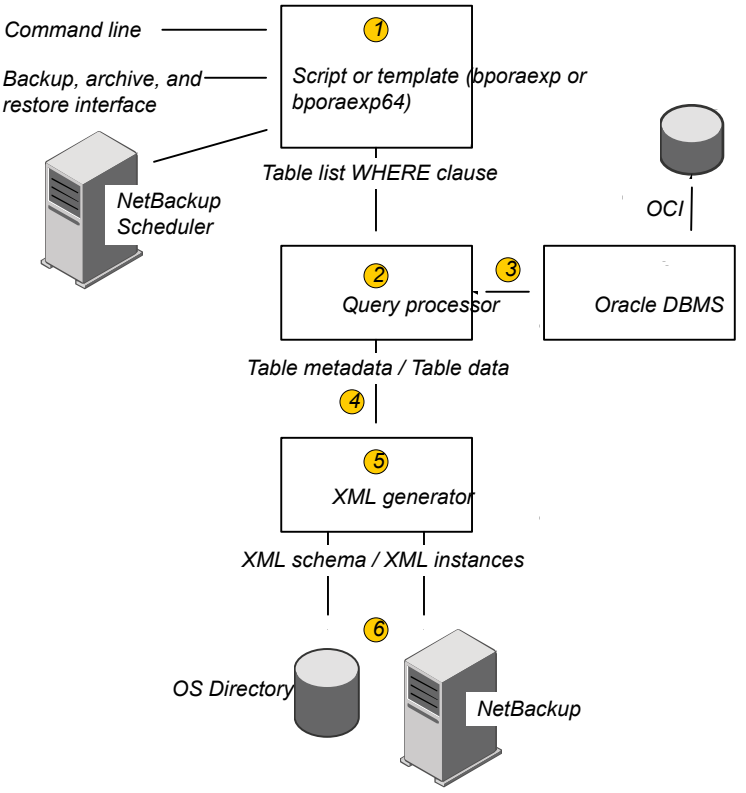


Table F-2 describes the archive activity.

Table F-2 Archive activity

Activity	Process
Oracle XML archive	NetBackup for Oracle extracts database table data, converts it into XML format, and stores XML data to either of the following types of repositories: ■ A directory ■ A storage unit

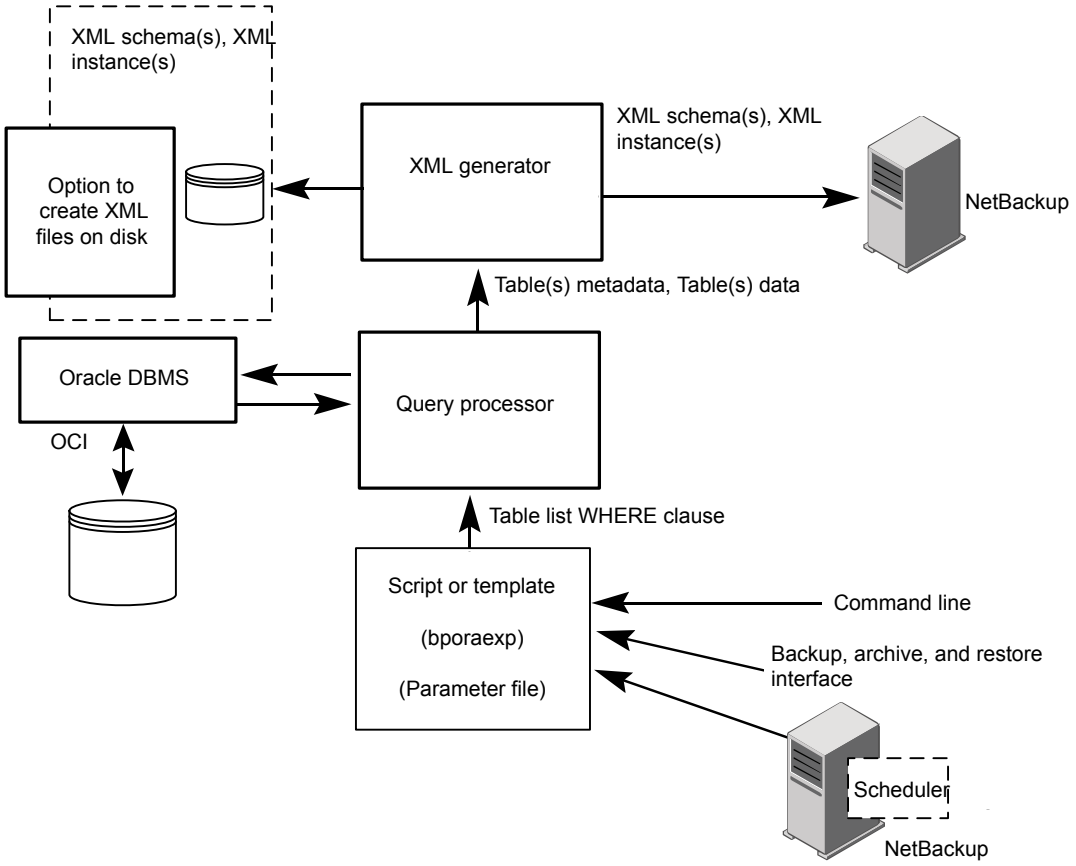
Table F-2 Archive activity *(continued)*

Activity	Process
XML export	NetBackup for Oracle converts Oracle table data to XML format (XML schema, or metadata, and XML instance, or data).
Archive	NetBackup stores the XML data on a NetBackup storage unit.
`bporaexp/bporaexp64` command	NetBackup for Oracle's XML export utility converts Oracle database table data into a self-identifying XML schema document and instance document. They can be archived by NetBackup or redirected to an OS directory.

Sequence of operation: XML export archive

Figure F-2 shows data flow.

Figure F-2 XML export archive data flow



NetBackup for Oracle users or automatic schedules start database XML export archives by performing a manual backup of an Oracle policy, by invoking the script or template at the command line on the client, or by invoking a template through the Backup, Archive, and Restore interface.

For an XML export archive:

- The NetBackup for Oracle script or template calls the `bporaexp` utility with a specified parameter file.
- The query processor uses the parameters in the specified file to build an SQL query for each table.
- Oracle's OCI API executes the queries on the Oracle database instance to be archived.

- The query processor passes the output (including metadata and data for a single table or multiple tables) to the XML Generator.
- For each table passed, the XML generator builds one or more sets of XML schema and XML instance documents.
- XML data streams are backed up by NetBackup.
- Alternately, `bporaexp` allows the files to be saved to an operating system directory.

XML import restore process

Figure F-3 shows the XML import restore process.

Figure F-3 XML import restores

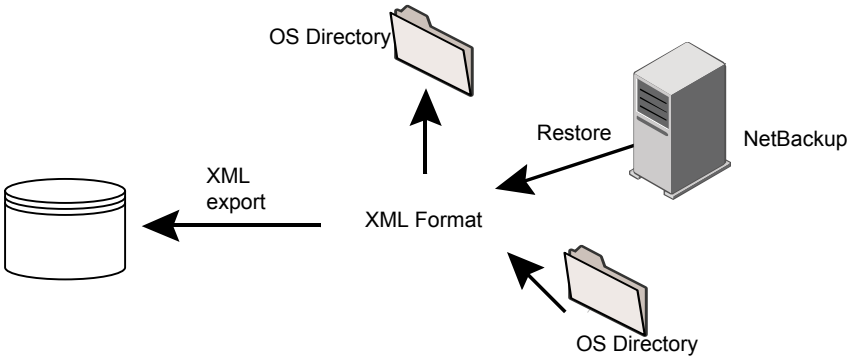


Table F-3 describes the restore activity.

