



Technical Report

Best Practices for SnapProtect Backup for Oracle RAC Solution

Subhash Athri, NetApp
June 2015 | TR-4432

TABLE OF CONTENTS

1	Introduction	3
2	Objective	3
3	Audience	3
4	SnapProtect Solution Overview	3
5	SnapProtect Sizing Considerations	4
6	SnapProtect for Oracle RAC	5
	6.1 Validated Lab Design.....	6
7	RPO and RTO Requirements	7
8	Configure Oracle RAC Backup Using SnapProtect	8
9	Configure Backups of Oracle RAC	14
10	Configure Restore Options	19
11	Configure Backups	23
	11.1 Configure Tape Backups	23
	11.2 Configure AltaVault Backups	26
12	SnapProtect and Oracle Disaster Recovery	27
	Appendix: Backup Test Validation	27
	References	28

LIST OF TABLES

Table 1)	Four-node NFS Oracle 12c RAC configuration.	6
Table 2)	Two-node ASM Oracle 12c RAC configuration.	6
Table 3)	Schedule and retention examples.	7
Table 4)	Validation test results.	27

LIST OF FIGURES

Figure 1)	SnapProtect solution.	4
Figure 2)	D2D2T architecture on Oracle RAC.	6

1 Introduction

NetApp® SnapProtect® offers centralized backup management of an IT infrastructure through a single interface. NetApp integrated data protection technology is the backbone of this architecture. Through this solution, NetApp SnapVault® manages backup and long-term retention use cases, and NetApp SnapMirror® manages disaster recovery (DR). The solution delivers application-consistent NetApp Snapshot® backup and recovery supporting all major enterprise applications, including Oracle, SQL Server, and Microsoft Exchange.

2 Objective

The objective of this document is to describe SnapProtect with Oracle Real Application Clusters (RAC) and other Oracle solutions and explain key features of Snapshot backup and recovery for Oracle RAC by using NetApp technologies such as SnapVault and SnapMirror within NetApp Data ONTAP®. This document also describes backup and recovery best practices for the SnapProtect with Oracle RAC solution.

3 Audience

The intended audience for this document includes sales engineers, field consultants, professional services, IT managers, partner engineers, and customers who want to deploy the SnapProtect for Oracle RAC backup and recovery solution.

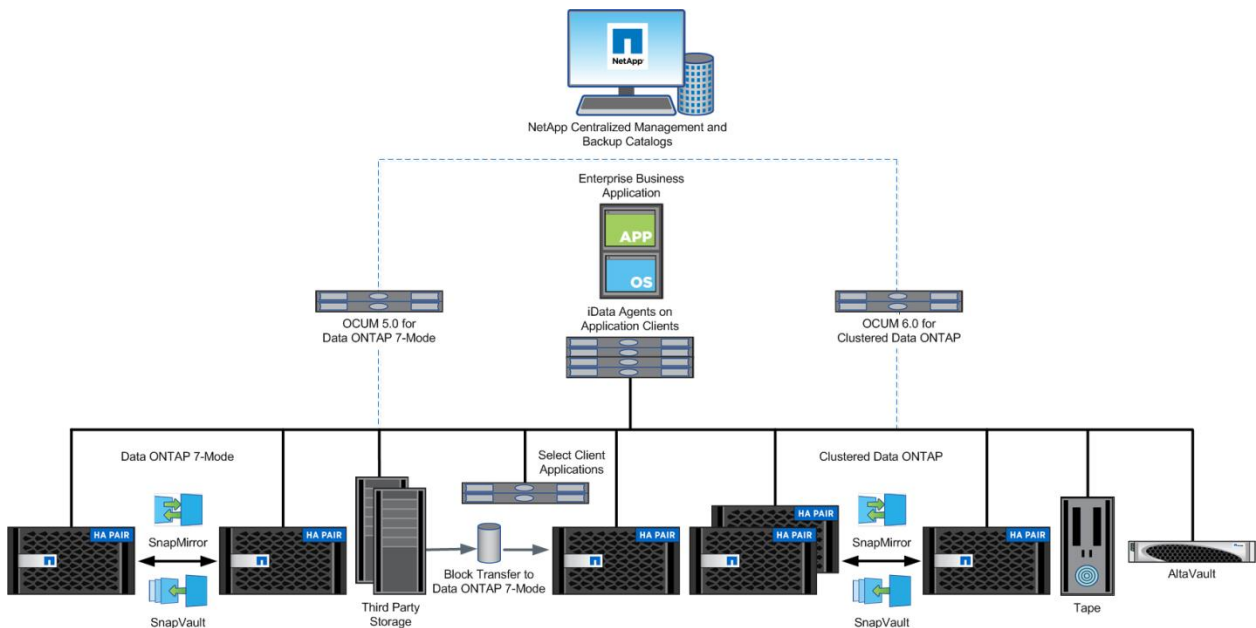
4 SnapProtect Solution Overview

The components of the SnapProtect solution are:

- **SnapProtect server.** Single interface for unified management
- **OnCommand® Unified Manager (OCUM).** Automated storage provisioning
- **NetApp FAS controller.** Snapshot copies integrated with NetApp Integrated Data Protection (IDP) technologies
- **Third-party storage or direct attached storage (DAS).** SnapProtect for Open Systems (SPOS) to back up heterogeneous storage
- **iData agents.** Client communication and application consistency

For more information about the components of this solution, refer to [TR-3920: NetApp SnapProtect Management Software Solution Overview](#).

Figure 1) SnapProtect solution.



5 SnapProtect Sizing Considerations

Sizing a SnapProtect deployment for application backups typically depends on the following factors:

- CommServe sizing.** CommServe is the master server of your backup infrastructure. The CommServe server ties the elements of the CommCell configuration together. It coordinates and administers the CommCell component. The CommServe server communicates with all agents in the CommCell component to initiate data protection, management, and recovery operations. Similarly, it communicates with media agents when the media subsystem requires management. The CommServe server maintains a database containing all the information related to the CommCell component. In addition, it provides several tools to administer and manage the CommCell component. For more information about CommServe, refer to the [CommServe system requirements](#) site.
- Storage sizing.** Storage sizing depends on your production database size and backup architecture. SnapProtect creates backups by using Snapshot technology, and it leverages Data ONTAP and SnapVault and SnapMirror replication technologies in the back end to protect data. The storage sizing for secondary and tertiary backup targets is planned depending on the backup topology.

Note: For assistance with sizing storage for your Oracle databases, contact your NetApp sales representative.

- SnapVault sizing.** The [Rapid SnapVault/OSSV Space Estimator](#) sizing tool can help you calculate how much storage is required on your secondary and tertiary targets, taking into consideration backup schedules, growth, and retention. SnapProtect is integrated with OCUM, which automatically provisions secondary volumes for SnapVault and SnapMirror targets. For SnapVault sizing, the most important consideration is how much storage, or how many disks, you should buy to accommodate backups. Volume sizing is intelligently managed by OCUM.
- OnCommand Unified Manager sizing.** OCUM is an important part of the SnapProtect solution. DataFabric Manager 5.x is used for Data ONTAP 7-Mode deployments, and OCUM 6.x is used for clustered Data ONTAP deployments. OCUM is the interface between CommServe and Data ONTAP used to provision volumes in the secondary target. The sizing of OCUM depends on the number of storage nodes and the number of relationships between SnapVault and SnapMirror that a single

instance of OCUM can manage. CommServe offloads the auxiliary copy operations to OCUM. Therefore, OCUM must be sized as a separate entity.

Note: For more information about sizing requirements or for assistance with accurately sizing the solution, contact your NetApp sales representative.

- **Tape backup sizing.** Disk or tape backups of applications are considered streaming backups. Sizing these types of backups depends on the following:
 - Backup size
 - Retention policy (daily, weekly, or monthly)
 - Storage capacity of the tape or disk

Note: NetApp recommends creating a backup copy on tape or disk by using either SnapVault or SnapMirror technologies, preferably from a proxy client so that the production environment is not affected by these performance-intensive tasks.

6 SnapProtect for Oracle RAC

SnapProtect offers the following unique capabilities that distinguish it from other applications used to back up Oracle RAC databases:

- Back up large databases (in terabytes and petabytes) within a few minutes by using NetApp Snapshot technology.
- Provide consistent backups by quiescing the database for a few seconds.
- Recover databases at any point in time by using multiple point-in-time Snapshot copies.
- Quickly recover data by using the application-aware revert operation.
- Create Snapshot copies simultaneously on multiple databases within the same LUN by using snap optimization.
- Open or mount databases on other clients by using Snapshot copies without actually restoring.
- Verify data files, control files, and archive log headers from Snapshot copies.
- Use Oracle Recovery Manager (RMAN) for SnapProtect backups.
- Support different types of databases, such as file system, Automatic Storage Management (ASM), and raw databases.

Oracle RAC is widely deployed on NetApp storage by using either NFS or SAN (ASM). SnapProtect supports backups of Oracle RAC hosted on Linux platforms only.

