NetBackup 7.6 Feature Briefing

Oracle Intelligent Policy

Version number: 1.0

Issue date: 28th August 2013

This document describes a feature introduced in NetBackup 7.6 and available in this and higher releases.

If you have any feedback or questions about this document please email them to **IMG-TPM-Requests@symantec.com** stating the document title.

This document is provided for informational purposes only. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Confidence in a connected world. Symantec.

Feature Description

NetBackup 7.6 introduces the Oracle Intelligent Policy feature which has been designed to simplify the process of Oracle backup, make it more reliable, and more user friendly. The new policy model includes a number of improvements to the way in which policies for protecting Oracle databases are configured and operate, including:

- Automatic discovery of Oracle Instances
- Simplified scheduling
- Checkbox policy options to control backup parameters
- Dynamic backup script generation

Existing Oracle users are not obliged to switch to the new policy model as NetBackup 7.6 supports both the old and new models.

Business Value

The Oracle Intelligent Policy represents a significant simplification of the way in which Oracle instances are detected and protected with NetBackup. This simplification translates into reduced operational expenditure and improved protection of Oracle databases. Automatically discovering Oracle instances ensures that newly created databases are included in the data protection plan. Dynamically creating the backup scripts reduces the man power required to both implement and modify the backup procedures as business requirements change.

Underlying Principles

The oracle Intelligent Policy feature in NetBackup 7.6 can be considered as consisting of several discrete components:

- The **auto discovery** component uses a persistent process on the NetBackup client to identify Oracle instances on the clients and passes that information to an XML database on the master server.
- The **registration process** uses the Application Management section of the administration GUI to allow the administrator to enter access credentials for them. Registered instances are then stored in the main NetBackup databases. Where common access credentials are used it is

possible to create “instance groups” for multiple instances. Instances can also be automatically registered under a default instance group. In environments where security restrictions prohibit the sharing of access credentials between DBAs and NetBackup Administrators the NetBackup Administrator can grant a DBA permission to register instances and update their credentials directly from the NetBackup client, avoiding the need to share credential information.

- Once an instance has been registered the **backup policy wizard** can be used to create a backup policy.
- The resulting **backup policies** are both simpler and more flexible than the old policy type with a single schedule for each backup type and the ability to specify attributes such as the number of filer per backup set and the way in which archived redo logs are handled.
- Because the **backup scripts** are created dynamically at backup run time there is no need to access the client machines or maintain scripts on them. Any changes made to the backup polices are picked up and executed the next time the policy is run.

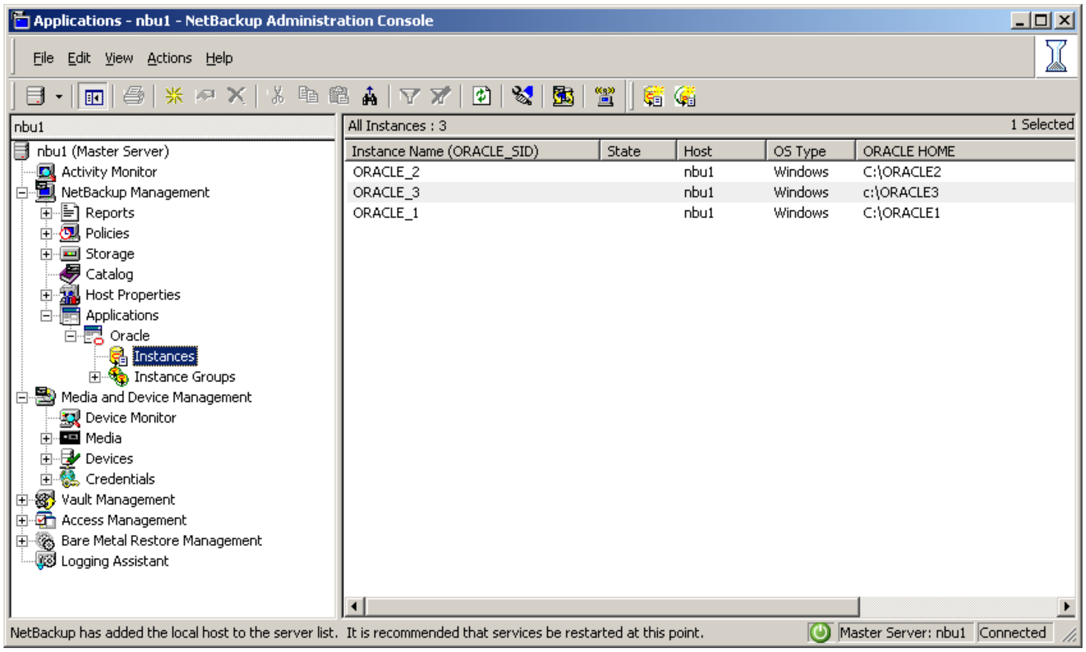
Guided Tour

Auto Discovery and Registration

Auto Discovery of Oracle instances involves a proactive communication from the client to the master server. A new persistent process (`nbdisco`) has been added to the NetBackup client and is started automatically when the client software is installed. Data about the client configuration, including any Oracle instances that exist on the client, is gathered and pushed to the master server’s discovery XML database even before a backup is run. This discovery process is repeated every 4 hours and each time the client services are started.