Table F-3 Restore activity

Activity	Process
Oracle XML Restore	NetBackup for Oracle manages the retrieval of archived database table data, the parsing of the XML format, and the insertion of the data back into the Oracle database.
Restore	NetBackup retrieves the XML-formatted data from the storage unit.
XML import	NetBackup for Oracle parses XML-formatted Oracle table data and inserts data into the Oracle database.

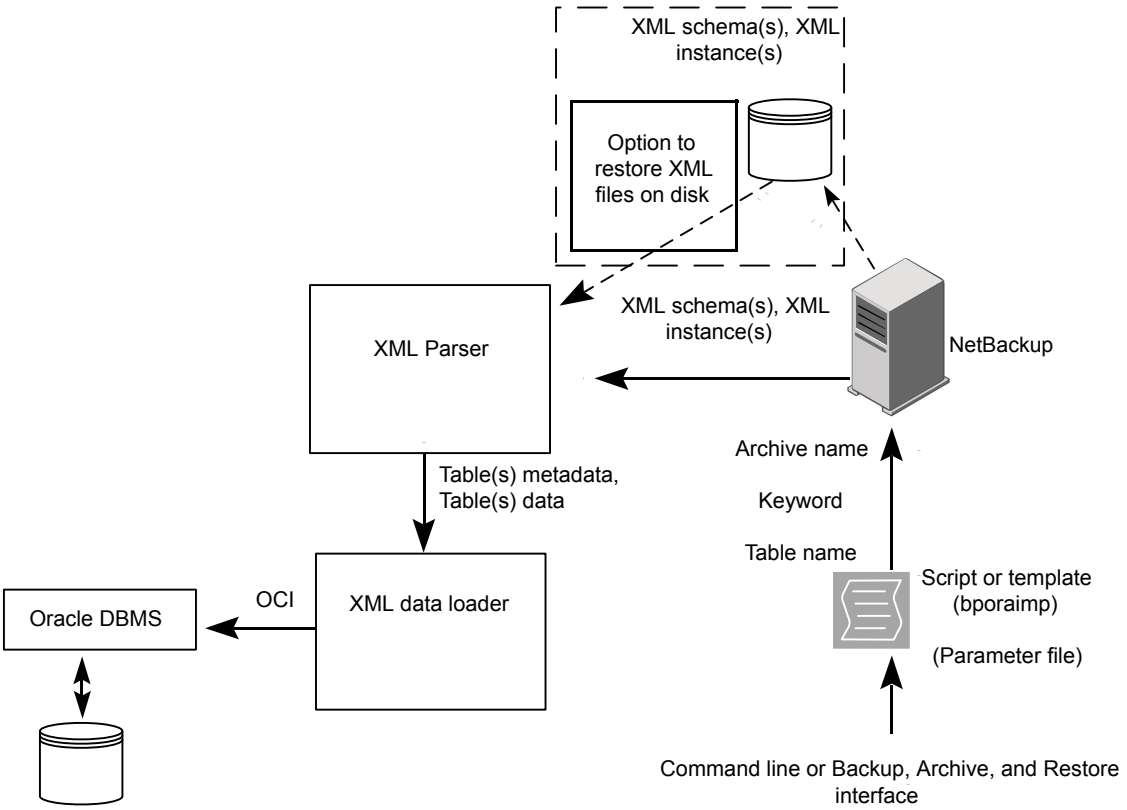
Table F-3 Restore activity *(continued)*

Activity	Process
`bporaimp/bporamip64` commands	NetBackup for Oracle's XML import utility can parse the XML-formatted data for re-insertion into the database or can redirect the data to an OS directory.

Sequence of operation: XML import restore

Figure F-4 shows data flow.

Figure F-4 XML import restore data flow



NetBackup for Oracle users start database XML import restores by invoking a NetBackup for Oracle script or template at the client command line or by invoking an XML import restore template through the Backup, Archive, and Restore interface.

For an XML import restore:

- The NetBackup for Oracle script or template calls the `bporaimp` utility with a specified parameter file.
- The input parameters that identify the XML archive to restore are passed to NetBackup.
- NetBackup locates and reads the set of XML schema and instance documents from the NetBackup storage unit.
- The XML data stream is passed to an XML parser, which passes the data to the XML data loader.
- The XML data loader uses Oracle's OCI API to insert the data into the database. Optionally, `bporaimp` allows the XML data stream to bypass the XML parser and be sent to an operating system directory. In addition, users can restore the table metadata only into an operating system directory. `bporaimp` also allows import from an operating system directory into Oracle.

About the environment variables set by a user in the XML export parameter file

You can set the XML export parameter file in the Oracle user's environment. If you use templates, use the template generation wizard to set these variables.

On Windows:

See "Creating XML export templates using the NetBackup for Oracle wizard (Windows)" on page 308.

On UNIX:

See "About the environment variables set by a user in the XML export parameter file" on page 305.

Table F-4 shows the NetBackup for Oracle environment variables.

Table F-4 NetBackup for Oracle environment variables

Environment variable	Purpose
`NB_ORA_SERV`	Specifies the name of NetBackup master server.
`NB_ORA_CLIENT`	Specifies the name of the Oracle client. On Windows, this variable is useful for specifying a virtual client name in a cluster.

Table F-4 NetBackup for Oracle environment variables *(continued)*

Environment variable	Purpose

NB_ORA_POLICY	Specifies the name of the policy to use for the Oracle backup. To define NB_ORA_POLICY, use the RMAN PARMS statement or send statement in Oracle shell scripts. For example:
	`ALLOCATE CHANNEL ch01 TYPE 'SBT_TAPE' ;`
	`send 'NB_ORA_POLICY=Oracle_Backup' ;`
	`BACKUP`

NB_ORA_SCHED	Specifies the name of the Application Backup schedule to use for the Oracle backup.

About XML export templates and shell scripts

The following sections describe XML export templates and shell scripts. The templates and scripts are as follows:

Templates. The NetBackup for Oracle XML export wizard creates XML export templates. This wizard is initiated from the NetBackup Backup, Archive, and Restore interface.

The NetBackup for Oracle XML export wizard does not support all of the parameters that the command line utility `bporaexp` provides. You can write a shell script if a template does not provide all of the required functionality.

Shell scripts. The user writes the shell scripts. They must conform to the operating system's shell syntax. Sample XML export and import shell scripts are installed on the client with the NetBackup for Oracle agent. Modify these scripts to meet your individual requirements.

NetBackup for Oracle also provides a utility, `bpdbsbora`, that can generate a shell script from an XML export or import wizard template. A user can then create a template with the wizard and generate a shell script from it. The user can run or modify the shell script.

Creating XML export templates using the NetBackup for Oracle wizard (UNIX)

NetBackup for Oracle provides a wizard that solicits information about desired XML export operations. The wizard uses the information to create a template that can

be run immediately or saved in a NetBackup-specific location on the current master server for later use.

To create XML export templates using the NetBackup for Oracle wizard

1. Open the Backup, Archive, and Restore interface.

   See "Starting the NetBackup Backup, Archive, and Restore interface" on page 106.

2. Click the **Backup Files** tab.
3. In the left pane of the Backup, Archive, and Restore interface, expand the Oracle node.
4. In the left pane, select the Oracle database instance.

   Database objects that can be exported are listed under the Users node. Only the schema owners and objects accessible by the current user logon displays.

5. Expand the **Users** list to the schema owners of the objects to be exported.
6. In the right pane, select the Oracle objects to export.
7. Choose **Actions > Backup** to start the wizard.

   The NetBackup for Oracle XML export wizard displays the following screens for you to enter information about the export operation you want to perform:

   - Welcome
   - Target Database Logon Credentials
   - Configuration Options
   - Archive Export Options
   - NetBackup Archive Destination Options

   If you need an explanation of any of the fields on the wizard screens or more details, click **Help** on the wizard screen.