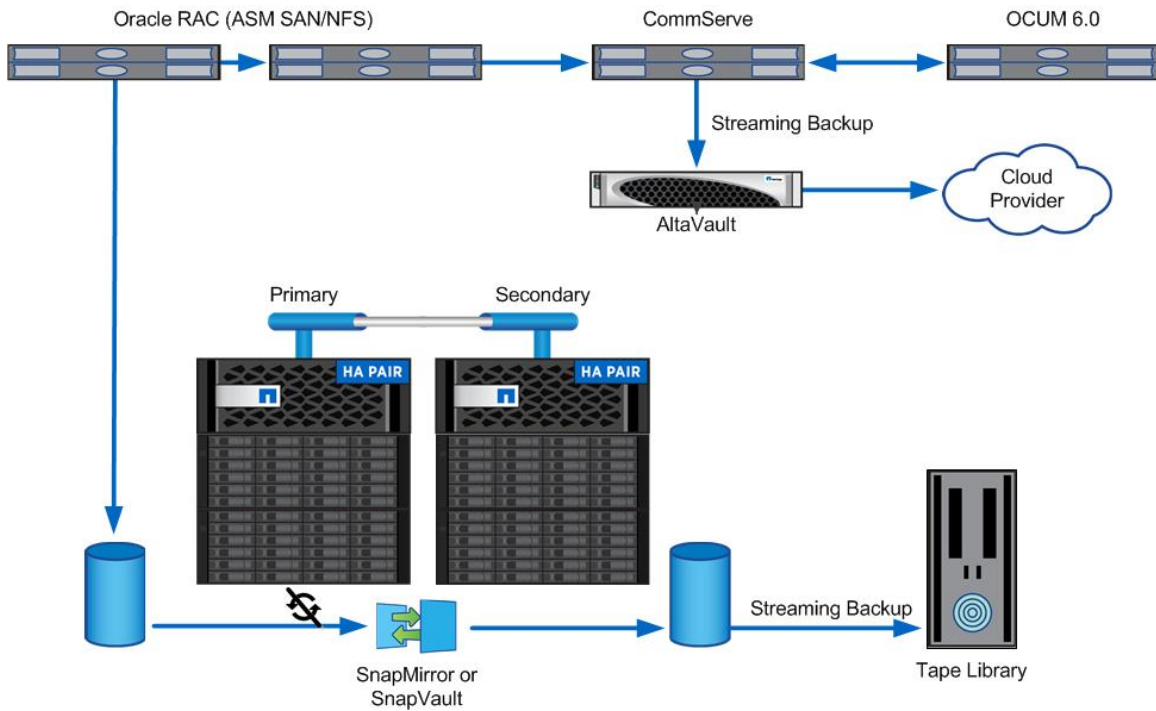
Figure 2 depicts the disk-to-disk-to-tape (D2D2T) architecture for an Oracle RAC instance. Disk-to-disk (D2D) backups leverage NetApp SnapVault or SnapMirror technologies, and they back up data to tape or to NetApp AltaVault[®] (formerly known as SteelStore), a cloud-integrated, streaming-based storage appliance.

Oracle RAC is set up by using the NetApp best practice guidelines described in [TR-4249: Oracle Database on NetApp Clustered Data ONTAP](#) and [TR-3633: Best Practices for Oracle Databases on NetApp Storage](#).

NetApp recommends deploying Oracle so that data files and archive logs are placed in two separate disk groups in an ASM configuration or in two separate NFS mounts (in case of a file system). This best practice enables better management of Snapshot copies and enables you to leverage the array-based restore capabilities of NetApp SnapRestore[®], also known as the hardware revert capability in the SnapProtect GUI.

Note: The hardware revert feature is only available for Oracle instances installed on NFS mounts.

Figure 2) D2D2T architecture on Oracle RAC.



6.1 Validated Lab Design

Table 1 and Table 2 list configuration details of the validated lab design used to test this solution.

Table 1) Four-node NFS Oracle 12c RAC configuration.

Cluster	SVM	Aggregate	Volume	Volume Size	Mount Point
Dsgcluster	Oracle SVM	aggr 01	Oradata	5TB	/oradata
			Oraarchive	500GB	/oraarchive
			Orclredo	500GB	/orclredo
			Shared config	50GB	/shared config

Table 2) Two-node ASM Oracle 12c RAC configuration.

Cluster	SVM	Aggregate	LUN	LUN Size
Dsgcluster	Oracle SAN	aggr 01	Orcldata	5TB
			Orclarchive	500GB
			Orclredo	500GB
			Orclctrl	500GB

7 RPO and RTO Requirements

Database corruption and total site failures are just two of the many catalysts for data recovery. Understanding your organization's recovery point objective (RPO) and recovery time objective (RTO) can help you mitigate data loss.

Oracle RAC archive log mirroring and backups typically control the RPO. Data file (database) mirroring and backups control the RTO.

The RPO for database corruption on a production server can be up to a minimum of 5 minutes or more. For an entire site failure, SnapProtect can provide up to a 15-minute RPO. SnapProtect is not an ideal solution for continuous data protection, because the RPO you can achieve with this solution is 5 minutes at a minimum.

Depending on the I/O quiesce time, it can take up to a 1 minute to create an application-consistent Snapshot copy by using SnapProtect with storage CPU utilization of less than 50%. To maintain an RPO as low as 5 minutes for database corruption use cases, schedule Snapshot copies for archive log volumes every 5 minutes and replay them on the production database. To maintain a 15-minute RPO for site failures, run replication jobs for the entire database on the secondary target by creating SnapMirror auxiliary copies every 15 minutes.

Note: To accurately schedule Snapshot copies, remember to account for data change rates, CPU utilization workloads on controllers, and the amount of network bandwidth available for replication.

Note: Be sure to test and validate the RPO and RTO requirements defined for your infrastructure before stating them in your DR documents.

For Oracle databases running on NFS, restoring to the previous state happens in a matter of seconds. Array-based restore technologies such as SnapRestore (hardware revert) and SnapRestore single-file restore operations are enabled by SnapProtect for these types of restore operations.

Note: SnapRestore is available only for recovery from primary Snapshot copies.

Databases hosted on ASM or raw devices employ a copy-based restore mechanism for database recovery. The time it takes for this type of restore operation depends mainly on network infrastructure limits.

Table 3 describes enterprise scheduling and retention policy examples.

Table 3) Schedule and retention examples.

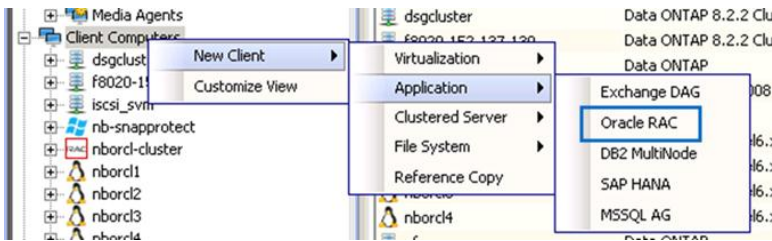
DB Backup Set	Subclient	Storage Policy	Backup Sched.	Local Retention	Archive Log Backup Sched.	SnapMirror Sched.	SnapVault Sched.	SnapVault Retention
A	SC1	SP1	Daily full backup at 6 p.m.	10 days (cycles); 6 weeks; set in primary Snapshot copy	Every 5 minutes	Daily at 6:30 p.m.; set in SnapMirror copy schedule	Daily at 9:30 p.m.; set in SnapVault copy schedule	90 days (cycles); 52 weeks; set in SnapVault copy

Note: Backup scheduling and retention policies depend on RPO and RTO requirements.

8 Configure Oracle RAC Backup Using SnapProtect

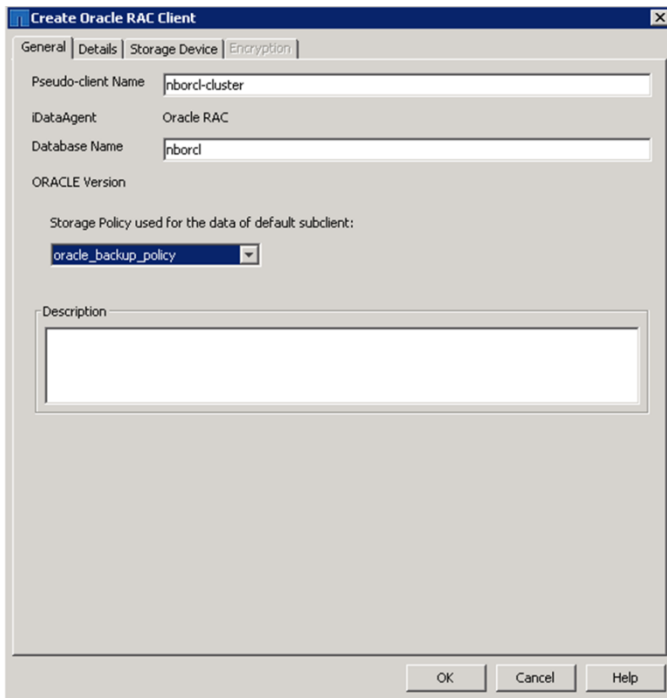
To configure Oracle RAC by using SnapProtect, complete the following steps:

1. Install SnapProtect on the CommServ server.
2. Install Oracle iData agents on all nodes (instances) of Oracle RAC. For more information about how to install iData agents on Oracle nodes, refer to the NetApp documentation [SnapProtect - Deployment - UNIX – Oracle](#).
3. Select New Client > Application > Oracle RAC.