The master server polls the discovery XML database on a regular basis to obtain data on the clients in the current master server domain. The information contained in the discovery XML database is transient and is transferred to NBDB by this polling process. By default the discovery XML database is polled every 4 hours, but this period can be changed by setting the parameter `NBARS_DISCOVERY_TIMER = <seconds>` in the client’s bp.conf file or registry.

Information about the Oracle instances discovered on the client can then be viewed under Applications > Oracle > Instances tab on the NetBackup Administration GUI as seen in Figure 1 below.



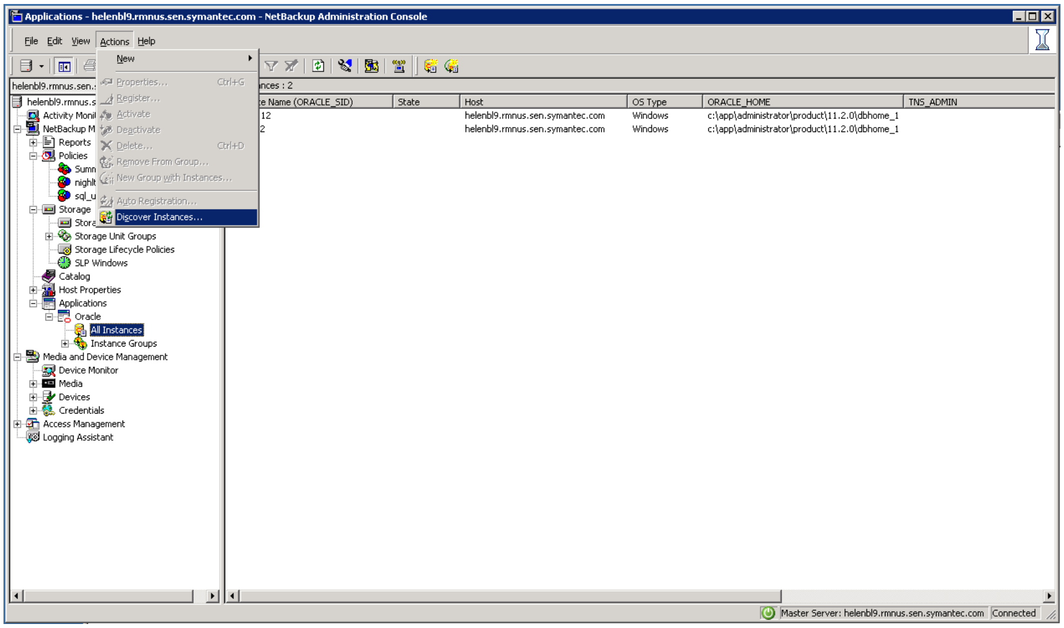
All Instances : 3 — 1 Selected

Instance Name (ORACLE_SID)	State	Host	OS Type	ORACLE HOME
ORACLE_2		nbu1	Windows	C:\ORACLE2
ORACLE_3		nbu1	Windows	c:\ORACLE3
ORACLE_1		nbu1	Windows	C:\ORACLE1

NetBackup has added the local host to the server list. It is recommended that services be restarted at this point.

Figure 1 – Discovered Oracle Instances

The GUI also provides a mechanism for manually performing discovery in the current master server domain as seen in Figure 2. When manual discovery is performed, the NetBackup master server initiates communication with each discovered client in the master server domain and requests updated discovery information.

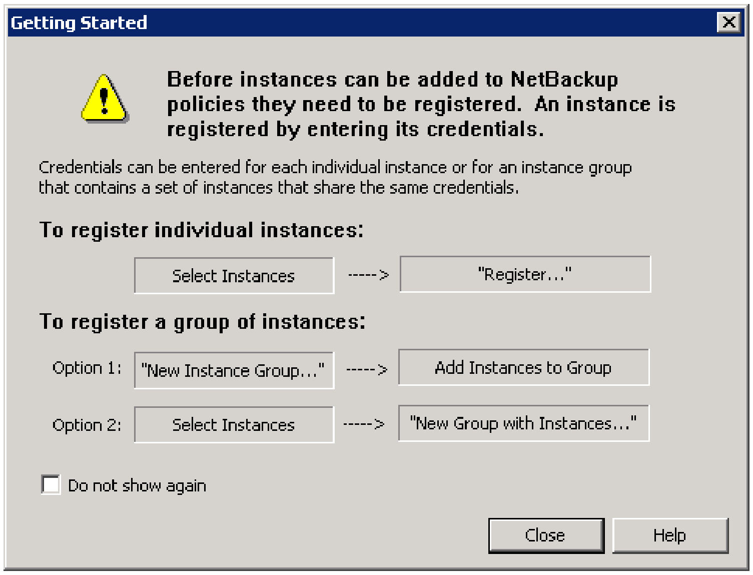


nces : 2

e Name (ORACLE_SID)	State	Host	OS Type	ORACLE_HOME	TNS_ADMIN
12		helenbl9.rmnus.sen.symantec.com	Windows	c:\app\administrator\product\11.2.0\dbhome_1	
2		helenbl9.rmnus.sen.symantec.com	Windows	c:\app\administrator\product\11.2.0\dbhome_1	

Figure 2 - Initiating manual Oracle Instance discovery

Once discovered, instances must be registered in NetBackup before they can be selected by the backup policy wizard and configured in a backup policy. A warning message reminding the administrator of this requirement is generated when Applications > Oracle > Instances is selected (Figure 3).