8. When you have completed the wizard, the **Template Summary** screen displays the summary of the XML export template.

   You can choose to run the template immediately after the wizard finishes, save the template to the master server, or both. For explanations of your choices, click **Help**.

   To save, to run, or to save and run the template, click **Finish**.

   See "About storing templates" on page 112.

Creating XML export templates using the NetBackup for Oracle wizard (Windows)

NetBackup for Oracle provides a wizard that solicits information about desired XML export operations. The wizard uses the information to create a template that can be run immediately or saved in a NetBackup-specific location on the current master server for later use.

To create XML export templates by using the NetBackup for Oracle wizard

1. Open the Backup, Archive, and Restore interface.

   See "Starting the NetBackup Backup, Archive, and Restore interface" on page 106.

2. Choose **File > Select Files and Folders to Backup**.
3. In the left pane, expand the Oracle node.

   Select a node in the left pane to view its details in the right pane.

4. (Optional) Enter your Oracle database logon **User name** and **Password** with SYSDBA privileges.

   Perform this step if your current logon does not have Oracle SYSDBA privileges.

   Optionally, also enter your Net service name (TNS alias).

5. In the left pane of the Backup, Archive, and Restore interface, select the Oracle database instance.

   Database objects that can be exported are listed under the Users node. Only the schema owners and objects accessible by the current user logon display.

6. Expand the User list to the schema owners of the objects to export.
7. In the right pane, select the Oracle objects to export.
8. Choose **Actions > Backup** to start the wizard.

   The NetBackup for Oracle XML Export Template Generation Wizard displays the following screens for you to enter information about the export operation that you want:

   - Welcome
   - Target Database Logon Credentials
   - Configuration Options
   - Archive Export Options
   - NetBackup Archive Destination Options

If you need an explanation of any of the fields on the wizard screens or more details, click **Help** on the wizard screen.

9 After you complete the wizard, the Selection Summary screen displays the summary of the XML export template.

You can run the template immediately after the wizard finishes, save the template to the master server, or both. For explanations of your choices, click **Help**.

To save, to run, or to save and run the template, click **Finish**.

Creating an XML export script from a template

You can use the `bpdbsbora` command to create a script from an XML export template. This command generates XML export shell scripts from the templates that the XML export wizard creates.

To create an XML export script from a template

- At the command prompt, type this command using the following options:

  `bpdbsbora -export -g` *`script_file`* `-t` *`templ_name`*`.tpl -S` *`server_name`*

  where:

`-export`	Specifies the template type.
`-g` *`script_file`*	Specifies the name of the file to which you want `bpdbsbora` to write the script. Enclose *script_file* in quotation marks if it contains blanks. This option cannot be used with the `-r` (run) option.
`-t` *`templ_name`*`.tpl`	Specifies the name of the template file name that you want to use as the basis for the script. Make sure that the template exists. `bpdbsbora` retrieves XML export templates from a known location on the master server, so specify only the template file name.
`-S` *`server_name`*	Specifies the master server upon which the template resides. When you specify the `bpdbsbora` command, it retrieves XML export templates from the specified master server.

Creating XML export scripts manually

When the database agent was initially installed, the installation software wrote example scripts to the following locations:

- For export:
  Windows:

  install_path\NetBackup\dbext\Oracle\samples\bporaexp

  UNIX:

  /usr/openv/netbackup/ext/db_ext/oracle/samples/bporaexp

- For import:
  Windows:

  install_path\NetBackup\dbext\Oracle\samples\bporaimp

  UNIX:

  /usr/openv/netbackup/ext/db_ext/oracle/samples/bporaimp

The example export scripts that are installed in `bporaexp` are as follows:

Windows:

```
data_archiver_export.cmd
```

UNIX:

```
data_archiver_export.sh

data_archiver_export64.sh

bporaexp_help.param
bporaexp_partitions.param
bporaexp_table_to_files.param
bporaexp_tables.param
bporaexp_tables_rows.param
```

The example import scripts that are installed in `bporaimp` are as follows:

Windows:

```
data_archiver_import.cmd
```

UNIX:

```
data_archiver_import.sh
```

```
data_archiver_import64.sh

bporaimp_archive.param
bporaimp_archive_schema_to_files.param
bporaimp_archive_to_users.param
bporaimp_bfile_table.param
bporaimp_help.param
bporaimp_ignore_rows_table.param
bporaimp_large_table.param
bporaimp_list.param
bporaimp_old_archive.param
bporaimp_partitions.pram
bporaimp_table_from_files.param
bporaimp_table_to_files.param
bporaimp_table_to_user.param
bporaimp_tables.param
```

To use the example scripts

1. Copy the example scripts to a different directory on your client. Oracle scripts can be located anywhere on the client.
2. Modify each script for your environment.
3. On UNIX, make sure that the `su` command logs into the correct user.

   If you do not include an `su - user` (*user* is Oracle administrator account) in your Oracle scripts, they do not run with the proper permissions and environment variables. The result is problems with your database backups and restores.

Performing an XML export archive

The following sections describe how to perform an XML export archive.

Table F-5 Tasks and commands

Task	Commands used to accomplish the task
Automatic backup of an Oracle policy	As with Oracle backups using RMAN, the most convenient way to create Oracle archives that consist of XML exports of data from your database is to set up schedules for automatic backups. The Oracle policy runs NetBackup for Oracle templates or shell scripts. For a backup using RMAN, a backup template is used, and for an XML export, an XML export template is used. When the NetBackup scheduler invokes a schedule for an automatic backup, the NetBackup for Oracle XML export templates or shell scripts run as follows: ■ In the same order as they appear in the file list ■ On all clients in the client list The NetBackup for Oracle XML export template or shell scripts start the XML export by running the NetBackup `bporaexp` or `bporaexp64` utility.
Manual backup of an Oracle policy	The administrator can use the NetBackup server software to manually run an automatic backup schedule for the Oracle policy. For more information, see the NetBackup Administrator's Guide, Volume I. See "Testing configuration settings for NetBackup for Oracle" on page 114.
User-directed XML exports from the client	The following sections describe procedures for performing user-directed XML exports. ■ Running NetBackup for Oracle XML export templates. See "Running NetBackup for Oracle XML export templates" on page 312. ■ Using bpdbsbora to run an XML export template. See "Using bpdbsbora to run an XML export template" on page 313. ■ Running the NetBackup for Oracle XML export script on the client. See "Running the NetBackup for Oracle XML export script on the client" on page 314. ■ Running bporaexp on the client as an Oracle user. See "Running bporaexp on the client as an Oracle user" on page 315. ■ Writing to a directory versus writing to a storage unit. See "Writing to a directory versus writing to a storage unit" on page 315. ■ bporaexp parameters See "About bporaexp parameters" on page 317.

Running NetBackup for Oracle XML export templates

The Template Administration interface is available in the Backup, Archive, and Restore interface.

Use this dialog to run, edit, delete, rename, and view existing XML export templates. These are the templates created by the NetBackup for Oracle XML Export Wizard and stored in a predetermined location on the master server. Before you can run,

edit, delete, or rename templates on the master server, the client must exist in a policy or in the NetBackup image catalog.

To use Oracle template administration

1. In the Backup, Archive, and Restore interface, click Actions > **Administer Database Templates > Oracle**.

   The Oracle template administration window appears.

   The **Select Template** list shows the names, descriptions, and types of the Oracle templates that are stored on the current master server.

2. Select the name of the XML export template you want to run.

3. Click **Run**.

   The Oracle template administration window provides the following functions:

Run	Runs the selected template.
Edit	Changes the contents of an existing template. The selected XML export template is loaded into the NetBackup for Oracle XML export template generation wizard.
Delete	Removes the selected template. On Windows, you must be the administrator or the template creator to delete a template. On UNIX, you must be the root user or the template creator to delete a template.
Rename	Changes the name of the selected template. On Windows, you must be the administrator or the template creator to rename a template. On UNIX, you must be the root user or the template creator to rename a template.
View	Displays a summary of the selected template.

