

Veritas NetBackup™ Replication Director Solutions Guide

UNIX, Windows, Linux

Release 8.1 Draft



Veritas NetBackup™ Replication Director Solutions Guide

Legal Notice

Copyright © 2017 Veritas Technologies LLC. All rights reserved.

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

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

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

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

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

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

Veritas Technologies LLC
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

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	8
	About NetBackup Replication Director	8
	About the roles of the Replication Director plug-ins	10
	Software required to use Replication Director	10
	NetBackup configuration for Replication Director	11
	Tools for troubleshooting Replication Director	12
Chapter 2	Additional configuration topics	14
	Configuring the NetBackup Client Service	14
	NetBackup naming conventions	15
	How to configure a multi-NIC environment	16
Chapter 3	Creating a NetBackup storage server for snapshot replication	18
	Creating a NetBackup storage server for snapshot replication	18
	Updating an OpenStorage storage server to reflect plug-in updates	23
	Adding the storage server credentials to a NetBackup server	24
Chapter 4	Configuring disk pools for snapshot and replication	26
	About disk pools for snapshots and snapshot replication	26
	About disk volumes for snapshots and snapshot replication	27
	Creating disk pools for snapshot replication	29
	Updating disk pools after volumes are added, are deleted, or are changed	31
	Updating an OpenStorage disk pool to reflect plug-in updates	33
	How to resolve snapshot disk volume changes	34
	Using bpstsinfo to view the replication topology of a device	40
	NetApp storage server sample bpstsinfo output	41

Chapter 5	Configuring storage units and storage unit groups for snapshots and snapshot replication	45
	Creating storage units for a Replication Director configuration	45
	Creating storage unit groups for snapshots	47
Chapter 6	Configuring storage lifecycle policies for snapshots and snapshot replication	50
	About configuring storage lifecycle policies for snapshots and snapshot replication	50
	Creating a storage lifecycle policy for snapshots and snapshot replication	52
	Operation types in a storage lifecycle policy	54
	Snapshot operation in an SLP	55
	Replication operation in an SLP	59
	Index From Snapshot operation in an SLP	61
	Backup From Snapshot operation in an SLP	68
	Duplication operation in an SLP	70
	Retention types for storage lifecycle policy operations	71
	Expire after copy retention type for SLP operations	72
	Fixed retention type for SLP operations	73
	Maximum snapshot limit retention type for SLP operations	73
	Mirror retention type for SLP operations	75
	Target retention type for SLP operations	75
Chapter 7	Configuring backup policies for snapshots and snapshot replication	76
	About configuring a backup policy for Replication Director	76
	Configuring an NDMP policy to protect a NAS host	77
	Configuring a Standard or MS-Windows policy to protect clients using NDMP with Data Mover	81
	Configuring a Standard or MS-Windows policy to protect NAS volumes or SAN-connected devices	84
	About NDMP support for Replication Director	87
	Limitations of Replication Director with NDMP	88
	Authorizing NetBackup access to a NAS (NDMP) host	89
	ALL_FILESYSTEMS and VOLUME_EXCLUDE_LIST directives	91
	Configuring an NDMP policy in a multi-network environment	94

Chapter 8	Restoring from a snapshot	95
	About restores from array-based snapshots	95
	Restoring files and folders from an array-based snapshot	97
	About restores from array-based snapshots of virtual machines	100
	Restoring files from array-based snapshots of virtual machines	101
	Using OpsCenter to restore from array-based snapshots	102
	How NetApp performs a volume-level rollback restore	102
	Restoring (rolling back) from an array-based snapshot	104
Chapter 9	OpsCenter reporting	109
	Veritas OpsCenter reporting	109
	Configuring an alert for OpenStorage events	109
	Storage lifecycle policy reporting	110
	Disk pool monitoring	110
	Monitoring snapshot replication jobs	111
	Reporting on storage units, storage unit groups, and storage lifecycle policies	111
Chapter 10	Using NetApp disk arrays with Replication Director	113
	Using NetApp disk arrays with Replication Director	113
	Supported NetApp topologies	117
	NetApp topologies that Replication Director does not support	118
	Using NetApp Data ONTAP 7-mode with Replication Director	120
	Configuration overview: NetApp 7-Mode with Replication Director	120
	Licenses required for NetApp Data ONTAP 7-Mode with Replication Director	122
	Software required to use NetApp Data ONTAP 7-Mode with Replication Director	126
	About using NetApp SAN-connected storage with Replication Director	127
	If the OnCommand Unified Manager root or administrator password has changed	130
	Considerations when configuring an OnCommand Unified Manager as a NetBackup storage server	130
	Importing existing NetApp relationships for NetBackup control	132

	Enabling Unicode and language settings on NetApp disk arrays	132
	Using NetApp Clustered Data ONTAP with Replication Director	133
	Configuration overview: NetApp Clustered Data ONTAP with Replication Director	134
	Licenses required for NetApp Clustered Data ONTAP with Replication Director	135
	Software required to use NetApp Clustered Data ONTAP with Replication Director	137
	Configuring Replication Director to work with Clustered Data ONTAP	138
	About creating backup policies for Clustered Data ONTAP with Replication Director	140
	Protecting volumes with nested junctions for Clustered Data ONTAP	148
	Limitations to using Clustered Data ONTAP with Replication Director	150
Chapter 11	Using Oracle with Replication Director	151
	Requirements for Oracle support	151
	About Oracle support for Replication Director	151
	Configuring an Oracle Intelligent Policy	152
	Configuring a script- or template-based Oracle policy	158
Chapter 12	Using Virtual Machines with Replication Director	164
	Requirements for virtual machine support	164
	About virtual machines and Replication Director	164
	Notes on Replication Director for virtual machines	167
	Configuring a policy for virtual machines to use Replication Director	169
	About jobs in the Activity Monitor that use Replication Director for virtual machines	172
Chapter 13	Terminology	175
	Replication terminology	175
Index		179

Introduction

This chapter includes the following topics:

- [About NetBackup Replication Director](#)
- [About the roles of the Replication Director plug-ins](#)
- [Software required to use Replication Director](#)
- [NetBackup configuration for Replication Director](#)
- [Tools for troubleshooting Replication Director](#)

About NetBackup Replication Director

Replication Director is the implementation of NetBackup OpenStorage-managed snapshots and snapshot replication, where the snapshots are stored on the storage systems of partnering companies. OpenStorage is a Veritas API that lets NetBackup communicate with the storage implementations that conform to the API.

Replication Director uses the functions of the OpenStorage partners to perform the following tasks:

- To share disks so that multiple heterogeneous media servers can access the same disk volume concurrently.
- To balance loads and tune performance. NetBackup balances backup jobs and storage usage among the media servers and disk pools.
- To make full use of disk array capabilities, including fast storage provisioning and almost unlimited storage.
- To use as an alternative to off-site vaulting. Storage replication technology provides an efficient means to send copies of user data (files, applications, databases) to off-site storage as part of a disaster recovery plan.

NetBackup stores snapshots of client data on the volumes that are available to the storage server.

Snapshots represent a point-in-time of primary storage data as captured by the storage hardware. NetBackup can then instruct the storage server to replicate the snapshot from primary volumes to other volumes available to the storage server. The snapshot can be replicated to multiple volumes within the storage server, or to storage outside of the storage server, such as a tape device or other disk storage. Replication Director can accommodate an assortment of scenarios to meet the specific data protection needs of an organization.

Replication Director offers a single NetBackup interface for end-to-end data protection management for the following tasks:

- Unified policy management.
Use the **NetBackup Administration Console** as the one, centralized backup infrastructure to manage the lifecycle of all data.
- Snapshot copy management.
Use NetBackup to manage the entire lifecycle of the snapshot. Replication Director uses OpenStorage with a media server to access the storage server volumes. No image can be moved, expired, or deleted from the disk array unless NetBackup instructs the storage server to do so.
The instruction to perform the initial snapshot comes from an operation in a NetBackup storage lifecycle policy (SLP). You can create one SLP that instructs NetBackup to create the initial snapshot, to replicate the snapshot to several locations, and to indicate a different retention period for each of the replications. Additional instructions (or operations) can be included in the SLP that create a backup from the snapshot, index the snapshot, and more.
- Snapshot copy monitoring.
Use NetBackup OpsCenter to monitor the creation of each copy at each storage location. OpsCenter provides extensive reporting on the entire replication environment.
- Global search and restore.
Recovery is available from any storage device in the environment that is defined to NetBackup. This includes recovery from the primary copy or any replicated copy on disk, or from any duplicated copy on disk or tape.

About the roles of the Replication Director plug-ins

Replication Director uses an OpenStorage plug-in on the media server to communicate with the disk array (through the storage server) and to make requests to move data.

The OpenStorage partner hosts a software plug-in that allows communication between NetBackup and the disk array.

[Table 1-1](#) lists the plug-ins used by NetBackup and by the OpenStorage partners.

Table 1-1 Names of plug-ins used in Replication Director

Plug-in name	Installation location
NetApp Plug-in for Veritas NetBackup	The NBUPugin communicates with the OnCommand Unified Manager. For installation instructions, see the <i>NetApp Plug-in for Veritas NetBackup Installation and Administration Guide</i>, available from the NetApp Support Site. The default communication between the two plug-ins is to use encryption. A change can be made to the NBUPugin config file to disable encryption. The Encryption policy attribute has no impact on the encryption between the plug-ins. By default, the NetApp Plug-in for Veritas NetBackup uses IPv4, however the system can be configured to use IPv6. Note: The NetApp Plug-in for cDOT support (2.0) cannot be installed on the OnCommand Unified Manager server, the master server, or any media servers. You should install the plug-in on a separate Windows or Linux computer.

Software required to use Replication Director

Install NetBackup on all master servers, media servers, and NetBackup clients to be used with Replication Director.

The following NetBackup licenses are required to use Replication Director.

Table 1-2 NetBackup licenses required for Replication Director

NetBackup host	License
Master server	The NetBackup Replication Director option.

Table 1-2 NetBackup licenses required for Replication Director (*continued*)

NetBackup host	License
Media servers	On each media server that can access the disk array, install: ■ The Data Protection Optimization Option only if you want to perform a snapshot backup to deduplication disk. ■ An NDMP license to perform a snapshot backup to disk or tape using NDMP.
Clients	Only NetBackup client software is required.

The [Veritas NetBackup Hardware Compatibility List \(HCL\)](#) lists the platforms on which Replication Director is supported.

NetBackup configuration for Replication Director

NetBackup configuration is performed by the NetBackup administrator, as described in [Table 1-3](#).

Table 1-3 NetBackup configuration tasks overview

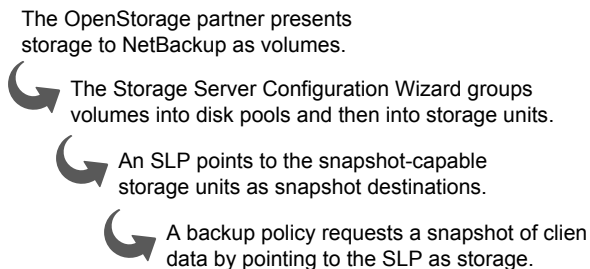
Step	Description	Reference topic
1	Install or upgrade NetBackup software on the master server and media server(s).	See “Software required to use Replication Director” on page 10.
2	Run the Storage Server Configuration Wizard to configure the OpenStorage partner as a NetBackup storage server. This wizard also configures the following: ■ The media servers that can access the storage server. ■ A disk pool that contains the primary snapshot. ■ A storage unit for the primary disk pool.	See “Creating a NetBackup storage server for snapshot replication” on page 18.
3	Create an additional disk pool for every group of disk volumes that will contain snapshot replications of the primary snapshot. As part of the Disk Pool Creation Wizard, a storage unit is configured for each disk pool.	See “Creating disk pools for snapshot replication” on page 29.
4	Create a storage unit for any operation that will produce duplications (non-snapshot copies).	See the NetBackup Administrator's Guide, Volume I .

Table 1-3 NetBackup configuration tasks overview (*continued*)

Step	Description	Reference topic
5	Configure a storage lifecycle policy. Create a new operation in the SLP for each task that the SLP is to perform. For example, create a Snapshot operation to perform the initial snapshot and a Replication operation to create a copy of the snapshot.	See “ Creating a storage lifecycle policy for snapshots and snapshot replication ” on page 52.
6	Configure a NetBackup backup policy to perform all of the operations indicated in the SLP. To do so, the Policy storage selection in the policy must indicate the SLP that is configured for snapshots and snapshot replication. Note: Do not use the Policy Configuration Wizard or the Getting Started Wizard to configure policies for Replication Director.	See “ Configuring a Standard or MS-Windows policy to protect NAS volumes or SAN-connected devices ” on page 84. See “ Configuring an NDMP policy to protect a NAS host ” on page 77. See “ About Oracle support for Replication Director ” on page 151. See “ About virtual machines and Replication Director ” on page 164.

The following figure is an overview of how the NetBackup components fit together to perform snapshots and snapshot replication. The following sections describe how to configure each part of this process.

Figure 1-1 How NetBackup uses OpenStorage partner storage



Tools for troubleshooting Replication Director

NetBackup has developed tools and checklists that make Replication Director configuration easier.

They are located on the following page, along with scripts that can verify whether or not the correct software and licenses are been installed.

<http://www.veritas.com/docs/DOC5240>

The following Veritas technote contains information that can help you solve various problems that you may encounter while using Replication Director. It is organized into general categories by problem or issue.

<http://www.veritas.com/docs/TECH231425>

Additional configuration topics

This chapter includes the following topics:

- [Configuring the NetBackup Client Service](#)
- [NetBackup naming conventions](#)
- [How to configure a multi-NIC environment](#)

Configuring the NetBackup Client Service

By default, the NetBackup Client Service is configured on Windows with the **Local System** account. The **Local System** account lacks sufficient rights to perform certain backup and restore operations.

For example, for NetBackup to access CIFS volumes, the account must be changed from **Local System** to an account with access to the CIFS share.

To change the NetBackup Client Service logon account on a Windows computer:

- Open the Windows Services application.
- To change the logon account, stop the NetBackup Client Service.
- Open the properties for the NetBackup Client Service.
- Provide the name and password of the account that has the necessary permissions. For example, change the logon to that of *Administrator*.
- Restart the service.

If the logon property is not changed for the NetBackup Client Service, the policy validation fails with status code 4206.

Situations in which the NetBackup Client Service logon account requires changing

The following list contains situations in which the NetBackup Client Service logon account needs to be changed:

- To access CIFS storage for a storage unit.
- To use UNC paths, the network drives must be available to the service account that the NetBackup Client Service logs into at startup. You must change this account on each Windows client that is backed up that contains data that is shared with another computer.
- During a snapshot: To have read access to the share for backup purposes and write access during restores.
The account must be for a domain user that is allowed to access and write to the share. To verify the account, log on as that user and try to access the UNC path. For example: `\\server_name\share_name`.
- For database agents and options, configure the service with a logon account that has the necessary permission or privileges. See the documentation for your agent or option for more information.
- For the database agents that support VMware backups on a NetApp disk array, configure the logon account to one that has access to the disk array.

NetBackup naming conventions

The following set of characters can be used in user-defined names, such as disk pools and storage lifecycle policies:

- Alphabetic (A-Z a-z) (names are case-sensitive)
- Numeric (0-9)
- Period (.)
- Plus (+)
- Minus (-)
Do not use a minus as the first character.
- Underscore (_)

Note: No spaces are allowed.

How to configure a multi-NIC environment

A NetBackup client can have multiple host names that correspond to multiple Network Interface Cards (NICs). To access the snapshots using a particular NIC, you must use the host name that corresponds to that NIC as a client name in the NetBackup backup policy.

Ensure that the route to the filer follows the same interface that is defined as the client name in backup policies.

Note: If the NIC information is not configured correctly, backup and restore jobs may fail.

Example of a client that uses multiple NICs

Consider an HP-UX 11.31 host with the host name `hp_nas.abc.xyz.com`. This host is configured as a client in a backup policy. This backup policy is intended to support the NAS volumes which are mounted on the host. The host has multiple NAS volumes mounted which are created on the filer with IP address `10.80.155.147`.

Host `hp_nas.abc.xyz.com` has two NICs configured, as shown in [Table 2-1](#).

Table 2-1 NICs on example host

NICs	IP address	Mapped to NAS volume
lan0	10.80.139.208	hp_nas.abc.xyz.com
lan1	10.80.139.210	hp_nas1.abc.xyz.com

The following is an example of the routing table that is defined for host `hp_nas.abc.xyz.com`:

```
netstat -nr
Routing tables
Destination  Gateway      Flags  Refs  Interface  Pmtu
127.0.0.1    127.0.0.1    UH     0     lo0        32808
10.80.139.210 10.80.139.210 UH     0     lan1       32808
10.80.139.208 10.80.139.208 UH     0     lan0       32808
10.80.139.0   10.80.139.210 U       2     lan1       1500
10.80.136.0   10.80.139.208 U       2     lan0       1500
127.0.0.0     127.0.0.1    U       0     lo0        32808
default      10.80.136.1   UG     0     lan0       1500
```

Since the IP/subnet address of the filer does not fall under any routing entry defined, network communication from the host happens using the default routing entry.

As previously mentioned, the default route entry has the same interface (`lan0`) as that of the entry corresponding to the client name `hp_nas.abc.xyz.com` (`lan0`).

Similarly, if there is an entry defined in the routing table explicitly for the subnet of the storage system's IP address, ensure that the same interface similarity exists.

Creating a NetBackup storage server for snapshot replication

This chapter includes the following topics:

- [Creating a NetBackup storage server for snapshot replication](#)
- [Updating an OpenStorage storage server to reflect plug-in updates](#)
- [Adding the storage server credentials to a NetBackup server](#)

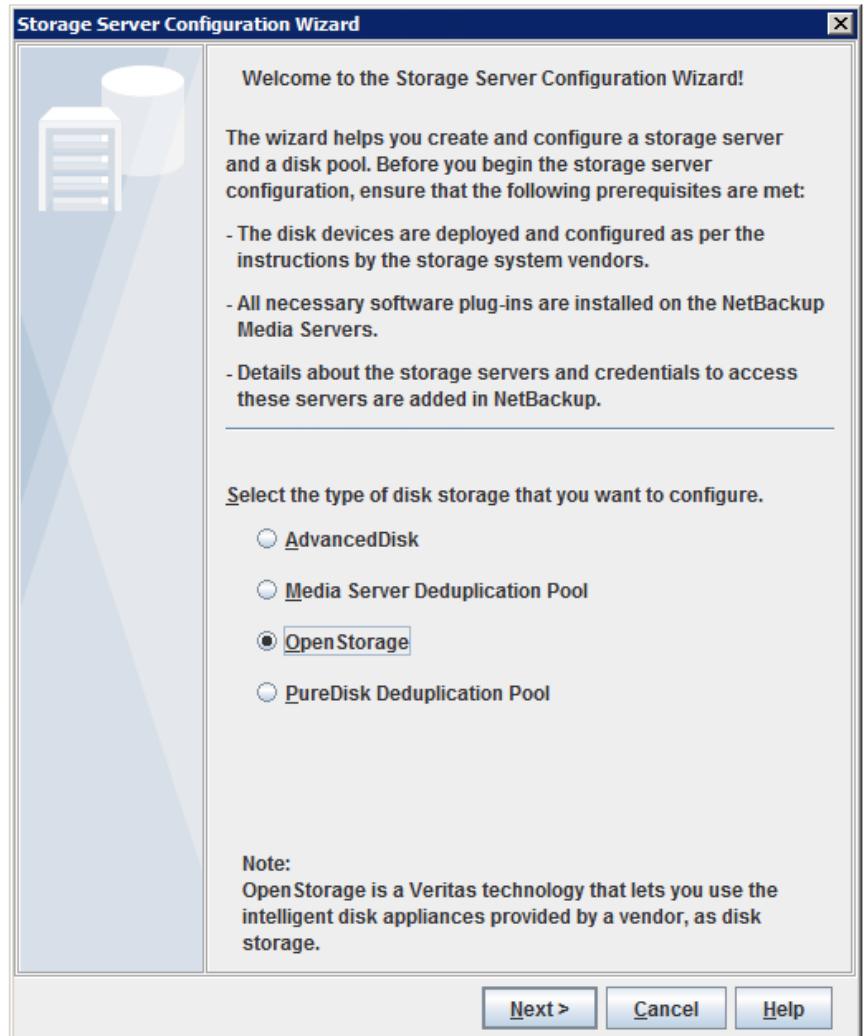
Creating a NetBackup storage server for snapshot replication

A NetBackup storage server is a NetBackup entity that has exclusive access to manage snapshots on the volumes of an OpenStorage partner. This procedure describes creating a storage server using the **Storage Server Configuration Wizard**. Specific partner considerations are referenced throughout.

To create a storage server

- 1 Before launching the **Storage Server Configuration Wizard**, make sure that the OpenStorage partner has the necessary software installed and is online. The volumes of the disk array must also be configured.
- 2 Click **Configure Disk Storage Servers** in the **NetBackup Administration Console** main window to launch the **Storage Server Configuration Wizard**.

- 3 Select **OpenStorage** as the disk storage type. Click **Next**.



- 4 Configure the details of the storage server.

Media server Select the media server to query the storage server. This is the media server that is assigned the credentials for the storage server. Credentials allow the media server to communicate with the storage server.

Note that all of the media servers in the configuration appear in the list, even if the OpenStorage plug-in is not installed. Select a media server where the OpenStorage plug-in is installed.

- Enter the user name to log on to the storage host.
If the storage host does not require logon credentials, enter dummy credentials.
- Enter the password for the logon account.
- Re-enter the password to confirm the password.

For a media server to communicate with and have access to a storage server, it must be added to the Replication Director environment.

See [“Adding the storage server credentials to a NetBackup server”](#) on page 24.

Storage server type Select the type of storage server to create:

- For a NetApp 7-mode configuration, select **NetApp OnCommand server (7-mode)** (Network_NTAP).
- For a NetApp Clustered Data ONTAP configuration, select **NetApp OnCommand server (cluster-mode)** (NTAP_CDOT).

Storage server name Enter the name of the storage server. The name that you use for the storage server must be used consistently throughout both the NetBackup environment and the storage vendor environment.

Enter the exact name of the storage server, whether a fully-qualified name or a short name.

- In a NetApp 7-mode configuration, this is the OnCommand Unified Manager.
- In a NetApp Clustered Data ONTAP configuration, this is the computer that hosts the NBUPlugin 2.0, not the OnCommand Unified Manager.

Click **Next**.

5 The **Additional Media Server Configuration for OpenStorage Devices** panel appears in environments where there are multiple media servers or where the master server is on a different host from the media server.

- Enable the check boxes for all media servers that are to be used to access the storage server for snapshots, snapshot replication, or restores.
- Enable the check box for the computer that hosts the master server, if it appears in the list. The master server host must be enabled so that the NetBackup catalog is updated correctly for rollback and restore operations.

Note: The master server does not appear in the list if it was already selected in the **Add Storage Server** wizard pane as a media server for the **Select media server** property (Step 4).

- 6 The wizard displays a summary panel that lists the configuration information that you've entered. Click **Back** to make any changes or **Next** to create the storage server.
- 7 The wizard declares that the storage server was successfully created. To create a disk pool, make a check in the check box labeled **Create a disk pool using the storage server that you have just created**. A disk pool is necessary for snapshots and snapshot replication.

Click **Next** to launch the **Disk Pool Configuration Wizard**.

- 8 Select the type of disk pool that you want to create. If an OpenStorage partner does not appear for selection, make sure that the license has been installed and that an OpenStorage storage server has been created
- 9 On the **Select Storage Server** panel, select the storage server that was created earlier in the wizard. Click **Next**.
- 10 The **Select Disk Pool Properties and Volumes** panel presents all of the volumes that have been configured in the storage of the OpenStorage partner by the storage administrator.

A disk pool can contain only those volumes that share similar properties. So that dissimilar volumes are not combined, NetBackup filters the volumes for selection.

Select the **Primary** property to configure this first disk pool for snapshots. The list displays all of the volumes that match the selected property.

- 11 Select a primary volume in the table to be part of this first disk pool. Notice that primary volumes also have the **Source** property set as well. Snapshots on the primary volume are the source for snapshot replication. Click **Next**.
- 12 In the **Additional Disk Pool Information** panel, name the disk pool and add any comments you want to make regarding the disk pool.

See [“NetBackup naming conventions”](#) on page 15.

Enable **Limit I/O streams** to limit the number of read and write streams (jobs) for each volume in the disk pool. Select the number of read and write streams to allow per volume. When the limit is reached, NetBackup chooses another volume for write operations, if available. If not available, NetBackup queues jobs until a volume is available.

Click **Next**.

- 13 Review the summary screen that lists the disk pool configuration. Click **Back** to make any changes or **Next** to create the disk pool.
- 14 The wizard declares that the disk pool was successfully created. To create a storage unit, make a check in the check box labeled **Create a storage unit using the disk pool that you have just created**. A storage unit is necessary for snapshots and snapshot replication.

Click **Next**.

- 15 In the **Storage Unit Creation** panel:

- Name the storage unit.
- Select the media server(s) that can use the storage unit:

Use any available media server to transport data

NetBackup selects any media server to access the storage unit.

Use only the selected media servers

NetBackup uses only the media server that is specified to access the storage unit.

Only the media servers that have the OpenStorage plug-in installed appear in this list. For a media server to communicate with and have access to a storage server, it must be added to the Replication Director environment.

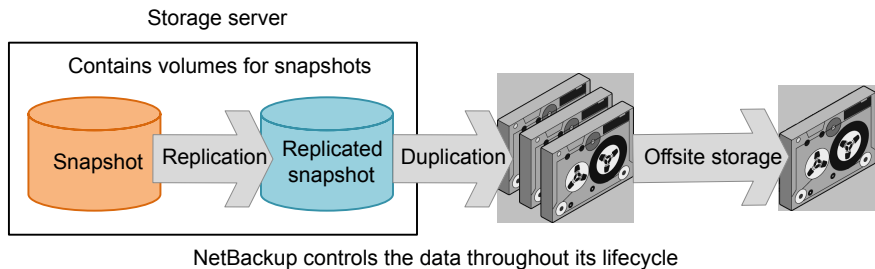
Note: A storage unit can represent many physical devices. When a storage unit is a replication target, NetBackup lets the plug-in select which device to use within the storage unit. For replication jobs, storage units and storage unit groups ignore the **Maximum concurrent jobs** setting. NetBackup does not attempt to throttle the parameters.

- 16 Click **Next**. The final wizard panel displays, announcing that the wizard has been completed.

You've just configured a storage server, a disk pool, and a storage unit to contain the primary snapshots. Configure additional disk pools (and storage units) for every group of disk volumes that will contain snapshot replications of the primary snapshots.

For example, in the following figure, two disk pools are necessary:

- One disk pool that contains volumes to hold primary snapshots and act as a source for other replications, and
- A second disk pool that contains the volumes that are replication targets for snapshot replications.



See the following topic for more information about creating more disk pools and storage units.

See [“Creating disk pools for snapshot replication”](#) on page 29.

Updating an OpenStorage storage server to reflect plug-in updates

If an OpenStorage partner updates their plug-in, update the NetBackup storage server to reflect the new functionality of the plug-in.

For example, the NetApp plug-in used for Replication Director is the NBUPlugin.

If the OpenStorage plug-in is updated on the storage server, use the following procedure to update the NetBackup storage server configuration to reflect this:

To update the NetBackup OpenStorage storage server from the NetBackup Administration Console

- 1 In the **NetBackup Administration Console**, expand **Media and Device Management > Credentials > Storage Servers**.
- 2 In the right pane, right-click the storage server.
- 3 Select **Update Storage Server Details**.
- 4 Update the existing disk pools so that each can use the new functionality. Any disk pools that were created after the storage server is updated inherit the new functionality.

See [“Updating an OpenStorage disk pool to reflect plug-in updates”](#) on page 33.

To update the NetBackup OpenStorage storage server configuration from the command line

- ◆ Run the following command on the master server or on one of the media servers:

On Windows:

```
install_path\NetBackup\bin\admincmd\nbdevconfig -updatests
-storage_server storage_server -stype server_type -media_server
media_server
```

On UNIX:

```
/usr/openv/netbackup/bin/admincmd/nbdevconfig -updatests
-storage_server storage_server -stype server_type -media_server
media_server
```

See the following descriptions of the options that require arguments:

<code>-storage_server</code> <code>storage_server</code>	The name of the disk appliance.
<code>-stype server_type</code>	The storage vendor provides the string that identifies the server type. For example, Network_NTAP or Network_NTAP_CDOT.
<code>-media_server</code> <code>media_server</code>	A NetBackup media server that connects to the storage server. The media server queries the storage server for its capabilities. The vendor plug-in must be installed on the media server. If the plug-in resides on more than one media server, you can specify any one of them.

Adding the storage server credentials to a NetBackup server

Use the following procedure to add the storage server credentials to a NetBackup server in a Replication Director environment.

Note: If you add or change credentials, make sure that the computer that hosts the master server is always selected.

To add OpenStorage server credentials

- 1** In the **NetBackup Administration Console**, expand **Media and Device Management > Credentials > Storage Servers**.
- 2** Select the storage server, then select **Edit > Change**.
- 3** Select the **Media Servers** tab.
- 4** Select the server you want to add. Also make sure that any servers already credentialed are selected.
- 5** Enter the credentials.
- 6** Click **Set** and then click **OK**.

Configuring disk pools for snapshot and replication

This chapter includes the following topics:

- [About disk pools for snapshots and snapshot replication](#)
- [Creating disk pools for snapshot replication](#)
- [Updating disk pools after volumes are added, are deleted, or are changed](#)
- [Updating an OpenStorage disk pool to reflect plug-in updates](#)
- [How to resolve snapshot disk volume changes](#)
- [Using bpstsinfo to view the replication topology of a device](#)

About disk pools for snapshots and snapshot replication

An OpenStorage disk pool represents the disk storage that is exposed to NetBackup through the OpenStorage API. A disk pool can represent one or more volumes. Disk pools inherit their properties from the volumes that comprise the disk pools.

Snapshot and snapshot replication disk pools differ from other NetBackup disk pool types as follows:

- Only one storage unit can access a snapshot or a snapshot replication disk pool.
- Snapshot and snapshot replication disk pools observe no high or no low water marks.

One disk pool to be used for snapshots can be configured as part of the **Storage Server Configuration Wizard**. At least one additional disk pool is necessary for snapshot replication. The **Disk Pool Configuration Wizard** can also be launched independently.

See [“Creating disk pools for snapshot replication”](#) on page 29.

The NetBackup administrator creates multiple disk pools to serve specific purposes in a replication configuration. The volumes in a disk pool must have the properties that match their intended purpose.

For example, the following disk pools are necessary to create a snapshot volume and replicate it to target volumes:

- A disk pool that contains a volume where the initial snapshot can be created. The volume must have the **Snapshot** and **Primary** attributes set. See [“Primary + Replication source snapshot storage unit”](#) on page 57.
- A disk pool that contains a volume with the **Snapshot** and the **Replication target** properties set to serve as the target for a replica snapshot. See [“Replication target snapshot storage unit”](#) on page 58.

The following topic describes the roles that disk pools and storage units can serve in a Replication Director configuration:

See [“About configuring storage lifecycle policies for snapshots and snapshot replication”](#) on page 50.

About disk volumes for snapshots and snapshot replication

For snapshots and snapshot replication, all of the volumes in a disk pool must be homogeneous; that is, they must have the same properties. The NetBackup **Disk Pool Configuration Wizard** enforces compliance, as does the **Change Disk Pool** dialog box.

The storage administrator defines the properties and the replication topology of the disk volumes. The NetBackup administrator creates disk pools, based on the properties of the volumes.

- The volume properties define in what capacity the volumes can be used:

Snapshot	The default property. All volumes that are used for snapshots or snapshot replication must have this property.
Primary	The volume can be used for snapshot creation.
Replication source	The volume can be used as a source for replicating snapshots.

Replication target	The volume can be used as a target for snapshot replication.
Mirror	The volume is a mirror for snapshots. Mirror snapshots have the same life span as the original snapshot.

- The replication topology defines the source and the target volumes for replication. For example, volume S1 replicates to T1, volume S2 replicates to T2, and so on.
When you configure your NetBackup disk pools, add the source volumes (Sn) to the disk pool you use for snapshot creation. Then, add the target volumes (Tn) to the disk pool that is the target of the replication.
- The **Disk Pool Configuration Wizard** may not display all of the properties, depending on the underlying volumes.
For example, if a NetApp SnapMirror relationship is not defined at the volume layer, then the **Mirror** property does not appear in the wizard panel for selection.

Table 4-1 shows the properties that are required for snapshots and snapshot replication volumes, depending on their intended purpose in the NetBackup snapshot and snapshot replication process.

Table 4-1 Purpose of volume and required volume properties

Purpose of volume	Snapshot property	Primary property	Replication source property	Replication target property	Mirror property
A volume to contain the initial snapshots of primary data.	X	X	X A primary volume is always a replication source as well.		
A volume to serve as a replication source or a replication target.	X		X The Source property allows the volume to serve as a source for snapshot copies.	X The Target property allows the volume to contain copies of snapshots.	X A target volume may have the Mirror property enabled or be Independent .

Creating disk pools for snapshot replication

One disk pool can be configured as part of the **Storage Server Configuration Wizard** to contain primary snapshots. Additional disk pools are necessary for snapshot replication.