Getting Started

Before instances can be added to NetBackup policies they need to be registered. An instance is registered by entering its credentials.

Credentials can be entered for each individual instance or for an instance group that contains a set of instances that share the same credentials.

To register individual instances:

Select Instances -----> "Register..."

To register a group of instances:

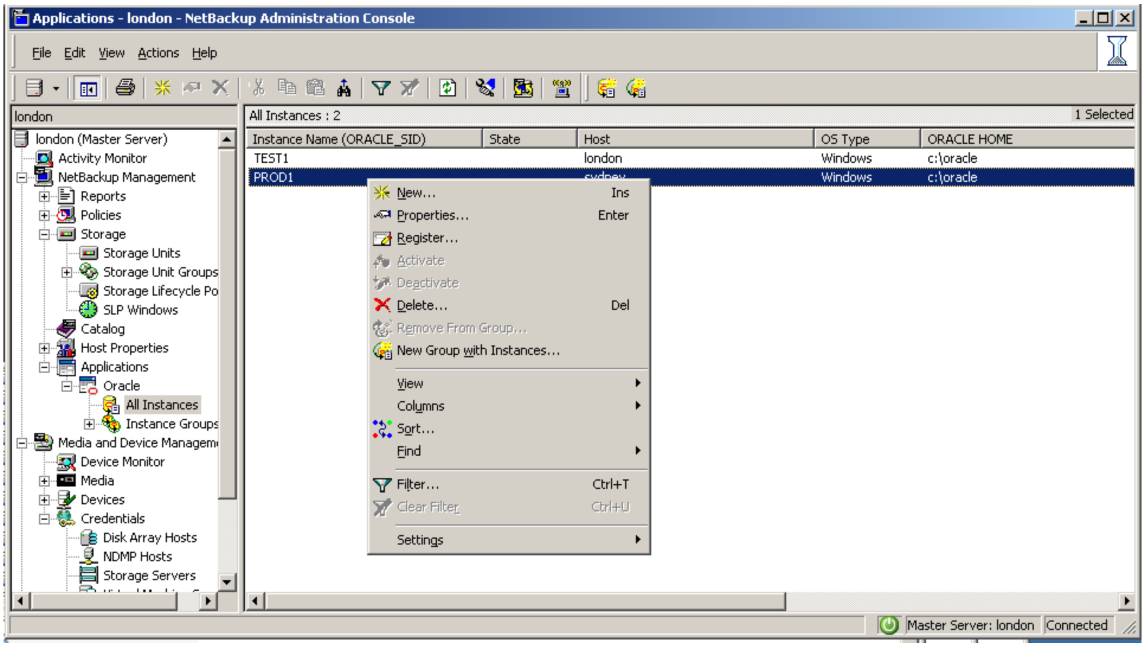
Option 1: "New Instance Group..." -----> Add Instances to Group

Option 2: Select Instances -----> "New Group with Instances..."

□ Do not show again

Figure 3 – Instance Registration Warning

To add credentials and register an instance select the instance and either right click and select "register" or select "Register" from the "Actions" on the tool bar (Figure 4).



Applications - london - NetBackup Administration Console

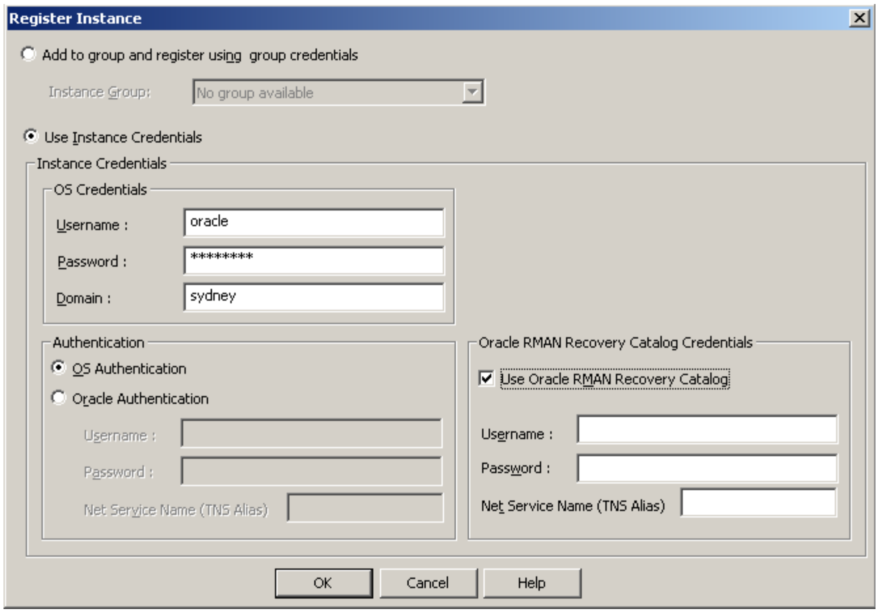
All Instances : 2 — 1 Selected

Instance Name (ORACLE_SID)	State	Host	OS Type	ORACLE HOME
TEST1		london	Windows	c:\oracle
PROD1		sydney	Windows	c:\oracle

Master Server: london Connected

Figure 4 – Selecting an instance to register.