Using bpdbsbora to run an XML export template

The `bpdbsbora` command lets you run an XML export template that the NetBackup for Oracle XML export wizard creates.

At the command prompt, type this command using the following options:

```
bpdbsbora -export -r -t templ_name.tpl [-S server_name] [-L prog_log]
```

Where:

`-export`	Specifies the template type.
`-r`	Runs the template.
`-t` *`templ_name`*`.tpl`	Specifies the name of the template file that you want to use. `bpdbsbora` retrieves the XML export templates from a known location on the master server, so specify only the file name.
`-S` *`server_name`*	Optional. Identifies the master server. `bpdbsbora` retrieves XML export templates from a specific master server when you specify this option.
`-L` *`prog_log`*	Optional. Specifies a run-time process log. Enclose *prog_log* in quotation marks (" ") if it contains space characters.

For example:

```
bpdbsbora -export -r -t sales.tpl -S my_server -L my_progress_log
```

Running the NetBackup for Oracle XML export script on the client

You can initiate a database XML export from the operating system command prompt: Type the full path to the shell script that performs the export. For example:

Windows:

```
install_path\oracle\scripts\data_archiver_export.cmd
```

UNIX:

```
/oracle/scripts/data_archiver_export.sh
```

The operating system shell starts the database XML export archive by running the XML export script. The XML export script contains commands to run `bporaexp`.

The NetBackup for Oracle installation script installs sample scripts in the following location:

Windows:

```
install_path\NetBackup\dbext\oracle\samples\bporaexp
```

UNIX:

```
/usr/openv/netbackup/ext/db_ext/oracle/samples/bporaexp
```

Running bporaexp on the client as an Oracle user

As an Oracle user you can also run the bporaexp command (bporaexp64 on some platforms) from the operating system command prompt and specify a parameter file.

To run bporaexp on the client as an Oracle user

1. Create a parameter file that specifies the settings that determine how the backup is to be performed. Information is available about the bporaexp parameters.

   See "About bporaexp parameters" on page 317.

2. Run the following command to specify the parameter file:

   ```
   # bporaexp [username/password] parfile = filename | help=y
   ```

3. Configure the runtime environment, because this method does not call the full script that includes the runtime configuration.

   On UNIX and Linux, check the sample scripts for runtime environment details.

   See "About configuring the run-time environment" on page 98.

bporaexp creates a set of XML schema and instance documents that can be used to archive Oracle table data. For each archive, one master XML schema (.xsd) document is generated. In addition, bporaexp generates a table-specific schema (.xsd) document and a table specific instance (.xml) document for each table. Additional files are created if the table contains LONG or LOB columns.

See "Performing an XML export archive" on page 311.

Writing to a directory versus writing to a storage unit

One important aspect of the parameter file is the DIRECTORY parameter. If you specify the DIRECTORY parameter, the bporaexp (bpdbsbora64 on some platforms) command writes the backup files to the operating system directory you specify. NetBackup does not write the files to a storage unit.

For example, assume that the archive test1 contains one table, USER1. If the directory parameter is specified, NetBackup creates certain files when you run the bporaexp command.

Windows:

```
DIRECTORY=\db\netbackup\xml
```

UNIX:

```
DIRECTORY=/db/netbackup/xml
```

Table F-6 shows the files NetBackup creates when you run the command.

Table F-6 NetBackup files for example table USER1

File	Content
Windows: `\db\netbackup\xml\test1\test1.xsd` UNIX: `/db/netbackup/xml/test1/test1.xsd`	Master XML schema for table `USER1`
Windows: `\db\netbackup\xml\test1\USER1\TEST1.xsd` UNIX: `/db/netbackup/xml/test1/USER1/TEST1.xsd`	Table schema for table `USER1`
Windows: `\db\netbackup\xml\test1\USER1\TEST1.xml` UNIX: `/db/netbackup/xml/test1/USER1/TEST1.xml`	XML document for table `USER1`

If the `DIRECTORY` parameter is not specified, NetBackup writes the backup images to a storage unit. A NetBackup backup set is created and cataloged under the name:

Windows:

```
\Oracle\XMLArchive
```

UNIX:

```
/Oracle/XMLArchive
```

All NetBackup for Oracle `bporaexp` backups are cataloged using this convention.

Alternatively, if the parameter file does not contain the `DIRECTORY` parameter, NetBackup creates and catalogs the following files:

Windows:

```
\Oracle\XMLArchive\test1\test1.xsd
\Oracle\XMLArchive\test1\USER1\TEST1.xsd
\Oracle\XMLArchive\test1\USER1\TEST1.xml
```

UNIX:

```
/Oracle/XMLArchive/test1/test1.xsd
/Oracle/XMLArchive/test1/USER1/TEST1.xsd
/Oracle/XMLArchive/test1/USER1/TEST1.xml
```

In production, do not use the `DIRECTORY` parameter in the `bporaexp` parameter file. When you write to a storage unit, NetBackup offers the features that include searching and cataloging with the NetBackup catalog and automatic handling of

output that exceeds file system limits. With the DIRECTORY parameter, file system limits, such as a 2 GB maximum, can cause an error.

To run bporaexp on the client, run the following command:

```
bporaexp [username/password] parfile = filename | help=y
```

On some UNIX platforms, the bporexp64 command is used.

About bporaexp parameters

This topic describes the available bporaexp (bporaexp64 on some platforms) parameters.

Note the following:

- Use the NetBackup parameters NB_ORA_SERV, NB_ORA_CLIENT, NB_ORA_POLICY, and NB_ORA_SCHED to specify the NetBackup runtime configuration. Otherwise, the order of precedence for the runtime configuration variable settings is used.
- Some parameters are valid only when you write to a storage unit. Other parameters are valid only when you write to a directory. In the following table, the Target Location column contains either Storage Unit or Directory to indicate whether the parameter in that row applies to writing to a storage unit or to a directory. Parameters that are recognized when you write to a directory are ignored when you write to a storage unit.

Table F-7 shows the available bporaexp parameters with their default values.

Table F-7 bporaexp parameters and default values

Parameter	Required?	Default	Description	Target location
CONSISTENT	N	N	Specifies if bporaexp uses the SET TRANSACTION READ ONLY statement to ensure that the data from all tables is consistent to a single point in time and does not change during the execution of the bporaexp command. If the default of CONSISTENT=N is used, each table is exported as an independent transaction.	Directory
DIRECTORY	N	no default	Optionally specifies a directory for the output of the bporaexp utility.	Directory
HELP	N	N	Displays a help message with descriptions of bporaexp parameters. Does not export data if HELP=Y.	Directory

Table F-7 bporaexp parameters and default values *(continued)*

Parameter	Required?	Default	Description	Target location
KEYWORD	N	no default	Optionally specifies a keyword phrase that NetBackup associates with the image being created by the archive operation. Values for KEYWORD must be in double quotes.	Storage Unit
LOG	N	no default	Optionally specifies a file name to receive informational and error messages. If so, messages are logged on the log file and not displayed to the terminal display.	Directory
NAME	Y	no default	The name of the master XML schema file.	Directory
NB_ORA_SERV	N	default master server	Optionally specifies the name of the NetBackup master server.	Storage Unit
NB_ORA_CLIENT	N	default client	Optionally specifies the name of the NetBackup for Oracle client.	Storage Unit
NB_ORA_POLICY	N	default Oracle policy	Optionally specifies the name of the NetBackup for Oracle policy.	Storage Unit
NB_ORA_SCHED	N	default backup policy schedule	Optionally specifies the name of the backup policy schedule to use.	Storage Unit
OWNER	N	no default	Lists the Oracle schema owners to export. For each owner, the tables, partitions, and views that are owned by that Oracle account are exported by default. The PARTITIONS and VIEWS parameters can be used to exclude partitions and views.	Directory
PARTITIONS	N	Y	Optionally specifies whether or not table partitions are included. Only valid when used with the OWNER parameter.	Directory