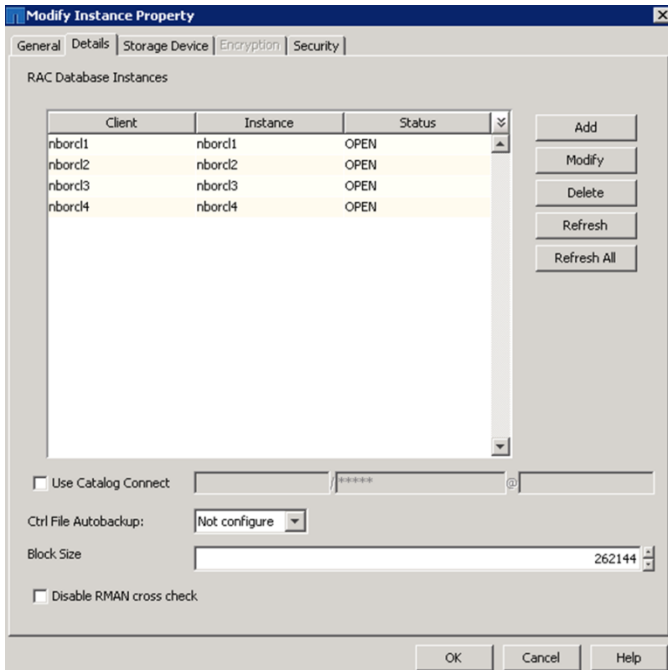


4. From the General tab, do the following:
 - a. Enter your RAC cluster name in the Pseudo-Client Name field.
Note: Run the `$CRS_HOME/bin/cemutlo -n` command to get your cluster name.
 - b. Enter the name of the database (the Oracle system ID [SID]).
 - c. Select a storage policy for your default subclient. The storage policy defines the SnapVault and SnapMirror schedules.

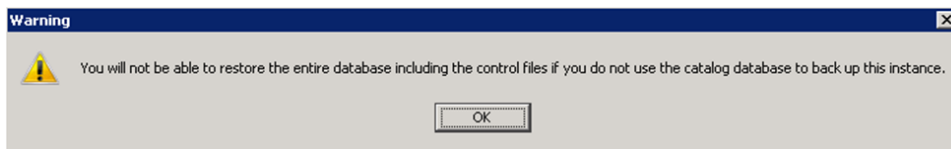
Note: For more information about how to configure the storage policy, refer to [Storage Policy – Getting Started](#).



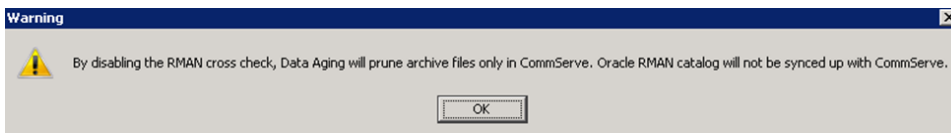
5. Click the Details tab and click Add.



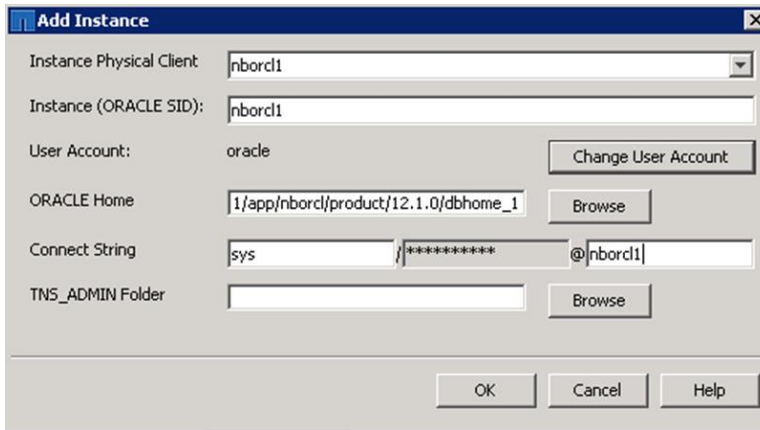
Note: Deselecting the Use Catalog Connect checkbox causes the following warning to appear. You may ignore this warning for Snapshot backups because the SnapProtect backup operation copies control files to archive log mount points and creates a backup of the entire volume. However, this SnapProtect functionality must be configured for tape backups and restores.



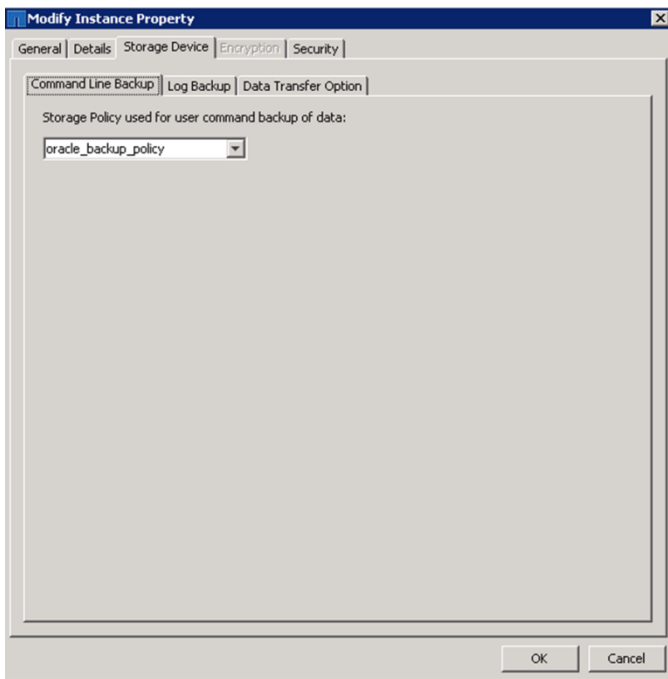
Note: Deselecting Disable RMAN Cross Check prunes archive log files in CommServe only and causes the Oracle RMAN catalog not to sync with CommServe. This option is required to enable restores from tape backups, but it is not required for SnapProtect operations.



6. In the Add Instance dialog box, do the following and click OK:
 - a. Enter the name of the instance physical client.
 - b. Enter the instance SID.
 - c. Click Change User Account to enter the user account into the access database.
 - d. Click Browse to select the Oracle Home location on your client.
 - e. In the Connect String fields, enter the sys credentials configured during the database installation.

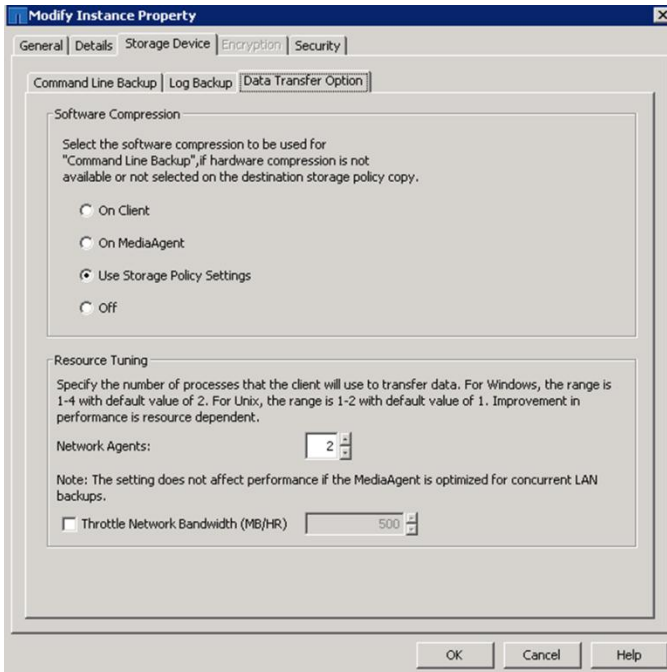


7. Click the Storage Device tab. From the Command Line Backup tab, select a storage policy for command-line backups from the drop-down list. This option allows user RMAN scripts to run backups by using SnapProtect storage policies to stream backups either to tape or to AltaVault.

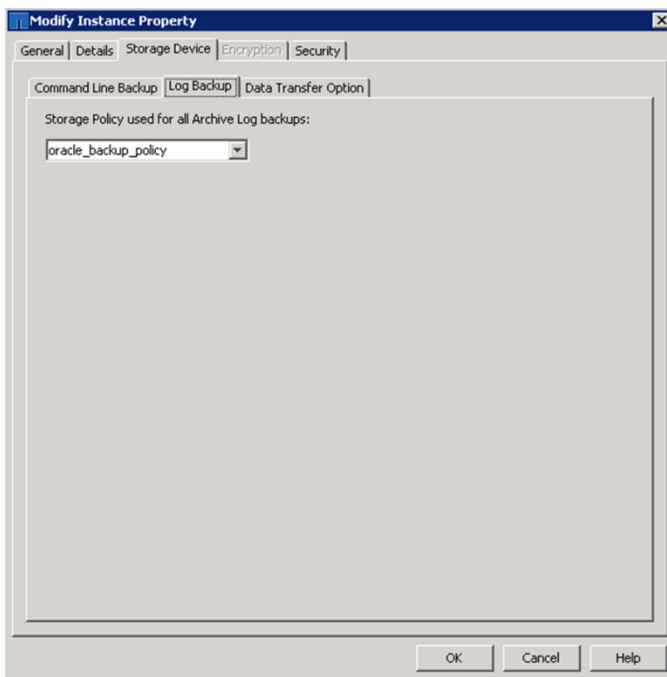


8. Click the Data Transfer Option tab. In the Software Compression pane, keep Use Storage Policy Settings selected; this option is the default.