You can run the `bpstsinfo` command to view the replication properties of the volumes and understand which volumes to include in the various disk pools.

See [“Using bpstsinfo to view the replication topology of a device”](#) on page 40.

To create a disk pool

- 1 Select **Media and Device Management**. In the right pane, click **Configure Disk Pool**.
- 2 In the **Disk Pool Configuration Wizard** welcome panel, click **Next**.
- 3 Select the type of disk pool that you want to create.
- 4 On the **Select Storage Server** panel, select the storage server. Click **Next**.

- 5 The **Select Volumes** panel presents all of the volumes that have been configured in the storage of the OpenStorage partner by the storage administrator.

You've already created one disk pool as part of the **Storage Server Configuration Wizard** to contain the primary snapshots that can serve as a source for replication. Now create a disk pool that can serve as a replication target.

To create a disk pool that is a target for replication, select **Replication target**. NetBackup filters the volumes for selection so that dissimilar volumes are not combined.

Note that in the **Replication** column, all the volumes have both **Source** and **Target** properties. That means that the volume can serve as both a target for replications as well as a source for another replication.

Expand the column to display other properties of the volume. For example, whether the volume is configured to be a mirror.

Another method to filter the volumes is to first clear the **Primary**, **Replication source**, and **Replication target** properties. Then, click on a specific volume. The wizard panel filters the volumes, displaying only those volumes that match the properties of the selected volume.

Note: For 7-mode, when the NBUPlugin is installed on the OnCommand Unified Manager, a NetBackup group is automatically created on that server. You must use the NetApp Management Console to add resource pools to the NetBackup group so that the resource pools are exposed to NetBackup.

See [the section called "Regarding disk pools for OnCommand Unified Manager storage servers"](#) on page 131.

- 6 Select the volume(s) to be part of this disk pool. Click **Next**.
- 7 In the **Additional Disk Pool Information** panel, name the disk pool.

See ["NetBackup naming conventions"](#) on page 15.

The available size that is listed is the total amount of space available in the pool. The raw size is the total raw, unformatted size of the storage in the disk pool. Click **Next**.

- 8 The disk pool summary panel displays the storage server configuration up to this point.

Click **Next** to configure the disk pool.

- 9 The wizard announces the successful creation of the disk pool. Click **OK**.

- 10** After the disk pool creation completes, create a storage unit that uses the new disk pool. A storage unit that uses this disk pool is necessary for snapshot replication.

Select **Create a storage unit that uses X** where X is the disk pool and then click **Next**.

- 11** In the **Storage Unit Creation** panel, name the storage unit.

Select the media server(s) that can use the storage unit.

Use any available media server to transport data.

NetBackup selects any media server to access the storage unit.

Use only the selected media servers.

NetBackup uses only the media server that is specified to access the storage unit.

Only media servers that have the OpenStorage plug-in installed appear in this list. For a media server to communicate with and have access to a storage server, it must be added to the Replication Director environment.

Configure additional disk pools (and storage units) for every group of disk volumes that will contain snapshot replications of the primary snapshots.

Updating disk pools after volumes are added, are deleted, or are changed

The storage administrator may change the properties of the volumes in a way that affects the topology of the volumes. If these volumes are used in a Replication Director environment, the changes may affect the capabilities of the disk pool. For example, a volume change may make a volume in the disk pool no longer usable by NetBackup.

If volume properties change, you must update the disk pools to which those volumes belong. Depending on the volume changes, you may also have to change storage units, storage unit groups, and storage lifecycle policies.

Note: If an OpenStorage partner updates the plug-in on a disk-array, update the NetBackup storage server and the disk pools to reflect the new functionality of the plug-in.

See [“Updating an OpenStorage storage server to reflect plug-in updates”](#) on page 23.

See [“Updating an OpenStorage disk pool to reflect plug-in updates”](#) on page 33.

To update the volumes in a disk pool after the storage changes

- 1** In the **NetBackup Administration Console**, in the left pane, expand **Media and Device Management > Devices > Disk Pools**.
- 2** In the right pane, select the disk pool you want to update.
- 3** Click **Edit > Change**.
- 4** In the **Change Disk Pool** dialog box, click **Refresh** to query the disk array for new, deleted, or changed volumes.

Change Disk Pool

Disk pool name: Target_DP
 Storage server: flappyvm4
 Disk pool configured for: Snapshot

Disk Pool Properties and Volumes
 A disk pool inherits the properties of its volumes. Only volumes with similar properties can be added to a disk pool.

☐ Primary
☒ Replication source
☒ Replication target

Select any additional volumes from this list to add to this disk pool:

Volume Name	Available Sp...	Raw Size	Replication	Primary
☒ Flexible1	28.7359 GB	38.6451 GB	Source, Targ...	No
☐ Flexible2	28.7359 GB	38.6451 GB	Source, Targ...	No

Find storage changes and available volumes **Refresh**

Total available space: 28.7359 GB
 Total raw size: 38.6451 GB

Comments:

Maximum I/O streams
 Concurrent read and write jobs affect disk performance.
 Limit I/O streams to prevent disk overload.

☒ Limit I/O streams per volume

OK Cancel Help

- 5** NetBackup communicates volume changes in the following manner:
 - If a new volume was added, the volume appears in the list. It may be eligible to be added to the disk pool.

- If volumes have been deleted, or changed, or are no longer homogenous, see the following topic:
 See [“How to resolve snapshot disk volume changes”](#) on page 34.

Updating an OpenStorage disk pool to reflect plug-in updates

If an OpenStorage partner updates their plug-in, update the existing disk pools to reflect the new functionality of the plug-in after you update the NetBackup storage server.

Any disk pools that are created after the storage server is updated inherit the new functionality.

To update an OpenStorage disk pool to reflect plug-in updates

- ◆ Run the following command on the master server:

On Windows:

```
install_path\NetBackup\bin\admincmd\nbdevconfig -changedp -dp  
disk_pool_name -stype server_type -setattribute attribute
```

On UNIX:

```
/usr/opensv/netbackup/bin/admincmd/nbdevconfig -changedp -dp  
disk_pool_name -stype server_type -setattribute attribute
```

See the following descriptions of the options that require arguments:

<code>-changedp</code> <code>disk_pool_name</code>	The name of the disk pool.
<code>-stype server_type</code>	The storage vendor provides the string that identifies the server type.
<code>-setattribute</code> <code>attribute</code>	The <i>attribute</i> is the name of the argument that represents the new functionality. For example, OptimizedImage specifies that the environment supports the optimized synthetic backup. SpanImages specifies that backup images can span across volumes on the disk appliance.

How to resolve snapshot disk volume changes

Veritas recommends that you take the following actions when volume properties or topology change:

- Discuss the changes with the storage administrator. You need to understand the changes so you can change your disk pools (if required) so that NetBackup can continue to use them.
- If the changes were unplanned, request that the changes be reverted so that NetBackup functions correctly again.

NetBackup can process changes to the following volume properties:

- Primary
- Replication Source
- Replication Target

If these volume properties change, NetBackup can update the disk pool to match the changes. NetBackup can continue to use the disk pool, although the disk pool may no longer match the storage unit or storage lifecycle purpose.

When you open the **Change Disk Pool** dialog box, NetBackup loads the disk pool properties from the catalog. NetBackup queries the storage server for changes when you either click the **Refresh** in the **Change Disk Pool** dialog box or when you configure a new disk pool for the storage server.

[Table 4-2](#) describes the possible outcomes and describes how to resolve them.

Table 4-2 Refresh outcomes

Outcome	Description
No changes are discovered.	No changes are required.
NetBackup discovers the new volumes that match the disk pool properties.	The new volumes appear in the Change Disk Pool dialog box. Text in the dialog box changes to indicate that you can add the new volumes to the disk pool.

Table 4-2 Refresh outcomes (continued)

Outcome	Description
The replication properties of all of the volumes changed, but they are still consistent.	A Disk Pool Configuration Alert pop-up box notifies you that the properties of all of the volumes in the disk pool changed, but they are all the same (homogeneous). Disk Pool Configuration Alert The replication properties of the volumes in the disk pool have changed. NetBackup will update the disk pool with the new configuration. The new disk pool properties may differ from their original use in the storage unit or the storage lifecycle policy. Old properties: Snapshot, Replication source, Replication target New properties: Snapshot, Primary, Replication source, Replication target Verify that the disk pool matches the intended purpose of the storage unit or the storage lifecycle policy. OK You must click OK in the alert box, after which the disk pool properties in the Change Disk Pool dialog box are updated to match the new volume properties If new volumes are available that match the new properties, NetBackup displays those volumes in the Change Disk Pool dialog box. You can add those new volumes to the disk pool. In the Change Disk Pool dialog box, select one of the following two choices: ■ OK. To accept the disk pool changes, click OK in the Change Disk Pool dialog box. NetBackup saves the new properties of the disk pool. NetBackup can use the disk pool, but it may no longer match the intended purpose of the storage unit or storage lifecycle policy. Change the storage lifecycle policy definitions to ensure that the replication operations use the correct source and target disk pools, storage units, and storage unit groups. ■ Cancel. To discard the changes, click Cancel in the Change Disk Pool dialog box. NetBackup does not save the new disk pool properties. NetBackup can use the disk pool, but it may no longer match the intended use of the storage unit or storage lifecycle policy.

Table 4-2 Refresh outcomes (continued)

Outcome	Description
The replication properties of the volumes changed, and they are now inconsistent.	A Disk Pool Configuration Error pop-up box notifies you that the replication properties of some of the volumes in the disk pool changed. The properties of the volumes in the disk pool are not homogeneous. Disk Pool Configuration Error The replication properties of the volumes in the disk pool have changed and the existing volumes in the disk pool have inconsistent properties. NetBackup cannot use the disk pool until the storage configuration is fixed. Change the volume properties on the storage server to match the disk pool properties or ensure that all volumes in the disk pool have similar properties. Click on 'Refresh' button to update the storage properties in this disk pool. OK You must click OK in the alert box. In the Change Disk Pool dialog box, the properties of the disk pool are unchanged, and you cannot select them (that is, they are dimmed). However, the properties of the individual volumes are updated. Because the volume properties are not homogeneous, NetBackup cannot use the disk pool until the storage configuration is fixed. NetBackup does not display new volumes (if available) because the volumes already in the disk pool are not homogeneous. To determine what has changed, compare the disk pool properties to the volume properties. Work with your storage administrator to change the volume properties back to their original values. The disk pool remains unusable until the properties of the volumes in the disk pool are homogenous. In the Change Disk Pool dialog box, click OK or Cancel to exit the Change Disk Pool dialog box.

Table 4-2 Refresh outcomes (continued)

Outcome	Description
The snapshot properties changed.	A Disk Pool Configuration Error pop-up box notifies you that the snapshot properties of some of the volumes in the disk pool changed. Disk Pool Configuration Error The snapshot property of one or more volumes in the disk pool has changed. This property cannot be changed after initial configuration. NetBackup cannot use the disk pool until the storage configuration is fixed. Change the volume's snapshot property on the storage server to match the disk pool properties. Click on 'Refresh' button to update the storage properties in this disk pool. OK You must click OK in the alert box. In the Change Disk Pool dialog box, the properties of the disk pool are unchanged, and you cannot select them (that is, they are dimmed). However, the properties of the individual volumes are updated. Because the volume properties are not homogeneous, NetBackup cannot use the disk pool until the storage configuration is fixed. NetBackup does not display new volumes (if available) because the volumes already in the disk pool are not homogeneous. To determine what has changed, compare the disk pool properties to the volume properties. Work with your storage administrator to change the volume properties back to their original values. The disk pool remains unusable until the properties of the volumes in the disk pool are homogenous. Click OK or Cancel to exit the Change Disk Pool dialog box.

Table 4-2 Refresh outcomes (*continued*)

Outcome	Description
The replication topology changed.	A Disk Pool Configuration Alert pop-up box notifies you that the replication topology changed.  You must click OK in the alert box. If NetBackup also discovers the new volumes that match the replication properties, they are displayed in the dialog box. You can add those new volumes to the disk pool. Work with your storage administrator to understand the topology changes. Alternatively, use the <code>bpstsinfo -lsuinfo</code> command to discover the current topology. Compare the new topology to the previous topology. See “Using bpstsinfo to view the replication topology of a device” on page 40. In the Change Disk Pool dialog box, select one of the following two choices: ■ OK. To accept the disk pool changes, click OK in the Change Disk Pool dialog box. NetBackup saves the new properties of the disk pool. NetBackup can use the disk pool, but it may no longer match the intended purpose of the storage unit or storage lifecycle policy. Change the storage lifecycle policy definitions to ensure that the replication operations use the correct source and target disk pools, storage units, and storage unit groups. ■ Cancel. To discard the changes, click Cancel in the Change Disk Pool dialog box. NetBackup does not save the new disk pool properties. NetBackup can use the disk pool, but it may no longer match the intended use of the storage unit or storage lifecycle policy.

Table 4-2 Refresh outcomes (*continued*)

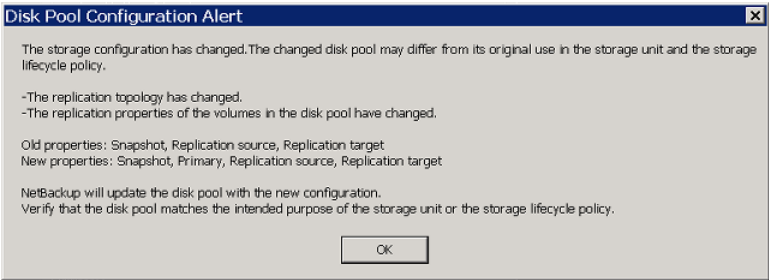
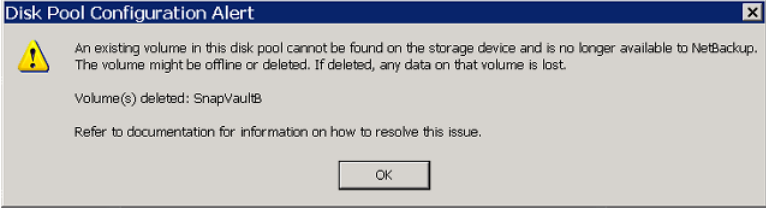
Outcome	Description
The replication topology changed and the replication properties of the volumes in the disk pool changed.	A Disk Pool Configuration Alert pop-up box notifies you that the replication topology changed and all of the replication properties of all of the volumes in the disk pool changed. The new properties are all the same (homogeneous).  You must click OK in the alert box. In the Change Disk Pool dialog box, the properties of the disk pool are updated to show the new properties. You cannot select the properties (that is, they are dimmed). If new volumes are available that match the new properties, NetBackup displays those properties in the Change Disk Pool dialog box. You can add those new volumes to the disk pool. Work with your storage administrator to understand the topology changes. Alternatively, use the <code>bpstsinfo -lsuinfo</code> command to discover the current topology. Compare the new topology to the previous topology. See “Using bpstsinfo to view the replication topology of a device” on page 40. In the Change Disk Pool dialog box, select one of the following two choices: OK. To accept the disk pool changes, click OK in the Change Disk Pool dialog box. NetBackup saves the new properties of the disk pool. NetBackup can use the disk pool, but it may no longer match the intended purpose of the storage unit or storage lifecycle policy. Change the storage lifecycle policy definitions to ensure that the replication operations use the correct source and target disk pools, storage units, and storage unit groups. Cancel. To discard the changes, click Cancel in the Change Disk Pool dialog box. NetBackup does not save the new disk pool properties. NetBackup can use the disk pool, but it may no longer match the intended use of the storage unit or storage lifecycle policy.

Table 4-2 Refresh outcomes (*continued*)

Outcome	Description
NetBackup cannot find a volume or volumes that were in the disk pool.	A Disk Pool Configuration Alert pop-up box notifies you that an existing volume or volumes was deleted from the storage device:  NetBackup can use the disk pool, but data may be lost. To protect against accidental data loss, NetBackup does not allow volumes to be deleted from a disk pool. To continue to use the disk pool, do the following: ■ Use the <code>bpimmedia</code> command or the Images on Disk report to display the images on the specific volume. ■ Expire the images on the volume. ■ Use the <code>nbdevconfig</code> command to set the volume state to DOWN so NetBackup does not try to use it.

Using `bpstsinfo` to view the replication topology of a device

For a replication operation to succeed, a volume which is a source of replication must have a replication partner which is the target of replication. The replication relationship between volumes is provided to NetBackup by the storage device using the OpenStorage APIs.

To understand the replication topology of the storage server, run the `bpstsinfo` command, specifying the storage server name and the OpenStorage server type. For example:

```
bpstsinfo -lsuinfo -storage_server storage_server_name -stype
storage_type
```

The command is located in the following directory:

- Windows:
`Install_path\NetBackup\bin\admincmd\`

- UNIX:

```
/usr/opensv/netbackup/bin/admincmd/
```

The output from the `bpstsinfo` command displays the following information:

- The name of the storage server (`Server Name`). The storage server name here must be the same as the storage server name used in the **Storage Server Configuration Wizard**.
- The name of the volume (`LSU Name`).
- The properties of the volume (`Media, Save As`).
- The replication sources of the volume (`Replication Sources`).
- The replication targets of the volume (`Replication Targets`).

Save the output to a file so that you can compare the current topology with the previous topology to determine what has changed.

NetApp storage server sample bpstsinfo output

The following examples show sample output from the `bpstsinfo` command for a NetApp storage server named `plinko` which contains four LSUs. The generic syntax for the command is as follows:

```
bpstsinfo -lsuinfo -storage_server storage_server_name -stype
storage_type
```

The following is an example of the command, run on the NetBackup media server, for storage server `plinko`:

```
bpstsinfo -lsuinfo -storage_server plinko -stype Network_NTAP
```

Output for first LSU:

LSU Info:

```
Server Name: Network_NTAP:plinko
LSU Name: PrimarySnapshot
Allocation : STS_LSU_AT_STATIC
Storage: STS_LSU_ST_NONE
Description:
Configuration:
Media: (STS_LSUF_REP_ENABLED | STS_LSUF_REP_SOURCE)
Save As : (STS_SA_PRIMARY | STS_SA_SNAPSHOT)
Replication Sources: 0 ( )
Replication Targets: 3 ( Network_NTAP:plinko:Netapp3140a2_SnapVault
Network_NTAP:plinko:Netapp3140a2_SnapMirror
Network_NTAP:plinko:Netapp3140a2_SecondSnapMirror )
```

.
.
.

The `bpstsinfo` output provides the following information about the volume:

Storage server name (Server Name).	plinko	The name preceding the server name is the storage server type. For example, <code>Network_NTAP</code> .
Volume name (LSU Name).	PrimarySnapshot	
Volume properties (Media, Save As).	The volume has the following properties: ■ Primary ■ Snapshot ■ Replication Source	
Replication sources of the volume (Replication Sources).	The volume has no replication sources. It cannot receive replication from any other volume.	
Replication targets of the volume (Replication Targets).	The volume has three replication targets. It can replicate to the following volumes: ■ Netapp3140a2_SnapVault ■ Netapp3140a2_SnapMirror ■ Netapp3140a2_SecondSnapMirror	

Output for second LSU:

```
LSU Info:
  Server Name: Network_NTAP:plinko
  LSU Name: Netapp3140a2_SnapVault
  Allocation : STS_LSU_AT_STATIC
  Storage: STS_LSU_ST_NONE
  Description:
  Configuration:
  Media: (STS_LSUF_REP_ENABLED | STS_LSUF_REP_SOURCE |
         STS_LSUF_REP_TARGET | STS_LSUF_MIRROR_FLEXIBLE)
  Save As : (STS_SA_SNAPSHOT | STS_SA_MIRROR)
  Replication Sources: 3 ( Network_NTAP:plinko:PrimarySnapshot
  Network_NTAP:plinko:Netapp3140a2_SnapMirror
  Network_NTAP:plinko:Netapp3140a2_SecondSnapMirror )
  Replication Targets: 2 ( Network_NTAP:plinko:Netapp3140a2_SnapMirror
  Network_NTAP:plinko:Netapp3140a2_SecondSnapMirror )
  .
```

.

The `bpstsinfo` output provides the following information about the volume:

Storage server name (Server Name).	plinko
	The name preceding the server name is the storage server type.
Volume name (LSU Name).	Netapp3140a2_SnapVault
Volume properties (Media, Save As).	The volume has the following properties: ■ Snapshot ■ ReplicationSource ■ ReplicationTarget ■ Mirror ■ MirrorFlexible Since the LSU is MirrorFlexible, it can be configured as Mirror-capable or not Mirror-capable as specified by the user.
Replication sources of the volume (Replication Sources).	The volume has three replication sources. It can receive replications from the following three volumes: ■ PrimarySnapshot ■ Netapp3140a2_SnapMirror ■ Netapp3140a2_SecondSnapMirror
Replication targets of the volume (Replication Targets).	The volume has two replication targets. It can replicate to the following two volumes: ■ Netapp3140a2_SnapMirror ■ Netapp3140a2_SecondSnapMirror

Output for third LSU:

```
LSU Info:
  Server Name: Network_NTAP:plinko
  LSU Name: Netapp3140a2_SnapMirror
  Allocation : STS_LSU_AT_STATIC
  Storage: STS_LSU_ST_NONE
  Description:
  Configuration:
  Media: (STS_LSUF_REP_ENABLED | STS_LSUF_REP_SOURCE |
        STS_LSUF_REP_TARGET | STS_LSUF_MIRROR_FLEXIBLE)
```

```
Save As : (STS_SA_SNAPSHOT | STS_SA_MIRROR)
Replication Sources: 3 ( Network_NTAP:plinko:PrimarySnapshot
Network_NTAP:plinko:Netapp3140a2_SnapVault
Network_NTAP:plinko:Netapp3140a2_SecondSnapMirror )
Replication Targets: 2 ( Network_NTAP:plinko:Netapp3140a2_SnapVault
Network_NTAP:plinko:Netapp3140a2_SecondSnapMirror )
.
.
.
```

Output for fourth LSU:

```
LSU Info:
Server Name: Network_NTAP:plinko
LSU Name: Netapp3140a2_SecondSnapMirror
Allocation : STS_LSU_AT_STATIC
Storage: STS_LSU_ST_NONE
Description:
Configuration:
Media: (STS_LSUF_REP_ENABLED | STS_LSUF_REP_SOURCE |
      STS_LSUF_REP_TARGET | STS_LSUF_MIRROR_FLEXIBLE)
Save As : (STS_SA_SNAPSHOT | STS_SA_MIRROR)
Replication Sources: 3 ( Network_NTAP:plinko:PrimarySnapshot
Network_NTAP:plinko:Netapp3140a2_SnapVault
Network_NTAP:plinko:Netapp3140a2_SnapMirror )
Replication Targets: 2 ( Network_NTAP:plinko:Netapp3140a2_SnapVault
Network_NTAP:plinko:Netapp3140a2_SnapMirror )
.
.
.
```

Configuring storage units and storage unit groups for snapshots and snapshot replication

This chapter includes the following topics:

- [Creating storage units for a Replication Director configuration](#)
- [Creating storage unit groups for snapshots](#)

Creating storage units for a Replication Director configuration

A storage unit is a label that NetBackup associates with physical storage. For snapshots and snapshot replication, a storage unit is configured to contain one snapshot disk pool.

Storage unit creation is part of several other wizards. However, a storage unit can be created directly from the **Storage** utility in the **NetBackup Administration Console**.

To create a storage unit for snapshots or snapshot replication

- 1 In the **NetBackup Administration Console**, select the **Storage** utility.
- 2 Select **Actions > New > New Storage Unit**.

3 Enter a **Storage unit name**.

See “[NetBackup naming conventions](#)” on page 15.

4 Select the **Storage unit type**. For snapshots and snapshot replication, select **Disk**.

5 Select a **Disk type**.

The **Disk type** identifies the type of storage unit. To configure snapshots and snapshot replication, select **OpenStorage (Vendor name)**.

6 A storage unit can contain either snapshot images or non-snapshot backup images, but it cannot contain both. In the **Storage unit configured for** drop-down list, indicate what the storage unit is to contain:

- **Backup storage unit**

Upon selection, only those disk pools that can contain non-snapshot backups are displayed in the dialog box.

- **Snapshot storage unit**

To configure snapshots and snapshot replication, select **Snapshot**.

Upon selection, only those disk pools that can contain snapshots are displayed in the dialog box. Once a storage unit contains snapshots, it cannot contain non-snapshot backups.

7 Specify the properties that are required for the storage unit. Selecting a property filters the disk pools and displays only those that have the property selected.

For example, select **Replication source** and **Replication target** to display the disk pools that are configured to be both replication sources and targets for other replications. If no properties are selected, all disk pools appear.

(If you already know the name of the disk pool that has the properties that you want, select the disk pool from the **Select disk pool** drop-down menu. In that case, no filtering is necessary.)

8 In the **Select disk pool** drop-down list, select the disk pool that this storage unit is to contain. A storage unit can contain only one disk pool.

Click **View Properties** to display the properties of the selected disk pool.

- 9 Select the media server(s) that can use the storage unit.

Use any available media server to transport data

NetBackup selects any media server to access the storage unit.

Use only the following media servers

NetBackup uses only the media server(s) that are specified to access the storage unit.

Only the media servers that have the OpenStorage plug-in installed appear in this list. For a media server to communicate with and have access to a storage server, it must be added to the Replication Director environment.

See [“Adding the storage server credentials to a NetBackup server”](#) on page 24.

Note: A storage unit can represent many physical devices. When a storage unit is a replication target, NetBackup lets the plug-in select which device to use within the storage unit. For replication jobs, storage units and storage unit groups ignore the **Maximum concurrent jobs** setting. NetBackup does not attempt to throttle the parameters.

- 10 Click **OK** to save the storage unit configuration.

Creating storage unit groups for snapshots

Creating storage unit groups is optional. A snapshot storage unit group must be comprised of storage units that have matching properties.

The following procedure describes how to create a storage unit group that consists of the storage units that can contain snapshots.

To create a snapshot storage unit group

- 1 In the **NetBackup Administration Console**, expand **NetBackup Management > Storage**.
- 2 Right-click **Storage Unit Groups** and select **New Storage Unit Group**.
- 3 Enter a storage unit group name for the new storage unit group. The storage unit group name is case-sensitive.

See [“NetBackup naming conventions”](#) on page 15.

- 4 For the storage unit group to contain snapshots, select **Snapshot** in the drop-down menu.

- 5 A storage unit group can contain only those storage units that share similar properties. NetBackup filters the storage units for selection so that dissimilar storage units are not combined in one storage unit group.

Note: The properties of the underlying storage units are read-only. You cannot change the storage unit properties from this dialog box.

Select one or more properties to filter the storage units in the list. Only those storage units that have the selected properties are displayed. For example, select **Replication source** and **Replication target** to display only those storage units that are configured to act as both replication sources and replication targets.

Filter the storage units on the following properties:

- **Primary**
Enable **Primary** to display the storage units that can contain the initial snapshot of primary data.
 - **Replication source**
Enable **Replication source** to display the storage units that can serve as a source for a replicated snapshot.
 - **Replication target**
Enable **Replication target** to display the storage units that can receive replicated snapshots from a replication source.
 - **Mirror**
Optionally, enable **Mirror** to display the storage units that can serve as a mirrored replication target. (For example, NetApp SnapMirror.)
 - **Independent**
Optionally, enable **Independent** to display the storage units that can act as either a **Mirror** replication target (SnapMirror) or a non-mirror replication target (SnapVault).
- 6 Add or remove storage units from the group:
- To add storage units to the group, select the storage units from the **Available storage units** list and click **Add**.
 - To remove storage units from the group, select the storage units from the **Storage units to be used in the group** list and click **Remove**.

- To change the priority of a storage unit, select the storage unit and click **Move Up** or **Move Down**. The units at the top of the list have the highest priority in the group.

7 Click **OK** to save and close the dialog box.

Figure 5-1 Snapshot storage unit group configuration dialog box

New Storage Unit Group

Storage unit group name:
Mirror_STU_G

Storage unit group configured for: Snapshot

A storage unit group inherits the properties of its storage units. Only storage units with similar properties can be added to a storage unit group. If properties are specified, the list displays storage units that match the selected properties.

☐ Primary
☒ Replication source
☒ Replication target
☒ Mirror
☒ Independent

Available storage units

Storage Unit Name	Replication	Primary

Storage units to be used in the group

Storage Unit Name	Replication	Primary
Wren.2.1.1.1*_meta...	Source, Target Mirror...	No

Change Priority: Move Up Move Down

OK Cancel Help

Configuring storage lifecycle policies for snapshots and snapshot replication

This chapter includes the following topics:

- [About configuring storage lifecycle policies for snapshots and snapshot replication](#)
- [Creating a storage lifecycle policy for snapshots and snapshot replication](#)
- [Operation types in a storage lifecycle policy](#)
- [Retention types for storage lifecycle policy operations](#)

About configuring storage lifecycle policies for snapshots and snapshot replication

A storage lifecycle policy (SLP) contains instructions in the form of storage operations, to be applied to the data. Operations are added to the SLP that determine how the data is stored and copied or replicated. For example, the NetBackup administrator creates an operation that determines where the data exists as a snapshot, as a replication, or as a duplication. The administrator also determines the retention of the data at each storage unit or storage unit group.

Storage operations that are defined in the SLP use storage units that represent disk pools. An SLP that is configured for snapshots or snapshot replication must contain a specific, hierarchical combination of operations.

The following figure represents an SLP for a replication scenario. In the example, the following operations are used:

- A **Snapshot** operation creates a snapshot.
- A **Replication** operation replicates the snapshot to another volume.
- A **Backup From Snapshot** operation creates a tar-formatted backup from the snapshot.
- A **Duplication** operation copies the backup to tape.

Table 6-1 describes the four types of operations that are required in this example replication scenario.

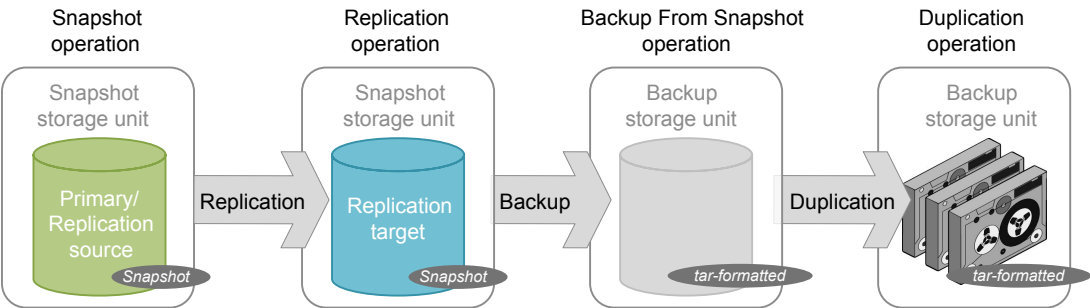


Table 6-1 Example of a storage lifecycle policy configured for snapshots and snapshot replication

Operation order in SLP	Operation	Description
1	Snapshot	Operation 1 creates a snapshot in the primary storage. The snapshot serves as the source for the other operations in the SLP. ■ The operation must be a Snapshot operation. ■ The storage must be a snapshot storage unit that has the following properties set: Primary and Replication source. Note: Only one operation to a Primary storage unit is permitted in an SLP.

Table 6-1 Example of a storage lifecycle policy configured for snapshots and snapshot replication (*continued*)

Operation order in SLP	Operation	Description
2 (Child to operation 1)	Replication	Operation 2 replicates the snapshot that the first operation created. ■ The operation must be a Replication operation and it must be the replication partner to the source storage unit. ■ The retention type determines what replication method is used. For example, if retention type Fixed or Expire after copy is selected for a NetApp storage system, the SnapVault replication method is used. ■ The storage must be a snapshot storage unit that has the Replication target property set. Since no other replica is created from this operation in this example, it does not need to have the Replication source property set.
3 (Child to operation 2)	Backup From Snapshot	Operation 3 creates a tar-formatted backup copy of the snapshot. ■ The operation must be a Backup From Snapshot operation. This operation creates a backup image from the snapshot. ■ The storage must be a backup storage unit.
4 (Child to operation 3)	Duplication	Operation 4 makes a duplicate copy from the tar-formatted backup copy. In this example, the copy is duplicated to tape media. ■ The operation must be a Duplication operation. This operation creates a backup copy of the tar-formatted image. ■ The storage must be a backup storage unit.

After the SLP is configured for different operations, the NetBackup administrator configures a backup policy that points to the snapshot SLP.

The **SLP Parameters** host properties in the **NetBackup Administration Console** allow administrators to customize how SLPs are maintained and how SLP jobs run.