Table F-7 bporaexp parameters and default values *(continued)*

Parameter	Required?	Default	Description	Target location
QUERY	N	no default	Selects a subset of rows from a set of tables. The value of the query parameter is a string that contains a WHERE clause for a SQL select statement that is applied to all tables and table partitions listed in the TABLES parameter. For example, if TABLES = emp, bonus and QUERY = "where job = 'SALESMAN' and sal < 1600", two SQL statements are run: ■ SELECT*FROM emp where job='SALESMAN' and sal<1600; ■ SELECT*FROM bonus where job='SALESMAN' and sal<1600; Each query that runs refers to a single table at a time in the FROM clause, so it is illegal to have a join in the WHERE clause.	Directory
ROW_BUFFER	N	1000	Specifies the size, in rows, of the buffer used to fetch rows. Tables with LONG columns are fetched one row at a time. The maximum value allowed is 32767.	Directory
TABLES	Y	no default	Lists the table names, view names, and partition names to export. The USERID must have SELECT privilege on the tables and views. The syntax used is:schema.table: partition name or schema.view name	Directory
USERID	Y	no default	Specifies the username/password (and optional connect string) of the user initiating the export. If a connect string is not provided, the ORACLE_SID environment variable is used.	Directory
VIEWS	N	Y	Optionally specifies whether or not views are included. Only valid when used with the OWNER parameter.	Directory

Browsing XML export archives using bporaimp parameters

To use the bporaimp (bporaimp64 on some platforms) command to browse XML export archives created by using bporaexp (bporaexp64 on some platforms), create a parameter file with the desired search criteria. First, set the variables LIST=Y and USERID=*username*/. Only the archives created using the Oracle USERID are listed.

The Oracle password is not required. The operating system account that is running bporaimp has access only to archives that were created using the same account.

Note: Only XML export archives created using NetBackup mode are searched. Exports stored in an operating system directory using the DIRECTORY parameter are not searched.

Use the NB_ORA_SERV and NB_ORA_CLIENT parameters to specify the NetBackup server and client. Otherwise, the order of precedence for the runtime configuration variable settings is used. You can also include the LOG parameter.

Information is available on the LIST, LOG, NB_ORA_CLIENT, NB_ORA_SERV, and USERID parameters.

See "About bporaimp parameters" on page 326.

Table F-8 shows other parameters you can include in the parameter file.

Table F-8 Parameters you can include in a parameter file

Parameter	Default	Description
ARCHIVE_DATE_FROM	no default	Optionally specifies a start date for the archive search. Used with ARCHIVE_DATE_TO to specify a range. The date format is *mm*/*dd*/*yyyy* [*hh*:*mm*:*ss*].
ARCHIVE_DATE_TO	no default	Optionally specifies an end date for the archive search. Used with ARCHIVE_DATE_FROM to specify a range. The date format is *mm*/*dd*/*yyyy* [*hh*:*mm*:*ss*].
KEYWORD	no default	Optionally specifies a keyword phrase for NetBackup to use when searching for archives.

Table F-8 Parameters you can include in a parameter file *(continued)*

Parameter	Default	Description
NAME	no default	The name of the master XML schema file.
FROMUSER	no default	Optionally specifies a comma-separated list of table owners.
TABLES	no default	Optionally specifies a list of table and partition names that were included in an archive.

For example, assume you named the list parameter file `bporaimp_list.param`. At the command prompt, type the following:

```
bporaimp parfile = bporaimp_list.param
```

Note: On some UNIX platforms, the `bporaimp64` command is used.

Browsing XML export archives using bplist

For a higher level view of the Oracle XML export archive list, you can use the `bplist` command. The result is the list of XML schema and instance document file names.

Note: Only XML export archives created using NetBackup mode are searched. Exports stored in an operating system directory using the `DIRECTORY` parameter are not searched.

The following UNIX or Linux example uses bplist to search all Oracle archives for a client named `jupiter`. The sample output is produced for two archives, `test1` and `little_sales`, where each archive has one Oracle table (`test1` has `USER1.TEST1` and `little_sales` has `USER1.LITTLE_SALES`).

```
/usr/openv/netbackup/bin/bplist -C jupiter -t 4 -R /Oracle/XMLArch/
/Oracle/XMLArchive/test1/test1.xsd
/Oracle/XMLArchive/test1/USER1/TEST1.xsd
/Oracle/XMLArchive/test1/USER1/TEST1.xml
/Oracle/XMLArchive/little_sales/little_sales.xsd
/Oracle/XMLArchive/little_sales/USER1/LITTLE_SALES.xsd
/Oracle/XMLArchive/little_sales/USER1/LITTLE_SALES.xml
/exb_n2bm5bco_1_1392342936
```

```
/exb_mabm02ko_1_1392170136
/exb_lqbltds6_1_1392083334
```

The following Windows example uses bplist to search all Oracle archives for a client named `jupiter`. The sample output is produced for one archive, `test`.

```
install_path\NetBackup\bin\bplist -C jupiter -t 4 -R Oracle:\XMLArch\
Oracle:\XMLArchive\test\test.xsd
Oracle:\XMLArchive\test\SCOTT\BONUS.xsd
Oracle:\XMLArchive\test\SCOTT\BONUS.xml
Oracle:\XMLArchive\test\SCOTT\DEPT.xsd
Oracle:\XMLArchive\test\SCOTT\DEPT.xml
Oracle:\XMLArchive\test\SCOTT\EMP.xsd
Oracle:\XMLArchive\test\SCOTT\EMP.xml
Oracle:\XMLArchive\test\SCOTT\SALGRADE.xsd
Oracle:\XMLArchive\test\SCOTT\SALGRADE.xml
```

The `-t 4` on this command specifies the Oracle backups or archives. The `-R` specifies the default number of directory levels to search, 999.

For more information on this command, see the `bplist` man page in the NetBackup Commands Reference Guide.

Restoring an XML export archive

Before you attempt to restore an archive, make sure that the XML archive has successfully completed. You can identify the correct archive to restore by browsing the XML export archives. NetBackup generates an error if an archive backup history does not exist.

Running the XML import wizard on the client

NetBackup for Oracle includes an XML import wizard that solicits information from the user about the desired import operations. The wizard uses the information to create a template. You can use the template immediately, or you can save it for later use.

The NetBackup for Oracle XML import wizard saves an XML import template locally in a user-specified location on the NetBackup client. XML import templates are not stored on the server because a restore is always user directed, not scheduled. Typically, you run an XML import template immediately and then delete it.

The restore process requires a password for Oracle database access. Templates store encrypted passwords that are decrypted at runtime.

To start the XML import wizard

1. Start the NetBackup Backup, Archive, and Restore interface.

   On UNIX and Linux, from the command line, run the following command:

   ```
   /usr/openv/netbackup/bin/jbpSA &
   ```

2. Do one of the following:

   - On Windows: From the Windows Start menu, choose **All Programs > Veritas NetBackup > Backup, Archive, and Restore**. To change the policy type, choose File > **Specify NetBackup Machines and Policy Type**. Perform this step if the Oracle node is not visible.
   - On UNIX and Linux: (Conditional) To change the policy type, choose Actions > **Specify NetBackup Machines and Policy Type**.

3. Do one of the following:

   - On Windows, click **Select for Restore**.
   - On UNIX and Linux, click the Restore Files tab.