Note: Compression is enabled while configuring provisioning targets in the storage policy.

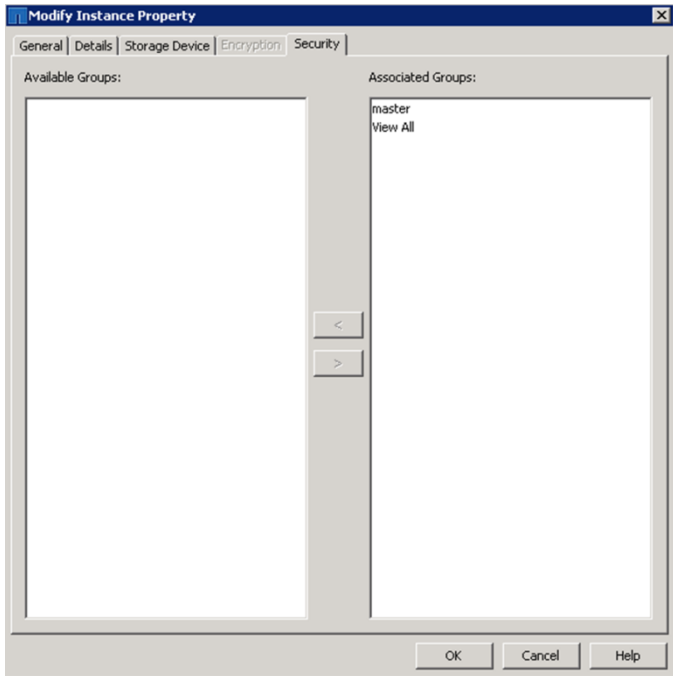


9. Click the Log Backup tab and select a storage policy to be assigned for all archive log backups.



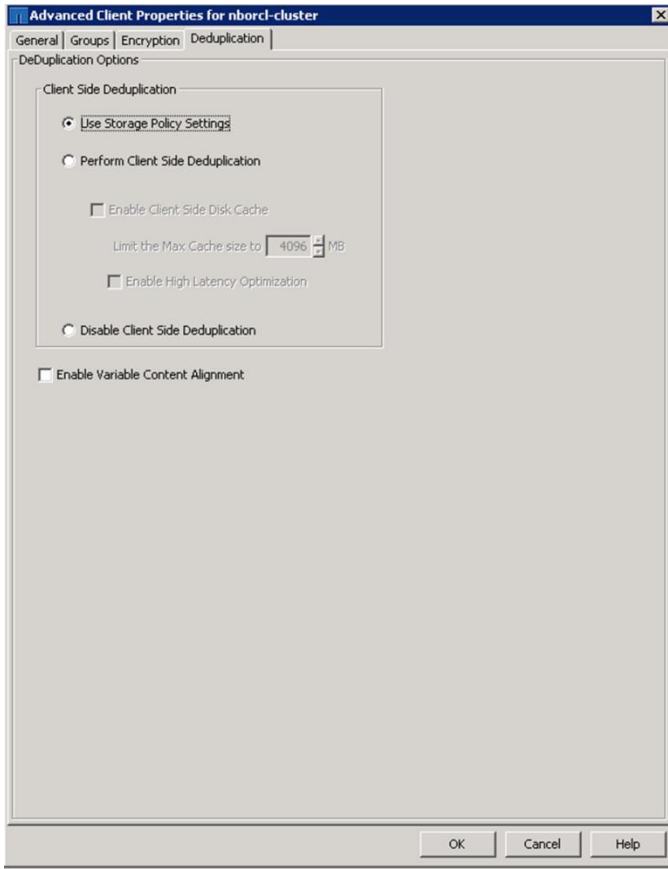
10. Click the Security tab to configure security settings, if applicable.

Note: The Security tab enables role-based access control (RBAC), which allows the SnapProtect admin to assign user roles and privileges. For more information about configuring RBAC, refer to [Getting Started with User Administration and Security](#).



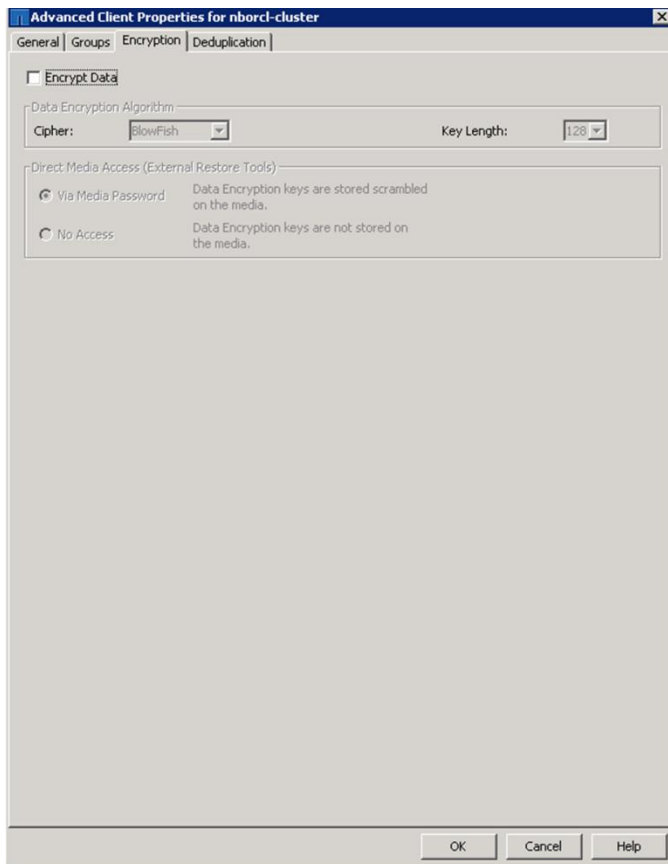
11. From the Advanced tab, right-click the RAC client and click Properties. Click the Deduplication tab and select Use Storage Policy Settings.

Note: Deduplication is enabled while configuring provisioning targets in the storage policy. Client-side deduplication is not supported for SnapProtect operations.



12. Click the Encryption tab to configure encryption settings, if applicable.

Note: Encryption settings are only applicable for backup copy operations and do not apply to auxiliary copy backups.



13. Click OK.

9 Configure Backups of Oracle RAC

To configure Oracle RAC backups, complete the following steps:

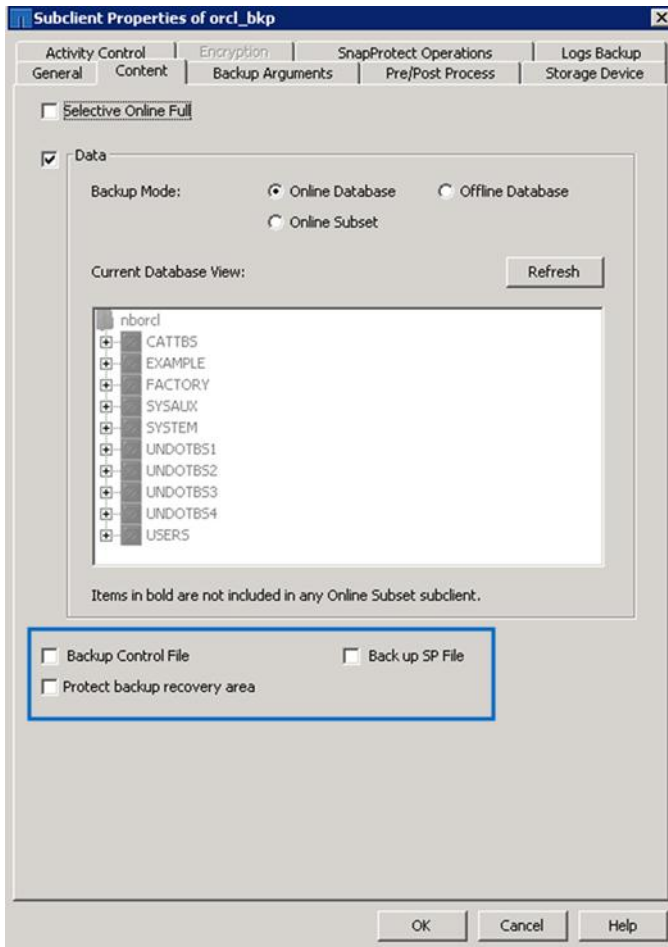
1. From the SnapProtect GUI, create a subclient under the Oracle RAC client. For more information about creating subclients, refer to the NetApp documentation [Storage Policy – Getting Started](#).
2. Right-click the new subclient. The Subclient Properties page appears.
3. From the Subclient Properties page, click the Content tab and configure the backup mode.