The credentials for the instance and any associated RMAN catalog can then be added (Figure 5)



Register Instance

○ Add to group and register using group credentials

Instance Group: No group available

● Use Instance Credentials

Instance Credentials

OS Credentials

Username : oracle

Password : ********

Domain : sydney

Authentication

● OS Authentication

○ Oracle Authentication

Username :

Password :

Net Service Name (TNS Alias)

Oracle RMAN Recovery Catalog Credentials

☑ Use Oracle RMAN Recovery Catalog

Username :

Password :

Net Service Name (TNS Alias)

Figure 5 – Registering an instance

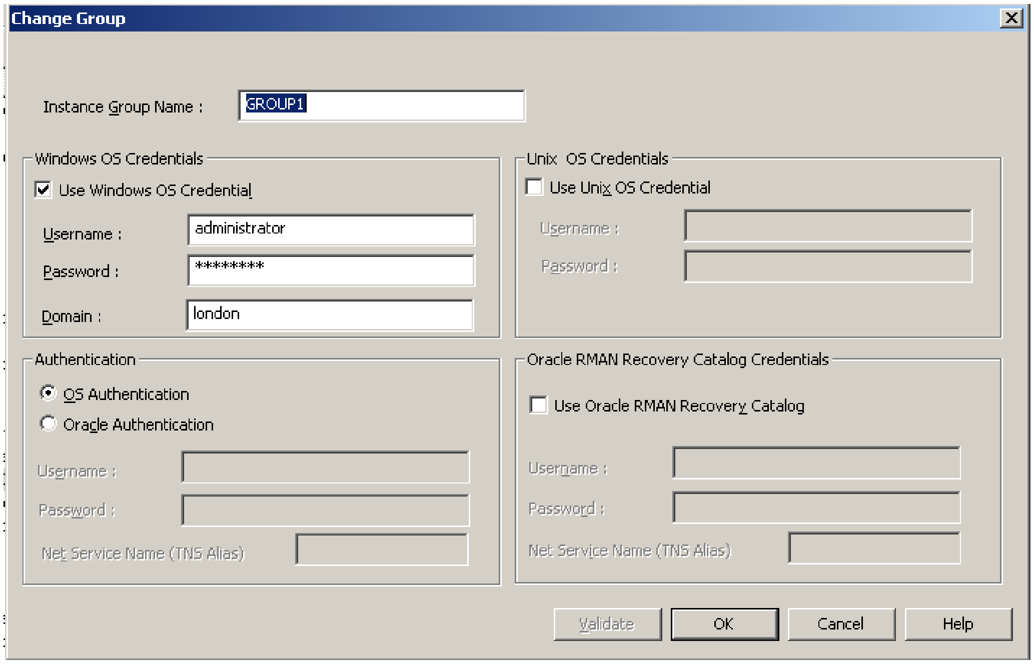
The Instance must be registered (credentials added) before it can be added to a NetBackup Oracle Policy. Once the credentials have been added, they are validated on the target host and an error message will pop up if the credentials are incorrect.

If the security policy does not allow the database administrator (DBA) to share the instance credentials with the NetBackup administrator an alternative registration method is available that allows the DBA to enter them directly from the NetBackup client machine. To use this feature the NetBackup administrator must first authorize the DBA to make changes on the master server by running the command:

```
nboraadm [-S master_server] -add_dba <client_name> <user_name>
```

The DBA can then use the `nboraadm` command to register instances on the specified client machine and modify access credentials for those instances without involving the NetBackup administartor.

As a typical Oracle environment may have many instances, an option to create instance groups has been included to simplify the credential process. Groups can be created by selecting the “New group with instances” option when registering an instance or “Add new instance group” from the Instance Groups. Group credentials are added in the same way that individual instance credentials are added (Figure 6).