4. Expand the Oracle node in the left pane to view an Oracle database instance hierarchy in the right pane.

To use the XML import wizard

1. In the left pane of the Backup, Archive, and Restore interface, select the Oracle database instance.

   Database objects that can be imported are listed under the **Users** node. The tool displays only the schema owners and objects accessible by the current user login.

2. Expand the **Users** list to the schema owners of the objects to be imported.
3. In the right pane, select database objects that exist in the archive to be restored.
4. Choose Actions > **Restore**.
5. Enter information about the restore operation you want to perform in the screens that the NetBackup for Oracle XML import wizard displays.

   The screens are as follows:

   - Welcome
   - Target Database Logon Credentials
   - Archive Import Options
   - NetBackup Archive Source Options

- NetBackup Import Destination Options (Windows)

If you need an explanation of any of the fields on the wizard screens, or more details, click **Help** on the wizard screen.

6 Review the summary.

When you have completed the wizard, the Selection Summary screen displays the summary of the XML import template.

You can choose to run the template immediately after the wizard finishes, save the template locally, or both.

See "About storing templates" on page 112.

Using bpdbsbora to run an XML import template

The `bpdbsbora` command lets you run an XML import template that the NetBackup XML Import Wizard creates.

At the command prompt, type this command with the following options:

```
bpdbsbora -import -r -t templ_name.tpl [-L progress_file]
```

where:

`-import`	Specifies the template type.
`-r`	Runs the template.
`-t templ_name.tpl`	Specifies the full path name of the template you want to use. Unlike export templates, XML import templates do not reside in a predetermined location on the master server. They are considered to be temporary in nature and should reside on the client. If the full path is not specified as part of the XML import template name, it must reside in the current directory.
`-L progress_file`	Optional. Specifies a run-time progress log. Enclose *progress_file* in quotation marks (" ") if it contains space characters.

For example:

Windows:

```
bpdbsbora -import -r -t H:\oracle\imp_tpls\sales_imp.tpl -L prog_file
```

UNIX:

```
bpdbsbora -import -r -t /oracle/imp_tpls/sales_imp.tpl -L prog_file
```

Running an XML import script on the client

You can initiate a restore from the operating system command prompt by typing the full path to the XML import script that initiates the restore. For example:

Windows:

```
install_path\oracle\scripts\data_archiver_import.cmd
```

UNIX:

```
/oracle/scripts/data_archiver_import.sh
```

The operating system shell starts the database restore by running the XML import script file. The XML import script file contains commands to run `bporaimp` (`bporaimp64` on some platforms).

The NetBackup for Oracle installation script writes sample scripts to the following location:

Windows:

```
install_path\NetBackup\dbext\oracle\samples\bporaimp
```

UNIX:

```
/usr/openv/netbackup/ext/db_ext/oracle/samples/bporaimp
```

Running bporaimp on the client

Run the `bporaimp` command from the operating system command line on the client using the appropriate parameter file.

The Windows account that runs `bporaimp` has access only to XML export archives that were created using the same Windows account.

The UNIX account that runs `bporaimp` has access only to XML export archives that were created using the same UNIX account. Be sure to configure the runtime environment, because this method does not call the full script that includes the runtime configuration. Check the sample scripts for runtime environment details.

To run bporaimp on the client

- At the command prompt, type the `bporaimp` command in the following format:

  ```
  bporaimp [username/password] parfile = filename | help=y
  ```

  On some UNIX platforms, the `bporaimp64` command is used.

  See "About bporaimp parameters" on page 326.

About bporaimp parameters

Use the NetBackup parameters NB_ORA_SERV and NB_ORA_CLIENT to specify the NetBackup runtime configuration. Otherwise, the order of precedence for the runtime configuration variable settings is used.

Some parameters are valid only when writing to a storage unit. Other parameters are valid only when writing to a directory. In the following table, the right-most column contains either “Storage Unit” or “Directory” to indicate whether the parameter in that row is applicable for either writing to a storage unit or to a directory. Parameters that are recognized when writing to a directory are ignored when writing to a storage unit.

Table F-9 describes the bporaimp (bporaimp64 on some platforms) parameters and default values.

Table F-9 bporaimp parameters and default values

Parameter	Required?	Default	Description	Target location
ARCHIVE_DATE_FROM	N	no default	Optionally specifies a start date for the archive to be imported. Used with ARCHIVE_DATE_TO to specify a range. If not used, the most recent archive is imported. If the range used results in more than one archive, the most recent from the range is used. The date format is *mm/dd/yyyy [hh:mm:ss]*.	Storage Unit
ARCHIVE_DATE_TO	N	no default	Optionally specifies an end date for the archive to be imported. Used with ARCHIVE_DATE_FROM to specify a range. If not used, the most recent archive is imported. If the range used results in more than one archive, the most recent from the range is used. The date format is *mm/dd/yyyy [hh:mm:ss]*.	Storage Unit
BFILE_DIRECTORY	Y (if any table being imported has BFILE columns)	no default	Specifies a directory for the output of any BFILE columns being imported. Oracle’s CREATE DIRECTORY command can be used to create the DIRECTORY in Oracle, and the name should match the name used in the export file.	Directory

Table F-9 bporaimp parameters and default values *(continued)*

Parameter	Required?	Default	Description	Target location
COMMIT	N	N	Specifies whether bporaimp should commit after each array insert. The size of the array is determined by ROW_BUFFER. By default, bporaimp commits only after loading each table, and performs a rollback when an error occurs, before continuing with the next object.	Directory
DIRECTORY	N	no default	Optionally specifies a directory for the input of the bporaimp utility.	Directory
FROMUSER	N	no default	Optionally specifies a comma-separated list of users to import from an archive containing multiple users' tables. If not specified, all of the tables are imported.	Directory
HELP	N	N	Displays a help message with descriptions of bporaimp parameters.	Directory
IGNORE_ROWS	N	N	Specifies whether or not rows should be inserted into a table that is not empty. The default is that the table already exists and that it is empty. If it is not empty, IGNORE_ROWS = N causes an error to be reported, and the table is skipped with no rows inserted. IGNORE_ROWS = Y causes rows to be inserted with errors reported in the log file. If IGNORE_ROWS = Y and an error such as a primary key constraint violation occurs, no data is inserted if COMMIT = N. However, if COMMIT = Y, the array of rows (size determined by ROW_BUFFER) is not inserted, but bporaimp continues to process additional row arrays in the order in which they were exported. To cause all rows that do not violate a primary key constraint to be inserted, set COMMIT = Y, ROW_BUFFER = 1, and IGNORE_ROWS = Y.	Directory
KEYWORD	N	no default	Optionally specifies a keyword phrase for NetBackup to use when searching for archives from which to restore files.	Storage Unit

Table F-9 bporaimp parameters and default values *(continued)*

Parameter	Required?	Default	Description	Target location
LIST	N	N	LIST = Y queries the NetBackup catalog and lists the archives available. Does not import the data if LIST = Y.	Storage Unit
LOG	N	no default	Optionally specifies a file name to receive informational and error messages. If this parameter is specified, messages are logged in the log file and not displayed to the terminal display.	Directory
NAME	Y	no default	The name of the master XML schema file. This parameter is required if LIST = N.	Directory
NB_ORA_SERV	N	default master server	Optionally specifies the name of the NetBackup master server.	Storage Unit
NB_ORA_CLIENT	N	default client	Optionally specifies the name of the NetBackup for Oracle client.	Storage Unit
RESTORE_SCHEMA_ONLY	N	N	Used with RESTORE_TO_DIRECTORY to restore the XML schema files only to a directory.	Storage Unit
RESTORE_TO_DIRECTORY	N	no default	Optionally specifies a directory for the output of the bporaimp utility. If used, the XML data is not parsed and inserted into Oracle.	Storage Unit
ROW_BUFFER	N	1000	Specifies the size, in rows, of the buffer used to insert rows. Tables with LONG or LOB columns are inserted one row at a time. The maximum value allowed is 32767.	Directory