Best-practice information about SLPs appears in the following document:

<http://www.veritas.com/docs/TECH208536>

Creating a storage lifecycle policy for snapshots and snapshot replication

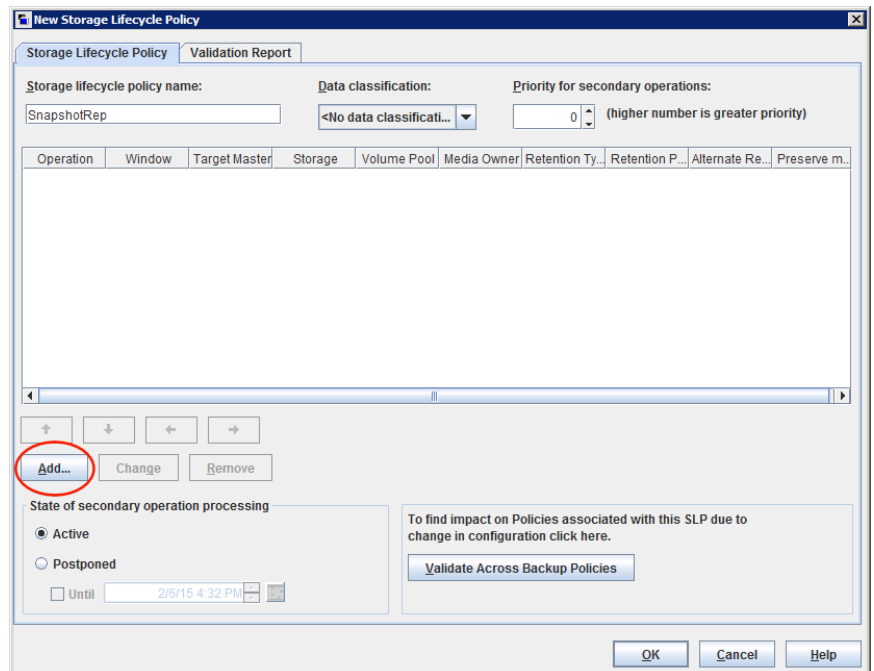
Use the following procedure to configure a storage lifecycle policy that creates snapshots and snapshot replications with Replication Director. Only those options that are necessary to configure an SLP for Replication Director are listed.

To configure a storage lifecycle policy to create snapshots and snapshot replication

- 1** In the **NetBackup Administration Console**, expand **NetBackup Management**, and then expand **Storage**. Select **Storage Lifecycle Policies**.
- 2** Click **Actions > New > Storage Lifecycle Policy**.
- 3** In the **New Storage Lifecycle Policy** dialog box, enter a **Storage lifecycle policy name**.

See [“NetBackup naming conventions”](#) on page 15.

- 4** Click **Add** to add operations to the SLP. The operations are the instructions for the SLP to follow and apply to the data that is specified in the backup policy.



- 5** In the **Properties** tab of the **New Storage Operation** dialog box, select **Snapshot** from the **Operation** drop-down menu.

This **Snapshot** operation creates a snapshot of the primary data and serves as the source for other operations in the SLP. For example:

- A **Replication** operation.

See [“Replication operation in an SLP”](#) on page 59.

- A **Backup From Snapshot** operation.
 See “[Backup From Snapshot operation in an SLP](#)” on page 68.
 - An **Index From Snapshot** operation.
 See “[Index From Snapshot operation in an SLP](#)” on page 61.
- 6 In the **Storage unit** drop-down menu, select a storage unit. NetBackup displays only those storage units that are configured to contain primary snapshots.
 - 7 Select the **Retention type** and the **Retention period** for the data in this storage unit. The **Retention period** option does not appear for all **Retention type** selections. Click **OK**.
 - 8 To replicate the primary snapshot, create a **Replication** operation that is based on the **Snapshot** operation. Click on the **Snapshot** operation and then select **Add**. The **New Storage Operation** dialog box appears.
 - 9 In the **Operation** drop-down menu, select **Replication**.
 - 10 Under **Storage**, select a **Storage unit** that is configured to contain replicated snapshots. NetBackup displays only those storage units that can act as target destinations.
 - 11 Select the **Retention type** and the **Retention period** for the data in this storage unit.

 A **Mirror** retention indicates that the NetApp volume SnapMirror method is to be used for the replication method. If a non-mirror retention type is selected, the NetApp SnapVault replication method is used.

 Optionally, indicate an **Alternate read server** that is allowed to read a snapshot that was originally written by a different media server. Click **OK**.
 - 12 The **Window** tab displays for the following operation types: **Backup From Snapshot**, **Duplication**, **Import**, **Index From Snapshot**, and **Replication**.

 Create a window during which secondary operations can run.
 - 13 Click **OK** to create the storage operation.

Continue to create operations, depending on the needs of your environment.

To cascade storage operations in the SLP, make sure to select the correct parent operation as the source for the child operation. If the correct operation is not selected, you unintentionally perform an operation on an incorrect source.

Operation types in a storage lifecycle policy

The **Operation** selections are the instructions in the storage lifecycle policy. The following topics describe the purpose of each operation.

- See “[Snapshot operation in an SLP](#)” on page 55.
 - See “[Replication operation in an SLP](#)” on page 59.
 - See “[Index From Snapshot operation in an SLP](#)” on page 61.
 - **Backup** operation. When a **Backup** operation appears in an SLP, it must be the first operation. In an SLP that is configured for Replication Director, the first operation must be a **Snapshot** operation. Since this guide concentrates on Replication Director, the **Backup** operation is not described here.
 - See “[Backup From Snapshot operation in an SLP](#)” on page 68.
 - See “[Duplication operation in an SLP](#)” on page 70.
 - **Import** operation. An **Import** operation is used in Auto Image Replication, in which an SLP is used to import a backup into a target NetBackup domain. Auto Image Replication does not apply to Replication Director in this release so the **Import** operation is not described here.
- All operations are described in the [NetBackup Administrator's Guide, Volume I](#) or the online Help in the **NetBackup Administration Console**.

Snapshot operation in an SLP

A **Snapshot** operation creates a point-in-time, read-only, disk-based copy of data. NetBackup provides several types of snapshots, depending on the device where the snapshot occurs.

Use a **Snapshot** operation as the first operation in a storage lifecycle policy for a NetBackup Replication Director configuration.

Figure 6-1 Snapshot operation in the New Storage Operation dialog box

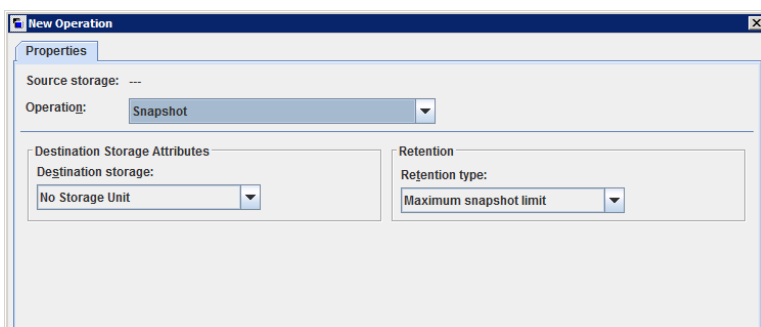


Table 6-2 Snapshot operation characteristics

Characteristic	Description
Storage unit selection	The following topics describe the types of snapshot storage units that can be used as the storage for a snapshot operation: ■ See “Primary snapshot storage unit” on page 57. ■ See “Primary + Replication source snapshot storage unit” on page 57. ■ See “Replication source + Replication target snapshot storage unit” on page 58. ■ See “Replication target snapshot storage unit” on page 58. ■ See “Replication source + Replication target + Mirror snapshot storage unit” on page 59. ■ See “Replication source + Replication target + Mirror snapshot storage unit” on page 59. A Storage unit selection is necessary in the following situations: ■ If the Snapshot is to be used by a subsequent Replication operation. The storage unit that is specified for the Snapshot operation must be a snapshot-capable storage unit that represents the primary storage. ■ If the SLP contains only one operation and that is a Snapshot operation, specify a storage unit. NetBackup uses that storage unit to determine which media server to use to launch the snapshot job. If neither situation applies to the SLP, the administrator may select No storage unit or may simply make no selection. NetBackup uses the storage unit that is selected for the Backup From Snapshot operation.
Child of	A Snapshot operation cannot serve as the child of any other operation. Therefore, do not click on any other operation in the SLP when adding a Snapshot operation. See “Creating a storage lifecycle policy for snapshots and snapshot replication” on page 52.
Source for	A Snapshot operation can be the source for the following operations: ■ Backup From Snapshot ■ Index From Snapshot ■ Replication operation
Hierarchy notes	If a Snapshot operation appears in an SLP, it must be first in the operations list.
Job type	A Snapshot operation generates a Snapshot job in the Activity Monitor.
Window	Snapshot operations do not offer the option to create an SLP window.

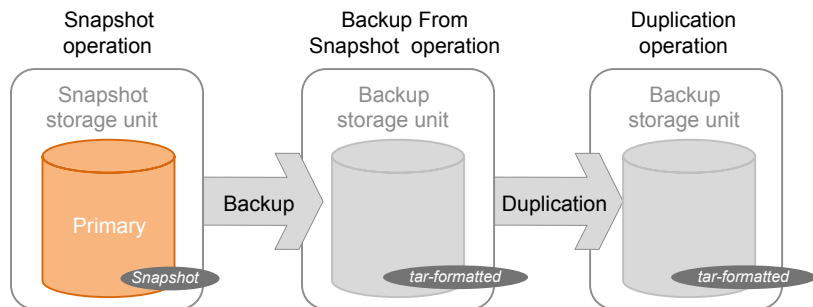
See [“About configuring storage lifecycle policies for snapshots and snapshot replication”](#) on page 50.

Primary snapshot storage unit

A snapshot operation can use a **Primary** snapshot storage unit. That is, the storage unit represents a disk pool that contains the volumes that have only the **Primary** property set.

[Figure 6-2](#) shows an SLP that contains one primary-only **Snapshot** operation, one **Backup From Snapshot** operation, and one **Duplication** operation. The **Backup From Snapshot** operation is used to create a backup from the snapshot on the primary-only **Snapshot** operation. After the backup is created, it is duplicated to a **Duplication** operation.

Figure 6-2 SLP that contains a Snapshot operation, a Backup From Snapshot operation, and a Duplication operation

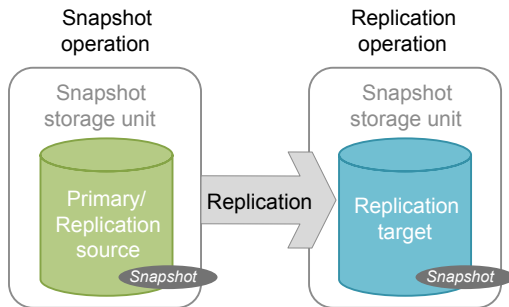


Primary + Replication source snapshot storage unit

An SLP operation can use a **Primary + Replication source** snapshot storage unit. That is, the storage unit represents a disk pool that contains volumes that have both the **Primary** property and the **Replication source** property set.

[Figure 6-3](#) shows an SLP that contains a **Primary + Replication source** snapshot storage unit as one operation and one **Replication target** snapshot storage unit as another operation. The **Primary + Replication source** storage unit can replicate to the **Replication target** storage unit.

Figure 6-3 SLP that contains a Snapshot operation and a Replication operation

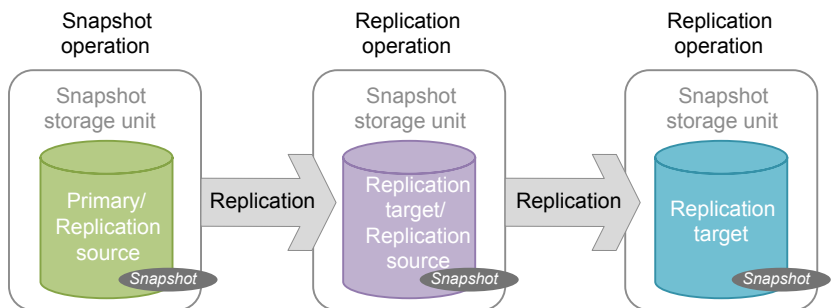


Replication source + Replication target snapshot storage unit

An SLP operation can use a snapshot storage unit that represents a disk pool that contains volumes that have the following properties: **Replication source** and **Replication target**.

A snapshot storage unit with these properties can serve as both the **Replication source** for another operation in the SLP, and as the **Replication target** for another operation in the SLP.

Figure 6-4 SLP that contains a Snapshot operation and two Replication operations

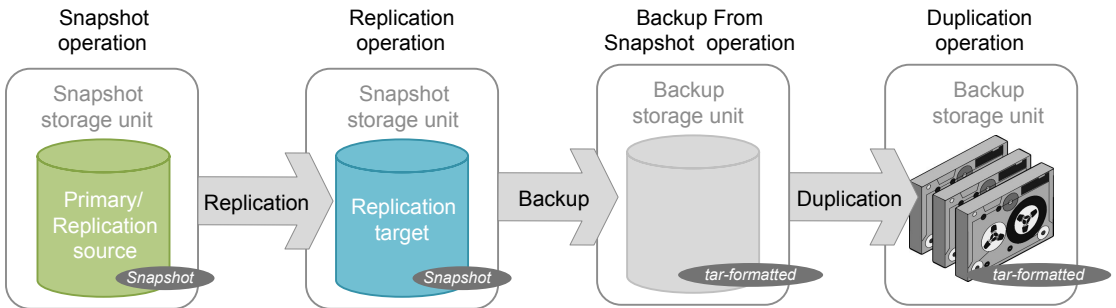


Replication target snapshot storage unit

An SLP operation can use a snapshot storage unit that represents a disk pool that contains volumes that have only the **Replication target** property set.

An operation with this property can serve only as a **Replication target** for another operation in the SLP. It cannot serve as source for a replica, but it can serve as the source for a **Duplication** operation.

Figure 6-5 SLP that contains a Snapshot operation, a Replication operation, a Backup From Snapshot operation, and a Duplication operation



Replication source + Replication target + Mirror snapshot storage unit

An SLP can use a snapshot storage unit that represents a disk pool that contains volumes that have the following properties: **Replication source**, **Replication target**, and **Mirror**.

An operation with these properties can serve as both:

- A **Replication source** in a cascading configuration.
- A mirrored **Replication target** in a cascading configuration. A mirrored **Replication target** must have a forced **Mirror** retention type.

Replication target + Mirror snapshot storage unit

An SLP can use a snapshot storage unit that represented a disk pool that contains volumes that have the following properties: **Replication target** and **Mirror**.

A mirrored **Replication target** must have a forced **Mirror** retention type.

Replication operation in an SLP

Use the **Replication** operation for the following types of replication:

- NetBackup Replication Director to replicate a snapshot, as shown in [Figure 6-6](#). See [“About NetBackup Replication Director”](#) on page 8.
- NetBackup Auto Image Replication to replicate a backup, as shown in [Figure 6-7](#).

Table 6-3 Replication operation characteristics

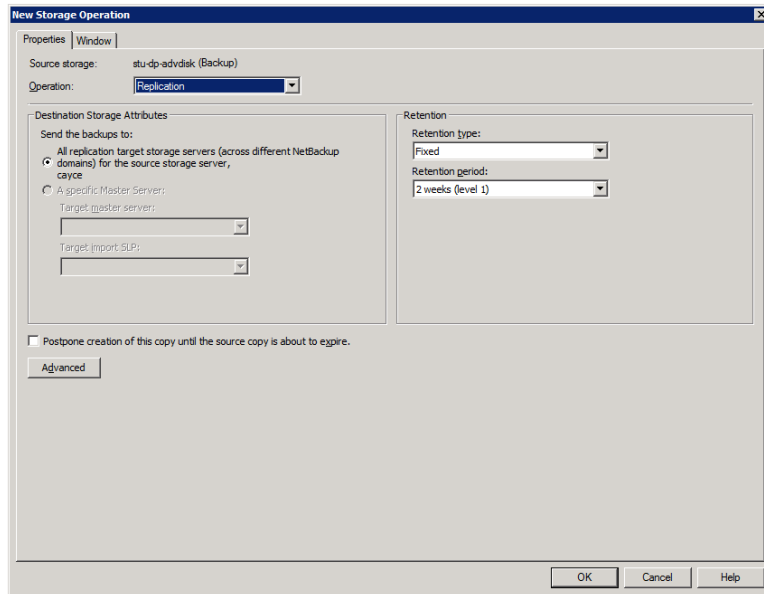
Characteristic	Description
Storage unit selection	Under Destination storage attributes : For Replication Director, select the Storage that is configured to contain replicated snapshots.
Child of	Click on the appropriate operation when adding a Replication operation. Using Replication Director, a Replication operation can be the child of a Snapshot operation or the child of another Replication operation. See “Creating a storage lifecycle policy for snapshots and snapshot replication” on page 52.
Source for	A Replication operation can be the source for the following operations: ■ Replication ■ Backup From Snapshot See “Backup From Snapshot operation in an SLP” on page 68.
Job type	A Replication operation generates a Replication job in the Activity Monitor .
Window	An SLP window can be created for a Replication operation.

Figure 6-6 Replication operation following a Snapshot operation

The screenshot shows the 'Change Storage Operation' dialog box with the following configuration:

- Properties** tab selected.
- Source storage:** wrendvm21_primary_stu (Snapshot)
- Operation:** Replication
- Destination Storage Attributes:**
 - Storage:** wrendvm21_vault_stu
- Retention:**
 - Retention type:** Fixed
 - Retention period:** 2 weeks (level 1)
- ☐ Postpone creation of this copy until the source copy is about to expire.
- Advanced** button.
- OK**, **Cancel**, and **Help** buttons at the bottom right.

Figure 6-7 Replication operation following a Backup operation



Index From Snapshot operation in an SLP

The **Index From Snapshot** operation indexes the contents of existing snapshots. When NetBackup indexes a snapshot, it creates an image catalog file in the NetBackup catalog for each snapshot. The presence of an image catalog file assists the user when a file needs to be restored from the snapshot, as described in [Table 6-4](#).

The **Backup From Snapshot** operation also creates an image catalog file. An **Index from Snapshot** may not be required if a **Backup From Snapshot** occurs frequently enough for the restore needs in your environment. For example, if the **Backup From Snapshot** runs once per week but file restores are required daily, consider using the **Index from Snapshot**.

The actual restore of the snapshot requires that the snapshot be mounted, regardless of whether an **Index from Snapshot** has been performed or not.

Table 6-4 Restore operations

Type of restore	Where performed	Description	Requirements
Live browse restore	- NetBackup Backup, Archive, and Restore interface - NetBackup OpsCenter Console	The user navigates the directory structure to locate and select the files for restore.	No image catalog file needs to be present in the NetBackup catalog. During a live browse restore, NetBackup automatically mounts the snapshot so that the user can see what files it contains. Mounting and unmounting the snapshot can be time-consuming. If an image catalog file is present, NetBackup does not mount the snapshot.
Search for restore (Also referred to as a Simplified File Restore or an Operational Restore)	NetBackup OpsCenter Console	- The user can search for files based on partial file name. Knowing the name of the client or of the policy that created the backup is not necessary. - Offers several filters to narrow search. - Search results display all the recovery points available to the user for both backups and snapshots.	The image catalog file must be present in the NetBackup catalog.

Table 6-5 Index From Snapshot operation characteristics

Characteristic	Description
Storage unit selection	The Index From Snapshot operation does not write data to a storage unit. However, a storage unit selection is needed to select the media server that to be used to access the snapshot. As a best practice, use the storage unit from the Snapshot or Replication operation that is the source for this operation.
Child of	When an Index From Snapshot operation appears in an SLP, it must be the child of a Snapshot or Replication operation. Therefore, click on either a Snapshot or a Replication operation in the SLP when adding an Index From Snapshot operation. See “Creating a storage lifecycle policy for snapshots and snapshot replication” on page 52.
Source for	While an Index From Snapshot operation cannot be the source for any operation, a Replication operation can follow it.

Table 6-5 Index From Snapshot operation characteristics (*continued*)

Characteristic	Description
Hierarchy notes	The Index From Snapshot operation can consume system resources and requires that each snapshot be mounted to create the image catalog file. See “Determining where and when the Index From Snapshot operation occurs” on page 63.
Job type	An Index From Snapshot operation generates an Index From Snapshot job in the Activity Monitor .
Window	An SLP window can be created for an Index From Snapshot operation.

Consider the following items before using the **Index From Snapshot** operation:

- The **Index From Snapshot** operation is supported only in a Replication Director configuration.
- **Standard**, **MS-Windows**, **NDMP**, and **VMware** backup policy types support the use of storage lifecycle policies that contain the **Index From Snapshot** operation.

Note: However, a **Standard** or **MS-Windows** policy with **NDMP Data Mover** enabled is not supported.

- The **Index From Snapshot** operation can run from a full or an incremental schedule. The file entries that are added to the image catalog file for either schedule are the full set of files since all files can be restored from that snapshot. To do so allows for the most efficient restore, however, more space is consumed in the NetBackup catalog by the image catalog file.

Determining where and when the Index From Snapshot operation occurs

Including the **Index From Snapshot** operation requires some consideration as the operation can consume system resources and require additional time to perform. For example, to perform the operation can require that a snapshot be mounted or that NetBackup gather content details from the file system to populate the catalog.

To help mitigate the extra resource and time that the operation may take, the system administrator can control when and where the **Index From Snapshot** operation runs:

- Use the storage lifecycle policy **Window** tab to schedule when the **Index From Snapshot** operation can run. Schedule the operation to run when it is least likely to interfere with other jobs.

- Use the following points to determine where to position the **Index From Snapshot** operation in the SLP operations list:
 - Each NetBackup environment needs to determine where the operation works best in a specific SLP. To place the **Index From Snapshot** operation too early (toward the top of the operations list), may consume time when the restore capabilities are not needed. To place the operation toward the end of the operations list may cause the administrator to delay a restore until earlier snapshots or replications complete.
 - Use the **Index From Snapshot** operation in an SLP only once. A restore can be performed from any snapshot after one image .*if* file is created.
 - Any operations list that includes a **Backup From Snapshot** operation does not need an **Index From Snapshot** operation. The **Backup From Snapshot** operation creates an image .*if* file. The only exception is if the index is needed for restores before the **Backup From Snapshot** operation occurs.
 - An **Index From Snapshot** operation cannot have any dependents. An SLP cannot validate an **Index From Snapshot** operation with children. [Figure 6-8](#) shows an SLP with a valid configuration.
- [Figure 6-9](#) is also a valid configuration. A **Replication** operation follows the **Index From Snapshot** operation, but it is not indented. The **Replication** operation is a child of the **Snapshot** operation, not a child of the **Index From Snapshot** operation.
- To add a **Replication** operation after an **Index From Snapshot** operation, click on the **Snapshot** operation, and then click **Add**.

Figure 6-8 Example 1 of a valid placement of the Index From Snapshot operation

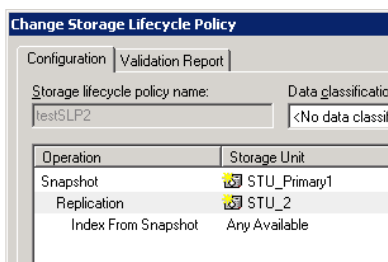
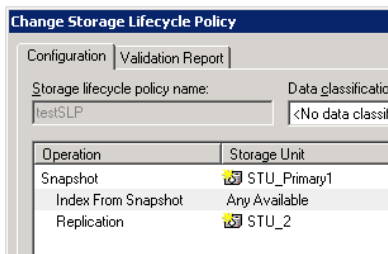


Figure 6-9 Example 2 of a valid placement of the Index From Snapshot operation



Pre-requisites for indexing for an NDMP policy

The following are pre-requisites to enable indexing for an NDMP policy:

- You must add a disk array host to NetBackup.
See [“Configuring indexing for an NDMP policy”](#) on page 66.
- Make sure that the Storage Virtual Machine (SVM) login account with the ontapi application is in the unlocked state.
Indexing jobs fail with error code 2113 if the account is in the locked state.

Note: Indexing NDMP policies is supported only for NetApp Clustered Data ONTAP configurations.

Indexing jobs fail with error code 2113 if the account is in the locked state.

Run the following command to check the account details and verify the status of the account, the Locked column shows ‘yes’ if the account is locked:

```
PUNBNRRDF_2240_01:> security login show -vserver Primary_VS_Auto_1
-user-or-group-name demo
```

The following is the output if the account is locked:

```
Vserver: Primary_SVM
User/Group Name  Application  Authentication  Role Name  Acct Locked
-----
demo             ontapi       password        vsadmin    yes
```

Run the following command on the cluster to unlock the account:

```
PUNBNRRDF_2240_01:> security login unlock -vserver Primary_VS_Auto_1
-username demo
```

Run the login command again to check the status, the 'Locked' column would show 'no' as shown in the output:

```
Vserver: Primary_SVM
User/Group Name  Application Method  Authentication  Role Name  Acct Locked
-----
demo            ontapi      password      vsadmin    no
```

After you unlock the account, you can proceed with the steps to configure indexing with an NDMP policy.

Note: The commands can change with the ONTAP version change. Please check your NetApp documentation for information about the latest commands.

Configuring indexing for an NDMP policy

For NDMP indexing, you must add a disk array host to NetBackup. The disk array host is the Storage Virtual Machine (SVM) that holds the snapshot or replica from which, the index would be generated. To connect to the SVM, you must use a logical interface (LIF) connection which has management access enabled.

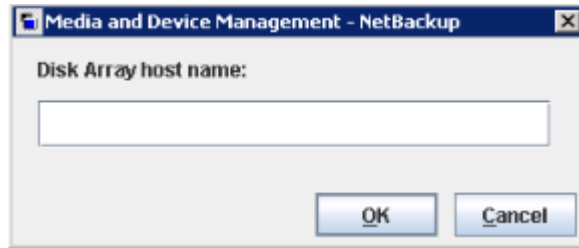
Note: Indexing NDMP policies is supported only for NetApp Clustered Data ONTAP configurations.

See [“About creating backup policies for Clustered Data ONTAP with Replication Director”](#) on page 140.

To configure indexing for an NDMP policy

- 1 On the NetBackup server NetBackup Administration Console, expand **Media and Device Management > Credentials > Disk Array Hosts**.
- 2 Under the Actions menu, select **New > New Disk Array Host**.
- 3 In the Media and Device Management – NetBackup dialog box, enter the name of the SVM that holds the snapshot or the replica copy that is to be used for indexing.

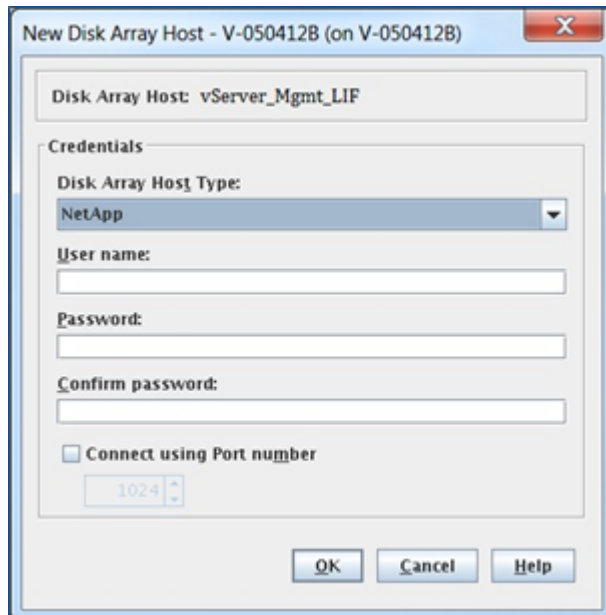
To connect to the SVM, you must use a logical interface (LIF) connection which has management access enabled.



- 4 Click **OK**.

The New Disk Array Host dialog box is displayed.

- 5 Select **NetApp** from the **Disk Array Host Type** drop-down list.



- 6 Enter the user name and password details and click **OK**.

The disk array credentials are the admin credentials of the NetApp SVM.

See ["Pre-requisites for indexing for an NDMP policy"](#) on page 65.

Note: The credentials that you provide for the SVM are not validated when you add the disk array host. Incorrect credentials can cause NDMP indexing job failure with error code 2113. Make sure that you provide the right disk array host credentials.

Backup From Snapshot operation in an SLP

Use the **Backup From Snapshot** operation to create a tar-formatted copy of the snapshot. The new copy is a backup copy. The process is sometimes referred to as a *snapdupe* job.

Figure 6-10 Backup From Snapshot operation in the New Storage Operation dialog box

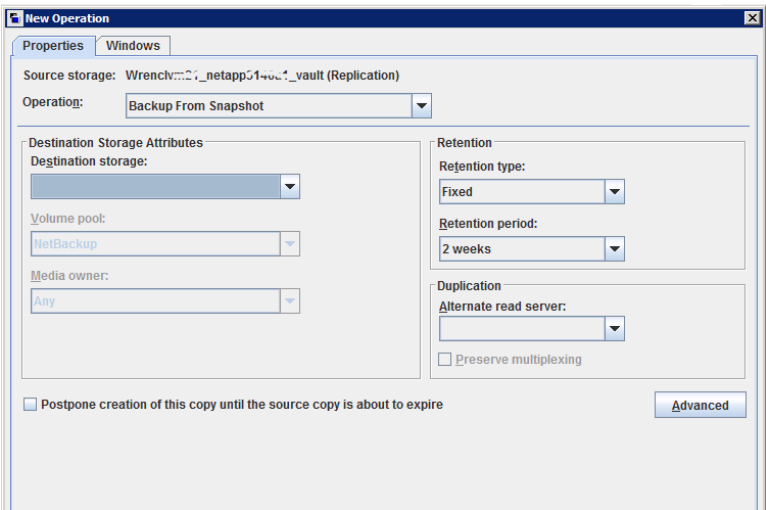


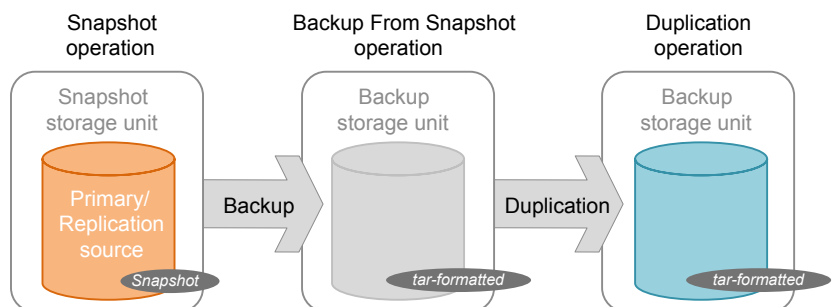
Table 6-6 Backup From Snapshot operation characteristics

Characteristic	Description
Storage unit selection	The selection must be a backup storage unit or a backup storage unit group. The selection cannot be a snapshot storage unit or a snapshot storage unit group.

Table 6-6 Backup From Snapshot operation characteristics (*continued*)

Characteristic	Description
Child of	A Backup From Snapshot operation must use a Snapshot operation as its source. Therefore, click on the Snapshot operation in the SLP when adding a Backup From Snapshot operation. See “Creating a storage lifecycle policy for snapshots and snapshot replication” on page 52.
Source for	A Backup From Snapshot operation can be the source for a Duplication operation. (See Figure 6-11.)
Hierarchy notes	An SLP may contain more than one Backup From Snapshot operation. If the first Backup From Snapshot operation fails with an unrecoverable error, NetBackup does not attempt the second one. Note: The SLP may contain only one Backup From Snapshot operation if the SLP is used by an NDMP policy (or a Standard or MS-Windows policy with NDMP Data Mover enabled).
Job type	A Backup From Snapshot operation generates a Backup job in the Activity Monitor. The Backup job that results from the Backup From Snapshot operation is under the control of the SLP Manager. If an SLP window is configured, the Backup job runs during the configured SLP window. If no SLP window is configured, the Backup job can run at any time; possibly outside of the backup window as configured in the backup policy. Users may experience a slight degradation in performance on the client or the client storage device while NetBackup accesses the snapshot.
Window	An SLP window can be created for a Backup From Snapshot operation.

Figure 6-11 SLP that contains a Backup From Snapshot operation



Duplication operation in an SLP

Use the **Duplication** operation to create a copy of a **Backup**, a **Backup from Snapshot**, or another **Duplication** operation. A media server performs the operation and writes the copy.

Note: Use the **Replication** operation to create a copy of a **Snapshot** operation. See [“Replication operation in an SLP”](#) on page 59.

Figure 6-12 Duplication operation in the New Storage Operation dialog box

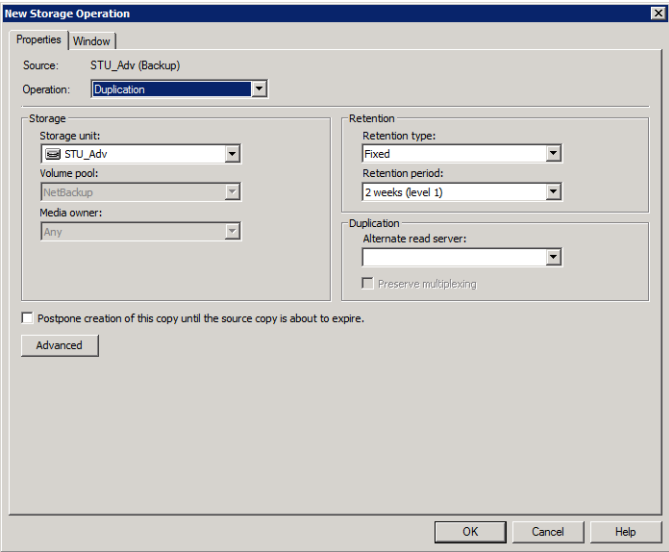


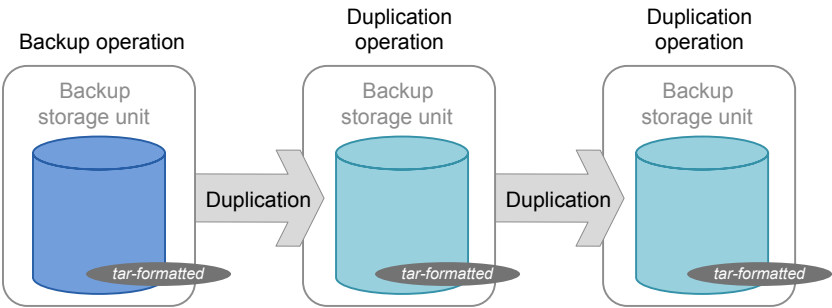
Table 6-7 Duplication operation characteristics

Characteristic	Description
Storage unit selection	The selection must be a backup storage unit or a backup storage unit group.
	The selection cannot be a snapshot storage unit or a snapshot storage unit group.