Change Group

Instance Group Name : GROUP1

Windows OS Credentials

☑ Use Windows OS Credential

Username : administrator

Password : *********

Domain : london

Unix OS Credentials

☐ Use Unix OS Credential

Authentication

● OS Authentication

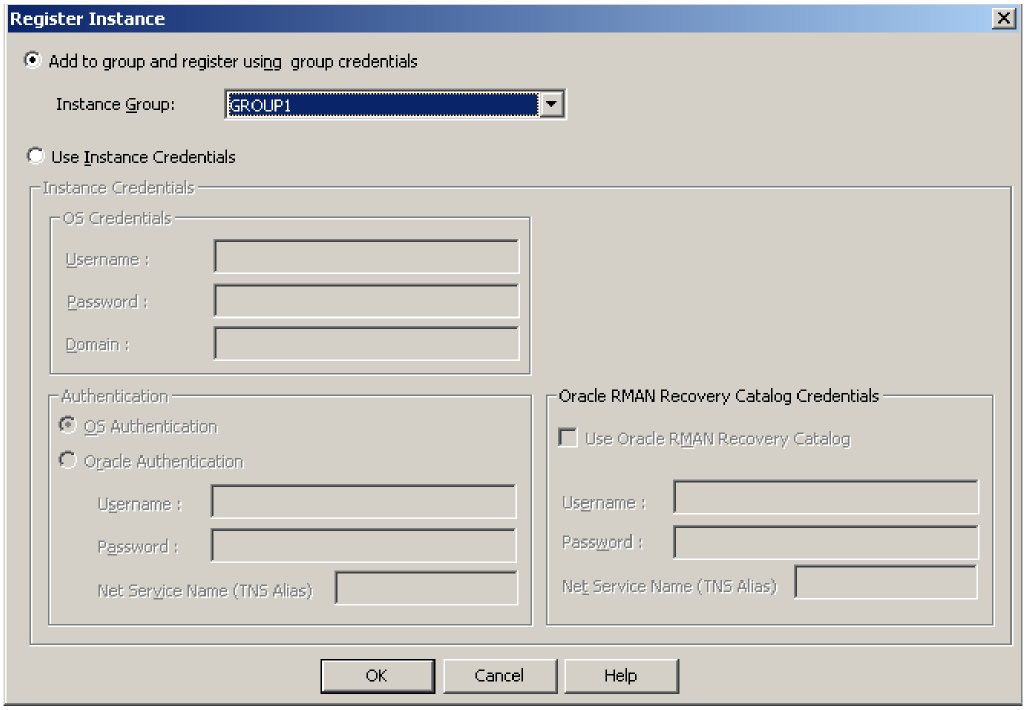
○ Oracle Authentication

Oracle RMAN Recovery Catalog Credentials

☐ Use Oracle RMAN Recovery Catalog

Figure 6 – Creating an Instance Group and adding credentials

Any instance added to a group must have the same credentials as the others in the same group. An instance can be added to a group by simply selecting the group at the registration menu (Figure 7).



Register Instance

● Add to group and register using group credentials

Instance Group: GROUP1

○ Use Instance Credentials

Instance Credentials

OS Credentials

Authentication

● OS Authentication

○ Oracle Authentication

Oracle RMAN Recovery Catalog Credentials

☐ Use Oracle RMAN Recovery Catalog

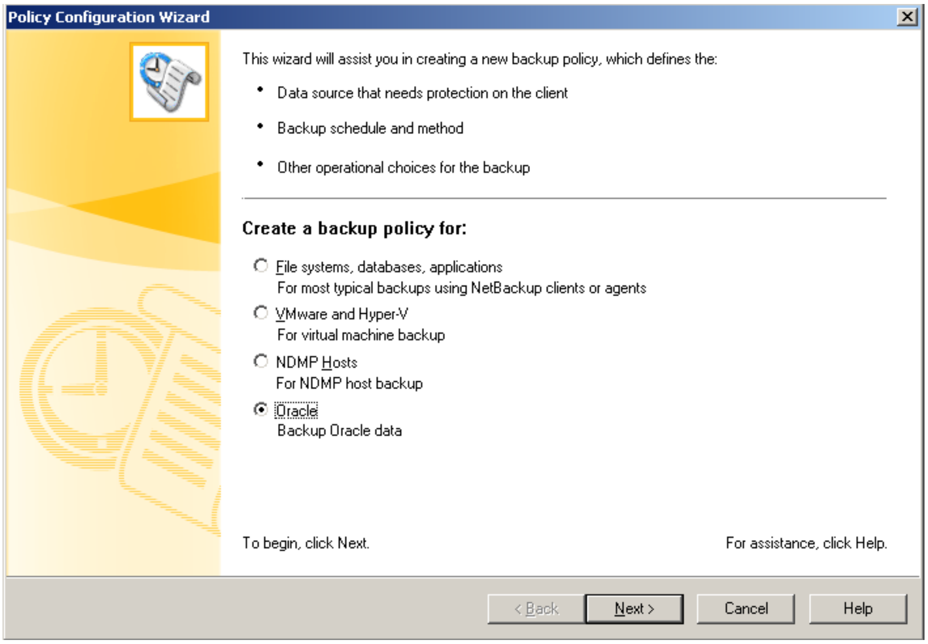
Figure 7 – Registering an instance with an existing group

It environments where common credentials are used is possible to configure a “default” instance group to which new instances are automatically added and registered, completely bypassing the manual registration process.

Once entered the credentials are AES encrypted and stored in the NBDB database.

Backup Policy Configuration

Once an instance or instance group has been registered a backup policy can be created using the backup policy wizard. The wizard now includes an option for Oracle (Figure 8).