Table F-9 bporaimp parameters and default values *(continued)*

Parameter	Required?	Default	Description	Target location
TABLES	N	no default	Optionally specifies a list of table, view, and partition names to import. If not used, all objects in the archive are imported. The objects must already exist, and the USERID must have INSERT privilege on the objects. The object names cannot be qualified with owner names, and the FROMUSER parameter is used to specify a particular owner. If a partition name is specified, it indicates the exported partition only and the rows are inserted according to the partitioning scheme of the target table. If the export contains partitions, and the import does not specify them, all are inserted.	Directory
TOUSER	N	no default	Optionally specifies a comma-separated list of users to import to that can be used with the FROMUSER parameter to change the table owners. The TOUSER Oracle accounts must already exist, and the USERID must have INSERT privilege on the tables that must also exist.	Directory
USERID	Y	no default	Specifies the username/password (and optional connect string) of the user initiating the import. If a connect string is not provided, the ORACLE_SID environment variable is used.	Directory

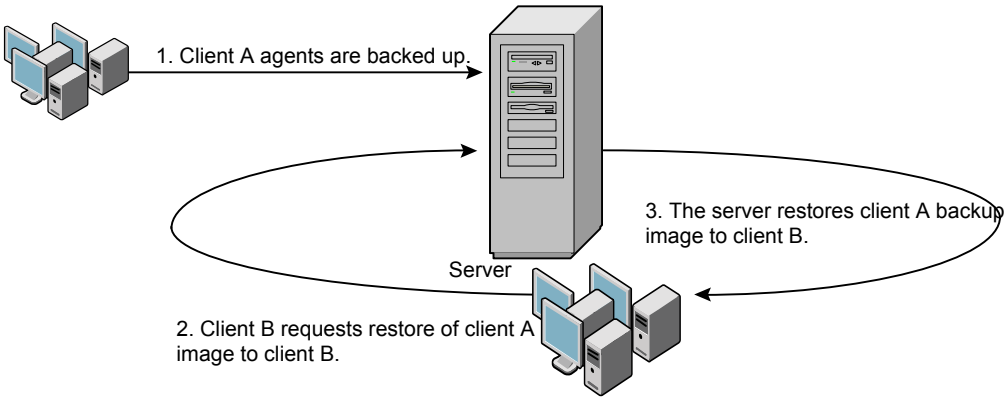
About redirecting a restore of an XML export archive to a different client

With NetBackup for Oracle you have the option to restore an XML export archive to a client other than the one that originally performed the XML export. The process of restoring data to another client is called a redirected restore.

Before you redirect the restore, see the following topic:

Figure F-5 illustrates a typical redirected restore.

Figure F-5 Redirected restore of an XML export archive to a different client



The user on client A cannot initiate a redirected restore to client B. Only the user on client B, which is the client receiving the backup image, can initiate the redirected restore. Any user who belongs to the database group that performed the backup can restore it, unless the BKUP_IMAGE_PERM variable is set to USER.

Redirecting a restore of an XML export archive to a new client using bporaimp

On UNIX and Linux, any user who belongs to the database group that performed the archive can restore XML export archive. The BKUP_IMAGE_PERM variable must be set to GROUP or ANY, not USER.

Perform the following procedure on the new client host if you want to restore XML export archives that are owned by another client.

To redirect a restore of an XML export archive to a new client using bporaimp

1. Set the environment variables for `bporaimp` (`bporaimp64` on some platforms) on the new client, including `ORACLE_HOME` and `ORACLE_SID`.
2. In the `bporaimp` parameter file, include the following lines:

   ```
   nb_ora_serv = NetBackup_server
   nb_ora_client =
   original_client_where_XML_export_occurred.
   ```

3. Specify any other `bporaimp` parameters.

   See “Running bporaimp on the client” on page 325.

4. Run `bporaimp`.

Example - Using bporaimp for a redirected restore

For example, assume the following:

- Original client is `jupiter`
- New client is `saturn`
- Server is `jupiter`
- `ORACLE_SID` is test on both `saturn` and `jupiter`
- Windows user is `ora` on both `jupiter` and `saturn`
- UNIX user is `ora` on both `jupiter` and `saturn`
- Archive name is `sales`

To use bporaimp for a redirected restore (example)

1. Create the following file on server `jupiter`:

   Windows:

   install_path\NetBackup\db\altnames\saturn

   UNIX:

   /usr/openv/netbackup/db/altnames/saturn

2. Edit the preceding file to contain the name `jupiter`.
3. Log on to `saturn` as `ora`.
4. Create file `bporaimp.param`.

   Include the following parameters:

   ```
   NAME = sales
   NB_ORA_SERV = jupiter
   NB_ORA_CLIENT = jupiter
   USERID = orauser/orapasswd
   ```

5. Run `bporaimp parfile=bporaimp.param` to restore `sales` archive to `saturn` and to import the data into the `test` database on `saturn`.

Troubleshooting XML export or XML import errors

An XML export or import error can originate from NetBackup or from Oracle, as follows:

- On the NetBackup side, an error can be from the bporaexp or bporaimp programs, the NetBackup server or client, or Media Manager.
- On the Oracle side, an error can be from the target database.

Use the following steps when troubleshooting a failed operation:

- Check the logs to determine the source of the error.
- Troubleshoot each stage of the XML export or XML import.
  The following sections describe these steps in detail.
  On UNIX and Linux, these sections describe the log files from the bporaexp and bporaimp commands. The logs are created in /usr/openv/netbackup/logs/bporaexp or /usr/openv/netbackup/logs/bporaimp.

Checking the logs to determine the source of an error

This topic describes how to check the logs to determine the source of an error.

To check the logs

1. Check the bporaexp or bporaimp log.

   If the LOG parameter is specified in the bporaexp or bporaimp command's parfile, the commands write logs to the file that is specified as the argument to the LOG parameter. The commands write log information to the screen if LOG is not specified.

   For example, incorrect installation or configuration causes the following common problems:

   - The ORACLE_HOME environment variable was not set.
   - The bporaexp or bporaimp program was unable to connect to the target database.

   When bporaexp and bporaimp are being used and the backup images are being written to an operating system directory, these logs are the only source of error logging and tracking.

2. Check the NetBackup logs.

   On Windows, the first NetBackup log to check is *install_path*\NetBackup\logs\bporaexp\log.mmddyy or *install_path*\NetBackup\logs\bporaimp\log.mmddyy.

   On UNIX, the first NetBackup log to check is /usr/openv/netbackup/logs/bporaexp/log.mmddyy or /usr/openv/netbackup/logs/bporaimp/log.mmddyy.

Examine these logs for messages that show how to determine the source of an error.

These logs are written by the NetBackup client and contain the following:

- Requests from bporaexp and bporaimp
- Activities between bporaexp and bporaimp and NetBackup processes

If the logs do not contain any messages, the following conditions could be present:

- bporaexp or bporaimp terminated before requesting service from NetBackup.
- bphdb (if started by the scheduler or graphical user interface) did not start the template or shell script successfully. Check the bphdb logs for stderr and stdout files.

Try to run the XML export or XML import template or script file from the command line to determine the problem.

On UNIX, the error is usually due to a file permission problem for bphdb itself or for the export or import script file.

Ensure that the full XML export or import script file name is entered correctly in the Backup Selections list of the Oracle policy configuration, or for templates, that the name is correct.

On UNIX, logs are not created in this directory if the permissions are not set for the Oracle user to write to the directory. The full permissions setting, chmod 777, is best.

For more information about debug logs and reports, refer to the NetBackup Administrator's Guide, Volume I.

Troubleshooting each stage of the XML export or XML import

The information in this section does not apply to you if DIRECTORY is specified in bporaexp or bporaimp command's parfile.