Table 6-7 Duplication operation characteristics (continued)

Characteristic	Description
Child of	A Duplication operation can be the child of the following operations: ■ Backup operation ■ Backup From Snapshot operation ■ A Duplication operation Therefore, click on one of these operations in the SLP when adding a Duplication operation. See “Creating a storage lifecycle policy for snapshots and snapshot replication” on page 52.
Source for	A Duplication operation can be the source for a Duplication operation. (See Figure 6-13.)
Hierarchy notes	When a Duplication operation appears in an SLP, it cannot be the first operation.
Job type	A Duplication operation generates a Duplication job in the Activity Monitor.
Window	An SLP window can be created for a Duplication operation.

Figure 6-13 SLP that contains one Backup operation and two Duplication operations



Retention types for storage lifecycle policy operations

The **Retention type** for an operation in a storage lifecycle policy determines how long the data is kept on that storage media.

Table 6-8 describes which retention types are valid selections for the various operations.

Table 6-8 Operation and retention type configurations

Retention type	Backup operation	Snapshot operation	Replication operation	Backup From Snapshot operation	Duplication operation
Fixed	Valid	Valid	Valid	Valid	Valid
Expire after copy	Valid	Valid	Valid	Valid	Valid
Maximum Snapshot limit	Invalid	Valid; SLP honors the policy setting.	Invalid	Invalid	Invalid
Mirror	Invalid	Invalid	Valid for snapshot storage only	Invalid	Valid for snapshot storage only
Target retention	Invalid	Invalid	Valid if the first operation in the SLP is an Import and if the storage is of the backup type.	Invalid	Valid if the first operation in the SLP is an Import.
Capacity managed	Valid; AdvancedDisk default; set on the storage server.	Invalid	Invalid	Invalid	Valid; AdvancedDisk default; set on the storage server.

Note: Retention is not associated with the **Index From Snapshot** operation because the operation does not create any copy.

Expire after copy retention type for SLP operations

The **Expire after copy** retention indicates that after all direct (child) copies of an image are successfully duplicated to other storage, the data on this storage is expired. The last operation in the SLP cannot use the **Expire after copy** retention type because no subsequent copy is configured. Therefore, an operation with this retention type must have a child.

Veritas recommends that you not enable **Expire after copy** retention for any storage units that are to be used with SLPs with either of the following: Accelerator or synthetic backups. The **Expire after copy** retention can cause images to expire while the backup runs. To synthesize a new full backup, the SLP backup needs the previous backup image. If the previous image expires during the backup, the backup fails.

Note: Although synthetic backups do support the use of storage lifecycle policies, SLPs cannot be used for the multiple copy synthetic backups method.

If a policy is configured to use an SLP for the backup, the retention that is indicated in the SLP is the value that is used. The **Retention** attribute in the schedule is not used.

An image copy with an **Expire after copy** retention is expired as soon as all of its direct child copies have been successfully created. Any mirrored children must also be eligible for expiration.

Fixed retention type for SLP operations

The **Fixed** retention indicates that the data on the storage is retained for the specified length of time, after which the backups or snapshots are expired.

An image copy with a **Fixed** retention is eligible for expiration when all of the following criteria are met:

- The **Fixed** retention period for the copy has expired.
- All child copies have been created.
- All child copies that are mirror copies are eligible for expiration.

The **Fixed** retention period is always marked from the original backup time of the image. For example, if a tape device is down, causing a 2-day delay in creating a duplicate tape copy, the expiration time of the duplicate copy is not different due to the 2-day delay. The expiration time of the duplicate copy is still x days from the time that the original backup was completed. It does not matter when the copy was created.

Maximum snapshot limit retention type for SLP operations

The **Maximum snapshot limit** determines the maximum number of snapshots that can be stored for a particular policy and client pair.

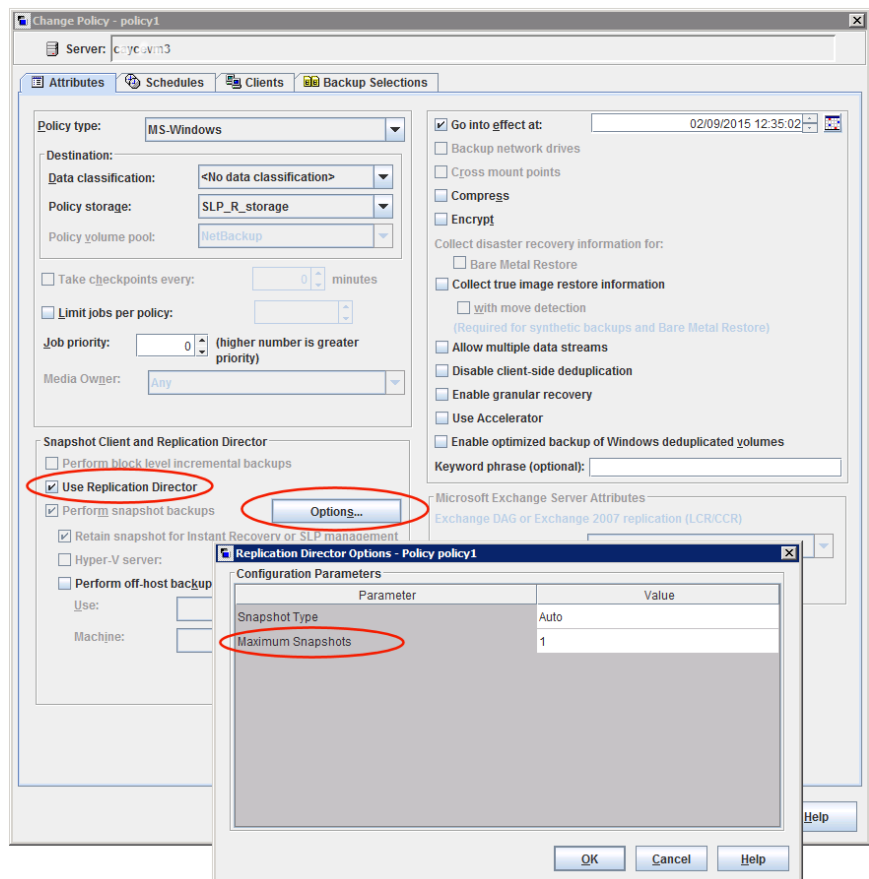
When the maximum is reached, the next snapshot causes the oldest job-complete snapshot to be deleted. A snapshot job is considered to be complete once all of its

configured dependent copies are complete. (Dependent copies are created as a result of **Backup From Snapshot**, **Index From Snapshot**, or **Replication** operations.) The practice is referred to as *rotation*. This retention type applies only to snapshots, and not to backups.

For example, Policy P1 contains two clients: C1 and C2. After the policy runs four times, it creates four snapshot images for C1 and four images for C2. If the **Maximum snapshot limit** is set to four, when the policy runs for the fifth time, NetBackup deletes the first snapshot that was created for both C1 and C2 to accommodate the fifth snapshot.

The **Maximum Snapshots** parameter in the **Replication Director Options** dialog box determines the maximum number of snapshots. To access the dialog box, click **Options** in the backup policy.

Figure 6-14 Replication Director Options dialog box



Mirror retention type for SLP operations

A mirror replica of a snapshot is eligible for expiration as soon as:

- All immediate child copies are successfully created.
- All immediate child copies that are mirrors are eligible for expiration.

The selection of the **Mirror** retention indicates that NetApp volume SnapMirror is to be used as the replication method. If any non-mirror retention type such as **Fixed** or **Expire after copy** is selected for the **Replication** operation, the NetApp SnapVault replication method is used.

In mirror replication, the replica copy is dependent on the existence of the source. (The source can be the original snapshot or another replica.) Therefore, the retention of the replica depends on the retention of the source. If the source is deleted, the mirror is automatically deleted.

In non-mirror replication, the replica is independent of the source and can have an independent retention. If the source is deleted, the non-mirror replica is not affected and can be used longer than the source. Or, if the replica is deleted first, it is not recreated and the source can be kept longer than the replica.

Target retention type for SLP operations

This setting is used in Auto Image Replication in an Import storage lifecycle policy. Every Import SLP must have at least one operation with a **Target retention**.

The **Target retention** is enforced at the target domain, but the actual retention for the data is specified by the administrator at the source domain.

Target retention indicates that the data at the target master shall use the expiration date that was imported with the image. The date is fixed because the copy must have a fixed retention.

Similar to the **Fixed** retention, an image copy with a **Target retention** retention is eligible for expiration when all of the following criteria are met:

- The **Fixed** retention period for the copy has expired.
- All child copies have been created.
- All child copies that are mirror copies are eligible for expiration.

Configuring backup policies for snapshots and snapshot replication

This chapter includes the following topics:

- [About configuring a backup policy for Replication Director](#)
- [Configuring an NDMP policy to protect a NAS host](#)
- [Configuring a Standard or MS-Windows policy to protect clients using NDMP with Data Mover](#)
- [Configuring a Standard or MS-Windows policy to protect NAS volumes or SAN-connected devices](#)
- [About NDMP support for Replication Director](#)

About configuring a backup policy for Replication Director

A backup policy must be configured and run in order to create and replicate snapshots as prescribed in a storage lifecycle policy.

See the following topics for more information about creating specific policy types:

- See [“About NDMP support for Replication Director”](#) on page 87.
Configure policies to use NDMP with Replication Director for creating snapshots of a NAS host without mounting the host, or of individual client data using CIFS or NFS.

- See [“Configuring a Standard or MS-Windows policy to protect NAS volumes or SAN-connected devices”](#) on page 84.
Configure policies that use Replication Director to create snapshots of NAS volumes.
- See [“About Oracle support for Replication Director”](#) on page 151.
Configure policies to create snapshots of the Oracle database and replicate the snapshots to other disk arrays.
- See [“About virtual machines and Replication Director”](#) on page 164.
Configure policies to protect virtual machines in a Replication Director environment.

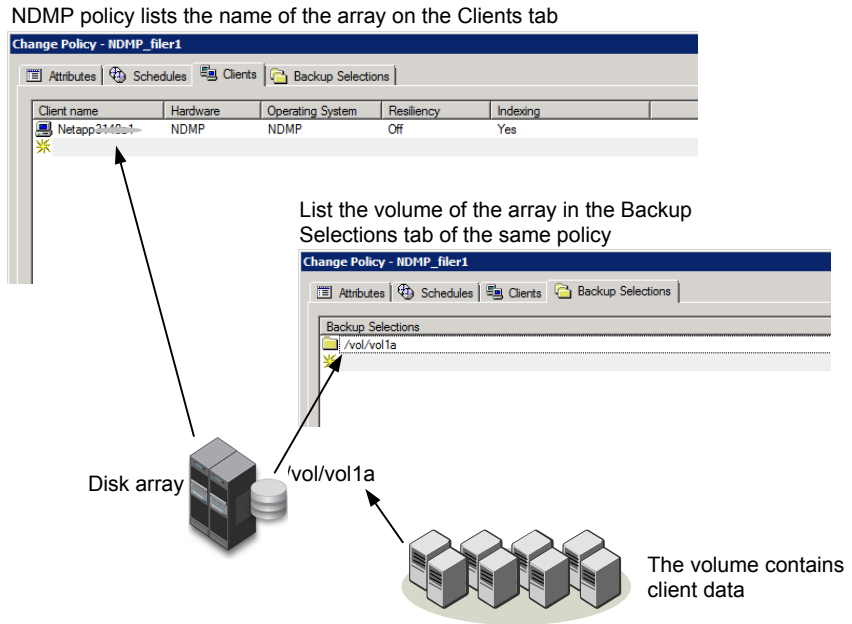
Configuring an NDMP policy to protect a NAS host

By creating a snapshot of a NAS host, NetBackup can protect the client data directly on the NAS host and avoid mounting each client.

[Figure 7-1](#) shows a disk array that many clients access to store data. Only the array name is listed in the **Clients** tab of the NetBackup policy, not individual production clients. The volume on the array that the clients use is listed in the **Backup Selections** tab of the policy.

Note: The figure below illustrates an example using NetApp Data ONTAP 7-mode.

Figure 7-1 Create a snapshot of the volume on the array to avoid mounting each client



The following procedure describes how to configure an **NDMP** backup policy to create a snapshot of a NAS host using NDMP with Replication Director.

To create an NDMP policy to use NDMP with Replication Director

- 1 Before NetBackup can perform NDMP backups:
 - Make sure that you've added the NDMP host credentials so NetBackup can access the NAS host.
 See [“Authorizing NetBackup access to a NAS \(NDMP\) host”](#) on page 89.
 - Make sure that NDMP is enabled on the NetApp storage by using the appropriate command. Refer to either of the following topics for more information:
 See [“Software required to use NetApp Data ONTAP 7-Mode with Replication Director”](#) on page 126.
 See [“Software required to use NetApp Clustered Data ONTAP with Replication Director”](#) on page 137.
- 2 In the **NetBackup Administration Console**, create a backup policy.
 Do not use the **Policy Configuration Wizard** to configure a policy for Replication Director.

3 Configure the options on the policy **Attributes** tab. The following items are specific to creating a policy for Replication Director:

- **Policy type:** Select **NDMP**.
- **Policy storage:** Select the SLP that you want to use that has been configured for snapshot replication.
 See [“Creating a storage lifecycle policy for snapshots and snapshot replication”](#) on page 52.
- **Use Replication Director:** Enable **Use Replication Director** to automatically select other options that Replication Director requires.
- Click the **Options** button to see the **Replication Director Options** dialog box and the default **Configuration Parameters** as follows:

- | | |
|----------------------|--|
| Snapshot Type | <ul style="list-style-type: none"> ■ 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.

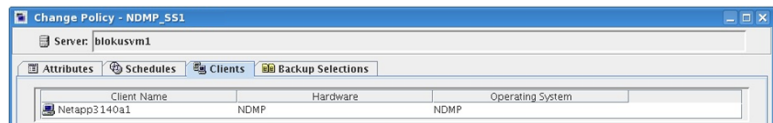
See [“Maximum snapshot limit retention type for SLP operations”](#) on page 73.

Managed by SLP retention is automatically selected if the **Fixed** or the **Expire after Copy** retention is currently selected in the SLP.

- 4 Select the **Schedules** tab and configure the schedules as you would for any other policy.
- 5 Select the **Clients** tab. Specify the name of the disk array (the NAS host) for 7-mode.

For Clustered Data ONTAP, specify the name of the SVM that will act as the NAS host.

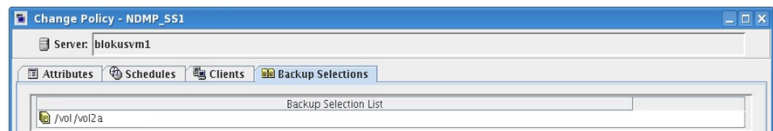
The following figure pertains to NetApp Data ONTAP 7-Mode and shows the name of a NetApp storage system in the **Clients** tab:



It may be helpful to refer to [Figure 7-1](#).

- 6 Select the **Backup Selections** tab to indicate the path to the volume on the disk array.

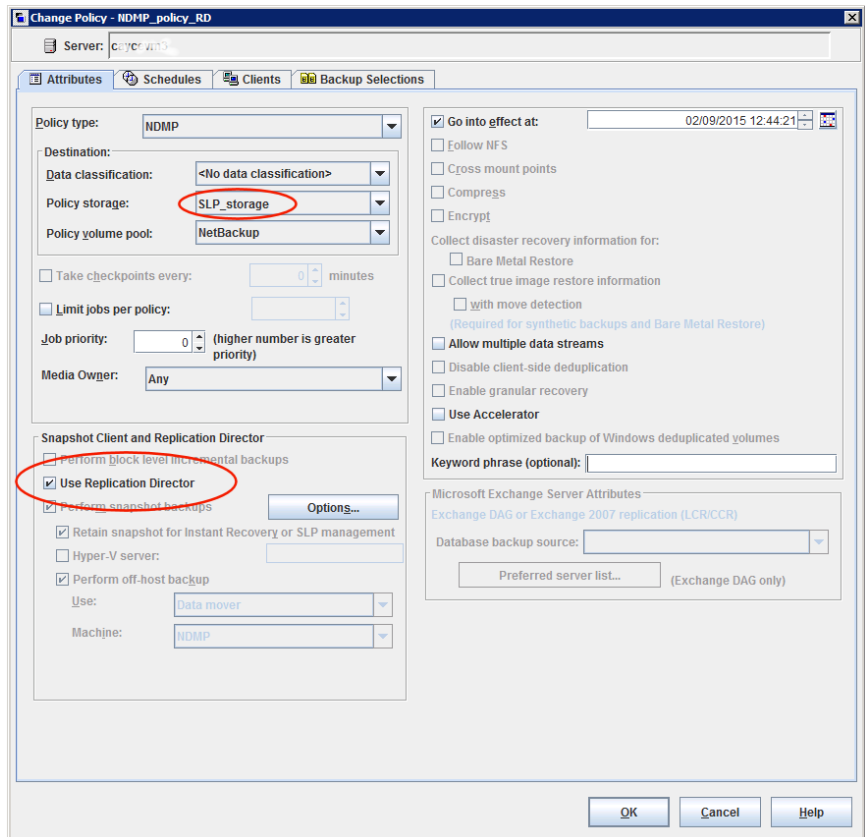
The following figure pertains to NetApp Data ONTAP 7-Mode and shows the **Backup Selections** tab and the volume that is to be backed up:



Note: Backup selections for both SAN devices and NAS volumes are not supported in a single backup policy.

- 7 When the policy configuration is complete, click **OK**.
- 8 NetBackup checks the policy to ensure that it can run successfully. Select **Complete** to perform the most comprehensive policy validation.

Figure 7-2 NDMP policy configuration to back up a NAS host



See the [NetBackup for NDMP Administrator's Guide](#) for more specific information about configuring NDMP policies.

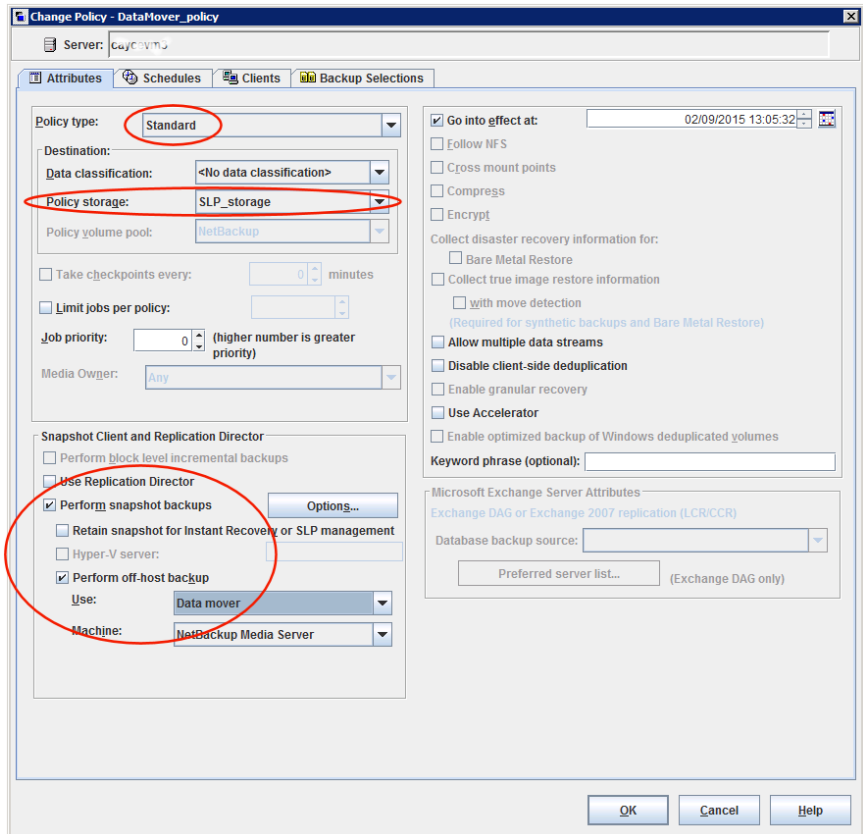
Only those policy options that are necessary to configure Replication Director are listed in the following procedure. For descriptions of all policy options, see the [NetBackup Administrator's Guide, Volume I](#) or the online Help.

Configuring a Standard or MS-Windows policy to protect clients using NDMP with Data Mover

The following procedure describes how to configure a **Standard** or **MS-Windows** backup policy to create Replication Director snapshots of NetBackup client data using NDMP with Data Mover.

This method requires that NetBackup mount each client to create the snapshot.

Figure 7-3 Example of a Standard policy configuration to use NDMP with Data Mover

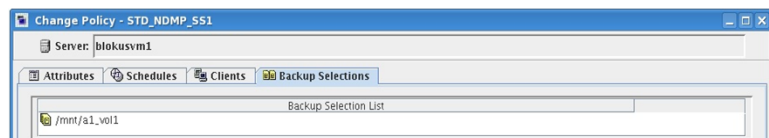


To create a Standard or MS-Windows policy to use NDMP with Data Mover

- 1 Before NetBackup can perform NDMP with Data Mover backups:
 - Make sure that you've added the NDMP host credentials so NetBackup can access the NAS host.
 See [“Authorizing NetBackup access to a NAS \(NDMP\) host”](#) on page 89.
 - Make sure that NDMP is enabled on the NetApp storage by using the appropriate command. Refer to either of the following topics for more information:
 See [“Software required to use NetApp Data ONTAP 7-Mode with Replication Director”](#) on page 126.

See [“Software required to use NetApp Clustered Data ONTAP with Replication Director”](#) on page 137.

- 2 In the **NetBackup Administration Console**, create a backup policy.
Do not use the **Policy Configuration Wizard** to configure a policy for Replication Director.
- 3 Configure the options on the policy **Attributes** tab. The following items are specific to creating a policy for Replication Director:
 - **Policy type:** Select **Standard** for a policy containing UNIX clients. Select **MS-Windows** for a policy containing Windows clients.
 - **Policy storage:** Select the SLP that you want to use that has been configured for snapshot replication.
See [“Creating a storage lifecycle policy for snapshots and snapshot replication”](#) on page 52.
 - **Use Replication Director:** Enable **Use Replication Director** to automatically select other options that Replication Director requires.
 - **Perform off-host backup:** Enable, then select the following:
 - Use **Data Mover**.
 - **NDMP** as the **Machine** selection.
- 4 Select the **Schedules** tab and configure the schedules as you would for any other policy.
- 5 Select the **Clients** tab. Specify the clients to be backed up.
- 6 Select the **Backup Selections** tab to specify the files and directories to be backed up on each client.



Note: Backup selections for both SAN devices and NAS volumes are not supported in a single backup policy.

- 7 When the policy configuration is complete, click **OK**.
- 8 NetBackup checks the policy to ensure that it can run successfully. Select **Complete** to perform the most comprehensive policy validation.

Configuring a Standard or MS-Windows policy to protect NAS volumes or SAN-connected devices

The following procedure describes how to create a policy that uses Replication Director to protect NAS volumes or SAN (block) devices.

Note: SAN-connected devices are not supported for Clustered Data ONTAP.

On Windows hosts, Replication Director uses the Windows Volume Shadow Services (VSS) framework.

To create a Standard or MS-Windows policy to protect NAS volumes or SAN-connected devices

- 1 In the **NetBackup Administration Console**, create a backup policy.
Do not use the **Policy Configuration Wizard** to configure a policy for Replication Director.
- 2 Configure the options on the policy **Attributes** tab. The following items are specific to creating a policy for Replication Director:
 - **Policy type:** Select **Standard** for a policy containing UNIX clients. Select **MS-Windows** for a policy containing Windows clients.
 - **Policy storage:** Select the SLP that you want to use that has been configured for snapshot replication.
See [“Creating a storage lifecycle policy for snapshots and snapshot replication”](#) on page 52.
 - **Use Replication Director:** Enable **Use Replication Director** to automatically select other options that Replication Director requires.
 - Click the **Options** button to see the **Replication Director Options** dialog box and the default **Configuration Parameters** as follows:

Snapshot Type	Auto (default): The OpenStorage partner uses the best snapshot technology available to that partner to create the snapshot.
----------------------	--

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.

See [“Maximum snapshot limit retention type for SLP operations”](#) on page 73.

Managed by SLP retention is automatically selected if the **Fixed** or the **Expire after Copy** retention is currently selected in the SLP.

- 3 Select the **Schedules** tab and configure the schedules as you would for any other policy.
- 4 Select the **Clients** tab and specify either:
 - The client.
 - The local mount point on the production client.

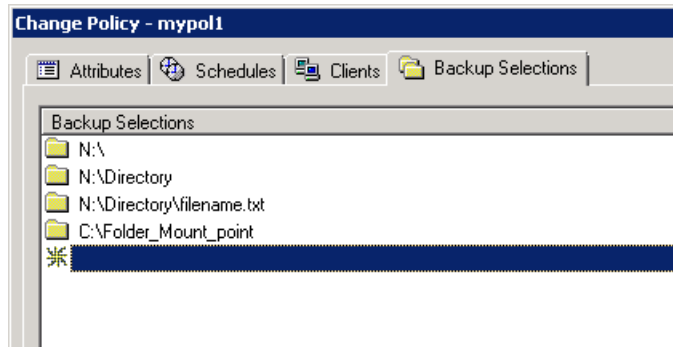
Note: To avoid creating multiple snapshots of the same share, do not include multiple clients in one policy that access the same share. Instead, add only one of the clients to the policy so that the share is backed up once. Or, create an NDMP policy to back up the share.

Similarly, do not protect the same share in multiple policies.

- 5 Select the **Backup Selections** tab:

To protect SAN data, indicate the path on the client to be backed up. The **Backup Selections** list may contain any combination of the following:

- Drive letters
- Folder mounts
- A directory on a drive
- A single file on a drive or in a directory



Do not specify more than 64 backup selections in a VSS policy. If more than 64 backup selections are specified, the snapshot jobs fail with status code 156. This is due to a documented limitation of the VSS infrastructure. To accommodate more than 64 backup selections, divide the backup selections between multiple policies.

Note: Backup selections for both SAN devices and NAS volumes are not supported in a single backup policy.

To protect NAS data, specify the backup selection from the client perspective. For example, suppose that the client data resides in a volume (`/vol/vol1`) on a filer (`NAS1`):

- **UNIX example:** The data is NFS-mounted to `/mnt2/home` on the UNIX client. Specify `/mnt2/home` in the **Backup Selections** list.
- **Windows example:** The data is shared by means of CIFS as `vol1` on the Windows client. Specify `\\nas1\vol1` in the **Backup Selections** list.

For a Clustered Data ONTAP policy, the backup selection refers to a volume on a Storage Virtual Machine (or Vserver).

- Windows path names must use the Universal Naming Convention (UNC), in the form `\\server_name\share_name`.
- For NFS mounts, the data must be manually mounted by means of the `mount` command (or by using `/etc/fstab`), but not auto-mounted.
- (NetApp 7-mode only) Use the `nosharecache` option to mount qtrees that are under the same volume. For example:

```
mount -o vers=3,nosharecache filer:/vol/volume1/qtreet1 /mnt1
```

- (NetApp 7-mode only) To back up a qtree, mount the qtree only. Do not mount the volume. That is, do not include the volume in the backup selection path.

If the volume is mounted and a qtree from the same is used as a backup selection, the NetApp Plug-in for Veritas NetBackup (NBUPugin) considers it to be a volume only and performs only volume-specific operations.

For example, to back up a qtree, enter: `\\filer\q1`

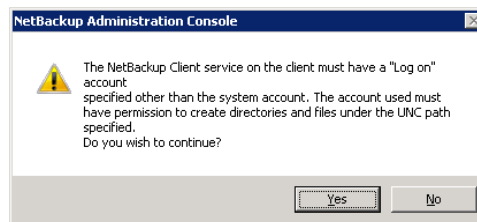
The following entry is incorrect and creates a snapshot of the entire volume:

`\\filer\volume1\q1`

- 6 For the NetBackup Client Service to write to the CIFS volume, it must have permission to do so. When a backup policy is saved, a message displays stating that this permission is necessary. By default, NetBackup is installed as a local system account and may not have the necessary CIFS permissions. Change the logon property of the NetBackup Client Service to an account with access to the CIFS share.

If the logon property is not changed for the NetBackup Client Service, the policy validation fails with status code 4206.

See [“Configuring the NetBackup Client Service”](#) on page 14.



- 7 When the policy configuration is complete, click **OK**.
- 8 NetBackup checks the policy to ensure that it can run successfully. Select **Complete** to perform the most comprehensive policy validation.

About NDMP support for Replication Director

Replication Director can use NDMP to back up, browse, and restore from snapshots. How you configure the backup policy determines whether NetBackup uses NDMP to create snapshots of the NAS host or volume.

When deciding whether to use NDMP consider the following aspects:

Table 7-1 Comparison of NDMP or non-NDMP policy types

Functionality	NDMP	Non-NDMP
Policy type	■ NDMP See “Configuring an NDMP policy to protect a NAS host” on page 77. ■ Standard or MS-Windows Enable NDMP Data Mover in the policy. See “Configuring a Standard or MS-Windows policy to protect clients using NDMP with Data Mover” on page 81.	Standard or MS-Windows (Do not enable NDMP Data Mover .)
Install NetBackup client software on the protected system	No	Yes
Mount snapshot for backup	No	Yes
Backup performance	Generally faster than NFS or CIFS, especially for many small files.	Generally slower than NDMP, but often faster for fewer, larger files.
Indexing of snapshots*	Yes	Yes. Use the Index From Snapshot operation in the SLP for the policy.
Restore capabilities	Can restore only from the NAS device.	Can restore files from any snapshot location.
Restore view of data	Filer view: All data on the filer is protected and available for restore from a given backup.	Host view: Only data belonging to a specific protected client is available for restore from a given backup.

*An indexed snapshot is useful in restore situations. Indexing is performed by the **Index From Snapshot** operation in an SLP.

See [“Index From Snapshot operation in an SLP”](#) on page 61.

Limitations of Replication Director with NDMP

Consider the following limitation before configuring NDMP to be used with Replication Director:

- The Solaris_x86 operating system is not supported.
- The **Multiple copies** NetBackup policy option is not supported for image copies in the NDMP data format.

- The **Restore the file using a temporary filename** restore option is not supported on Windows clients.
- Restores to a local file system are not supported with an **MS-Windows** or a **Standard** policy that has the NDMP **Data Mover** enabled.
- Do not include both the qtree and the volume on which the qtree resides in the same **Backup Selection** list.
- Only one NDMP backup of a snapshot per `backupid` is allowed.
- The **Index From Snapshot** operation is supported only in a Replication Director configuration, however, a Standard or MS-Windows policy with NDMP Data Mover enabled is also not supported.

Note: The **Index From Snapshot** operation is not supported for media servers on AIX platforms. This operation is supported only on Linux, Windows, HP-UX, Solaris media servers. See the [NetBackup Master Compatibility List](#) for information about supported operating systems.

Note: The **Index From Snapshot** operation is not supported for NetApp ONTAP 7-mode.

See “[Index From Snapshot operation in an SLP](#)” on page 61.

- When you make changes to the NDMP policy after the last full or incremental schedule (for example, if you add or delete a backup selection), the content for the next incremental retrieves the entire content of the snapshot rather than retrieving only the content that has changed. The next incremental schedule however, after only retrieves content that has changed as expected.

Authorizing NetBackup access to a NAS (NDMP) host

Before NetBackup can perform backups using NDMP, it must have access to the NAS (or NDMP) host.

Note: Perform the following procedure on the master server (not media server) if you plan to create snapshots using Replication Director.

To authorize NetBackup access to the NDMP host

- 1 On the NetBackup server **NetBackup Administration Console**, expand **Media and Device Management > Credentials > NDMP Hosts**.
- 2 Under the **Actions** menu, select **New > New NDMP Host**.

- 3
- In the **Add NDMP Host** dialog box, enter the name of the NDMP server for NetBackup to back up.
- If you are using NetApp's Clustered Data ONTAP, the NDMP host must be a Storage Virtual Machine (SVM).
- The NDMP host name is case-sensitive. The name must match the name that is entered here whenever this host name is used.

Note: If you do not plan to use Replication Director and you add NDMP host credentials using the fully qualified domain name (FQDN), you must also indicate the fully qualified domain name on the client for lookups. That is, the server list in the **Backup, Archive, and Restore** client interface must list the NDMP host by the FQDN as well.

If you add NDMP host credentials using a short name, you can use either the short name or the FQDN in the client server list.

- 4
- Click **OK**.
- 5
- In the **New NDMP Host** dialog box, specify the following:
- (The term credentials refers to the user name and password that NetBackup uses to access the NDMP host.)

Use global NDMP credentials for this NDMP host

Enables all NetBackup media servers under the master server to access this NDMP host using a predefined global NDMP logon.