Policy Configuration Wizard

This wizard will assist you in creating a new backup policy, which defines the:

- Data source that needs protection on the client
- Backup schedule and method
- Other operational choices for the backup

Create a backup policy for:

○ File systems, databases, applications
For most typical backups using NetBackup clients or agents

○ VMware and Hyper-V
For virtual machine backup

○ NDMP Hosts
For NDMP host backup

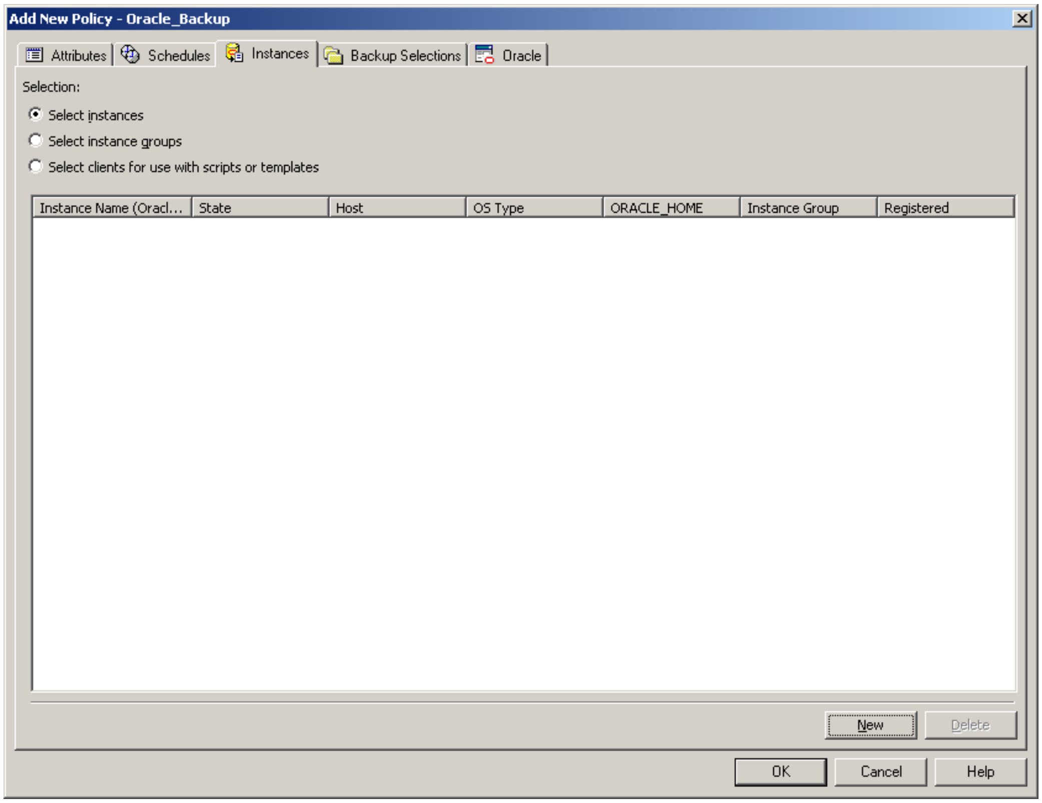
● Oracle
Backup Oracle data

To begin, click Next.

For assistance, click Help.

Figure 8 – Backup Policy Configuration Wizard

The configuration process involves selecting either instances or instance groups as shown in Figure 9 below. Note that it is also possible to use the wizard to configure Oracle backups in the old way by selecting clients to be backed up with scripts or templates.



Add New Policy - Oracle_Backup

Selection:

● Select instances

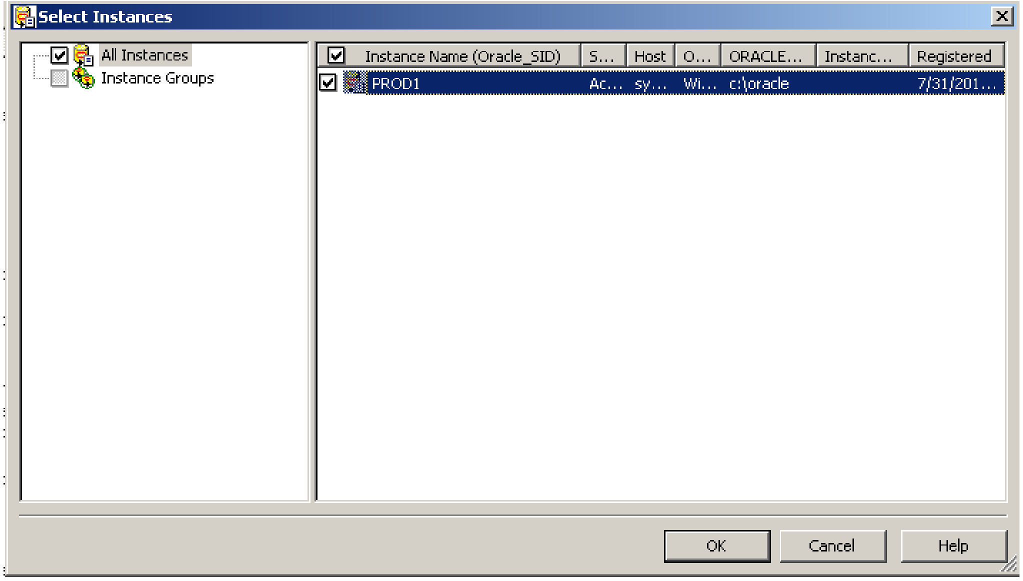
○ Select instance groups

○ Select clients for use with scripts or templates

Instance Name (Oracl…	State	Host	OS Type	ORACLE_HOME	Instance Group	Registered

Figure 9 – Policy Creation – Instance Selection

With “select instances” set, selecting the “new” button will display the list of registered instances which can then be added to the policy (Figure 10)