The following explains the sequence of events for an action that bporaexp or bporaimp initiates in NetBackup mode. This situation occurs when DIRECTORY is not specified in the bporaexp or bporaimp command's parfile. It suggests solutions for the problems that can occur at each point in the sequence.

To troubleshoot by stage

1 bporaexp or bporaimp starts.

An export or import can be started in any of the following ways:

- Command line from the system prompt.
  For example:

  ```
  bporaexp parfile = parameter_filename
  bporaimp parfile = parameter_filename
  ```

- Using a template that is run from the NetBackup client GUI or `bpdbsbora`.
- Manually from the NetBackup Administration Console on the master server.
- Automatically by an automatic export schedule.

If an error occurs now, check the `bporaexp` or `bporaimp` log.

2 `bporaexp` or `bporaimp` verifies its environment and then connects to Oracle and NetBackup.

An Oracle environment problem, a database problem, an incorrect user ID, or an incorrect password can cause Oracle connect errors.

A NetBackup error now is usually due to a problem with client and server communication. Check the messages in the `bprd` and `bpcd` logs for clues.

Also verify the `bp.conf` entries on the UNIX or Linux client.

3 `bporaexp` or `bporaimp` issues a backup or restore request.

Before the backup or restore request proceeds, `bporaexp` or `bporaimp` commands perform three functions:

- Gather necessary parameters
- The backup or restore request is sent to the NetBackup server
- Wait until the server and client are ready to transfer data

The NetBackup client interfaces gather information from the following places:

- The environment, including `bporaexp` and `bporaimp` parameter files. If you use templates, the parameter files are generated from the template.
  If you use scripts, you have to generate the parameter file manually.
- Server configuration parameters on Windows.
- The user's `bp.conf` and `/usr/openv/netbackup/bp.conf` files on the UNIX or Linux client.

This information is sent to the master server's `bprd` process.

To troubleshoot a backup problem in this part of the sequence, examine the following file:

Windows:

install_path\NetBackup\logs\bporaexp\log.*mmddyy*

UNIX:

/usr/openv/netbackup/logs/bporaexp/log.*mmddyy*

If the bprd process failed, check the bprd and bpbrm logs.

During this sequence, most failures occur because of incorrect NetBackup server or Oracle policy configuration parameters.

NetBackup can usually select the correct Oracle policy and schedules. However, NetBackup can select a policy or schedule in error if there are several Oracle policies in its database.

In Windows, try setting the SERVER and POLICY values in the client environment or by setting the following bporaexp parameters:

NB_ORA_POLICY=*policyname*
NB_ORA_SCHED=*schedule*
NB_ORA_SERV=*NetBackup_server*
NB_ORA_CLIENT=*NetBackup_client*

In UNIX, try setting the SERVER and POLICY values in the bp.conf file on the client or by setting the following bporaexp parameters:

NB_ORA_POLICY=*policyname*
NB_ORA_SCHED=*schedule*
NB_ORA_SERV=*NetBackup_server*
NB_ORA_CLIENT=*NetBackup_client*

To troubleshoot a restore, examine the following log file:

Windows:

install_path\NetBackup\logs\bporaimp*mmddyy*.log

UNIX:

/usr/openv/netbackup/logs/bporaimp/log.*mmddyy*

Make sure that the correct NetBackup server and NetBackup client values are used by setting the following bporaimp parameters:

NB_ORA_SERV=*NetBackup_server*
NB_ORA_CLIENT=*NetBackup_client*

Set these parameters to the same values that were used for the XML export operation.

4 bporaexp or bporaimp issues read or write requests to the NetBackup client, which then transfers data to or from the NetBackup server.

bporaexp builds an SQL query for each table being archived, and it uses the Oracle Call Interface (OCI) to run the query. The query results are translated into XML. The XML output is passed to the NetBackup client interfaces.

bporaimp uses the reverse process. That is, XML data is restored, parsed, and inserted into the database.

A failure here is probably due to an Oracle error, or to a NetBackup media, network, or timeout error.

5 bporaexp or bporaimp tells the NetBackup client to close the session and disconnects from the Oracle database.

The NetBackup client waits for the server to complete its necessary actions (backup image verification and so on) and then exits.

Additional XML export and import logs

The bporaexp and bporaimp utilities perform error logging and tracing in the file that is specified by the LOG parameter. The log files contain Oracle errors and other errors that are not related to NetBackup.

When bporaexp and bporaimp are used and the backup images are written to a storage unit, these errors are also logged in the NetBackup debug logs. These logs appear in the following directories:

Windows:

install_path\NetBackup\logs\bporaexp
install_path\NetBackup\logs\bporaimp

UNIX and Linux:

/user/openv/netbackup/logs/bporaexp
/user/openv/netbackup/logs/bporaimp

When you use bporaexp and bporaimp and the backup images are written to an operating system directory, the file that is specified by the LOG= parameter is the only source of error logging and tracing.

Appendix G

Register authorized locations

This appendix includes the following topics:

Registering authorized locations used by a NetBackup database script-based policy

During a backup, NetBackup checks for scripts in the default script location and any authorized locations. The default, authorized script location for UNIX is `usr/openv/netbackup/ext/db_ext` and for Windows is `install_path\netbackup\dbext`. If the script is not in the default script location or an authorized location, then the policy job fails. You can move any script into the default script location or any additional authorized location and NetBackup recognizes the scripts. You need to update the policy with the script location if it has changed. An authorized location can be a directory and NetBackup recognizes any script within that directory. An authorized location can also be a full path to a script if an entire directory does need to be authorized.

If the default script location does not work for your environment, use the following procedure to enter one or more authorized locations for your scripts. Use `nbsetconfig` to enter an authorized location where the scripts reside. You can also use `bpsetconfig`, however this command is only available on the master or the media server.

Note: One recommendation is that scripts should not be world-writable. NetBackup does not allow scripts to run from network or remote locations. All scripts must be stored and run locally. Any script that is created and saved in the NetBackup `db_ext` (UNIX) or `dbext` (Windows) location needs to be protected during a NetBackup uninstall.

For more information about registering authorized locations and scripts, review the knowledge base article:

http://www.veritas.com/docs/000126002

To add an authorized location

1. Open a command prompt on the client.
2. Use `nbsetconfig` to enter values for an authorized location. The client privileged user must run these commands.

   The following examples are for paths you may configure for the Oracle agent. Use the path that is appropriate for your agent.

   - On UNIX:

     ```
     [root@client26 bin]# ./nbsetconfig
     nbsetconfig>DB_SCRIPT_PATH = /Oracle/scripts
     nbsetconfig>DB_SCRIPT_PATH = /db/Oracle/scripts/full_backup.sh
     nbsetconfig>
     <ctrl-D>
     ```

   - On Windows:

     ```
     C:\Program Files\Veritas\NetBackup\bin>nbsetconfig
     nbsetconfig> DB_SCRIPT_PATH=c:\db_scripts
     nbsetconfig> DB_SCRIPT_PATH=e:\oracle\fullbackup\full_rman.sh
     nbsetconfig>
     <ctrl-Z>
     ```

Note: Review the NetBackup Command Reference Guide for options, such as reading from a text file and remotely setting clients from a NetBackup server using `bpsetconfig`. If you have a text file with the script location or authorized locations listed, `nbsetconfig` or `bpsetconfig` can read from that text file. An entry of `DB_SCRIPT_PATH=none` does not allow any script to execute on a client. The `none` entry is useful if an administrator wants to completely lock down a server from executing scripts.

3 (Conditional) Perform these steps on any clustered database or agent node that can perform the backup.

4 (Conditional) Update any policy if the script location was changed to the default or authorized location.

Index

C

D

E

F

G

H

I

J

K

L

M

N

O

T

U

V

W

X