To create this logon, click **Host Properties > Master Server > Properties > NDMP** in the **NDMP Global Credentials** dialog box.

Note: Because NetApp generates a separate, encrypted password for each SVM, this option cannot be used with NetApp's Clustered Data ONTAP.

Use the following credentials for this NDMP host on all media servers

Enables all NetBackup media servers that are connected to the NDMP host to access the NDMP host using the logon you specify:

- **User name:** The user name under which NetBackup accesses the NDMP server. This user must have permission to run NDMP commands.
 You can find out whether your NDMP host vendor requires a particular user name or access level.
 For information about supported NDMP operating systems and NAS vendors, access [NetBackup for NDMP: NAS Appliance Information](#) from the Veritas Support website.
- **Password and Confirm Password:** Enter the password for this user.
 For information about passwords for NAS devices, see the *NetBackup for NDMP: NAS Appliance Information* from the Veritas Support website:
<http://www.veritas.com/docs/000027113>

Use different credentials for this NDMP host on each media server

Specifies NDMP logons for particular NetBackup servers. Then click **Advanced Configuration**.

- In the **Advanced NDMP Credentials** dialog box, click **Add**.
- In the **Add Credentials** dialog box, select a NetBackup server and specify the user name and password it uses to access the NDMP host.
- Click **OK**. NetBackup validates the user name and password.
- The NetBackup server and user name appear in the **Advanced NDMP Credentials** dialog box.
- If necessary, click **Add** again to specify other servers and user

6 Repeat this procedure for each NDMP host that NetBackup backs up.

ALL_FILESYSTEMS and VOLUME_EXCLUDE_LIST directives

The `ALL_FILESYSTEMS` directive provides a method to include all file systems and volumes on an NDMP filer in an NDMP backup policy.

You can exclude specific volumes from an `ALL_FILESYSTEMS` backup selection if you do not want to back up every volume on an NDMP filer. Use the `VOLUME_EXCLUDE_LIST` directive for this purpose. You may use valid wildcard characters in the `VOLUME_EXCLUDE_LIST` statement.

Note: The following examples use selections that are specific to NetApp Data ONTAP 7-mode. For specific examples of backup selections for other configurations, refer to the appropriate documentation.

The `VOLUME_EXCLUDE_LIST` statements must precede `ALL_FILESYSTEMS` statement. For example:

```
VOLUME_EXCLUDE_LIST=/vol/Hr_allfiles_vol01
ALL_FILESYSTEMS
```

or

```
VOLUME_EXCLUDE_LIST=/vol/testvol*
ALL_FILESYSTEMS
```

To specify multiple values in a `VOLUME_EXCLUDE_LIST` statement, separate the values with a comma. For example:

```
VOLUME_EXCLUDE_LIST=/vol/Hr_allfiles_vol01,/vol/testvol*
ALL_FILESYSTEMS
```

You can also specify more than one `VOLUME_EXCLUDE_LIST` statement with an `ALL_FILESYSTEMS` directive. For example:

```
VOLUME_EXCLUDE_LIST=/vol/Hr_allfiles_vol01
VOLUME_EXCLUDE_LIST=/vol/testvol*
ALL_FILESYSTEMS
```

A `VOLUME_EXCLUDE_LIST` statement may include a maximum of 256 characters. Create multiple `VOLUME_EXCLUDE_LIST` statements if necessary to avoid exceeding the limit of 256 characters. If you specify more than 256 characters, the volume list is truncated. A truncated statement may result in a backup job failure, and the error message `Invalid command parameter(20)` is displayed.

If the backup selection includes read-only volumes or full volumes, an NDMP backup job fails with the status code 20 (`Invalid command parameter(20)`). If you encounter a similar NDMP backup job error, review the `ostfi` logs to identify the volumes for which the failure occurred. You can use `VOLUME_EXCLUDE_LIST` statements with the `ALL_FILESYSTEMS` statement to exclude the read-only volumes and the volumes with insufficient space.

In a NetBackup Replication Director environment where snapshots are replicated to a secondary filer, Veritas recommends that you use storage lifecycle policies to control backups on the secondary filer.

On NetApp 7-mode storage systems, it is generally not recommended for users to store files in `/vol/vol0` because the volume contains filer system files. For this reason, `vol0` should be excluded from the backup if the `ALL_FILESYSTEMS` directive is used in the backup policy. The following is a backup selection list that excludes `/vol/vol0`:

```
VOLUME_EXCLUDE_LIST=/vol/vol0
ALL_FILESYSTEMS
```

- Do not use `ALL_FILESYSTEMS` to backup all volumes on a secondary filer. Inconsistencies may occur when automatically created NetApp FlexClone volumes are backed up or restored. Such volumes are temporary and used as virtual copies or pointers to actual volumes and as such do not need to be backed up.
- If you must back up all volumes on a secondary filer, Veritas recommends that you exclude the FlexClone volumes as well as replicated volumes. For example:

```
VOLUME_EXCLUDE_LIST=/vol/Clone_*
VOLUME_EXCLUDE_LIST=/vol/*_[0-9]
VOLUME_EXCLUDE_LIST=/vol/*_[0-9][0-9]
VOLUME_EXCLUDE_LIST=/vol/*_[0-9][0-9][0-9]
ALL_FILESYSTEMS
```

This example assumes all FlexClone volumes and only FlexClone volumes begin with `/vol/Clone_`. Adjust the volume specifications appropriately for your environment.

- `VOLUME_EXCLUDE_LIST` applies only to `ALL_FILESYSTEMS`. It does not apply to explicit backup selections or wildcard-based backup selections. If you use the `ALL_FILESYSTEMS` directive in an NDMP policy for Clustered Data ONTAP, you must exclude each selected SVM's root volume using the `VOLUME_EXCLUDE_LIST` directive. Otherwise the backups fail. For more information, refer to the following topic:
See [“About creating backup policies for Clustered Data ONTAP with Replication Director”](#) on page 140.

Backups from snapshots for NDMP policies fail when the import of a snapshot fails for volumes where logical unit numbers (LUNs) reside with status code 4213 (Snapshot import failed). To avoid this error, use the `VOLUME_EXCLUDE_LIST` directive to exclude any volumes that are used to create LUNs accessed through a storage area network (SAN).

Configuring an NDMP policy in a multi-network environment

In an environment where NetApp storage systems are connected to multiple networks, the NDMP policy for Replication Director can be configured to use a specific network for the NDMP backup traffic. To do this, use the **Backup From Snapshot** operation in the storage lifecycle policy.

If the backup is from the primary storage system (that is, a **Snapshot** operation plus a **Backup From Snapshot** operation in one SLP), then the host name associated with the network to use should be entered in the **Clients** tab of the policy.

Note: The following examples use commands that are specific to NetApp Data ONTAP 7-mode. Commands can change from version to version. For the latest vendor-specific commands, refer to the vendor's documentation.

For cases where the snapshot is replicated, the default primary name of the secondary storage system is used. To use a different network, set the `ndmpd.preferred_interface` options on the storage system to the interface that is connected to that network.

For example, in a setup where the secondary storage system is connected to a private network on the `e0b` interface, connect to the storage system and set the `ndmpd.preferred_interface` to `e0b`, as follows:

```
Netapp3140a2> options ndmpd.preferred_interface e0b  
  
ndmpd.preferred_interface e0b
```

In this way, the NDMP backup of all the snapshots that are replicated to that storage system will use the private network.

In NetBackup, add NDMP host credentials to indicate the IP address or hostname that is associated with `e0b`.

See [“Authorizing NetBackup access to a NAS \(NDMP\) host”](#) on page 89.

Restoring from a snapshot

This chapter includes the following topics:

- [About restores from array-based snapshots](#)
- [Restoring files and folders from an array-based snapshot](#)
- [About restores from array-based snapshots of virtual machines](#)
- [Using OpsCenter to restore from array-based snapshots](#)
- [How NetApp performs a volume-level rollback restore](#)
- [Restoring \(rolling back\) from an array-based snapshot](#)

About restores from array-based snapshots

NetBackup manages array-based snapshot creation and replication. NetBackup also can create backup images from those snapshots.

See [“About configuring storage lifecycle policies for snapshots and snapshot replication”](#) on page 50.

In this release of NetBackup, you can do the following restore operations from an array-based snapshot:

File-level restore from the snapshot

NetBackup directs the storage device to restore individual files or folders from the snapshot. The storage device moves the data on the storage device.

Several methods exist for file-level restore from a snapshot, a replica, or a backup, as follows:

- The **Backup, Archive, and Restore** interface.
 See [“Restoring files and folders from an array-based snapshot”](#) on page 97.
- The NetBackup `bprestore` command.
 For more information, see the [NetBackup Commands Reference Guide](#).
- The Veritas OpsCenter interface.
 See [“Using OpsCenter to restore from array-based snapshots”](#) on page 102.
 For more information, see the [NetBackup OpsCenter Administrator's Guide](#).

Volume-level rollback restore from the snapshot (copy one)

NetBackup directs the storage device to replace the volume with the snapshot of the volume. The storage device may be able to restore the volume without moving data.

See [“How NetApp performs a volume-level rollback restore”](#) on page 102.

See [“Restoring \(rolling back\) from an array-based snapshot”](#) on page 104.

Note: NetBackup supports snapshot restore of copy one only to the primary site. To restore at a remote site, use file-level restore.

Only a system administrator can perform an array-based restore.

Note: To restore from backups created using Replication Director: If you select more than one image in the **Backup, Archive, and Restore** interface, it may take longer than expected to display the contents of the images. NetBackup performs a separate browsing operation for each selected image. For faster restores, select one image at a time.

Note: To access snapshots from the clients that use multiple NICs, and if using NetApp storage, see the following topic:

See [“How to configure a multi-NIC environment”](#) on page 16.

Restoring files and folders from an array-based snapshot

This topic describes how to restore individual items from array-based snapshots.

The **Backup, Archive, and Restore** client interface displays the files and folders from the primary backup copy.

See [“About restores from array-based snapshots”](#) on page 95.

To restore files and folders from an array-based snapshot

1 Start the restore, as follows:

Windows

In the Windows **Backup, Archive, and Restore** client interface:

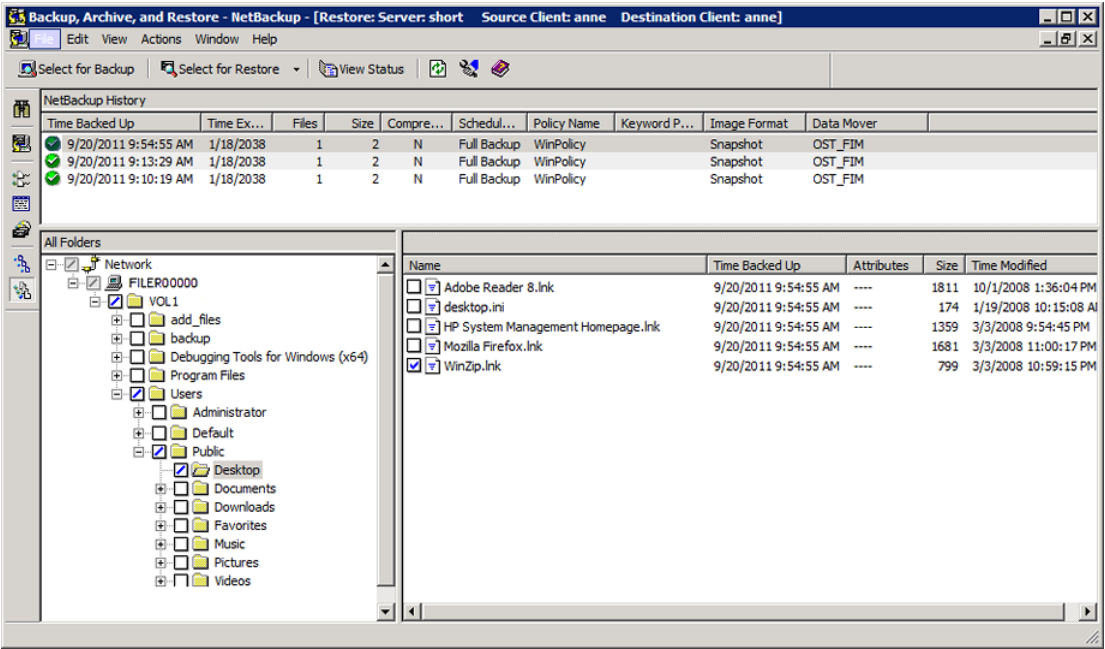
- Click **File > Select Files and Folders to Restore**, and then select **from Normal Backup**.

UNIX

In the Java-based **Backup, Archive, and Restore** client interface:

- Click the **Restore Files** tab.
- In the **Restore type** drop-down list, select **Normal Backups**.
- Click **View > Refresh**.

The following is an example of the restore window on a Windows computer:



2 Select a snapshot as follows:

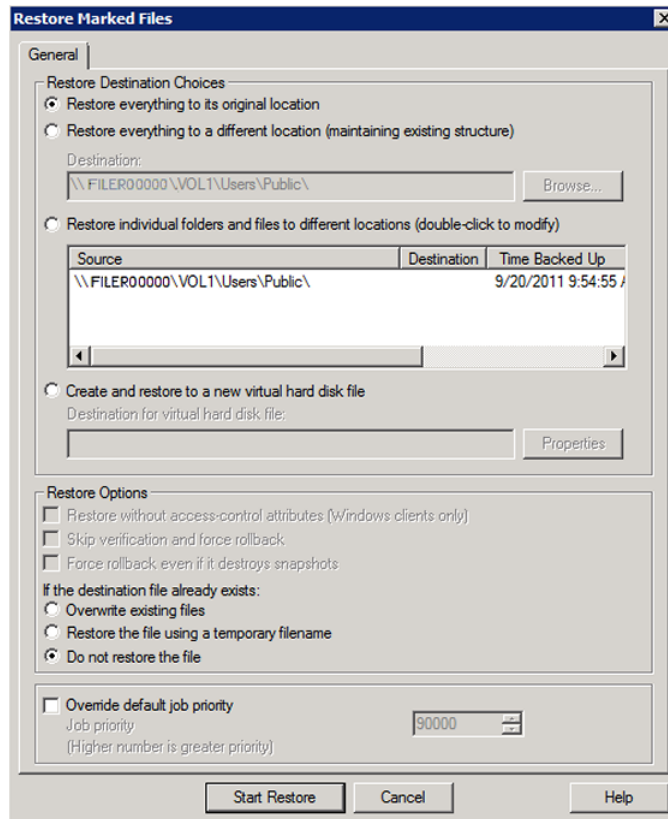
- Windows

In the **NetBackup History** pane, select the snapshot to restore.
The snapshot appears in the **All Folders** pane.
- UNIX

Open the **Date Range** or the **Backup History** to select a snapshot to restore. Select a snapshot from the list and click **OK**.
The snapshot contents appear in the **Directory Structure** pane.

- 3 Expand the directory tree and click the check box next to the items that you want to restore.
- 4 To set up how to restore the selected items, do the following:
- On Windows, click **Actions > Restore**.
 - On UNIX, click **Restore**.

The following is an example of the **Restore Marked Files** dialog box:



- 5** In the **Restore Marked Files** dialog box, select from the following options to meet the requirements for the restore.

For details about each option, see the **Backup, Archive, and Restore** online Help.

**Restore
Destination
Choices**

Select one of the following destination options:

- **Restore everything to its original location** (default)
- **Restore everything to a different location (maintaining existing structure)**
- **Restore individual folders and files to different locations** or **Restore individual directories and files to different locations**
- **Create and restore to a new virtual hard disk file**

Restore Options Select from the following restore options in the Windows **Backup, Archive, and Restore** interface:

- **Restore without access control attributes (Windows clients only)**
- **Skip verification and force rollback**
- **Force rollback even if it destroys later snapshots**
- If the destination file already exists, indicate what NetBackup should do:
 - **Overwrite existing files**
 - **Restore the file using a temporary file name**
 - **Do not restore the file**

Select from the following restore options in the Java-based **Backup, Archive, and Restore** interface:

- **Overwrite existing files**
- **Restore directories without crossing mount points**
- **Restore without access control attributes (Windows clients only)**
- **Rename hard links**
- **Rename soft links**
- **Force rollback even if it destroys later snapshots**

Job Priority To change the priority of this restore, click the **Override default priority** and then set a priority number.

The default is 90000. The available range is 0 to 99999. Higher numbers are higher priority.

6 Click **Start Restore**.

7 To view the restore progress, click **Yes** in the **View Status** or the **View Progress** dialog box.

The restore may take a few minutes to complete. After you start a restore operation, you can close **Backup, Archive, and Restore** and perform other tasks. NetBackup continues the operation in the background.

About restores from array-based snapshots of virtual machines

From a Replication Director snapshot of a virtual machine, you can restore the following:

- The entire virtual machine.

See the topic on restoring the full VMware virtual machine in the *NetBackup for VMware Guide*.

- Individual files in virtual machines.
To restore virtual machine files, refer to the following topic.

Restoring files from array-based snapshots of virtual machines

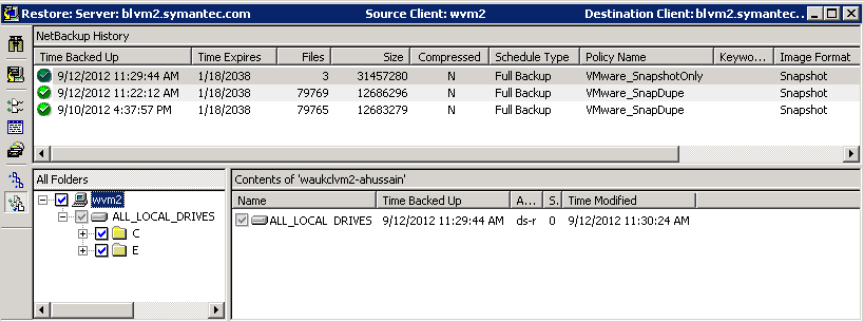
Note: When you browse files to restore, the Backup, Archive, and Restore interface displays the files and folders from the primary backup copy. A storage lifecycle policy however can create several images or copies from one job. To restore files from a different copy, set that copy as the primary. See the topic on how to promote a backup copy to a primary copy in the *NetBackup Administrator's Guide, Volume I*.

The initial steps for restoring individual files are described in the *NetBackup for VMware Guide*.

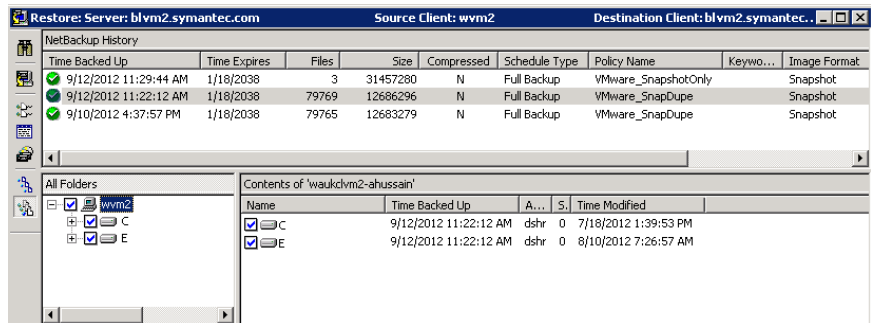
Note the following when restoring files from Replication Director snapshots:

In the **Backup, Archive, and Restore** interface, under **Files > Specify NetBackup Machines and Policy Type**, select **VMware** for the policy type.

If the SLP does not index the VM (or indexing is not complete), the BAR interface browses the files directly from the hardware snapshot. The **All Folders** pane displays an `ALL_LOCAL_DRIVES` node at the top level:



If the SLP was configured to index the virtual machine, the folders appear as follows when the indexing is complete:



Note: If you select an indexed snapshot and a non-indexed snapshot for the same virtual machine, the folders appear twice under **All Folders**. Do not select files to restore from two different images: the restore fails.

See [“Configuring a policy for virtual machines to use Replication Director”](#) on page 169.

Using OpsCenter to restore from array-based snapshots

Replication Director enables administrators to use the Restore operation in OpsCenter to browse and restore files and directories from any copy of a snapshot that is created as part of a storage lifecycle policy, even those in long-term storage. The Restore operation in OpsCenter also offers greater flexibility with the advanced search capabilities.

To use the Restore operation in OpsCenter requires that the **Index From Snapshot** operation was used in the SLP that generated the snapshots and replications.

See [“Index From Snapshot operation in an SLP”](#) on page 61.

For more information about Operational Restore using OpsCenter, see the [Veritas NetBackup OpsCenter Administrator's Guide](#).

How NetApp performs a volume-level rollback restore

NetBackup directs the array or storage device to do a volume-level rollback restore (point-in-time restore) of the snapshot. The device determines how to accomplish the restore.

Several factors affect how the array accomplishes the restore, as follows:

- Whether the rollback is from the most recent snapshot or not.
- The NetBackup restore option: **Force rollback even if it invalidates later snapshots restore.**
- Whether the mount point from backup selection is a volume or qtree/folder in the volume.

Note: Using NetApp storage, if a point-in-time rollback restore is performed for one of the volumes in a backup image that consists of multiple volumes, the snapshots corresponding to the remaining volumes will not be immediately deleted from the storage system but they will be immediately removed from the NetBackup catalog. Any subsequent image cleanup job will cause the remaining snapshots to be deleted from the storage system.

Table 8-1 describes the interaction between the various factors.

Table 8-1 Volume-level rollback restore factors

From the most recent or an older snapshot	Force rollback even if it invalidates later snapshots restore option	Backup selection mount point*	Description
From the most recent snapshot	Either selection	Volume	The device performs a rollback restore of the volume. Because it is a rollback restore, the restore occurs almost immediately.
From the most recent snapshot	Either selection	Qtree or folder	The device performs a file-level restore of the backup selection mount point* rather than a volume-level rollback restore. Such a restore is much slower than a volume-level rollback restore in which no data moves.
From an older snapshot	Checked	Volume	The device performs a rollback restore of the volume. Because it is a rollback restore, the restore occurs almost immediately. Because the rollback restore replaces the current volume with the older snapshot, more recent snapshots are lost.

Table 8-1 Volume-level rollback restore factors (continued)

From the most recent or an older snapshot	Force rollback even if it invalidates later snapshots restore option	Backup selection mount point*	Description
From an older snapshot	Either selection	Qtree or folder	The device performs a file-level restore of the backup selection mount point* rather than a volume-level rollback restore. Such a restore is much slower than a volume-level rollback restore in which no data moves. Unlike a volume-level rollback restore, this type of restore does not destroy more recent snapshots.
From an older snapshot	Unchecked	Volume	The restore fails.

* For NDMP backups the entire backup selection is considered and not just the part that is mounted.

Restoring (rolling back) from an array-based snapshot

The following procedure describes how to perform a volume-level rollback restore (point-in-time restore) from a snapshot that NetBackup Replication Director manages. The storage device replaces the protected volume with the snapshot of the volume.

NetBackup supports point-in-time rollback restores for only NAS devices and only for copy one. Point-in-time rollback restores are not supported for SAN devices on Windows or UNIX.

Note: Do not perform a point-in-time rollback restore on a volume which is shared across multiple policies because it retains the stale catalog entries for another policy or policies.

See [“About restores from array-based snapshots”](#) on page 95.

See [“How NetApp performs a volume-level rollback restore”](#) on page 102.

To restore from an array-based snapshot

1 Begin the restore procedure as follows:

Windows

Click **File > Select Files and Folders to Restore > from Point in Time Rollback**.

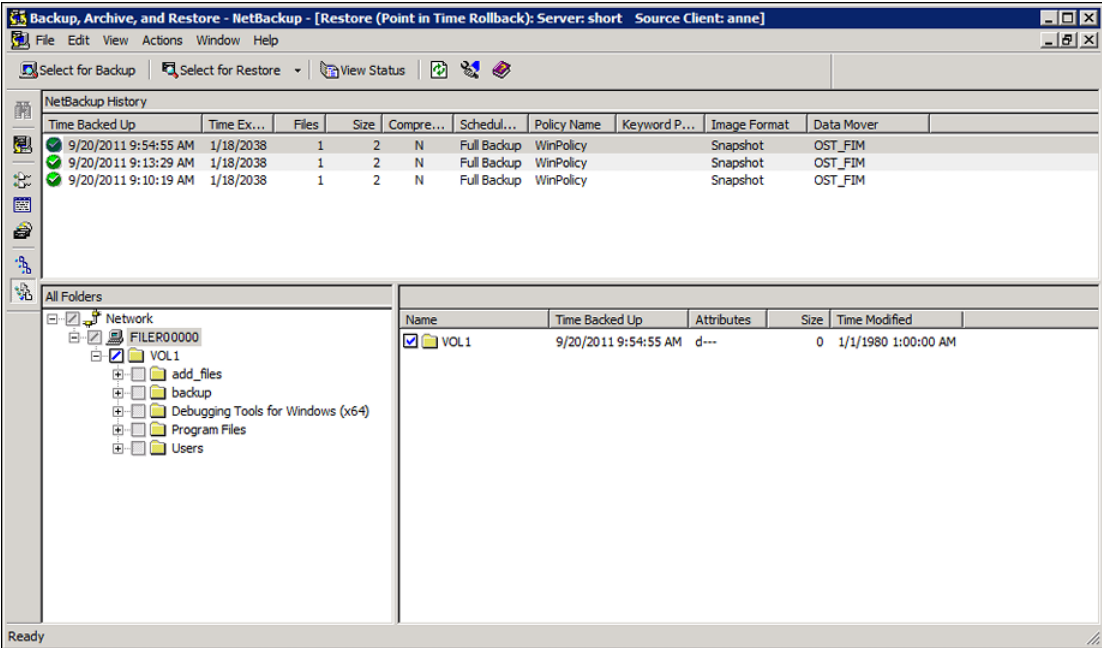
The **NetBackup History** pane shows the available snapshots from which you can restore.

UNIX

Click the **Restore Files** tab, then select **Point in Time Rollback** for the **Restore Type**.

The **Date Range** dialog box appears.

The following is an example of the restore window on a Windows computer:



2 Select a snapshot as follows:

- | | |
|---------|--|
| Windows | In the NetBackup History pane, select the snapshot to restore.
The snapshot appears in the All Folders pane. |
| UNIX | In the Date Range dialog box, select a snapshot from the list and click OK .
The snapshot contents appear in the Directory Structure pane. |

3 Select the volume, as follows:

- | | |
|---------|--|
| Windows | In the All Folders pane, expand the directory tree to find the volume mount point (if necessary) and then click the check box next to the mount point for the volume. |
| UNIX | In the Directory Structure pane, expand the directory tree to find the volume mount point (if necessary) and then click the check box next to the mount point for the volume. |

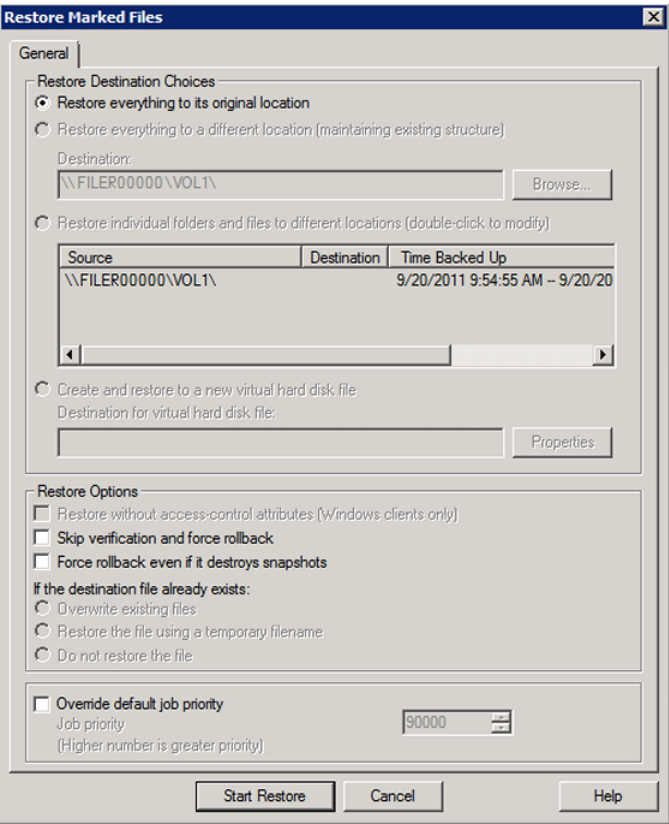
4 Begin the restore, as follows:

- Windows Click **Actions > Restore....**
- UNIX Click **Restore.**

The **Restore Marked Files** dialog box appears.

Most options are selected by default and cannot be changed.

The following is an example of the **Restore Marked Files** dialog box on a Microsoft Windows computer:



5 In the **Restore Marked Files** dialog box, select from the following options to meet the requirements for the restore:

Restore Options ■ **Skip verification and force rollback**

By default, NetBackup performs several checks on the file system during the restore. If the checks fail, the restore stops. Select this option to skip verification.

Warning: Select this option only if you are sure that you want to replace all of the files in the original location with the snapshot. Rollback deletes all files that were created after the creation-date of the snapshot from which you restore.

■ **Force rollback even if it invalidates later snapshots**

This option applies only if you restore from a snapshot other than the most recent one.

Warning: Select this option only if you are sure that you want to replace the original volume with the snapshot. If more recent snapshots that have been replicated exist and you do *not* select this option, the rollback restore fails.

See [“How NetApp performs a volume-level rollback restore”](#) on page 102.

Job Priority To change the priority of this restore, click **Override default priority** and then set a priority number.

The default is 90000. The available range is 0 to 99999.

6 Click **Start Restore**.

7 In the dialog box that appears, click **Yes** to view the restore status.

If file verification fails, a message appears in the **View Status** dialog box (Windows) or **Task Progress** tab (UNIX) that indicates the restore was not performed.

After a restore operation begins, you can close **Backup, Archive, and Restore** to perform other tasks on your computer. NetBackup continues the restore operation in the background.

OpsCenter reporting

This chapter includes the following topics:

- [Veritas OpsCenter reporting](#)
- [Configuring an alert for OpenStorage events](#)
- [Storage lifecycle policy reporting](#)
- [Disk pool monitoring](#)
- [Monitoring snapshot replication jobs](#)
- [Reporting on storage units, storage unit groups, and storage lifecycle policies](#)

Veritas OpsCenter reporting

Use Veritas OpsCenter to provide unified reporting on Replication Director-related activity. This includes monitoring the lifecycle of the snapshot copies at the various storage locations. Administrators can use this information to help make retention-related decisions.

Veritas OpsCenter offers the following reports:

- Storage space utilization
- Capacity planning reports that display forecasted and historical views.

All OpsCenter reports are described in the [NetBackup OpsCenter Reporting Guide](#).

Configuring an alert for OpenStorage events

The administrator can configure OpsCenter to send alerts based on events on OpenStorage devices (storage servers):

- The storage server can generate threshold or **Volume Almost Full** alarms.

- Alerts based on the auto-discovery of unprotected NAS file services data.

The alert policy can consider the following information before OpsCenter sends an alert:

- Whether the event is considered to be an error, an informational notification, or a warning; or to consider all events regardless of classification. For example, send alerts only when the storage server generates a warning.
- Whether the event contains specific words or if it is generated by a specific vendor. For example, send alerts that are generated only from the NetApp device of label xyz.
- Whether the event is from a specific master server; or to consider events from all master servers.

When alerts occur, they are sent at a specified severity level to multiple email addresses. When the alerts are cleared, the same email addresses are notified. The severity level for the clearing alerts can also be specified.

See the [Veritas OpsCenter Administrator's Guide](#) for information about configuring alerts.

Storage lifecycle policy reporting

The **Storage Lifecycle Policy** status report provides a summary of the SLPs of a selected master server.

Many columns in the report contain data that links to additional reports:

- **SLP Status by SLP**
- **SLP Status by Client**
- **SLP Status by Image**
- **SLP Status by Image Copy**

The **SLP Status by Image Copy** report displays the details of any snapshot copy that is a part of a SLP.

Disk pool monitoring

To view disk pool details, select the **Monitor** tab, and then the **Devices** subtab.

Select the **Disk Pools** tab above the table. Disk pool monitoring is divided into three tabs:

General tab

The **General** tab contains information about the selected disk pool, including the used and available space in the selected disk pool and whether the images in the disk pool have been imported.

The table also contains the following columns that pertain to snapshot replication:

- **Configured for Snapshots**

Identifies whether the disk pool is configured to contain snapshots, making it eligible for snapshot replication.

- **Mirror**

- **Primary**

- **Replication**

Disk Volume tab

The **Disk Volume** tab contains information about the selected disk pool, including the location or path to the volume, and whether the volume is configured for snapshots.

Storage Server tab

The **Storage Server** tab contains information about the selected disk pool, including the server type and the number of active jobs for the storage server.

The table also contains a **Configured for Snapshots** column, which identifies whether the storage server is configured to contain snapshots.

Monitoring snapshot replication jobs

To view the details of snapshot replication jobs, select the **Monitor** tab, and then the **Jobs** subtab.

From the drop-down **Filter** menu, select **Snapshot Replication** to display only those jobs generated from snapshot replication.

The **General** tab displays details about the selected job, including the duplication method (**Method**) used to create the backup and the data transferred for each job (**Job Size**).

Reporting on storage units, storage unit groups, and storage lifecycle policies

To view the details of storage units, storage unit groups, and storage lifecycle policies, select the **Manage** tab, and then the **Storage** subtab.