Select Instances

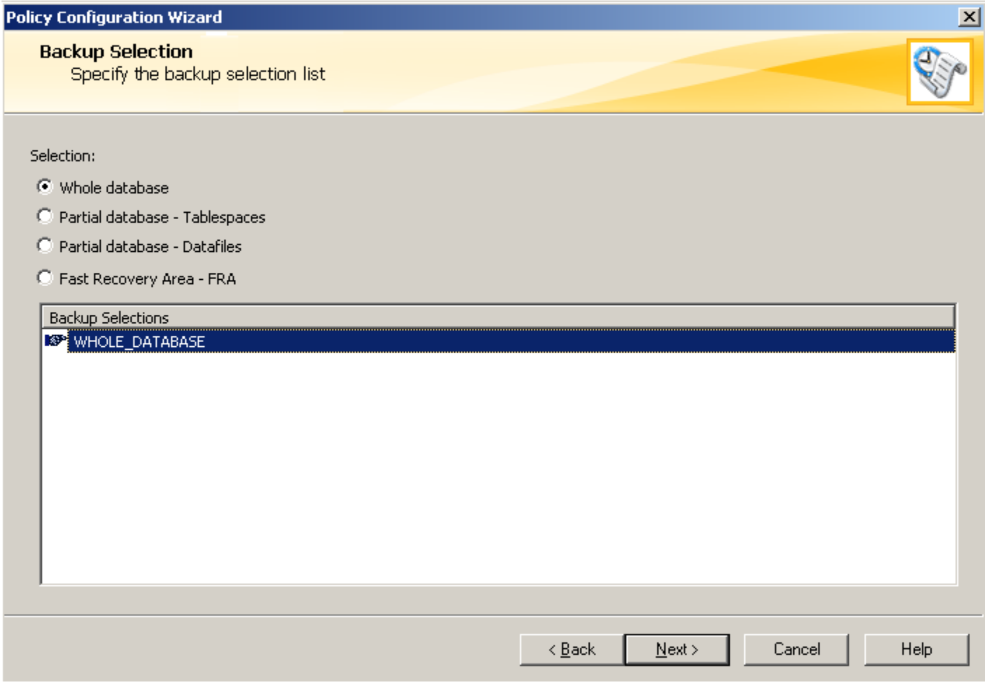
☑ All Instances

□ Instance Groups

☑	Instance Name (Oracle_SID)	S…	Host	O…	ORACLE…	Instanc…	Registered
☑	PROD1	Ac…	sy…	Wi…	c:\oracle		7/31/201…

Figure 10 – Selecting an instance to back up.

With the instance selected the next task is to select what needs to be backed up. Again options are available; the backup may be of the whole database or parts of the database including the Oracle Fast Recovery Area (Figure 11)



Policy Configuration Wizard
Backup Selection
Specify the backup selection list

Selection:

● Whole database

○ Partial database - Tablespaces

○ Partial database - Datafiles

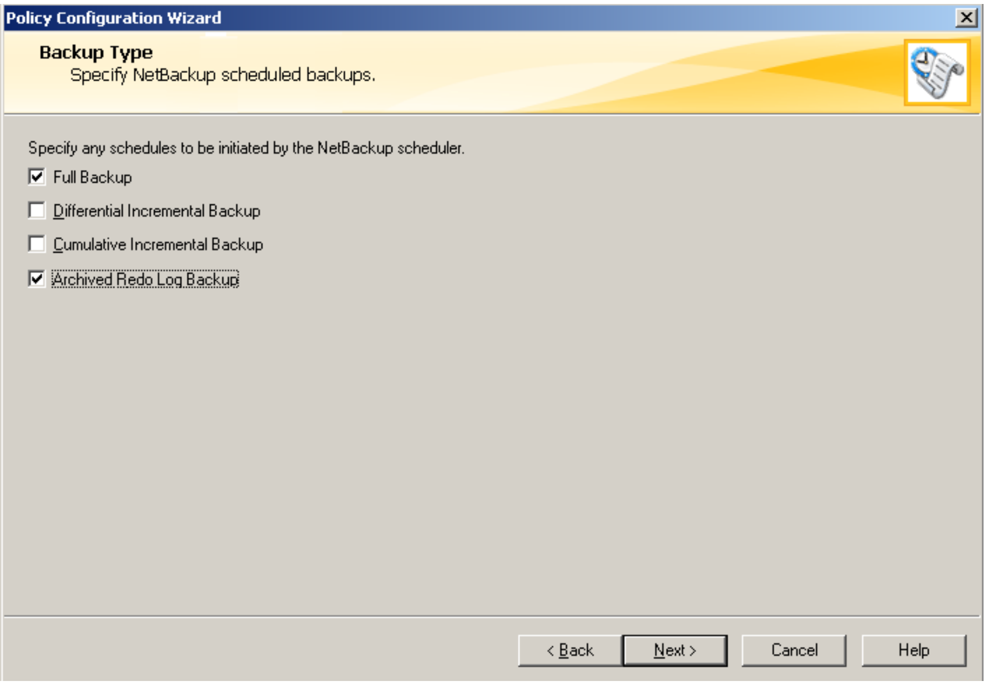
○ Fast Recovery Area - FRA

Backup Selections
WHOLE_DATABASE

< Back
Next >
Cancel
Help

Figure 11 – Selecting what to back up

Having selected what to back up the next question is when. This is where the new policy model differs significantly from the old model. Under the new model there is just one schedule for each backup type, including a schedule that deals specifically with Archived Redo Log backup. A schedule for each required backup type can be selected and is automatically created by the wizard as shown in Figure 12. (Note that in most cases it will be necessary to adjust the backup windows for individual schedules once the policy has been created.)