- a. Select one of the following states:

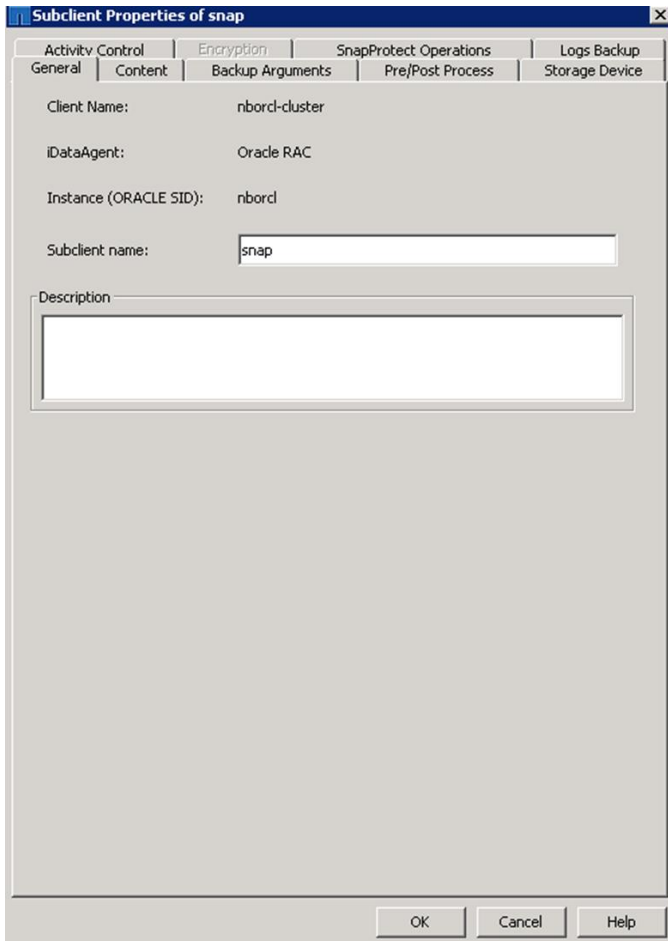
Note: You cannot back up a database that is not mounted.

- **Online.** Database is mounted and open.
 - **Offline.** Database is mounted.
 - **Online Subset.** An individual database is mounted and open. You can select table spaces and data files by using this option.
- b. Optional: Select the Backup Control File checkbox to move the control file to the archive log destination, at which point, SnapProtect creates a Snapshot copy of the archive log volume.

Note: The Selective Online Full option is used to move backups to tape by using selective copy options during a backup copy operation. Selecting the Selective Online Full checkbox automatically selects all of your data, archives, and control files for backup; you cannot deselect any of these items for backup. Verify that the database is online, mounted, and open before you start this type of backup.

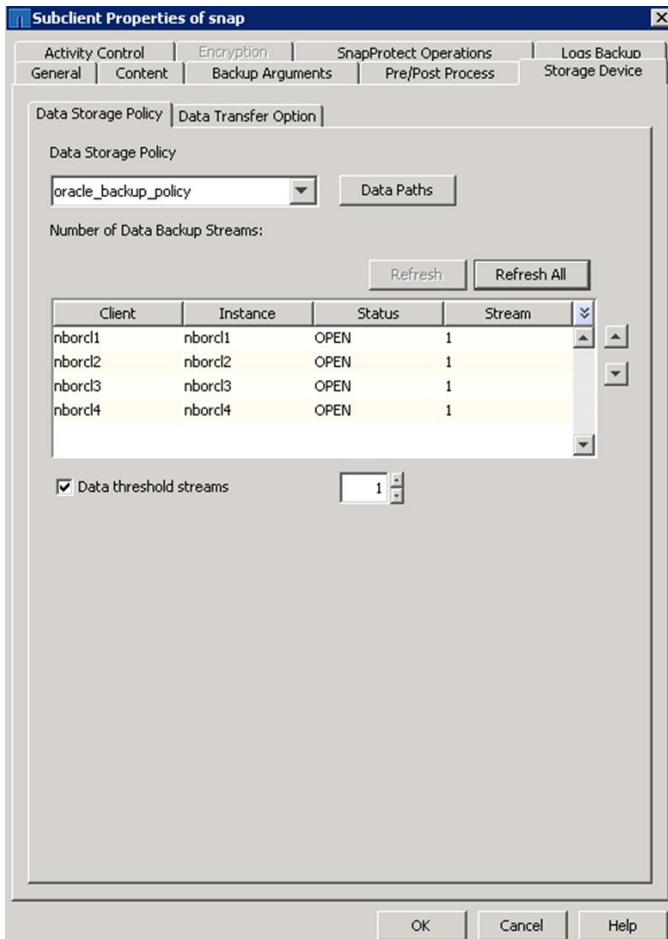


4. Click the General tab and enter the name of the subclient.

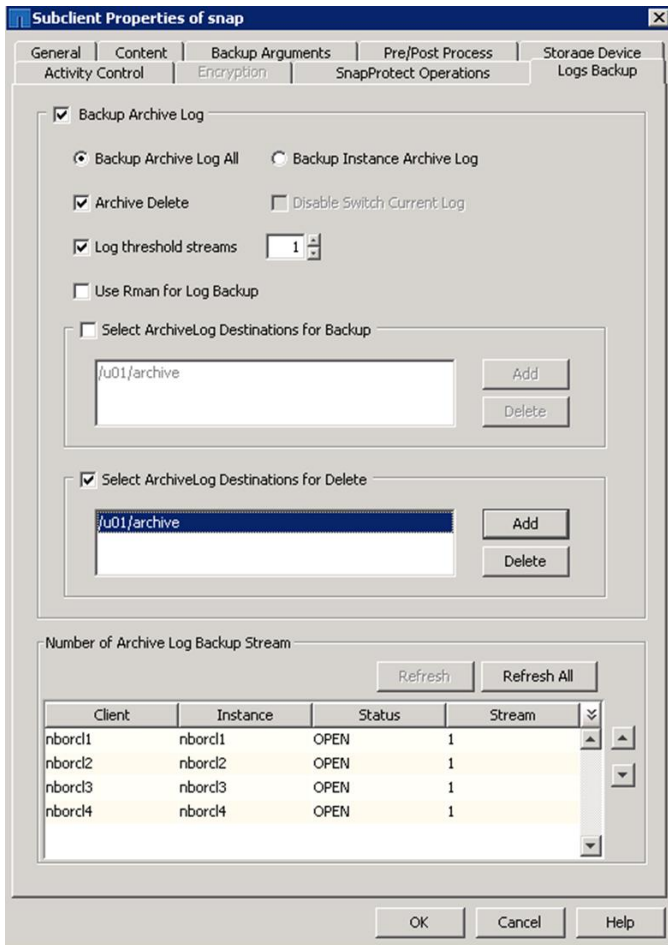


5. Click the Storage Device tab and select a data storage policy from the drop-down list to define the D2D2T workflow. For more information about how to create a storage policy, refer to [Storage Policy – Getting Started](#).

Note: Streams for SnapProtect backup and restore operations work differently from traditional RMAN streaming backup and restore operations. In the example screenshot, all of the RAC nodes have multiple streams, but only one node can be used to create the Snapshot copy. After the discover phase, which detects which RAC nodes are up and running, select one node at random and perform all SnapProtect operations from that node. The value for the number of streams doesn't matter because no RMAN streams are allocated to create Snapshot copies, and the value is only used during RMAN streaming backup to tape.

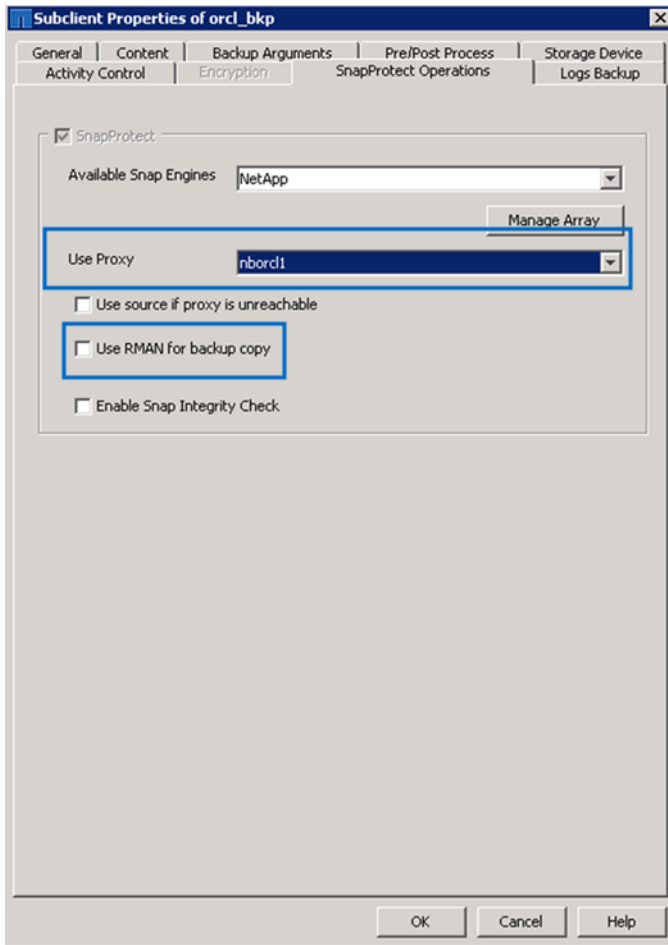


6. Click the Logs Backup tab, select the Backup Archive Log checkbox, and configure the following options:
 - a. Select the Archive Delete checkbox to delete archive logs after the backup is complete.
 - b. Select the Archive Log Destinations for Delete checkbox, if necessary, and add the location of the archive logs.
 - c. Optional: Select the Use Rman for Log Backup checkbox to configure backup copy operations to tape.