Select the **Storage Unit** tab above the table to display storage unit details, including whether the storage unit is enabled for snapshots and the name of the disk pool to which the storage unit belongs.

Storage Unit tab

The **General** tab contains information about the selected storage unit. The table also contains the following columns that pertain to snapshot replication:

- **Configured for Snapshots**
Identifies whether the storage unit is configured to contain snapshots, making it eligible for snapshot replication.
- **Mirror**
- **Primary**
- **Replication**

Storage Unit Group tab

The **Storage Unit Group** tab contains information about the selected storage unit group. The table contains a **Configured for Snapshots** column which identifies whether the storage unit group can contain snapshots.

Storage Lifecycle Policy tab

The **Storage Lifecycle Policy** tab contains two subtabs:

- **General**
Displays SLP details, including whether the SLP is configured to preserve multiplexing, and the data classification on the SLP.
- **Operations**

Displays the operation type and storage unit that is assigned to each operation in the SLP.

Using NetApp disk arrays with Replication Director

This chapter includes the following topics:

- [Using NetApp disk arrays with Replication Director](#)
- [Supported NetApp topologies](#)
- [Using NetApp Data ONTAP 7-mode with Replication Director](#)
- [Using NetApp Clustered Data ONTAP with Replication Director](#)

Using NetApp disk arrays with Replication Director

Replication Director can replicate snapshots on a NetApp disk array in two different situations:

- In non-cluster mode: 7-mode is used to replicate snapshots on NAS and SAN. The plug-in must be installed on the OnCommand Unified Manager (OCUM) server ([Figure 10-1](#)).
- In cluster-mode: Clustered Data ONTAP (cDOT) is used to replicate snapshots between storage virtual machines (SVMs or vServers). Support is for NAS only. The plug-in must be installed on either a Windows or a Linux computer other than the OCUM server, the master server, or any media servers ([Figure 10-2](#)).

Both modes support the same topologies.

[Table 10-1](#) describes the association between NetBackup versions and the NetApp plug-ins.

Table 10-1 Version compatibility

NetBackup version	NetApp plug-in version	Description	Ratio of master server to OCUM server	Supported policy types
7.7 and later	1.1	Provides 7-mode support for all NetBackup 7.7 Replication Director features.	One master server supports many OCUM servers. The plug-in must be installed on the OnCommand Unified Manager (OCUM) server.	MS-Windows, Standard, NDMP, VMware, Oracle
	1.1 P1	Provides 7-mode support for all NetBackup 7.7 Replication Director features.	One master server supports many OCUM servers.	MS-Windows, Standard, NDMP, VMware, Oracle
	2.0	Provides cDOT support.	One master server supports many OCUM servers. The plug-in must be installed on either a Windows or a Linux computer other than the OCUM server, the master server, or any media servers.	MS-Windows, Standard, NDMP, VMware, Oracle

Note: You must upgrade the entire NetBackup environment before upgrading the plug-in. Upgrade all master servers, media servers, clients, and any hosts which communicate with the plug-in.

Figure 10-1 Communication between NetBackup and the NBUPugin for 7-mode

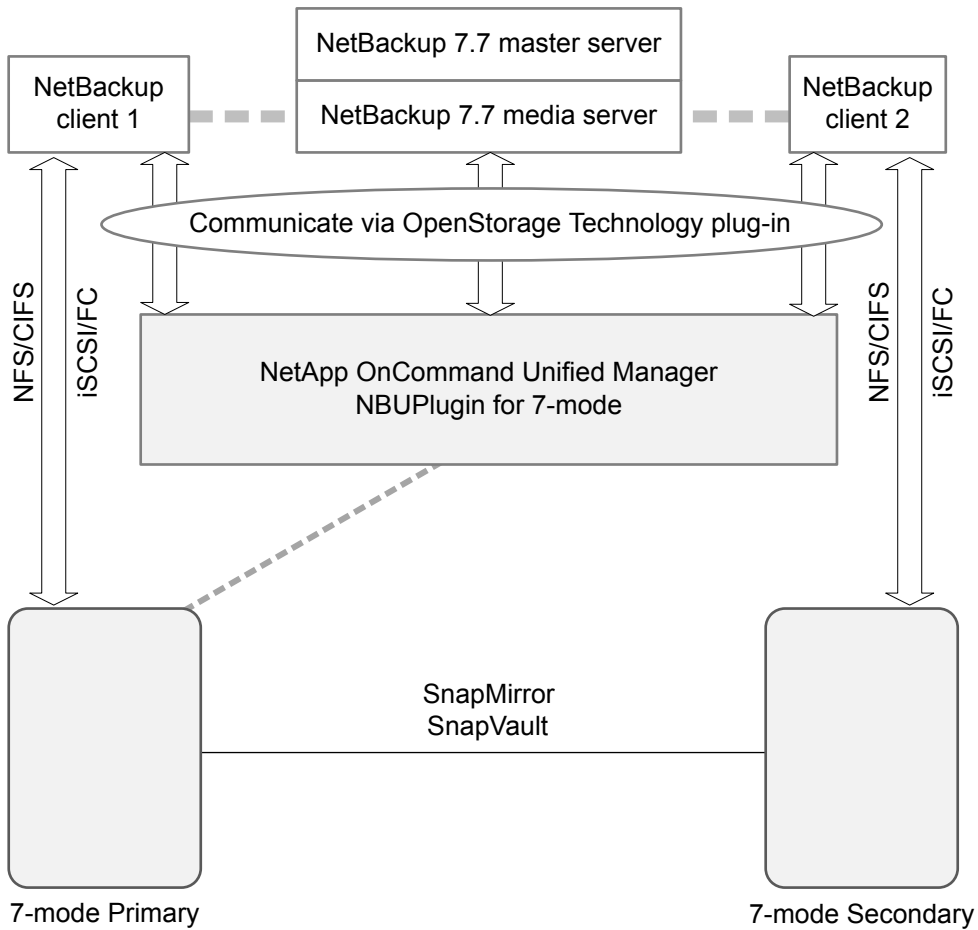
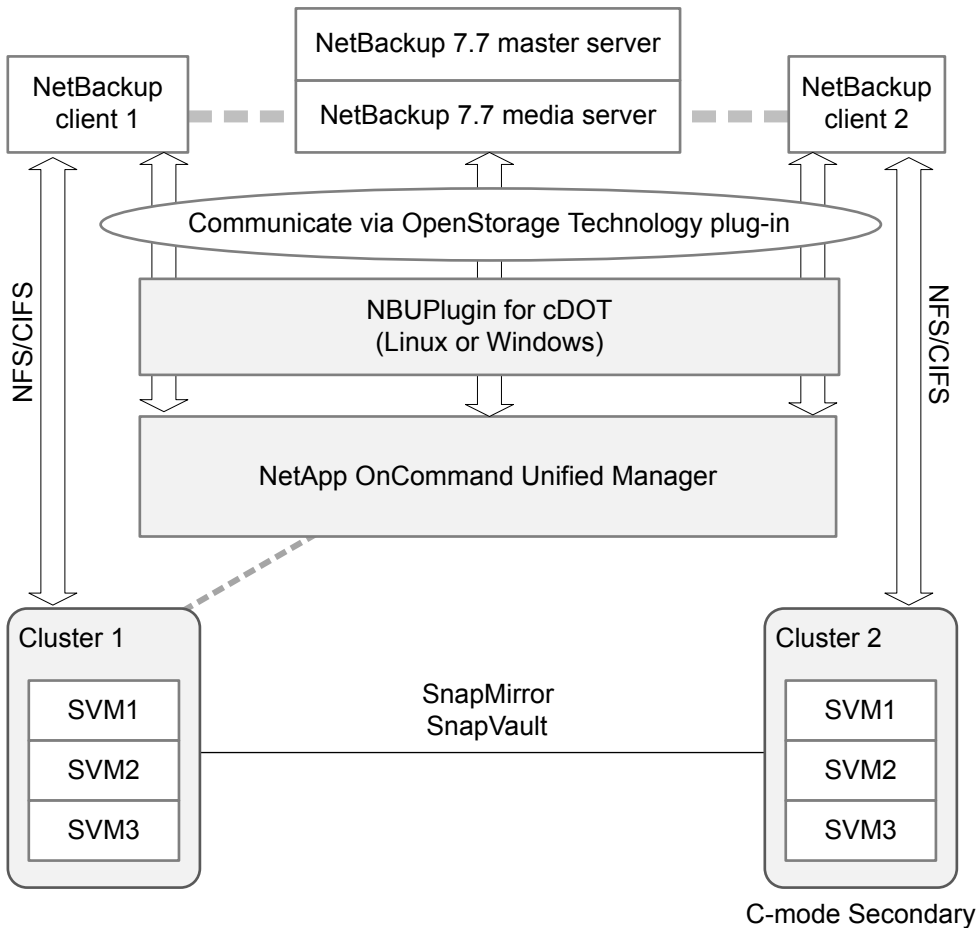


Figure 10-2 Communication between NetBackup and the NBUPugin for Clustered Data ONTAP



Determining the version of the plug-in

To determine the NBUPugin version, look for the following version file on the system where the NBUPugin is installed:

On Windows: `Install_path\Program Files\Netapp\NBUPugin\version.txt`

On UNIX: `/usr/NetApp/NBUPugin/version.txt`

The contents of the file lists the product name, the build date, and the NBUPugin version. If more than one plug-in is installed, both are listed.

Upgrading the plug-in

If upgrading the NetApp Plug-in for Veritas NetBackup, make sure that all storage lifecycle policy jobs that use the old plug-in are complete before upgrading.

To determine whether all of the jobs that are associated with a storage lifecycle policy are complete, in process, or not started, use the following command:

On Windows: `install_path\NetBackup\bin\admincmd>nbstlutil.exe stlilist -U`

On UNIX: `/usr/openv/netbackup/bin/admincmd/nbstlutil stlilist -U`

Supported NetApp topologies

Table 10-2 describes the NetApp topologies that Replication Director supports. Replication Director supports the same NetApp topologies for both cDOT and 7-mode. All begin with a snapshot of the data on the primary volume.

Table 10-2 Supported NetApp snapshot replication topologies

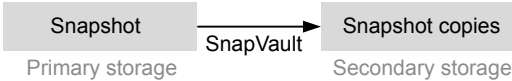
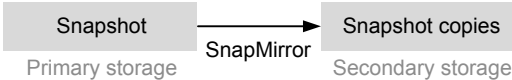
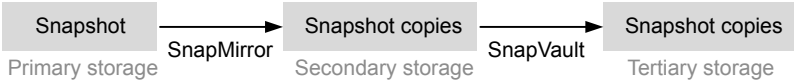
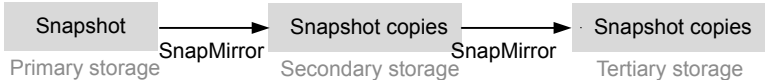
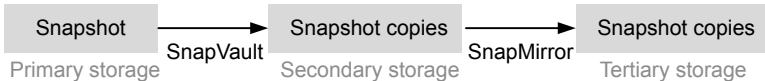
Representation	Description
 <pre>graph LR; A[Snapshot Primary storage] -- SnapVault --> B[Snapshot copies Secondary storage]</pre>	The snapshot can be replicated using SnapVault.
 <pre>graph LR; A[Snapshot Primary storage] -- SnapMirror --> B[Snapshot copies Secondary storage]</pre>	The snapshot can be replicated using SnapMirror.
 <pre>graph LR; A[Snapshot Primary storage] -- SnapMirror --> B[Snapshot copies Secondary storage]; B -- SnapVault --> C[Snapshot copies Tertiary storage]</pre>	The snapshot can be replicated using SnapMirror, and then replicated again using SnapVault.
 <pre>graph LR; A[Snapshot Primary storage] -- SnapMirror --> B[Snapshot copies Secondary storage]; B -- SnapMirror --> C[Snapshot copies Tertiary storage]</pre>	The snapshot can be replicated using SnapMirror, and then replicated again using SnapMirror.
 <pre>graph LR; A[Snapshot Primary storage] -- SnapVault --> B[Snapshot copies Secondary storage]; B -- SnapMirror --> C[Snapshot copies Tertiary storage]</pre>	The snapshot can be replicated using SnapVault, and then replicated again using SnapMirror.

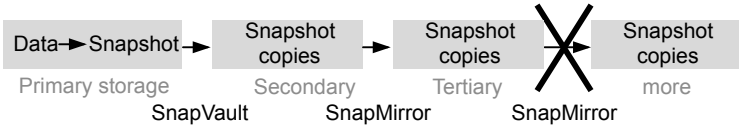
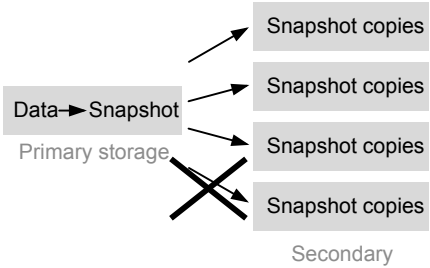
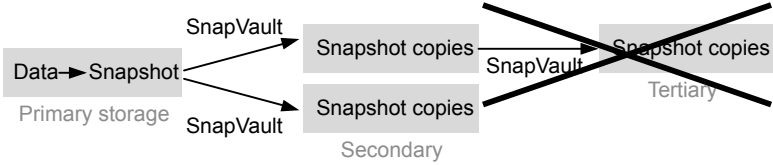
Table 10-2 Supported NetApp snapshot replication topologies (*continued*)

Representation	Description
Two examples of many supported configurations: Or:	The snapshot replications can fan out to two or three resource pools. (The Representation column shows two examples of many possible configurations.)
A tar-formatted backup can be created from any snapshot by using the Backup from Snapshot operation in the storage lifecycle policy. The backup can be created on tape using NDMP or to NFS or CIFS disk. In the following example, a tar-formatted copy is created from each snapshot copy.	Use the Backup from Snapshot SLP operation to create a backup from any snapshot.

NetApp topologies that Replication Director does not support

Table 10-3 lists the topologies that are not supported in this release.

Table 10-3 Unsupported snapshot replication topologies

Example of an unsupported configuration	Description
One example of an unsupported configuration: 	The snapshot can be replicated in succession, or cascaded, no more than two times.
One example of an unsupported configuration: 	Snapshot replications can fan out to no more than three resource pools.
One example of an unsupported configuration: 	Snapshot replications can fan out only from the primary snapshot.
One example of an unsupported configuration: 	Snapshots in succession can accommodate any combination of SnapMirror and SnapVault, except from one SnapVault to another SnapVault.

Note: The NetApp qtree fan-in configuration is not supported.

Note: Mixed aggregate replications are not qualified or tested with Replication Director in this NetBackup release. For example, from a 32-bit aggregate to a 64-bit aggregate and vice versa.

Using NetApp Data ONTAP 7-mode with Replication Director

In non-cluster mode, NetApp Data ONTAP 7-mode is used to replicate snapshots on NAS and SAN. The plug-in must be installed on the OnCommand Unified Manager (OCUM) server.

Configuration overview: NetApp 7-Mode with Replication Director

The following tables list the general configuration steps necessary to set up NetApp 7-Mode with Replication Director. NetApp configuration is also described in the [NetApp Plug-in for Veritas NetBackup Installation and Administration Guide](#), found at the following NetApp website:

<http://support.netapp.com/documentation/docweb/index.html?productID=61512>

Table 10-4 NetApp configuration tasks overview

Description	Reference topics
Install the NetApp Management Console.	See NetApp documentation .
Enable and turn on NetApp licenses, which can include the following: ■ SnapMirror ■ SnapVault ■ SnapRestore ■ FlexClone ■ SnapDrive	See NetApp documentation . Not all licenses may be necessary.
Install necessary licenses on NAS systems: ■ CIFS licenses for MS-Windows policies ■ NFS licenses for Standard policies	See NetApp documentation . See “Enabling Unicode and language settings on NetApp disk arrays” on page 132.

Table 10-4 NetApp configuration tasks overview (*continued*)

Description	Reference topics
Install necessary licenses on SAN devices: ■ iSCSI licenses ■ Fibre Channel licenses	See NetApp documentation. See “About using NetApp SAN-connected storage with Replication Director” on page 127. The following Veritas technote contains additional information: Configuring the primary NetApp device to use VSS with Replication Director.
Install the NetApp Plug-in for Veritas NetBackup (NBUPugin).	After the NBUPugin is installed, the NetBackup resource group is automatically added in the OnCommand Unified Manager. The primary volumes that are configured on NetApp storage are exposed as primary snapshot logical storage units to the NBUPugin. This lets NetBackup initiate and manage snapshots of the primary volumes. The plug-in uses port 8086 by default. See NetApp documentation. See “Using NetApp disk arrays with Replication Director” on page 113.
Configure IPv6 if necessary. By default, the NBUPugin is configured for IPv4.	See NetApp documentation.
Consider using the NetApp import tool.	Consider importing existing data sets and Data ONTAP relationships into Replication Director using the NetApp import tool. After the snapshot data is imported, it can be managed using NetBackup. See NetApp documentation. See “Importing existing NetApp relationships for NetBackup control” on page 132.
Add resource pools.	■ Configure resource pools in the OnCommand Unified Manager and add aggregates to the resource pools. (Use the NetApp Add Resource Pool Wizard or the command line.) Create a resource pool for each replication target. An aggregate can belong to a single resource pool. Do not create a resource pool for the source or primary data; that is handled automatically. ■ Add resource pools to the NetBackup resource group in the OnCommand Unified Manager. NetBackup can now access the resource pools as disk volumes during the NetBackup disk pool creation step. See NetApp documentation. The following Veritas technote contains additional information: See http://www.veritas.com/docs/HOWTO73062.

Table 10-4 NetApp configuration tasks overview (*continued*)

Description	Reference topics
Run the Storage Server Configuration Wizard to configure the OpenStorage partner as a NetBackup storage server. For example, configure the OnCommand Unified Manager as a storage server. This wizard also configures the necessary: - Media servers that can access the storage server. - Disk pools. - Storage units.	See “Creating a NetBackup storage server for snapshot replication” on page 18. The following video demonstrates NetBackup configuration: http://www.veritas.com/community/videos/netbackup-75-replication-director-configuration-demo

- One NetBackup domain can support multiple OnCommand Unified Manager servers.
- Five master servers can communicate efficiently with one NBUPlugin on an OnCommand Unified Manager. The OnCommand Unified Manager determines the number of concurrent jobs that it can run from any number of media servers.

Additional documents and demonstrations provide supporting information:

- Replication Director tools for use with NetApp storage systems:
<http://www.veritas.com/docs/DOC5240>
- A video demonstration:
<http://www.veritas.com/community/videos/configuring-netapp-replication-director>
- A step-by-step description of configuring NetApp storage using the NetApp Management Console:
<http://www.veritas.com/docs/HOWTO73062>

Licenses required for NetApp Data ONTAP 7-Mode with Replication Director

The following NetApp licenses are required to use Replication Director.

Table 10-5 NetApp licenses required for Replication Director*

License	OnCommand Unified Manager	Primary storage system	Secondary storage systems
OnCommand Core Package* The package includes OnCommand server software (enabled by default) and the NetApp Management Console (install separately). 5.0.2, 5.2 (includes the DataFabric Manager server).* 5.2 and later must be used in 7-mode.	Yes	No	No
NetApp Plug-in 1.1 or 1.1 P1 for Veritas NetBackup Download from the NetApp Support Site. Earlier plug-in versions are supported, but they do not support new features. See "Using NetApp disk arrays with Replication Director" on page 113.	Yes	No	No
Data ONTAP Versions can include: 7.3.6, 7.3.7, 8.0.3, 8.0.4, 8.0.5, 8.1, 8.1.1, 8.1.2, 8.1.3.* All storage systems must be at the same version. ONTAP versions 8.0.3 and later must be used in 7-mode.	No	Yes	Yes

*See the [NetApp Interoperability Matrix Tool](#) for the latest information about supported versions.

The NetApp licenses that are required to use Replication Director depends on the replication configuration in use.

Table 10-6 NetApp licenses required on storage systems*

License	On primary	Primary to SnapMirror destination	SnapVault destination	SnapVault to SnapMirror destination	Notes
SnapMirror	Only if SnapMirror Source	Yes	Only if SnapMirror source	Yes	Use to create mirrored snapshots. Install the license on both the source and the destination storage systems in a SnapMirror relationship. Enable SnapMirror access between storage systems. Install and enable the license on both the source and the destination storage systems in a SnapMirror relationship. Allow access between source and all targets.
SnapVault	Only if SnapVault source		Yes	No	Use to create a SnapVault snapshot copy on the primary or the secondary storage system. Install and enable the SnapVault license on the SnapVault source and destination storage systems. Older platforms have separate SnapVault primary licenses for SnapVault primary (source) and secondary (designation) storage systems.

Table 10-6 NetApp licenses required on storage systems* (*continued*)

License	On primary	Primary to SnapMirror destination	SnapVault destination	SnapVault to SnapMirror destination	Notes
SnapRestore Data ONTAP 7.3.6P1 and later is required for SnapRestore support on Windows.	Optional for fast FlexVol level restores	No	Yes		Install the SnapRestore license on all the source storage systems to enable fast pointer-based FlexVol-level restores from primary snapshots. SnapRestore is required on all SnapVault destination storage systems. For the Primary-SnapVault-SnapMirror cascade (PVM) topology, install the license on the SnapMirror destination storage system.
FlexClone	Only for block data or indexing, restore, or tar-formatted backup of NAS data	Only indexing, restore, or tar-formatted backup of NAS data			Install the FlexClone license on the secondary storage system that contains the SnapVault destination volumes. For the Primary-SnapVault-SnapMirror cascade (PVM) topology, install the license on the SnapMirror destination. The FlexClone license is required on any controller that is used for indexing, restoring, or performing a streaming (tar-formatted) backup of NetApp block data.
CIFS	CIFS NAS data only (Windows)				Install the CIFS license on the storage system that is in a SnapMirror or SnapVault relationship that contains the CIFS file systems.
NFS	NFS NAS data only; (UNIX)				Install the NFS license on the storage system that is in a SnapMirror or SnapVault relationship that contains the NFS systems.
iSCSI and FCs	iSCSI and Fibre Channel block data only (SAN)				Install either iSCSI or FC licenses on both the source and the destination storage systems. See “ About using NetApp SAN-connected storage with Replication Director ” on page 127.

Table 10-6 NetApp licenses required on storage systems* (*continued*)

License	On primary	Primary to SnapMirror destination	SnapVault destination	SnapVault to SnapMirror destination	Notes
SnapDrive for Windows SnapDrive 6.3.1R1, 6.4.1, 6.4.2, 6.5.	Only for Windows block data only	No			Use to automate storage provisioning tasks and to manage data in Windows environments. Install the SnapDrive license on the local host or on the primary storage system with Microsoft Windows server SAN data. Note that SnapDrive is not required for UNIX or Linux systems on NetApp LUNs.

*See the [NetApp Interoperability Matrix Tool](#) for the latest information about supported versions.

Software required to use NetApp Data ONTAP 7-Mode with Replication Director

The following NetApp software is required to use Replication Director.

Table 10-7 NetApp software required for Replication Director

Configuration	Applies to OCUM?	Primary storage system	Secondary storage systems
NetApp storage systems, FAS series Must be added to the OnCommand Unified Manager.	No	Yes	Yes
vFiler Can serve as a source only, not as a target. Enable if NDMP is used.	No	Enable	No

Table 10-7 NetApp software required for Replication Director (*continued*)

Configuration	Applies to OCUM?	Primary storage system	Secondary storage systems
NDMP Enable on all storage systems, including vFiler. You can verify that the NDMP service is enabled with the following NetApp command: <pre>ndmpd status</pre> On the OnCommand Unified Manager, make sure that the NDMP Status is Up and that the NDMP credentials are Good.	No	Enable	Enable

About using NetApp SAN-connected storage with Replication Director

Use Replication Director to back up NetApp block data on SAN-connected storage using Fibre Channel or iSCSI.

If the same LUN is accessible through iSCSI and Fibre Channel, Fibre Channel is used to mount the LUN.

If using the iSCSI protocol, establish sessions with the disk array using the CHAP security protocol. The client and the alternate client may have sessions with different users. The different sessions do not affect snapshot imports and restores, and do not affect the following operations: **Snapshot**, **Replication**, and **Backup From Snapshot**. If a session is already established on the alternate client, the LUN is exposed to that host without any CHAP authentication.

See the following topics for iSCSI setup information:

- See “[Using SnapDrive for iSCSI setup on Windows](#)” on page 128.
- iSCSI initiator configuration on Red Hat Enterprise Linux (RHEL) for Replication Director
<http://www.veritas.com/docs/TECH228275>
- Configuring the primary NetApp device to use VSS with Replication Director
<http://www.veritas.com/docs/TECH228279>

Note: For iSCSI to support block devices, make sure that no HBA cards are attached to the host.

Using SnapDrive for iSCSI setup on Windows

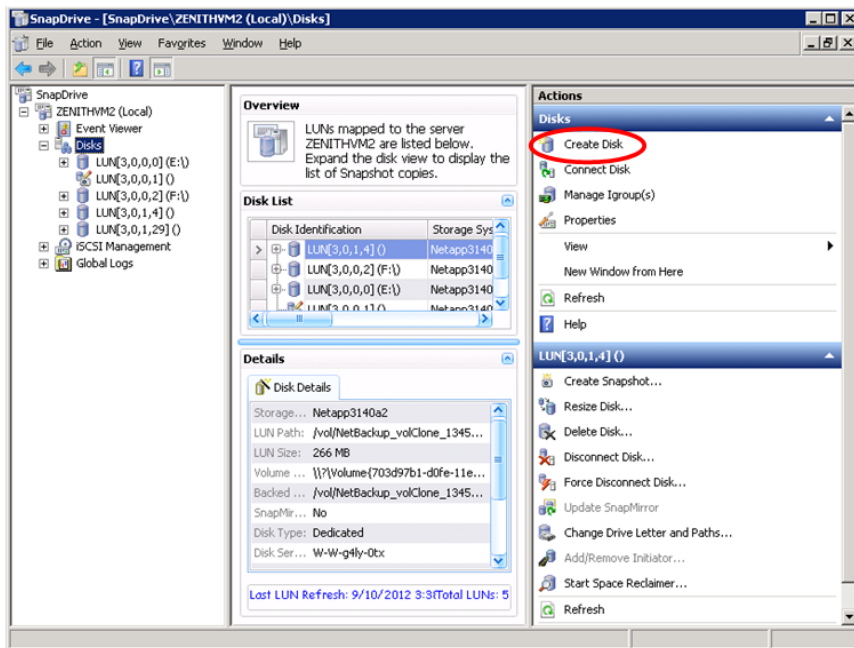
Use the NetApp SnapDrive software to simplify iSCSI setup on Windows hosts. See the following NetApp documentation for the most complete instructions. Instructions are listed here for ease of use.

For additional information, see: [SnapDrive 6.5 for Windows Installation and Administration Guide](#).

Configuration is done on the host where the data resides. This is the host that is used to access the data.

To use SnapDrive to simplify iSCSI setup on Windows

- 1 Enable iSCSI on each storage system.
- 2 Windows iSCSI Initiator is included with Windows 2008 R2 but must be enabled. (It must be installed separately for Windows 2003.)
- 3 Install NetApp SnapDrive.
- 4 Create the NetApp volume.
- 5 Use SnapDrive to establish a connection to the target storage system.
- 6 In the NetApp SnapDrive console, select the **Create Disk** action to start the **Create Disk Wizard**. The wizard helps to create LUNs and to map the LUN to a local drive letter.



SAN-connected storage limitations

These items are limitations to consider when using SAN-connected NetApp storage with Replication Director:

- The following are not supported:
 - Windows boot file system on SAN.
 - RAW disks (on both Windows and UNIX).
 - Dynamic disks on Windows.
 - Fibre Channel over Ethernet (FCoE) protocol.
 - Point-in-time rollback restores are not supported when using SAN-connected devices.
 - Using the volume GUID to indicate the backup selection.
 - Fibre Channel LUNs on vfiler.
- Per the SnapDrive limit, a maximum of 168 LUNs per client is allowed, including LUN and volume clones.

If the OnCommand Unified Manager root or administrator password has changed

If the root or the administrator password for the OnCommand Unified Manager is changed, you must also perform the following actions:

- Use the `tpconfig` command to update the storage server password in NetBackup.

On Windows:

```
Install_path\Veritas\NetBackup\Volmgr\bin\tpconfig -update  
-storage_server sshostname -stype server_type -sts_user_id UserID  
-password Password
```

On UNIX:

```
usr/openv/volmgr/bin/tpconfig -update -storage_server sshostname  
-stype server_type -sts_user_id UserID -password Password
```

The `server_type` is the vendor-provided string that identifies the type of storage server. In the case of NetApp, enter `Network_NTAP`.

Note: The `server_type` is case-sensitive.

- Restart the NBUPlugin service.

The `processmanager` command can be used.

On Windows:

```
Install_path\Program Files\NetApp\NBUPlugin\ProcessManager.exe  
shutdown  
Install_path\Program Files\NetApp\NBUPlugin\ProcessManager.exe  
startup
```

On UNIX:

```
/usr/Netapp/NBUPlugin/processmanager shutdown  
/usr/Netapp/NBUPlugin/processmanager startup
```

A replication job run after the password has been changed may fail with a status 83 (media open error) or a policy validation error of 4225. However, the job details may indicate that the job ran successfully.

Considerations when configuring an OnCommand Unified Manager as a NetBackup storage server

The following items are OCUM-specific and are helpful when configuring an OCUM as a storage server.

Storage server type

Select **NetApp OnCommand server (7-mode)** to create a storage server (for either NAS volumes or SAN devices).

By default, the storage server has 5 minutes to communicate with NetBackup before it times out. When creating a NetApp storage server (type NETWORK_NTAP), more time may be required. To increase the timeout, edit the `nbsl.xml` file, the configuration file that interacts with the NetBackup Service Layer process (NBSL).

Locate the `nbsl.xml` file in the following directory:

On Windows: `C:\Program Files\Veritas\NetBackup\var\global\nbsl.xml`

On UNIX: `/opt/opensv/var/global/nbsl.xml`

Find the entry for `TPCommandTimeout` and change the default from 300 to a greater value. For example:

```
TPCommandTimeout="600"
```

After making the change, restart the NBSL process so that the change takes effect.

Determining whether the OCUM server name is fully qualified or short

Use the `bpstsinfo` command to verify whether a short name or a fully qualified name is used for the storage server. The command is located in the following directory:

- Windows: `Install_path\NetBackup\bin\admincmd\`
- UNIX: `/usr/opensv/netbackup/bin/admincmd/`

Enter the `bpstsinfo` command as follows:

```
bpstsinfo -serverinfo -storage_server known_storage_server_name -stype
storage_server_type
```

For example, to ensure that the name of the OnCommand Unified Manager is `OCUMServer`, enter the following command:

```
bpstsinfo -serverinfo -storage_server OCUMServer -stype Network_NTAP
```

Use the storage server name that is indicated in the output.

Regarding disk pools for OnCommand Unified Manager storage servers

In the **Disk Pool Configuration Wizard**

- The total sizes on the primary volume always display as 0 bytes, as indicated by a dash.

- When the NBUPugin is installed on the OnCommand Unified Manager, a NetBackup group is automatically created on the OnCommand Unified Manager. On the OnCommand Unified Manager, use the NetApp Management Console to add resource pools to the NetBackup group so that the resource pools are exposed to NetBackup. If the NetBackup group does not contain resource pools, no LSUs display in the disk pool configuration wizard.
The available size that is listed is the total amount of space available in the pool. The raw size is the total raw, unformatted size of the storage in the disk pool. For OnCommand Unified Managers, the sizes on the primary volume always display as 0 bytes, as indicated by a dash.

Importing existing NetApp relationships for NetBackup control

NetApp offers an import tool to migrate OnCommand Unified Manager data sets and Data ONTAP relationships into NetBackup. Once in NetBackup, the snapshot data can be managed using Replication Director.

The NetApp import tool allows the administrator to perform the following actions:

- Export the data set configuration from the OnCommand Unified Manager into an XML file.
- Edit the XML file to change the backup policies or topology.
- Import the XML file into NetBackup.

For more information on the import tool, see the *NetApp Plug-in for Veritas NetBackup Installation and Administration Guide*, available from the [NetApp Support Site](#).

Enabling Unicode and language settings on NetApp disk arrays

Enable Unicode on each volume of the storage system. Use the NetApp `vol` command options to enable `convert_unicode` and `create_unicode` on all NetApp storage:

- `convert_unicode on`
Forces the conversion of all directories to Unicode format.
- `create_unicode on`
Forces the creation of Unicode directories by default.

Enable the volume language setting using UTF-8 so that the correct language format is used for the NAS data.

Note: Replication Director does not support widelinks in a CIFS environment on NetApp disk arrays.

Using NetApp Clustered Data ONTAP with Replication Director

Replication Director for NetBackup 7.7 supports the NetApp Clustered Data ONTAP operating system versions 8.2 and 8.3. Upgrade your master server, any media servers, and any NetBackup clients to NetBackup 7.7 to protect the data in a Clustered Data ONTAP environment using the existing Replication Director tools and features.

Replication Director requires the NetApp OnCommand Unified Manager for Clustered Data ONTAP 6.x for Clustered Data ONTAP support. The Clustered Data ONTAP operating system lets you host Storage Virtual Machines (SVMs, formerly known as Vservers). When you create backup policies in NetBackup, you work with volumes on SVMs. Use Replication Director to protect volumes on SVMs with snapshot, replication, and backup operations. You can replicate volumes to an SVM residing on the same cluster as the source SVM or to a different cluster entirely (inter-cluster replication).