Policy Configuration Wizard

Backup Type

Specify NetBackup scheduled backups.

Specify any schedules to be initiated by the NetBackup scheduler.

☑ Full Backup

☐ Differential Incremental Backup

☐ Cumulative Incremental Backup

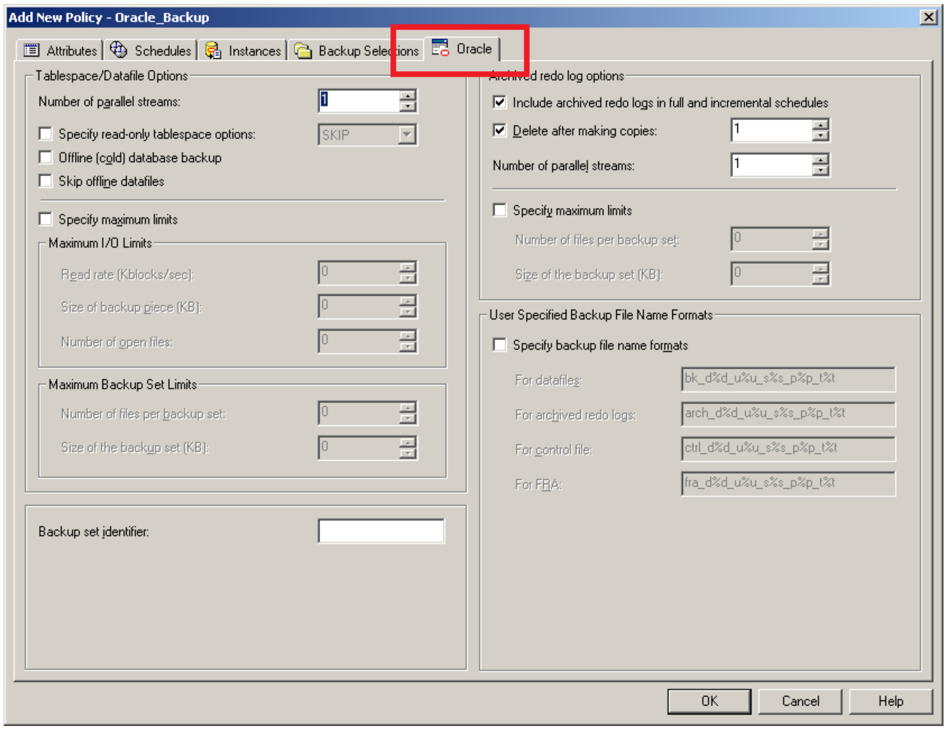
☑ Archived Redo Log Backup

Figure 12 – Selecting schedule types

Checkbox Policy Options – RMAN Script Generation

Once the basic backup policy has been created using the wizard it is possible to do things like specify the storage to be used and fine tune the schedules and other parameters. A new tab has been added to the policy called “Oracle” as seen in Figure 13 below.

The information on this screen is used to control the RMAN attributes such as the number of streams and redo logs and the size of backup sets. This information is used dynamically generate the RMAN script when the backup runs. This means that if changes are needed, the RMAN script does not need to be edited manually, the user can simply come to this screen and change the parameters and the new settings will be picked up the next time the backup runs.



Tablespace/Datafile Options

Number of parallel streams: 1

☐ Specify read-only tablespace options: SKIP

☐ Offline (cold) database backup

☐ Skip offline datafiles

☐ Specify maximum limits

Maximum I/O Limits

Read rate (Kblocks/sec): 0

Size of backup piece (KB): 0

Number of open files: 0

Maximum Backup Set Limits

Number of files per backup set: 0

Size of the backup set (KB): 0

Backup set identifier:

Archived redo log options

☑ Include archived redo logs in full and incremental schedules

☑ Delete after making copies: 1

Number of parallel streams: 1

☐ Specify maximum limits

Number of files per backup set: 0

Size of the backup set (KB): 0

User Specified Backup File Name Formats

☐ Specify backup file name formats

For datafiles: bk_d%d_u%u_s%s_p%p_t%t

For archived redo logs: arch_d%d_u%u_s%s_p%p_t%t

For control file: ctrl_d%d_u%u_s%s_p%p_t%t

For FRA: fra_d%d_u%u_s%s_p%p_t%t

Figure 13 – Oracle Tab to Create Dynamic RMAN Scripts

All in all these changes should make protecting the Oracle Databases much easier. Additional database options are planned in the near future.

Licensing and support considerations

No changes have been made with regards to licensing of the Oracle agent as part of this enhancement.

Related documents

[NetBackup for Oracle Administrator's Guide]

About Symantec:

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site: **www.symantec.com**

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934