- Click the SnapProtect Operations tab and select the Use Proxy option for backup copy operations. The proxy must be of the same OS/application type as the client. If RMAN is configured, it can be used for backup copy operations.

Note: For an ASM instance, if a proxy is being used, make sure the `ASM_DISKSTRING` parameter is not empty. For mount operations to succeed, you must also verify that the `kfed` binary exists inside `$GRID_HOME/bin`.

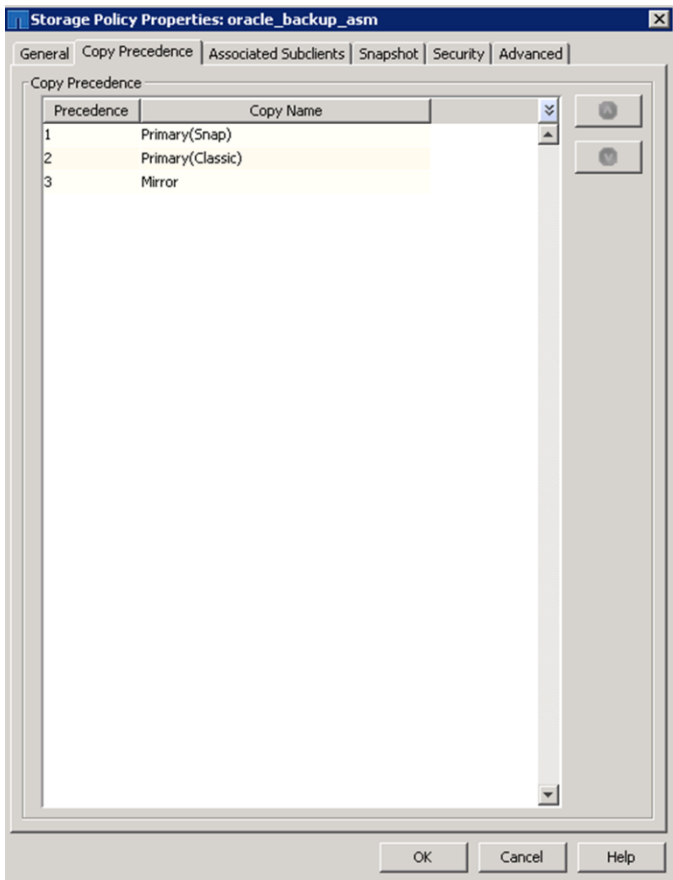


8. Click OK.

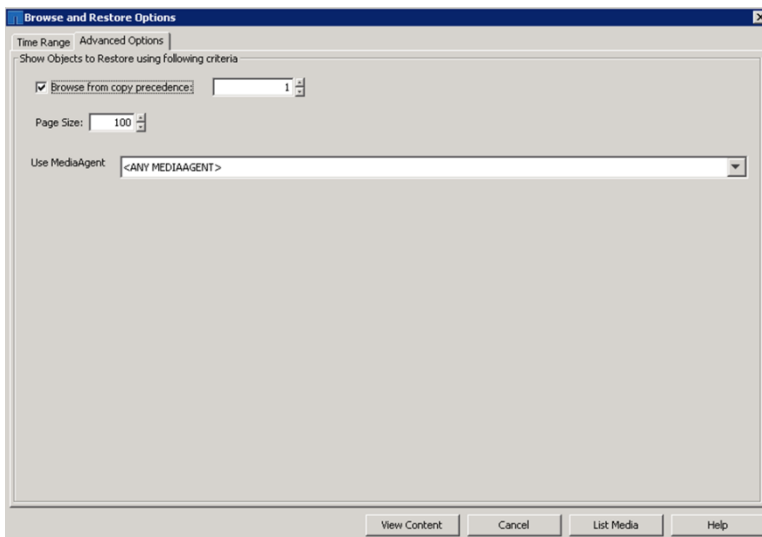
10 Configure Restore Options

Restore operations can be initiated for all of the copies configured in your storage policy. To configure restore options, complete the following steps:

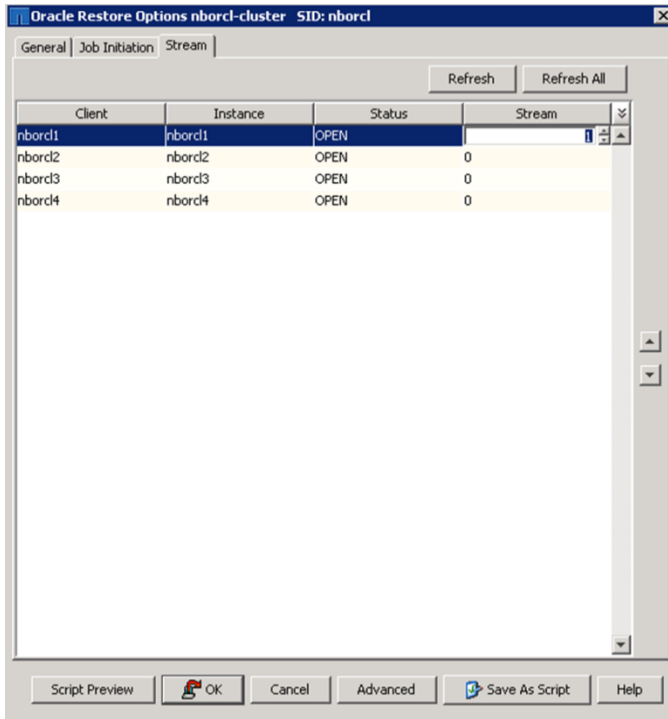
1. From the Storage Policy Properties page, click the Copy Precedence tab to set the order in which restore copies are selected.



2. Right-click the database, select Browse and Restore, and click the Advanced Options tab to set the copy precedence.

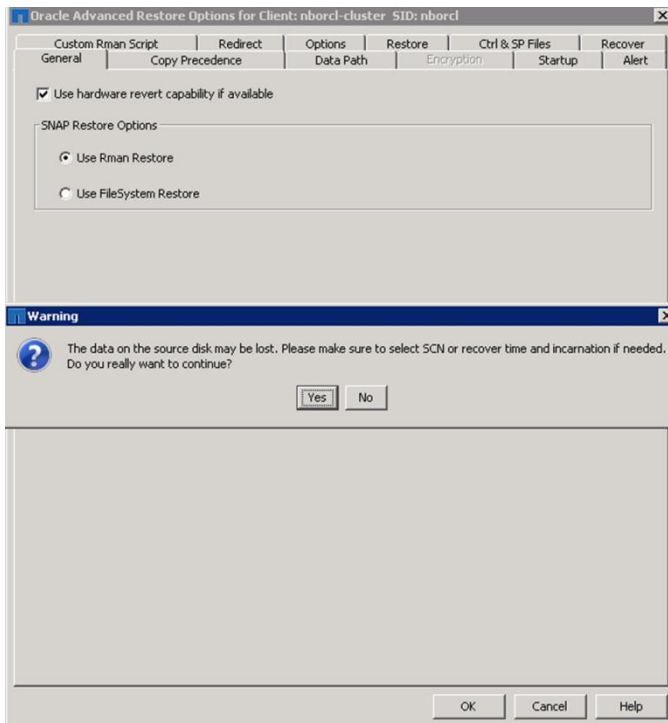


3. Click View Content and click the General tab.

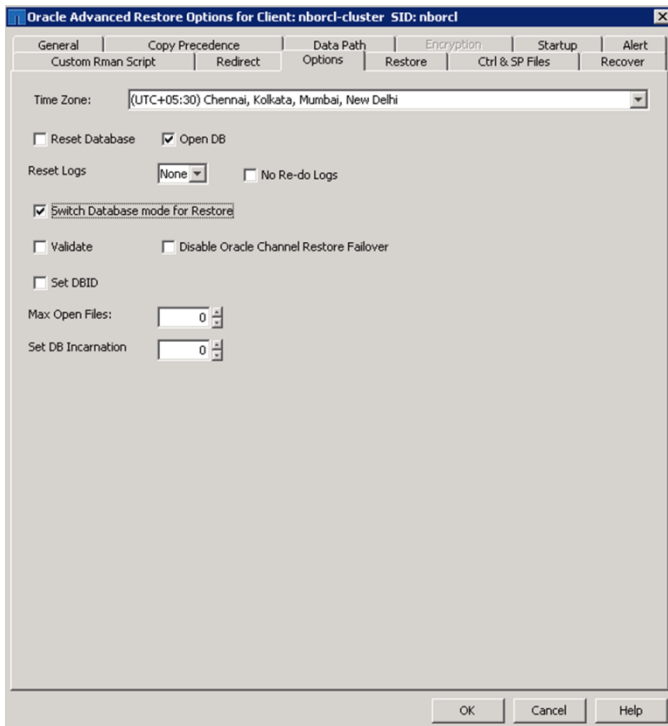


- From the General tab, click Advanced and select the Use Hardware Revert Capability checkbox to revert Snapshot copies to the previous point in time and erase all existing data.

Note: The hardware revert capability feature is available only for Oracle installed on NFS.