NetApp developed an OST plug-in for Clustered Data ONTAP called the NBUPlugin 2.0. You install the NBUPlugin 2.0 to allow Replication Director to work with Clustered Data ONTAP. The plug-in cannot be installed on the OnCommand Unified Manager server, the master server, or any media servers. You must install the plug-in on a separate Windows or Linux computer.

See [“Configuration overview: NetApp Clustered Data ONTAP with Replication Director”](#) on page 134.

See [“Licenses required for NetApp Clustered Data ONTAP with Replication Director”](#) on page 135.

See [“Software required to use NetApp Clustered Data ONTAP with Replication Director”](#) on page 137.

See [“Configuring Replication Director to work with Clustered Data ONTAP”](#) on page 138.

See [“Limitations to using Clustered Data ONTAP with Replication Director”](#) on page 150.

Configuration overview: NetApp Clustered Data ONTAP with Replication Director

The following table lists the general configuration steps necessary to set up NetApp Clustered Data ONTAP with Replication Director.

Table 10-8 NetApp Clustered Data ONTAP with Replication Director configuration tasks overview*

Description	Reference topics
NetApp ONTAP Cluster	1 Install a supported version of NetApp ONTAP Cluster on the cluster storage system with the appropriate licenses. 2 Set up any Storage Virtual Machines (SVMs). ■ Add any required protocols (for example CIFS, NFS, NDMP). ■ Assign logical interfaces. ■ Create export policies for NFS volumes and export shares for CIFS. See NetApp documentation.
OnCommand Unified Manager for Clustered Data ONTAP	1 Deploy the OnCommand Unified Manager, version 6.x. 2 Add the cluster. 3 Configure Resource Pools for the replication target. Configure resource pools in the OnCommand Unified Manager and add aggregates to the resource pools. Create a resource pool for each replication target. An aggregate can belong to a single resource pool. Do not create a resource pool for the source or primary data; that is handled automatically. NetBackup can now access the resource pools as disk volumes during the NetBackup disk pool creation step. 4 Create required Storage Virtual Machine associations. See NetApp documentation.
Enable and turn on NetApp licenses, which can include the following: ■ SnapMirror ■ SnapVault ■ SnapRestore	See NetApp documentation. Not all licenses may be necessary.

Table 10-8 NetApp Clustered Data ONTAP with Replication Director configuration tasks overview* (*continued*)

Description	Reference topics
Install the NetApp Plug-in for Veritas NetBackup 2.0 (NBUPugin2.0).	1 Install the plug-in on either a Windows or a Linux computer other than the OnCommand Unified Manager server, the master server, or any media servers. This computer becomes the storage server in NetBackup. 2 Configure the plug-in to point to the OnCommand Unified Manager server. The plug-in uses port 8086 by default. See NetApp documentation. See “Using NetApp disk arrays with Replication Director” on page 113.
Install necessary licenses on NAS systems: ■ CIFS licenses for MS-Windows policies ■ NFS licenses for Standard policies	See NetApp documentation .
Configure IPv6 if necessary. By default, the NBUPugin is configured for IPv4.	See NetApp documentation .

*See the NetApp Interoperability Matrix Tool for the latest information about supported versions.

See “[Using NetApp Clustered Data ONTAP with Replication Director](#)” on page 133.

See “[Licenses required for NetApp Clustered Data ONTAP with Replication Director](#)” on page 135.

See “[Software required to use NetApp Clustered Data ONTAP with Replication Director](#)” on page 137.

Licenses required for NetApp Clustered Data ONTAP with Replication Director

The NetApp licenses that are required for storage systems depends on the replication configuration in use.

Table 10-9 NetApp licenses required on storage systems*

License	On primary	Primary to SnapMirror destination	SnapVault destination	SnapVault to SnapMirror destination	Notes
SnapMirror	Only if SnapMirror Source	Yes	Only if SnapMirror source	Yes	Use to create mirrored snapshots. Install the license on both the source and the destination storage systems in a SnapMirror relationship. Enable SnapMirror access between storage systems. Install and enable the license on both the source and the destination storage systems in a SnapMirror relationship. Allow access between source and all targets.
SnapVault	Only if SnapVault source		Yes	No	Use to create a SnapVault snapshot copy on the primary or the secondary storage system. Install and enable the SnapVault license on the SnapVault source and destination storage systems. Older platforms have separate SnapVault primary licenses for SnapVault primary (source) and secondary (designation) storage systems.
SnapRestore	Optional for fast FlexVol level restores	No	Yes		Install the SnapRestore license on all the source storage systems to enable fast pointer-based FlexVol-level restores from primary snapshots. SnapRestore is required on all SnapVault destination storage systems. For the Primary-SnapVault-SnapMirror cascade (PVM) topology, install the license on the SnapMirror destination storage system. Without a SnapRestore license, NetBackup performs a copy-back restore.
CIFS	CIFS NAS data only (Windows)				Install the CIFS license on the storage system that contains the SVM that is in the SnapMirror or SnapVault relationship with the CIFS file systems.

Table 10-9 NetApp licenses required on storage systems* (*continued*)

License	On primary	Primary to SnapMirror destination	SnapVault destination	SnapVault to SnapMirror destination	Notes
NFS	NFS NAS data only (UNIX)				Install the NFS license on the storage system that contains the SVM that is in the SnapMirror or SnapVault relationship with the NFS file systems.

*See the NetApp Interoperability Matrix Tool for the latest information about supported versions.

See [“Using NetApp Clustered Data ONTAP with Replication Director”](#) on page 133.

See [“Configuration overview: NetApp Clustered Data ONTAP with Replication Director”](#) on page 134.

Software required to use NetApp Clustered Data ONTAP with Replication Director

The following NetApp software is required to use Replication Director.

Table 10-10 NetApp software required for Replication Director

Configuration	Applies to OnCommand Unified Manager?	Primary cluster storage system	Secondary cluster storage systems
NetApp cluster storage systems Must be added to the OnCommand Unified Manager.	No	Yes	Yes
CIFS Applies to Windows only; NAS only.	No	Yes	Yes
NFS Applies to UNIX only; NAS only.	No	Yes	Yes

Table 10-10 NetApp software required for Replication Director (*continued*)

Configuration	Applies to OnCommand Unified Manager?	Primary cluster storage system	Secondary cluster storage systems
NDMP Make sure that the NDMP service is enabled on any Storage Virtual Machines (SVMs) that you want to back up. You can verify that the NDMP service is enabled with the following NetApp command: <pre>vserver services ndmp show</pre> Make sure that the node-scoped NDMP is disabled. You can verify that node-scoped NDMP is disabled with the following NetApp command: <pre>system services ndmp node-scope-mode status</pre>	No	Enable	Enable
Settings for all storage systems See the NetApp documentation for information about configuring the settings on all storage systems.	No	Yes	Yes
Settings for OnCommand Unified Manager See the NetApp documentation for information about configuring the settings on the OnCommand Unified Manager.	Yes	No	No

See “Using NetApp Clustered Data ONTAP with Replication Director” on page 133.

See “Configuration overview: NetApp Clustered Data ONTAP with Replication Director” on page 134.

Configuring Replication Director to work with Clustered Data ONTAP

Once you have installed NetApp ONTAP Cluster and configured the OnCommand Unified Manager server and any other NetApp components, you can configure Replication Director to work with Clustered Data ONTAP.

To configure Replication Director to work with Clustered Data ONTAP

- 1 In NetBackup, use the Storage Server Configuration Wizard to create a storage server. When the wizard prompts you for the storage server details, enter the information for the computer on which the NBUPlugin 2.0 is installed.

Storage server type:

Storage server name:

Enter storage server credentials

User name:

Password:

Confirm password:

Selection for cluster mode

Host name or IP for computer with NBUPlugin 2.0 installed

OnCommand Unified Manager server credentials

See the following topic for additional information:

See [“Creating a NetBackup storage server for snapshot replication”](#) on page 18.

- 2 As part of the Storage Server Configuration Wizard, configure disk pools and storage units for the primary snapshot.
- 3 Configure disk pools and storage units for the replication target.
See [“Creating disk pools for snapshot replication”](#) on page 29.
- 4 Configure the storage and create storage units for any media (for example tape or AdvancedDisk) if you want to perform a **Backup From Snapshot** operation.
- 5 Create the storage lifecycle policy.
See [“Creating a storage lifecycle policy for snapshots and snapshot replication”](#) on page 52.
- 6 Configure the client with any necessary policy-specific modifications. For example, you can create NFS mount-points that refer to a volume on a Storage Virtual Machine (SVM).
- 7 Create any necessary backup policies.

See [“About creating backup policies for Clustered Data ONTAP with Replication Director”](#) on page 140.

See [“Using NetApp Clustered Data ONTAP with Replication Director”](#) on page 133.

See [“Protecting volumes with nested junctions for Clustered Data ONTAP”](#) on page 148.

See [“Limitations to using Clustered Data ONTAP with Replication Director”](#) on page 150.

About creating backup policies for Clustered Data ONTAP with Replication Director

Keep in mind the following considerations when you configure backup policies for Clustered Data ONTAP with Replication Director.

Table 10-11 Backup policies for Clustered Data ONTAP

Policy type	Considerations
Standard	For a Standard policy, make sure that the Storage Virtual Machine (SVM) can resolve the NetBackup client's host name by running the following command on the cluster shell: <pre>network ping -lif-owner vserver -lif lif-name -destination NetBackup-client</pre> When you create a mount point, you should keep the following in mind: ■ If the SVM name is used to create a mount point for a volume that is exported by an SVM on the NetBackup client, you should enter the name of the SVM exactly as the OnCommand Unified Manager sees it. If the SVM name in the OnCommand Unified Manager is a fully qualified domain name, you must use the SVM's fully qualified domain name when you create the mount point. The name is case-sensitive. ■ Alternatively, you can use the IP address of the SVM LIF to specify a mount point instead of the SVM name. Consider the following examples: ■ When you create a mount point on the NetBackup client for volume "vol_nfs" that is exported by an SVM named "vs1", the nfs volume name must be specified as "vs1:/vol_nfs". You would use the command "mount vs1:/vol_nfs /mnt/vol_nfs". If you specify the nfs volume name as "VS1:/vol_nfs" or "vs1.example.com:/vol_nfs" then the snapshot job fails. ■ When you create a mount point on the NetBackup client for volume "vol_nfs2" that is exported by an SVM named "VS2.example.com", the nfs volume name must be specified as "VS2.example.com:/vol_nfs2". You would use the command "mount VS2.example.com:/vol_nfs2 /mnt/vol_nfs2". If you specify the nfs volume name as "vs2.example.com:/vol_nfs2" or "VS2:/vol_nfs2" then the snapshot job fails. ■ When you create a mount point on the NetBackup client for volume "vol_nfs3" that is exported by an SVM with the LIF "10.67.212.20", the nfs volume name must be specified as "10.67.212.20:/vol_nfs3". You would use the command "mount 10.67.212.20:/vol_nfs3 /mnt/vol_nfs3". See "Configuring a Standard or MS-Windows policy to protect NAS volumes or SAN-connected devices" on page 84. Note: Replication Director for NetApp Clustered Data ONTAP supports NAS only at this time.

Table 10-11 Backup policies for Clustered Data ONTAP (*continued*)

Policy type	Considerations
MS-Windows	For a MS-Windows policy, make sure that clocks are in sync for the following: the domain controller that is used for the Storage Virtual Machine's (SVM) CIFS server and the cluster hosting the SVM. Make sure that the NetBackup Client Service and the NetBackup Legacy Client Service are running under an account which has read and write access to the shares that the SVM exports. When you create a mount point, you should keep the following in mind: ■ If the SVM name is used to specify a share that is exported by an SVM in a policy, you should enter the name of the SVM exactly as the OnCommand Unified Manager sees it. If the SVM name in the OnCommand Unified Manager is a fully qualified domain name, you must use the SVM's fully qualified domain name when you create the mount point. The name is case-sensitive. ■ Alternatively, you can use the IP address of the SVM LIF to specify a share instead of the SVM name. Consider the following examples: ■ When you select a share "vol_cifs" that is exported by an SVM named "vs1" as a backup selection, the selection must be entered as "\\vs1\vol_cifs". If you enter the backup selection as "\\VS1\vol_cifs" or \\vs1.example.com\vol_cifs" then the snapshot job fails. ■ When you select a share "vol_cifs2" that is exported by an SVM named "VS2.example.com" as a backup selection, the selection must be entered as "\\VS2.example.com\vol_cifs2". If you enter the backup selection as "\\VS2\vol_cifs2" or "\\vs2.example.com\vol_cifs2" then the snapshot job fails. ■ When you select a share "vol_cifs2" that is exported by an SVM with the LIF "10.67.212.20" as a backup selection, the selection must be entered as "\\10.67.212.20\vol_cifs3". See "Configuring a Standard or MS-Windows policy to protect NAS volumes or SAN-connected devices" on page 84. Note: Replication Director for NetApp Clustered Data ONTAP supports NAS only at this time.

Table 10-11 Backup policies for Clustered Data ONTAP (*continued*)

Policy type	Considerations
Standard or MS-Windows with NDMP Data Mover enabled	For a Standard policy with NDMP Data Mover enabled: ■ The Storage Virtual Machine (SVM) must be added as an NDMP host in NetBackup. ■ You should keep in mind the following naming conventions: ■ The junction name cannot be different from the volume name. When you mount the volume in the SVM's namespace, make sure that the junction name is the same as the volume name. For example, if you have a volume "vol_nfs" on the SVM "vs1", you should use the junction name "vol_nfs" when you mount the volume. ■ The mount path must use the host name as the SVM name. The SVM name must be spelled out exactly as it appears in the OnCommand Unified Manager. You cannot use the IP address of a data LIF when you mount an SVM's volumes. For example, the mount point "/mnt/vol_nfs" on the NetBackup client refers to "vs1:/vol_nfs", where vs1 is the SVM name and "vol_nfs" is the junction path for the volume "vol_nfs". For a Windows policy with NDMP Data Mover enabled: ■ The SVM must be added as an NDMP host in NetBackup. ■ You should keep in mind the following naming conventions: ■ Any share that is created as an export volume must have the same name as the volume name. For example, the volume "cifs_vol" on SVM "vs1" must be exported using the share name "cifs_vol". The name is case-sensitive. ■ The share name must use the host name as the SVM name. The SVM name must be spelled out exactly as it appears in the OnCommand Unified Manager. You cannot use the IP address of a data LIF as the share name. For example, the share "cifs_vol" on the SVM "vs1", must be specified as "\\vs1\cifs_vol". See "Configuring a Standard or MS-Windows policy to protect clients using NDMP with Data Mover" on page 81.

Table 10-11 Backup policies for Clustered Data ONTAP *(continued)*

Policy type	Considerations
NDMP	

Table 10-11 Backup policies for Clustered Data ONTAP (*continued*)

Policy type	Considerations
	■ Make sure that the node-scoped NDMP is disabled: <code>system services ndmp node-scope-mode off</code> <code>system services ndmp node-scope-mode status</code> ■ To generate a password for the NDMP user, run the following command: <code>vserver services ndmp generate-password -vserver vserver_name -user user</code> ■ Remote NDMP and three-way NDMP backups are supported for Clustered Data ONTAP Backup From Snapshot operations. To perform three-way backup operations, any devices and storage units must be configured for the tape devices that are attached to the clustered storage system. You must add the NDMP host using the cluster-management LIF in NetBackup. After the storage units are configured for the cluster storage system, they can be used as the destination in an SLP for three-way backups. Refer to the <i>NetBackup NDMP Administrator's Guide</i> for more information. ■ Add the Storage Virtual Machine (SVM) as an NDMP host in NetBackup. You must enter the SVM name exactly as the OnCommand Unified Manager sees it when you create the policy. For example, if the SVM name in the OnCommand Unified Manager is a fully qualified domain name, you must use the SVM's fully qualified domain name when you create the policy. The entry is case-sensitive. When you select a volume named "vol_nfs" that is on an SVM named "vs1" as a backup selection, the selection must be entered as "/vs1/vol_nfs". Alternatively, you can use the IP address of a LIF belonging to the SVM to configure a backup policy for NDMP. ■ For the Backup From Snapshot operation to work correctly, make sure that an Intercluster LIF is created on each node of the cluster. You should enable a firewall policy for NDMP service on the Intercluster LIF: ■ You can use following NetApp command to verify that the firewall policy is enabled for NDMP: <code>system services firewall policy show-policy intercluster</code> Make sure that the NDMP services are allowed for the "intercluster" policy. If the "Allowed" column displays "0.0.0.0/0", it means that the firewall policy is enabled and that all clients can connect to the NDMP service on the Intercluster LIF. ■ If the firewall policy is not enabled for NDMP, use the following NetApp command to enable it: <code>system services firewall policy modify -vserver cluster1 -policy intercluster -service ndmp 0.0.0.0/0</code> ■ The destination SVM must be added as an NDMP host in NetBackup for Backup From Snapshot to work from a replica. ■ For a Live Browse to work, enable the following extension on Clustered ONTAP

Table 10-11 Backup policies for Clustered Data ONTAP (*continued*)

Policy type	Considerations
	8.3: <pre>set advanced vserver services ndmp extensions modify -is-extension-0x2050-enabled true</pre> ■ If you use the <code>ALL_FILESYSTEMS</code> directive in an NDMP policy for Clustered Data ONTAP, you must exclude the SVM's root volume using the <code>VOLUME_EXCLUDE_LIST</code> directive. For example, to exclude the root volume "root_vs1" of the SVM "VS1" you would use the following directive: <pre>VOLUME_EXCLUDE_LIST=/VS1/root_vs1 ALL_FILESYSTEMS</pre> For more information, refer to the following topic: See "ALL_FILESYSTEMS and VOLUME_EXCLUDE_LIST directives" on page 91. ■ To enable indexing, you must add a disk array host to NetBackup. Complete the steps in the following procedure: See "Configuring indexing for an NDMP policy" on page 66. See "Configuring an NDMP policy to protect a NAS host" on page 77.

Table 10-11 Backup policies for Clustered Data ONTAP (*continued*)

Policy type	Considerations
VMware	When you create an NFS datastore on a VMware ESX host and the datastore refers to a volume that the SVM exported, the server name must be entered exactly as it appears in the OnCommand Unified Manager. The server name entry refers to the SVM name. This entry is case-sensitive. If the server name is not entered correctly, the NetBackup snapshot job fails. Alternatively, you can use the IP address of the SVM LIF to specify a server name instead of the SVM name. If the NetBackup VMware host is a Windows computer, make sure that the appropriate name-mapping rule is created on the SVM that exports the volume for the VMware datastore. The name-mapping rule should map the user under which the NetBackup Client Service is running to the UNIX user "root". For example, SVM1 is a storage virtual machine that exports a volume to the ESX NFS datastore. You should create a Windows-UNIX name-mapping rule on SVM1 that maps the Windows user "DOMAINNAME1\Administrator" to the UNIX user "root", where "DOMAINNAME1\Administrator" is the account for NetBackup Client service on the VMware backup host. You should create similar name-mapping rules on any other peer SVMs where replicated volumes are created. Refer to the following NetApp document for more information: https://kb.netapp.com/support/index?page=content&id=1013831&actp=RSS Refer to the following topic for more information about configuring VMware backup policies: See "Configuring a policy for virtual machines to use Replication Director" on page 169.
Oracle	Oracle provides specific requirements for the mount commands that you use when you mount Oracle database components to NetApp filers. Refer to your Oracle documentation for more information. When you create a mount point for Oracle operations, you must use an NFS version 3 volume. Make sure that the volume is created using the parameters that are specified in the Oracle documentation. Oracle backup policies may only include any data files that exist on the filer mount point. Backup selections can include tablespaces, individual data files, or whole databases so long as they exist on the filer mount point. If backup selections include any file other than a data file or any files that do not exist on the mount point, the backup operations fail. Refer to the following topics for more information about configuring Oracle backup policies: ■ See "Configuring an Oracle Intelligent Policy" on page 152. ■ See "Configuring a script- or template-based Oracle policy" on page 158.

See ["Using NetApp Clustered Data ONTAP with Replication Director"](#) on page 133.

See [“Protecting volumes with nested junctions for Clustered Data ONTAP”](#) on page 148.

See [“Limitations to using Clustered Data ONTAP with Replication Director”](#) on page 150.

Protecting volumes with nested junctions for Clustered Data ONTAP

When you snapshot or replicate volumes, any mounted volumes that reside under the top-level volume are not necessarily protected. You should consider the following example scenarios when you create backup policies for volumes with nested junctions.

You may have a volume that is mounted under another volume, as in the example below. Volume B is mounted under Volume A in the SVM VS1's namespace.

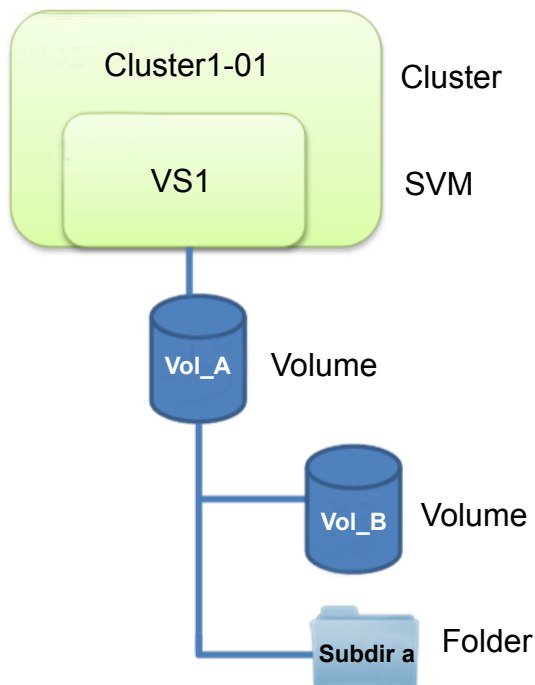


Table 10-12 To protect volumes with nested junctions

Policy type	Level	Protection strategy
Standard	Top level	To protect the top-level volume in a Standard policy: ■ Create an NFS mount point for the volume "vs1:/vol_A" on the NetBackup client. For the example above, you would create the mount point "/mnt/vs1_vol_A". ■ Create the Standard policy and use "/mnt/vs1_vol_A" as the backup selection. Any snapshot operations or replication operations now protect "vs1:/vol_A". An empty directory for vol_B is created under the replica of vol_A, however vol_B is not protected.
Standard	Lower level	To protect the lower level volume in a Standard policy: ■ Create an NFS mount point for the volume "vs1:/vol_A/vol_B" on the NetBackup client. For the example above, you would create the mount point "/mnt/vs1_vol_B". ■ Create the Standard policy and use "/mnt/vs1_vol_B" as the backup selection. Any snapshot operations or replication operations now protect "vs1:/vol_A/vol_B".
Windows	Top level	To protect the top-level volume in a Windows policy, specify the backup selection as "\\vs1\vol_A" where "vol_A" represents the share that is exported for "vol_A". Any snapshot operations or replication operations now protect "vol_A". An empty directory for vol_B is created under the replica of vol_A, however vol_B is not protected.
Windows	Lower level	To protect the lower level volume in a Windows policy, specify the backup selection as "\\vs1\vol_B" where "vol_B" represents the share that is exported for "vol_B". The volume, "vol_B" is mounted under "vol_A". Any snapshot operations or replication operations now protect "vol_B".

See [“Using NetApp Clustered Data ONTAP with Replication Director”](#) on page 133.

See [“About creating backup policies for Clustered Data ONTAP with Replication Director”](#) on page 140.

Limitations to using Clustered Data ONTAP with Replication Director

Consider the following limitations before you configure Clustered Data ONTAP to work with Replication Director:

- Replication Director with Clustered Data ONTAP supports NAS only. Currently, it does not support SAN.
- Replication Director does not support Storage Virtual Machine (SVM) root volume protection.
- Replication Director does not support Infinite volumes.
- NetApp Clustered Data ONTAP does not support qtree-level, SnapVault replication. 7-mode supports qtree-level replication, however.
- Clustered Data ONTAP SnapVault only supports volume level replication

The following limitations concern using Clustered Data ONTAP with NDMP:

- NDMP Live Browse is supported with Clustered Data ONTAP 8.3 and higher only.
For Clustered Data ONTAP 8.2, you can select the **Index From Snapshot** option for any NDMP policies, so that you can search images for backed up data.
- Snapshot and Replication SLP workflows do not support NDMP backups to local, node-attached tape devices.
- Replication Director enabled NDMP policies only support any NDMP hosts that are added using data LIFs. Any NDMP hosts that are added using Cluster-management or Intercluster LIFs are not supported as Replication Director enabled policies.
- NDMP policies fail if you do not enter the SVM name exactly as the OnCommand Unified Manager sees it when you create the policy. For example, if the SVM name in the OnCommand Unified Manager is a fully qualified domain name, you must use the SVM's fully qualified domain name when you create the policy. The entry is case-sensitive.

See [“Using NetApp Clustered Data ONTAP with Replication Director”](#) on page 133.

Using Oracle with Replication Director

This chapter includes the following topics:

- [Requirements for Oracle support](#)
- [About Oracle support for Replication Director](#)

Requirements for Oracle support

Oracle support for Replication Director allows the backup and restore of snapshots of the Oracle database.

The following software is required:

- Oracle Extension.
- NetBackup Snapshot Client.

Currently, support is for NetApp NAS on UNIX platforms only.

The Oracle database must be installed on the NetApp disk array.

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”](#) on page 152.
- Create a script- or template-based Oracle policy.
See [“Configuring a script- or template-based Oracle policy”](#) on page 158.

[Table 11-1](#) describes the differences between the two methods:

Table 11-1 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

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.

Only those policy options that are necessary to configure Replication Director are listed in the following procedure. For descriptions of all policy options, see the [NetBackup Administrator's Guide, Volume I](#) or the online Help.

For Oracle-specific information, see the *NetBackup for Oracle Administrator's Guide*.

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.

See "[NetBackup naming conventions](#)" on page 15.

- 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.

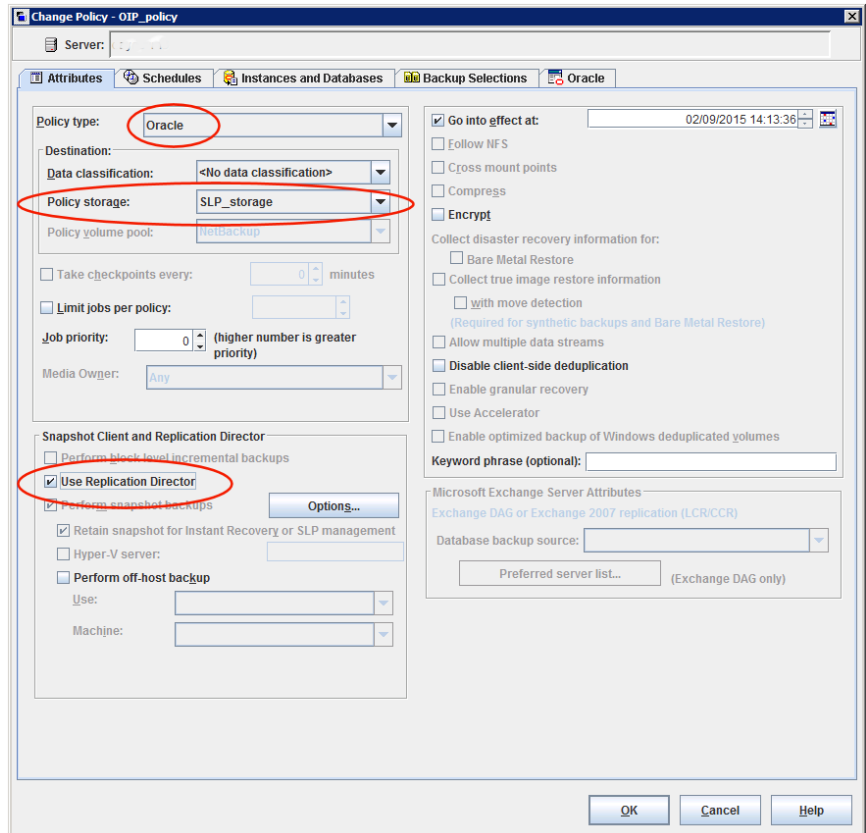
Maximum Snapshots Sets the maximum number of snapshots to be retained at one time.

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.

See [“Maximum snapshot limit retention type for SLP operations”](#) on page 73.

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

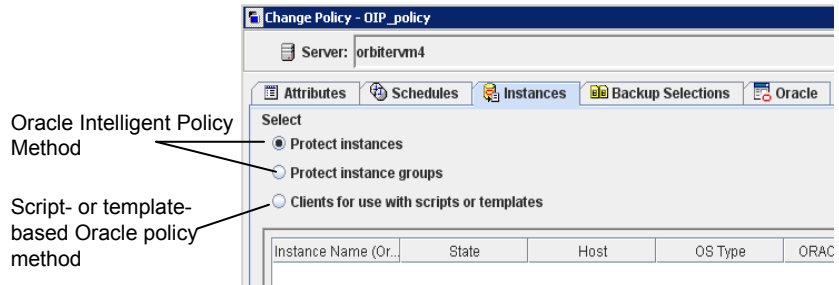
first operation is a snapshot operation.) This option must be enabled so that the schedule storage overrides the policy storage with a snapshot SLP.

- **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.

The screenshot shows the 'Add Schedule - Policy OIP_policy' dialog box. The 'Name' field contains 'Oracle_FULL_schedule'. The 'Type of backup' dropdown is set to 'Full Backup'. The 'Destination' section has 'Override policy storage selection' checked, and the 'Oracle_snapshot_SLP' dropdown is selected. The 'Retention' is set to 'Infinity (Retention Level 9)'. The 'Frequency' is set to '1 weeks'. The 'Instant Recovery' section has 'Snapshots and copy snapshots to a storage unit' selected. The 'OK' button is highlighted.

- 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.

Only those policy options that are necessary to configure Replication Director are listed in the following procedure. For descriptions of all policy options, see the [NetBackup Administrator's Guide, Volume I](#) or the online Help.

For Oracle-specific information, see the *NetBackup for Oracle Administrator's Guide*.

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.

See "[NetBackup naming conventions](#)" on page 15.

- 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

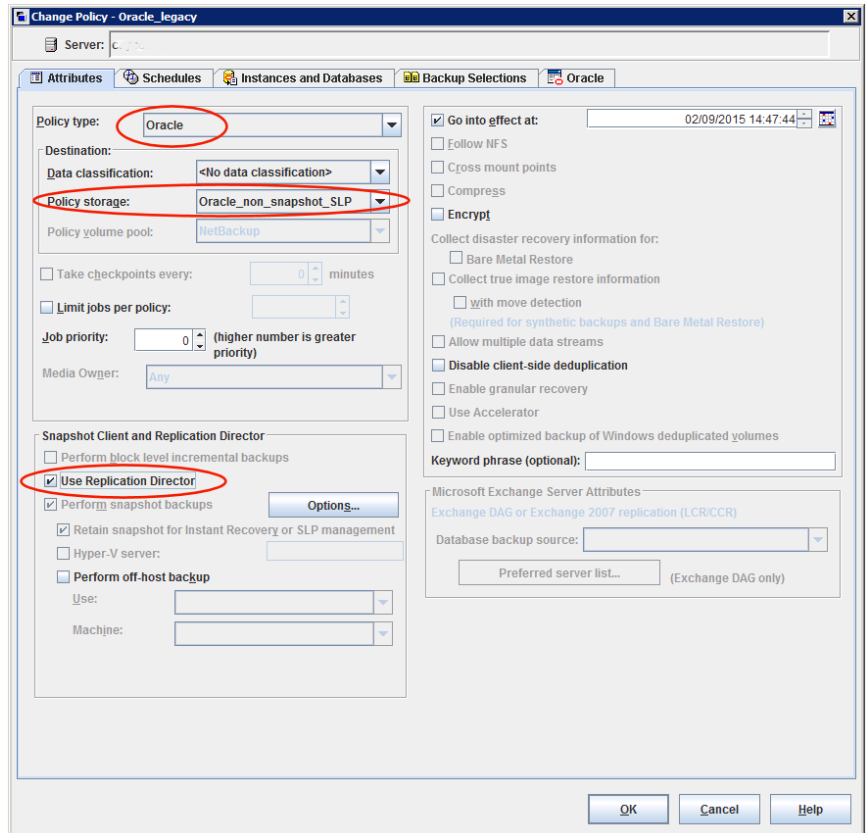
Sets the maximum number of snapshots to be retained at one time.

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.

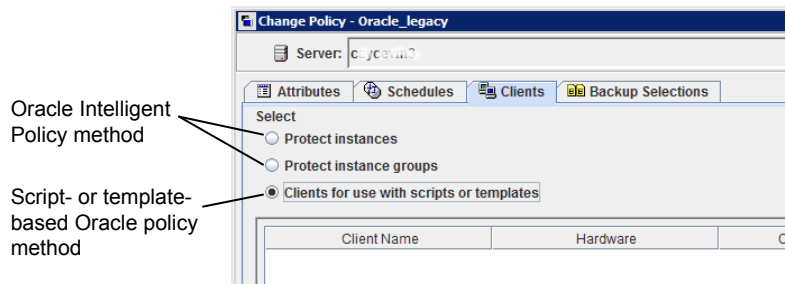
When the maximum is reached, snapshot rotation occurs: The next snapshot causes the oldest to be deleted.