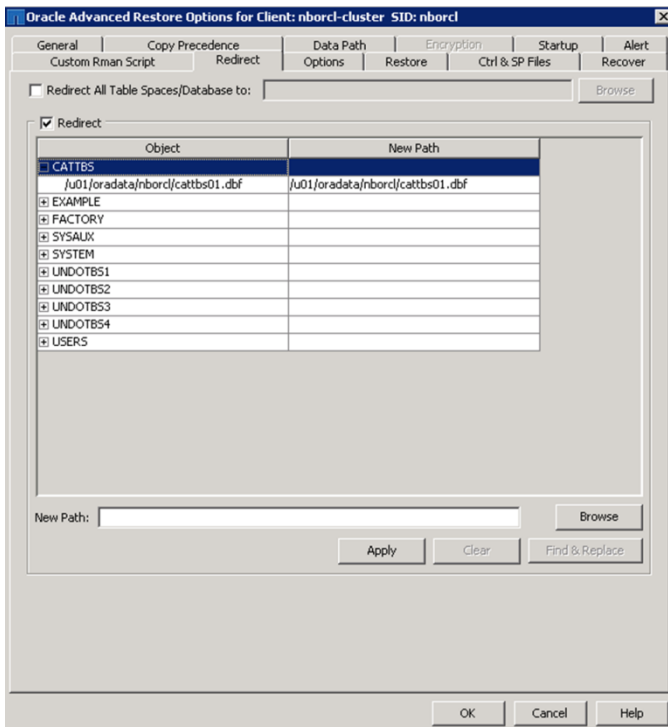


- Click the Options tab and select Switch Database Mode for Restore.



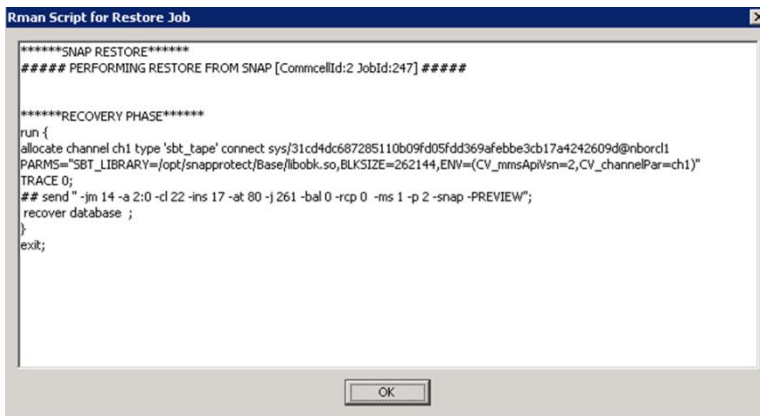
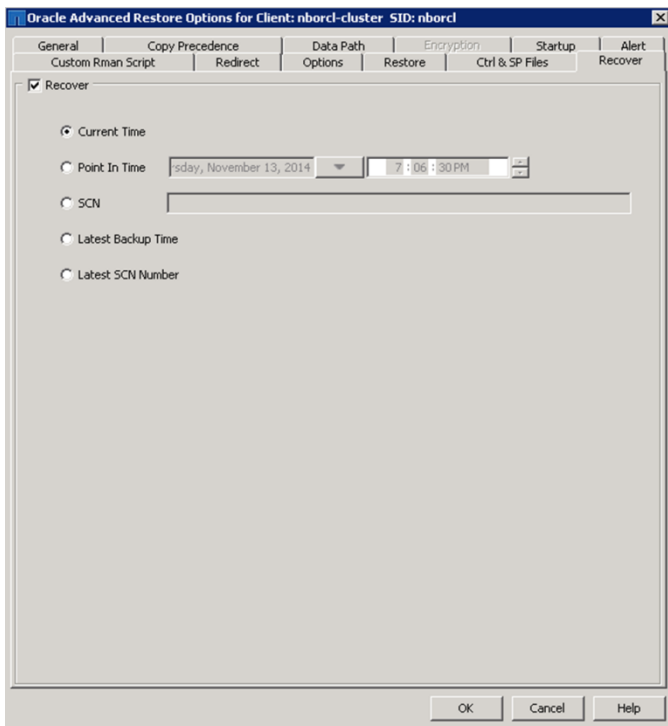
- Click the Redirect tab to redirect data files to a different location, if necessary.

Note: If the database is hosted on a file system, the redirect location should be a file system. If the database is hosted on an ASM instance, the redirect location should be an ASM disk group.



- Click the Recover tab to configure recovery of the archive logs and restore the database.

- Current Time restores the database to the last available archive log backup.
- Point In Time restores the database to the requested date and time.
- SCN restores the database to a known system change number (SCN).



11 Configure Backups

You can back up data to tape, Virtual Tape Library (VTL), or AltaVault.

11.1 Configure Tape Backups

Tape backups can be configured in two ways:

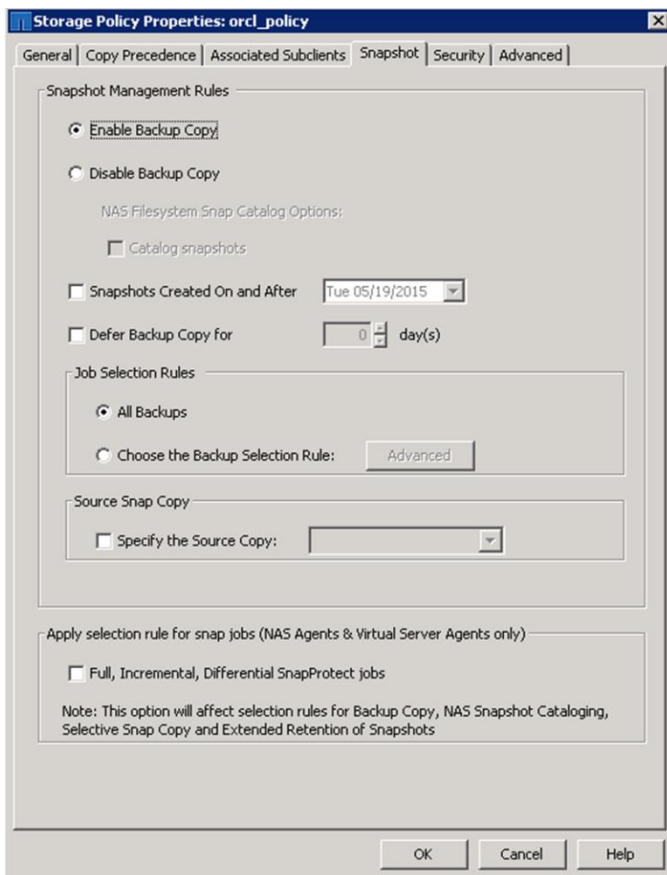
- **Server-to-storage controller backup.** During a server-to-storage controller backup, the tape library is connected to the controller and configured using NDMP.

- **System-to-server backup.** During a system-to-server backup, the tape library is connected to the media agent and configured as a generic SCSI device. This backup type is also called a remote backup.

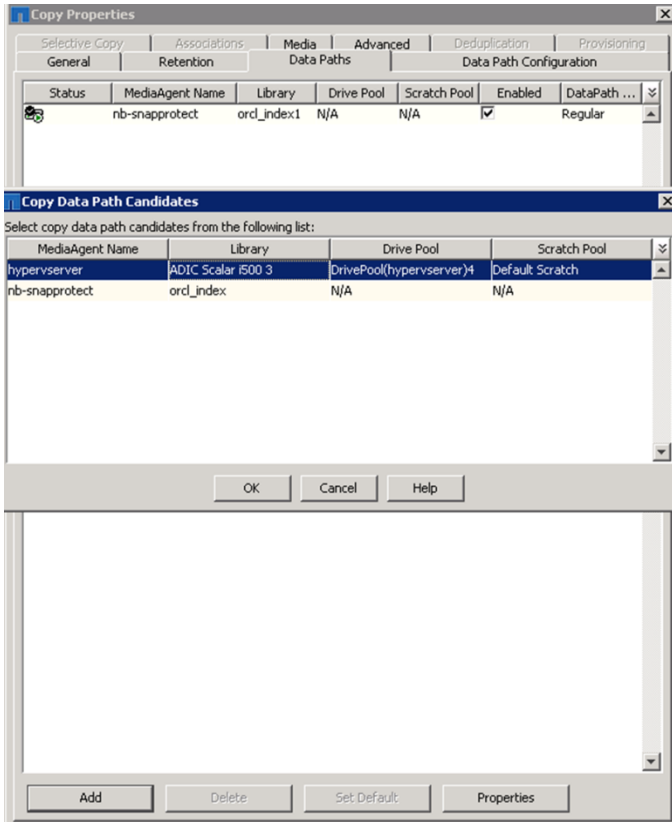
Configure Server-to-Storage Controller Backup

To configure a server-to-storage controller backup, complete the following steps:

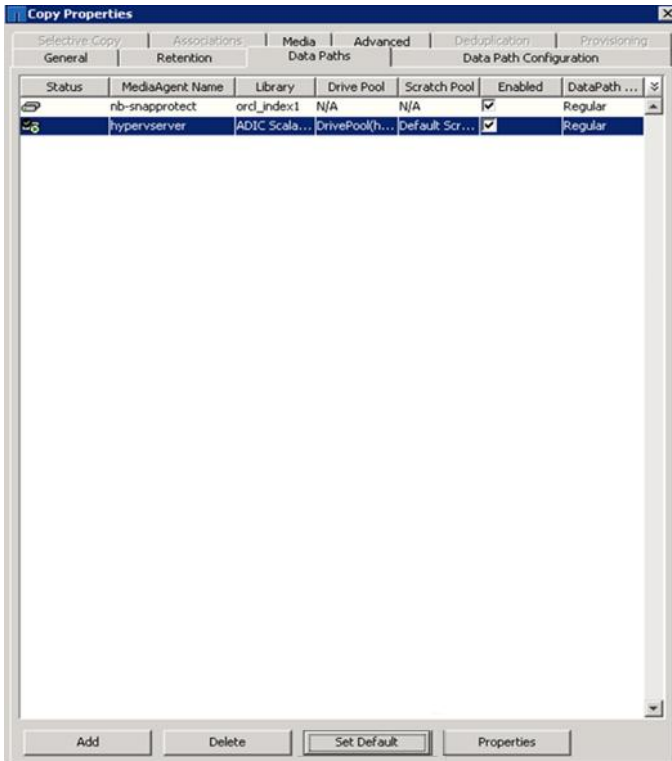
1. Verify that the tape library is shared across a media agent and the storage node.
2. Configure the tape library by using an NDMP intercluster LIF on the storage node. For more information about how to perform this configuration, refer to [TR-4330: Cluster-Aware Backup Configuration for SnapProtect and Simpana](#).
3. From the SnapProtect GUI, right-click the storage policy and select Properties. The Storage Policy Properties page opens.
4. From the Storage Policy Properties page, configure the Snapshot management rules and click OK.
 - a. Click the Snapshot tab and select Enable Backup Copy.
 - b. Select Specify the Source Copy and select Primary (Classic) Copy from the drop-down menu. This storage policy is the one that is usually configured for streaming backup operations.



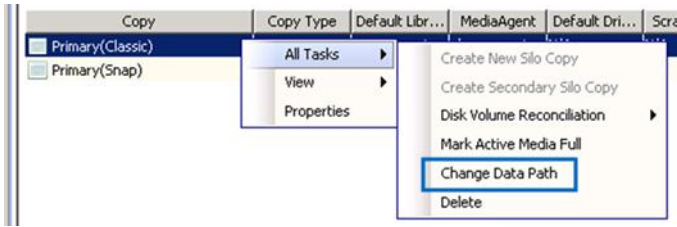
5. From the SnapProtect GUI, click the Storage Policies tab. Right-click Primary (Classic) Copy, select Properties, and click the Data Paths tab. Click Add to add the tape library.



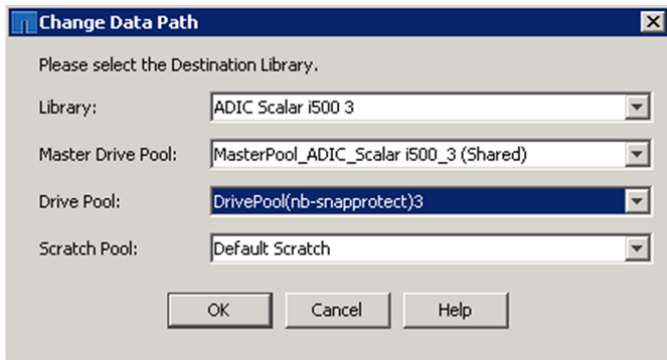
6. Select the newly added tape library and click Set Default to set it as the default library.



- Right-click the Primary (Classic) policy and select Change Data Path.



- From the Drive Pool drop-down list, select the data path to NDMP and click OK to change the data path.



Configure System-to-Server Backup

To configure the tape library on the media agent by using the default settings, complete the following step:

Note: For more information, refer to the “Remote Backup” section of [TR-4330: Cluster-Aware Backup Configuration for SnapProtect and Simpana](#).

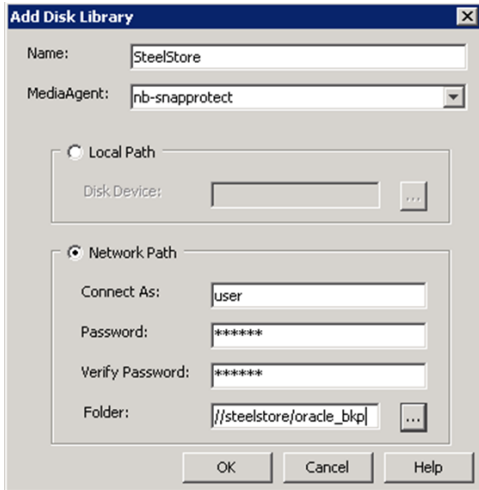
- Point the data path of the primary (classic) copy to the SCSI device on the media agent that is configured to run the backup.

11.2 Configure AltaVault Backups

An AltaVault device can be connected to SnapProtect as a disk library through CIFS or NFS protocols.

To configure AltaVault backups, complete the following steps:

- From the SnapProtect GUI, expand Storage Resources, right-click Libraries, and select Add > Disk Library.
- Configure the Add Disk Library page and click OK.
 - Enter a name.
 - Select a media agent.
 - Select Network Path.
 - Enter a user name in the Connect As field.
 - Enter and confirm the password.
 - Browse to select a folder.



- Right-click the Primary (Classic) policy and select Change Data Path. Change the data path to the newly added disk library for the primary (classic) copy in your storage policy and point the backups to the AltaVault device.

Note: Configuring the AltaVault device to move data to the cloud is not managed by SnapProtect and is therefore outside of the scope of this document. For more information about how to configure AltaVault, refer to the [NetApp SteelStore Solution Guide](#).

12 SnapProtect and Oracle Disaster Recovery

SnapProtect cannot orchestrate the entire disaster recovery (DR) workflow for Oracle. However, you can use SnapProtect to configure SnapMirror and then use the destination of the mirrored volumes to manually bring up Oracle at the DR location. Using scripts, an Oracle administrator can run this configuration outside of SnapProtect.

Appendix: Backup Test Validation

NetApp validated a cascade backup D2D2T and used the results of that validation test to create the best practices guidance provided in this report. We ran the validation tests using configuration information listed in Table 1 and Table 2.

We created a primary Snapshot copy of the production server. Using SnapMirror, we created an auxiliary copy of the production server and mirrored on the secondary server. From the mirrored destination, we used SnapVault to create another copy and stored it on the tertiary server. We then performed a backup copy operation and streamed it from the SnapVault destination to an AltaVault appliance and tape library. In short, we created the primary Snapshot copy of the production server, mirrored it by using SnapMirror technology, stored it by using SnapVault, and streamed it to an AltaVault appliance.

Table 4 lists the results of the validation test.

Table 4) Validation test results.

SnapProtect Operation	Average Time
Snapshot copy	1 minute
SnapMirror to secondary cluster (baseline)	8 hours
SnapMirror updates to secondary cluster at data	14 minutes

SnapProtect Operation	Average Time
change rate of 3%	
SnapVault baseline	8 hours
SnapVault updates at data change rate of 10% per day	30 minutes
Restore and recovery (SnapRestore)	7–8 minutes
Restore and recovery from SnapVault destination (copy-based full restore)	Close to 9 hours
Database clone operation	2 minutes

Note: Plan for 15 minutes of overhead from the native replication operation on Data ONTAP. These overheads might include 5 minutes for the job start notification to OCUM, 5 minutes for the confirmation job run by OCUM (a one-time activity for provisioning storage on secondary target), and 5 minutes for the job completion notification from OCUM to the server running SnapProtect server.

References

This report references the following documents and resources:

- Getting Started with User Administration and Security
http://docs.snapprotect.com/netapp/v10/article?p=features/user_admin/user_admin.htm
- NetApp Interoperability Matrix Tool
<http://mysupport.netapp.com/matrix/mtx/login.do;jsessionid=639F09FCB35AB91A7D7F59084D63834A>
- NetApp SteelStore Solution Guide for CommVault Simpana
<https://fieldportal.netapp.com/?oparams=278858>
- Rapid SnapVault/OSSV Space Estimator
<https://fieldportal.netapp.com/?oparams=65793>
- SnapProtect - Deployment - UNIX – Oracle
http://docs.snapprotect.com/netapp/v10/article?p=products/oracle_rac/snap/deployment_unix.htm
- SnapProtect Software Binder
<https://fieldportal.netapp.com/Modules/FieldPortal/Binders/Content.aspx?contentID=77903>
- Storage Policy – Getting Started
http://docs.snapprotect.com/netapp/v10/article?p=features/storage_policies/storage_policies.htm
- System Requirements - CommServe
<http://docs.snapprotect.com/netapp/v10/article?p=products/cs/commserve.htm>
- TR-3633: Best Practices for Oracle Databases on NetApp Storage
<https://fieldportal.netapp.com/?oparams=140244>
- TR-3920: NetApp SnapProtect Management Software Solution Overview
<https://fieldportal.netapp.com/?oparams=206689>
- TR-4249: Oracle Database on NetApp Clustered Data ONTAP
<https://fieldportal.netapp.com/?oparams=223045>
- TR-4330: Cluster-Aware Backup Configuration for SnapProtect and Simpana
<https://fieldportal.netapp.com/?oparams=265140>

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, SnapCenter, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, WAFL and other names are trademarks or registered trademarks of NetApp Inc., in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>. TR-4432-0615