See ["Maximum snapshot limit retention type for SLP operations"](#) on page 73.

Managed by SLP retention is automatically selected if the **Fixed** or the **Expire after Copy** retention is currently selected in the SLP.



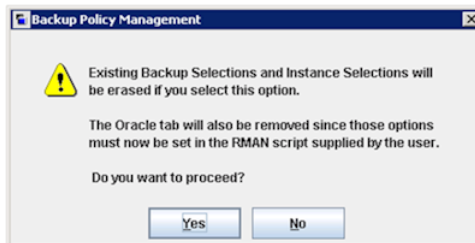
- 5 Select the **Instances and Databases** tab and specify the instances to back up. Select **Clients for use with scripts and templates**. If either of the other two are selected, the Oracle Intelligent Policy is used and the scripts are created automatically.



After selecting the **Clients for use with scripts and templates** option, a message appears that describes the effect of this choice:

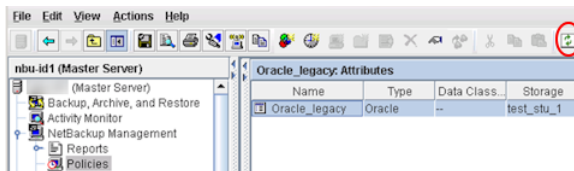
- Existing selections (if any) for this policy are erased.
- The **Oracle** tab is removed from this policy.
- Another effect is that the **Selections** tab turns into the **Clients** tab.

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.

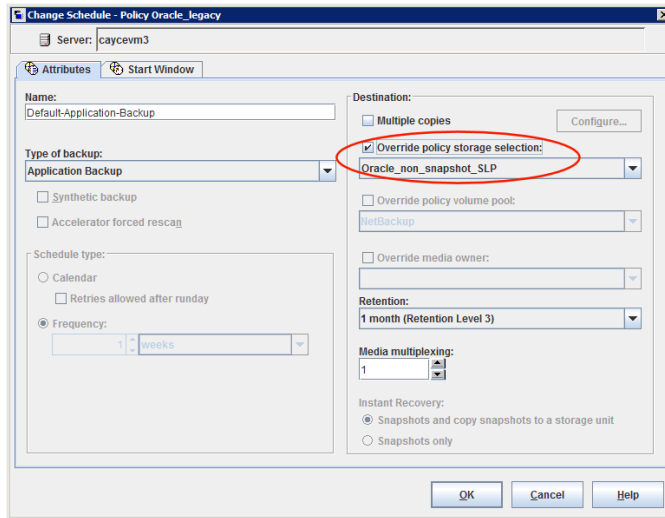


8 Re-open the policy and select the **Schedules** tab.

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.

Add Schedule - Policy Oracle

Server: TRUST

Attributes | Start Window | Exclude Dates

Name: Oracle_Full_Sched

Type of backup: Full Backup

☐ Synthetic backup

☐ Accelerator forced rescan

Schedule type:

☐ Calendar

☐ Retries allowed after runday

☒ Frequency: 1 weeks

Destination:

☐ Multiple copies

☒ Override policy storage selection: Oracle_snapshot_SLP

☐ Override policy volume pool: NetBackup

☐ Override media owner:

Retention: Determined by SLP

Media multiplexing: 1

Instant Recovery:

☒ Snapshots and copy snapshots to a storage unit

☐ Snapshots only

Add OK Cancel Help

- 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**.

Using Virtual Machines with Replication Director

This chapter includes the following topics:

- [Requirements for virtual machine support](#)
- [About virtual machines and Replication Director](#)

Requirements for virtual machine support

Virtual machines must have a NetBackup client installed.

Virtual machine support allows the backup and restore of snapshots of various VMware guests:

- VMware guests
- Exchange databases
- SQL Server

About virtual machines and Replication Director

Replication Director for NetBackup for VMware includes the following features for protecting the virtual machine snapshots and replicated copies:

- Creates an instantaneous hardware snapshot of virtual machines.
- Backs up the virtual machines from the snapshots at primary locations and from replicated snapshots at remote locations.
- Supports browsing of virtual machine snapshots.
- Restores a virtual machine from its vmdk files that are in a snapshot.

- Restores the individual files from the vmdk files in a snapshot.
- Supports the storage lifecycle policies.

Table 12-1 describes the scenarios for virtual machine protection with Replication Director.

Table 12-1 Examples of virtual machine protection with Replication Director

Operation	Description and notes
Make array-based snapshots of virtual machines on NFS datastores	Configure a storage lifecycle policy (SLP) and a backup policy to create array snapshots of virtual machines. The snapshots remain on the array or filer (NetBackup storage server) and are not backed up to a NetBackup media server storage unit. This type of backup is the foundation for the other Replication Director operations. Note the following: ■ The snapshots are created on NFS datastores only. ■ The virtual machine or its individual files can be restored directly from the snapshots on the storage server. The snapshots can also be replicated to other locations. ■ For faster browsing of files to restore, include the Index From Snapshot option in the SLP. This option catalogs the metadata of the virtual machine.
Back up quiesced virtual machines from a snapshot (or snapshot replica) that is on an NFS datastore	Configure an SLP and a backup policy to make a backup image from the virtual machine snapshot. NetBackup backs up only the virtual machines that were quiesced before the snapshot occurred. The backup image is written to a NetBackup storage unit. The image is retained according to the policy's retention period. Note: The Application consistent snapshot option in the policy must be enabled (under Options > Snapshot Client Options).
Restore a virtual machine from a snapshot (or snapshot replica) that is on an NFS datastore	Use the Backup, Archive, and Restore interface to restore the virtual machine. Supported restore destinations are the original (NFS) datastore or an alternate datastore (NFS or non-NFS).

Table 12-1 Examples of virtual machine protection with Replication Director
(continued)

Operation	Description and notes
Restore individual files from a snapshot (or snapshot replica) that is on an NFS datastore	Use the Backup, Archive, and Restore interface to restore the files. Note the following: ■ To restore files from a replica of the snapshot, the replica must exist in the same NetBackup domain as the snapshot. ■ To restore files to the original virtual machine, a NetBackup client must be installed on the original virtual machine. ■ As an alternative, you can use an alternate client to restore to a shared UNC location. You must manually copy the files back to the original location. See the topic on restoring individual files in the <i>NetBackup for VMware Guide</i>. ■ To restore multiple directories that have named streams, the Windows NetBackup client on the destination virtual machine must be at 7.6 or later.

For setting up Replication Director for virtual machines, the initial steps are the same as Replication Director for physical computers as follows:

- Verify that your backup environment contains the necessary hardware and software to configure and run Replication Director. Make sure you can successfully back up a physical computer with Replication Director.

Note: NDMP is not required for Replication Director and virtual machines.

- Install or upgrade NetBackup.
- Configure the following:
 - The disk array storage of the OpenStorage partner.
 - The NetBackup storage server.
 - The disk pool(s).
 - The NetBackup storage lifecycle policy (SLP).
Create a new operation in the SLP for each task that the SLP is to perform. For example, create a snapshot operation to perform the snapshot and a replication operation to copy the snapshot.
 - The NetBackup Client Service.
See [“Configuring the NetBackup Client Service”](#) on page 14.

More information is available on all the procedures for configuring a NetBackup environment that uses Replication Director:

See [“Configuration overview: NetApp 7-Mode with Replication Director”](#) on page 120.

The following table lists the additional steps that are required for Replication Director and virtual machines.

Table 12-2 Replication Director for virtual machines: Configuration tasks overview

Step	Description	Reference topic
1	Configure the virtual machine NFS datastores on the OpenStorage storage server. Replication Director makes the snapshots on these NFS datastores.	See the <i>NetBackup for VMware Guide</i> .
2	Add the VMware backup host to your NetBackup configuration.	See the topic on adding the VMware backup host to NetBackup, in the <i>NetBackup for VMware Guide</i> .
3	Configure NetBackup access credentials for the VMware vCenter server or ESX server.	See the topic on adding NetBackup credentials for VMware, in the <i>NetBackup for VMware Guide</i> .
4	Configure a NetBackup policy (VMware policy type) to perform the operations that are specified in the SLP.	See “Configuring a policy for virtual machines to use Replication Director” on page 169.

Notes on Replication Director for virtual machines

Note the following about Replication Director for virtual machines:

- For supported vCenter versions and datastores, see the NetBackup Software Compatibility List available from the following location:
[NetBackup Master Compatibility List](#)
- For additional support details, see the following Veritas tech note:
[Support for NetBackup 7.x in virtual environments](#)
- Replication Director for virtual machines does not support Accelerator.
- Instant Recovery supports disk storage units only. To use Instant Recovery to restore a VM that was backed up with Replication Director for virtual machines, note: The virtual machine backup must have been copied to a disk storage unit.
- Although applicable to Replication Director for physical computers, NDMP backup does not apply to Replication Director for virtual machines.
- Replication Director supports virtual machines on NetApp NFS datastores only.
- To create virtual machines on the NFS datastore, enter `anon=0` in the `/etc/exports` NetApp file on the NetBackup storage server. The `anon=0` entry is the equivalent of the `no_root_squash` option. See the following VMware document for more information on the `anon=0` entry:

Best Practices for running VMware vSphere on Network Attached Storage

- The NetApp OnCommand Unified Manager (formerly DataFabric Manager) must be able to resolve the host name that was used to mount the vCenter datastore. Hardware snapshots cannot succeed if the OnCommand server is unable to resolve the host name
- If the NetBackup master and media server are UNIX and the backup host is Windows, the backup host must have a fully qualified domain name. Otherwise, the backup fails.
- You must have a valid NFS export (share) for each qtree that is mounted as an NFS datastore.
- Supports restore of virtual machines and of individual files in virtual machines. Does not support volume-level rollback restore. (In the *Replication Director Solutions Guide*, references to rollback restore do not apply to virtual machines.)
- If the datastore name contains special characters, the datastore name in the backup image contains @ followed by the value of the special character. For example, a datastore that has the name “NFS datastore1” (with a space) appears in the NetBackup catalog as NFS@20datastore1.
- If changes occur to virtual machine configuration (such as adding, deleting, or moving VMDKs), it may be necessary to set **Reuse VM selection query results for** to 0. (**Reuse VM selection query results for** is on the policy **Clients** tab.) With a setting of 0, NetBackup rediscovers the virtual machines and their configuration each time the policy runs. Note: If the vmdk files are reconfigured and the next backup runs without rediscovery, NetBackup is not aware of the vmdk changes. It attempts to back up the virtual machines in their previous configuration. The result may be an incorrect backup.
- VMware vSphere uses the Space Efficient Virtual Disk (SEsparse) for snapshots of the disks that are larger than 2 TB. VMware's VDDK however does not support backup or restore of SEsparse disks with the host-based file transport mode. Because Replication Director for VMware requires host-based file transport, Replication Director cannot support the vmdk files that are larger than 2 TB. To back up the vmdk files that are larger than 2 TB, use NetBackup for VMware without Replication Director.
- When restoring from Replication Director backups, note the following:
 - If you select more than one image in the **Backup, Archive, and Restore** interface, it may take longer than expected to display the image contents. NetBackup performs a separate browsing operation for each selected image. You should select one image at a time when browsing for restore.
 - Do not select files or folders from two different images. The NetBackup **Backup, Archive, and Restore** interface, and the OpsCenter interface do

not support restoring data from two different images in the same restore job. Restore from one image at a time.

- When you use the **Backup, Archive, and Restore** interface to browse for an image to restore, only the primary copy is made available for restore. In the **NetBackup Administration Console**, use the **Catalog** node to select a different copy (such as a backup image or replica) as the primary copy.

Note: NetBackup automatically selects the correct hardware (datastore) snapshot to restore, based on the virtual machine snapshot that is designated as the primary copy. Make sure the virtual machine snapshot that you want to restore is set as the primary.

See [“About jobs in the Activity Monitor that use Replication Director for virtual machines”](#) on page 172.

Configuring a policy for virtual machines to use Replication Director

The following procedure describes how to configure a **VMware** policy to create snapshots of virtual machines using Replication Director.

See the [NetBackup for VMware Administrator's Guide](#) for more specific information about configuring VMware policies.

Only those policy options that are necessary to configure Replication Director are listed in the following procedure.

To create a policy to use virtual machines with Replication Director

- 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**.

See [“NetBackup naming conventions”](#) on page 15.

- 4 Configure the options on the policy **Attributes** tab. The following items are specific to creating a VMware policy for snapshots with Replication Director:
 - **Policy type:** Select **VMware**.
 - **Policy storage:** Select the SLP that you want to use that has been configured for snapshot replication.
 - **Use Replication Director:** Enable **Use Replication Director** to automatically select other options that Replication Director requires.

■ **Replication Director Options**

Click the **Options** button to see the **Replication Director Options** dialog box and the default **Configuration Parameters** as follows:

Maximum Snapshots parameter Sets the maximum number of Instant Recovery snapshots to be retained at one time. When the maximum is reached, snapshot rotation occurs: The next snapshot causes the oldest to be deleted.

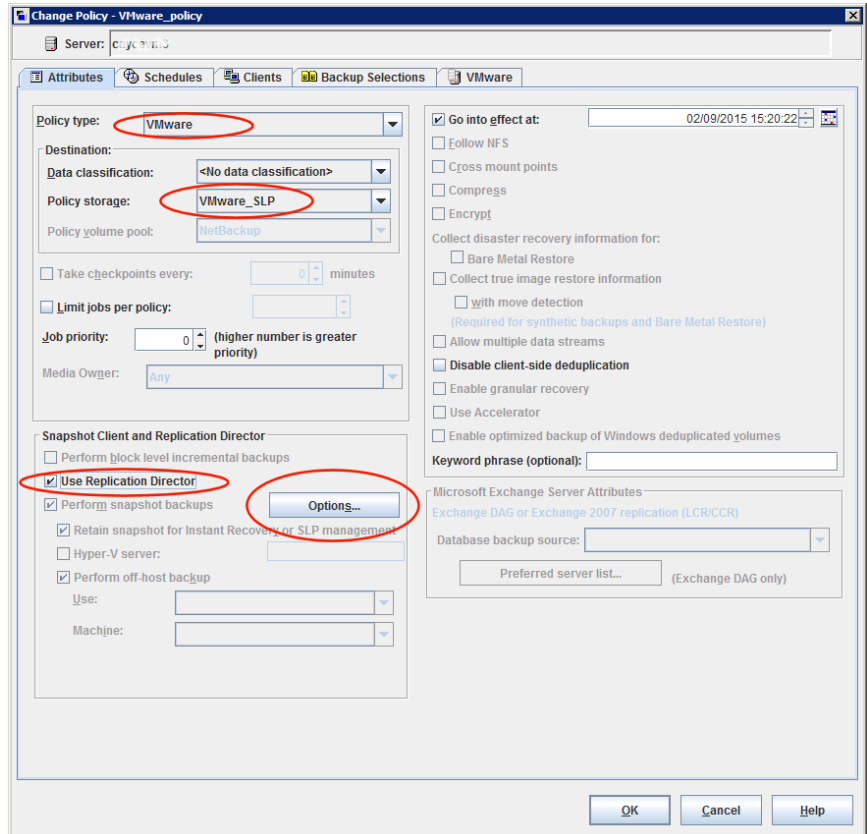
Managed by SLP retention is automatically selected if the **Fixed** or the **Expire after Copy** retention is currently selected in the SLP.

Application Consistent Snapshot This option is enabled by default. In most cases, Veritas recommends that you keep this option enabled.

If this option is disabled, data in the virtual machine may not be in a consistent state when the snapshot occurs. The snapshot may not capture all the data in the virtual machine.

Note the following:

- To allow the SLP to create a backup image from the snapshot, this option must be enabled.
- If this option is disabled, note the following about the **VMware** tab:
 - **Exclude deleted blocks** and **Exclude swap and paging files** are disabled.
 - The **Application Protection** options are disabled.
 - Only two of the **Advanced** parameters are available: **Multiple organizations per policy** and **VMware server list**.



5 Use the **Schedule** tab to create a schedule. Note that only the **Full Backup** type is supported.

6 Use the **Clients** tab to create a query for the automatic selection of virtual machines.

Select automatically through VMware Intelligent Policy query is pre-selected. Manual selection of virtual machines is not supported.

For instructions on creating a query, see the topics about configuring the automatic selection of virtual machines for backup in the [NetBackup for VMware Administrator's Guide](#).

7 Use the **VMware** tab to select virtual machine backup options.

Note the following:

- The **Enable file recovery from VM backup** option is pre-selected and cannot be disabled.

- The **Enable block-level incremental backup** option is not supported and is disabled.
- The **Transport modes** are not supported and are disabled. NetBackup uses the VMware file transport mode to move the data between the backup host and the storage volumes.
- Under the options for **Application Protection**, only Exchange and SQL are supported.
- If the **Application Consistent Snapshot** option is disabled under **Replication Director Options**, only two of the **Advanced** parameters on the **VMware** tab are available:
 - Multiple organizations per policy
 - VMware server listThe other **Advanced** parameters are ignored.
- All other options on the **VMware** tab are supported for Replication Director.

8 When the policy configuration is complete, click **OK**.

About jobs in the Activity Monitor that use Replication Director for virtual machines

You can use the NetBackup **Activity Monitor** to keep track of virtual machines backups as they occur. The number of jobs that appear in the **Activity Monitor** depends on the policy's **Application Consistent Snapshot** option.

Note: The **Application Consistent Snapshot** option is enabled by default. In most cases, Veritas recommends that you keep this option enabled. If this option is disabled, data in the virtual machine may not be in a consistent state when the snapshot occurs.

[Table 12-3](#) describes the **Activity Monitor** jobs that appear in each configuration: with the **Application Consistent Snapshot** option enabled or disabled.

Table 12-3 Job flow in the Activity Monitor for the jobs that use Replication Director for virtual machines

Application Consistent Snapshot option	Job flow in the Activity Monitor
Enabled	The first job discovers the virtual machines. This job is labeled Backup. The Backup job starts the following: ■ A Snapshot job for each virtual machine. ■ A Snapshot job for each datastore.
Disabled	The first job discovers the virtual machines. This job is labeled Backup. The Backup job starts the following: ■ A Snapshot job to collect all the virtual machines' configuration data. ■ A Snapshot job for each datastore.

Example 1: Virtual machine jobs with the **Application Consistent Snapshot** option enabled.

Job ID	Parent Job ID	Type	Job State	Job Policy	Client
 105	99	Snapshot	Done	AppConsistent_VMwareRD	wauk_c3
 104	99	Snapshot	Done	AppConsistent_VMwareRD	wauk_c2
 103	99	Snapshot	Done	AppConsistent_VMwareRD	wauk_c1
 102	99	Snapshot	Done	AppConsistent_VMwareRD	waukvm15,...
 101	99	Snapshot	Done	AppConsistent_VMwareRD	waukvm14,...
 100	99	Snapshot	Done	AppConsistent_VMwareRD	waukvm13,...
 99	99	Backup	Done	AppConsistent_VMwareRD	bwarevm1,...

The jobs occurred as follows:

- The discovery (parent) Backup job for virtual machine discovery is ID 99.
- Jobs 100, 101, and 102 made VMware snapshots of the virtual machines waukvm13, 14, and 15.
- Jobs 103, 104, and 105 made snapshots of datastores wauk_c1, c2, and c3.

Example 2: Virtual machine jobs with the **Application Consistent Snapshot** option disabled.

Job ID	Parent Job ID	Type	Job State	Job Policy	Client
 110	106	Snapshot	Done	AppConsistentDisabled_VMwareRD	wauk_c3
 109	106	Snapshot	Done	AppConsistentDisabled_VMwareRD	wauk_c2
 108	106	Snapshot	Done	AppConsistentDisabled_VMwareRD	wauk_c1
 107	106	Snapshot	Done	AppConsistentDisabled_VMwareRD	bwarevm1....
 106	106	Backup	Done	AppConsistentDisabled_VMwareRD	bwarevm1....

The jobs occurred as follows:

- The discovery (parent) Backup job for virtual machine discovery is ID 106.
- Job 107 collected the virtual machines' configuration data.
- Jobs 108, 109, and 110 made snapshots of the virtual machines' datastores: wauk_c1, c2, and c3.

Terminology

This chapter includes the following topics:

- [Replication terminology](#)

Replication terminology

Use the following table as a reference for understanding many terms that are used frequently when describing replication processes.

Table 13-1 Replication terms

Term	Definition
Backup	The process of creating a copy of user data and creating backup images of the data. ■ The process of creating a new tar-formatted backup image of the client's data. ■ The process of creating a snapshot of the client's data.
Cluster Data ONTAP	The operating system that is used on NetApp storage systems in a clustered mode.
Copy	An instance of a NetBackup image which can standalone; it can be read or deleted without affecting any other copy.
Data mover	The mechanism that is used to copy data from storage on the production client to backup storage. Or, to duplicate, the data mover copies data from backup storage to different backup storage. Traditionally, NetBackup functions as the data mover and data travels through clients and media servers. Storage devices can provide more efficient mechanisms to move the data, such as NDMP, built-in replication, or OST (as in Optimized Duplication).
Data ONTAP	The operating system that is used on NetApp storage systems in 7-Mode.
Device	A general term for a logical volume, appliance, or disk array.

Table 13-1 Replication terms (*continued*)

Term	Definition
Disk array	A disk array which exposes storage or network shares to a host server over SAN, NFS, CIFS, or iSCSI protocols.
Duplication	NetBackup creates a copy by using a media server to move the data or by using the optimized duplication method.
Local domain	The domain in which the storage device resides and in which it is configured.
Mirror	This term can mean either of the following: ■ A disk that maintains an exact copy (duplicate or replica) of another disk. A mirror disk is often called a secondary, and the source disk is called the primary. All writes to the primary disk are also made to the mirror disk. ■ A type of snapshot that is captured on a mirror disk. At the appropriate moment, all further writes to the primary disk are held back from the mirror, which splits the mirror from the primary. As a result of the split, the mirror becomes a snapshot of the primary. The snapshot can then be backed up.
Mount host	The host on which NetBackup mounts a snapshot when NetBackup needs to access the snapshot for any reason. Typically, NetBackup accesses the mount host to browse or to restore backups, or to perform either an Index From Snapshot or a Backup From Snapshot operation in a storage lifecycle policy. To mount a snapshot on a host other than the production client is generally more efficient because it avoids a negative impact on the performance of the production client. Media servers make excellent mount hosts because the media server is both a client and a media server (data mover). As such, NetBackup can often avoid an additional network hop. If no compatible media servers exist, dedicated clients are the next best choice. Note: The mount host and the production client must run the same operating system for the mount host to access the production client. The mount host must be at the same OS version or later. See the NetBackup Snapshot Client Administrator's Guide for more details.
NetApp Plug-in for Veritas NetBackup	Also referred to as the NBUPugin, this plug-in communicates with the OSTPlugin to query the OnCommand Unified Manager. The <i>NetApp Plug-in for Veritas NetBackup Installation and Administration Guide</i> is available from the NetApp Support Site.
OnCommand Unified Manager (OCUM)	OnCommand Unified Manager (formerly known as DataFabric Manager or DFM) is the software application installed on a host that is identified to be a DataFabric Manager (DFM) server. The software provides infrastructure services such as discovering, monitoring, role-based access controls, auditing, and logging for products in the Data and Storage suites.

Table 13-1 Replication terms (*continued*)

Term	Definition
NetApp Management Console	The NetApp interface that is used to configure and manage the OnCommand Unified Manager.
NetBackup OpenStorage Plug-in for Replication Director	Also referred to as the OSTPlugin, NetBackup uses this to communicate with the vendor's plug-in.
OST device	A storage server that has implemented the OST plug-in interface.
Point-in-time rollback	A snapshot is a point-in-time, disk-based copy of a file system or volume. A restore from a snapshot rolls the entire file system or volume back to a specific point in time. Therefore, a snapshot restore is called restoring from a Point-in-time rollback. All of the data in the snapshot is restored. Any data changes or snapshots that were made after that point-in-time are lost.
Primary volume	A unit of storage space that a disk array exposes to a host in the form of a network share (NFS or CIFS) or LUN block device. Primary volumes store an application's active data.
Replica	A replica is a block copy of the snapshot.
Replication	The process of replicating a snapshot onto a separate disk array using NetBackup Replication Director.
Replication source	A NetBackup-configured disk pool and storage unit that contains the volumes that serve as the source for subsequent replications.
Replication target	A NetBackup-configured disk pool and storage unit that can receive or accept replications from a replication source.
Snapshot	A point-in-time, read-only, disk-based copy of a client volume or of a filer. A snapshot is created with minimal impact on other applications. NetBackup provides several types of snapshots, depending on the device where the snapshot occurs. An image copy that is a snapshot is also considered a replica. A snapshot copy consists of one or more snapshot fragments.
Snapshot method	A set of routines for creating a snapshot. The NetBackup administrator can select the method, or let NetBackup select it when the snapshot begins (auto method).
Snapshot mirror	A disk mirror that is an exact replica of a primary volume at a particular moment, reproduced on a physically separate device.
Snapshot source	The production data (file system, raw partition, or logical volume) to which a snapshot method is applied. NetBackup automatically selects the snapshot source according to the entries in the Backup Selections list of the snapshot policy.
Storage device	See <i>disk array</i> .

Table 13-1 Replication terms (*continued*)

Term	Definition
Storage lifecycle policy (SLP)	NetBackup uses storage lifecycle policies to manage the lifecycle of a backup or snapshot image. An SLP controls the image migration, duplication, and replication within a single NetBackup master server domain.
SVM	Storage virtual machines. These were formerly known as Vservers.
Storage unit	A storage unit is configured for one of two types of data: ■ Backup storage units contain backup images. A backup storage unit cannot contain snapshots. ■ Snapshot storage units contain snapshots. A snapshot storage unit cannot contain backups. Replication Director uses snapshot storage units in snapshot replication configurations.
Storage server	A storage device that is configured in NetBackup. A storage server is a NetBackup entity that represents a disk array.
vFiler	vFilers are ONTAP 7-mode virtual containers that create separate virtual filer instances withing a physical controller (doesn't matter if FAS or V-Series).

Index

Symbols

.f files in catalog 64

A

Accelerator

 Expire after copy retention type 73

Activity Monitor

 displaying Backup jobs 69

 displaying Duplication jobs 71

 displaying Index From Snapshot jobs 63

 displaying Replication jobs 60

 displaying Snapshot jobs 56

administrator

 account for NetBackup Client Service 14

aggregate support 120

ALL_FILESYSTEMS 91

ALL_FILESYSTEMS directive for Clustered Data
 ONTAP 146

authorization

 NDMP host access 89

 NDMP user and password 89

Auto Image Replication

 role of Import operation 55

 role of Replication operation 59

 Target retention type 75

Auto snapshot type 79, 84, 154, 159

B

Backup

 job 69

 operation 55

 storage units 46

Backup From Snapshot operation 64, 68, 139, 145

backup policies 84

 configuring for Replication Director 76

Backup Selections list

 64 backup selections limit VSS policy 86

 ALL_FILESYSTEMS directive 91

 combining SAN devices and NAS volumes
 prohibited 80, 83, 86

Backup Selections list *(continued)*

 VOLUME_EXCLUDE_LIST directive 91

bpstsinfo command 29, 40, 131

C

case sensitivity

 in NetBackup names 15

 in storage unit names 47

cataloging snapshots 61, 64

cDOT. *See* NetApp Clustered Data ONTAP (cDOT)

CHAP security protocol 127

checklist, configuration 12, 122

CIFS

 licenses on NetApp storage 120, 125, 135–136

 no widelinks support 133

 required software 137

 volumes 14, 76, 86, 88, 118, 176–177

 NetBackup Client Service access to 87

Client Service, NetBackup 14, 87

Clone snapshot type 79, 154, 159

configuration checklist 12, 122

Copy-on-write technology 79, 154, 159

D

Data Mover off-host backup method 63, 69, 83, 89

Differential snapshot type 79, 154, 159

disk pools

 creating 29

 for snapshot replication 26

 updating to reflect plug-in partner updates 23,
 31, 33

disk volumes

 for replication 27

domains, NetBackup 122

Duplication

 job 71

 SLP operation 70

Dynamic disks 129

E

Exchange databases 164, 172
 Expire after copy retention type 72–73

F

FCoE. *See* Fibre Channel over Ethernet (FCoE)
 Fibre Channel over Ethernet (FCoE) 125, 127, 129
 Fixed retention type 73

G

Getting Started Wizard 12, 78, 83–84, 153, 158

H

Hardware Compatibility List (HCL) from NetBackup 11
 HBA cards 127

I

image .f files 64
 import tool from NetApp 121, 132
 Independent property 48
 Index From Snapshot operation 61, 64, 72, 102
 Clustered Data ONTAP 150
 Interoperability Matrix Tool from NetApp 123, 126,
 135, 137
 IPv6 support 10, 121, 135
 iSCSI 127
 configuring for Windows 128
 license for NetApp 125, 127

M

Managed by SLP retention 79, 85, 154, 159, 170
 Maximum concurrent jobs storage unit setting 47
 Maximum snapshot limit retention type 73, 79, 85,
 154, 159, 170
 Maximum Snapshots parameter 73, 79, 85, 154, 159,
 170
 media servers
 adding to a snapshot replication environment 24
 selecting for storage unit 31, 47
 Mirror property 48, 59
 Mirror retention type 75
 Mirror-break-off technology 79, 154, 159
 mount host 176
 multiple copies
 synthetic backups method 73

N

NAS host, authorizing access to 89
 NAS snapshot 89
 NBUPlugin
 2.0 133, 135, 150
 default installation location 10
 definition 176–177
 determining the version 116
 IPv4 and IPv6 10, 121, 135
 NetBackup group on OnCommand Unified
 Manager 30, 132
 service, restarting 130
 updating the storage server for 23
 upgrading 117
 NBUPlugin service 130
 NDMP 89
 ALL_FILESYSTEMS directive in backup
 policies 91
 Credentials on OnCommand Unified
 Manager 127
 Data Mover and Clustered Data ONTAP
 policies 143
 Data Mover off-host backup method 83, 89
 determining backup traffic 94
 host, authorizing access 89
 licensing 11
 limitations with Clustered Data ONTAP 150
 policy type 69, 104
 Replication Director support for 88
 service, enabling 138
 Status on OnCommand Unified Manager 127
 NetApp
 Add Resource Pool Wizard 121, 134
 configuration demonstration video 122
 disk arrays 15
 documentation 10, 176
 FlexClone volumes 93
 import tool 121, 132
 Interoperability Matrix Tool 123, 126, 135, 137
 Management Console 30, 122, 132
 number of snapshots per volume 79, 85, 154,
 159
 Plug-in for Veritas NetBackup 10, 176–177
 resource pools 121, 134
 SnapMirror 126
 SnapMirror or SnapVault replication method 52,
 54, 75
 SnapVault 126
 supported topologies 118

NetApp (*continued*)
 unsupported topologies 118
 volume language setting 132

NetApp Clustered Data ONTAP. *See* Clustered Data ONTAP

NetApp Clustered Data ONTAP (cDOT)
 backup policies overview 140
 configuration 138
 configuration overview 134
 limitations 150
 NBUPugin 2.0 133, 135, 150
 nested junctions 148
 required licenses 135
 required software 137

NetBackup
 Client Service (bpcd) 14, 87
 clients using NICs 16, 96
 domains 122
 Hardware Compatibility List (HCL) 11
 naming conventions 15

NetBackup for NDMP Administrator's Guide 81

NetBackup Service Layer (NBSL) 131

Network Interface Cards (NICs) 16, 96

NFS
 licenses on NetApp storage 120, 125, 135, 137
 required software 137
 volumes 76, 86, 88, 118, 176–177

NIC (Network Interface Card) 16, 96

O

OnCommand servers
 software 123, 134, 138

OnCommand Unified Manager
 changing root or administrator password 130
 creation of NetBackup group 30, 132
 licenses 123
 multiple in one NetBackup domain 122

OpenStorage
 plug-in role 10
 storage server, updating 23

Operational Restore, OpsCenter 61, 102

OpsCenter 9, 102, 109–111

OpsCenter Operational Restore 61, 102

Oracle
 policy for Clustered Data ONTAP 147
 policy for snapshot backups
 Oracle Intelligent Policy 152
 using script- or template-based Oracle policy
 creation method 158

Oracle (*continued*)
 required software 151

OSTPlugin 177

P

Plex snapshot type 79, 154, 159

plug-ins
 about the roles of 10
 NBUPugin 2.0 133, 135, 150
 NetApp 10, 113, 176
 NetBackup 177
 on media servers that can access storage units
 for Replication Director 47
 updates 23, 31, 33
 upgrading from NetApp 117

Point-in-time copy 79, 154, 159

Point-in-time rollback restores
 definition 177
 limitations using NetApp SAN 129
 Oracle policy 157

policies
 clients using NICs 16
 creating 84
 for NetApp Clustered Data ONTAP (cDOT) 140

Policy Configuration Wizard 12, 78, 83–84, 153, 158

Primary property 48, 57

processmanager 130

Q

qtrees 87, 89, 119

R

RAW disks 129

replication
 disk pools for 26
 disk volumes for 27
 job 60
 method 52, 54, 75
 source property 48, 57–59
 target property 48, 58–59

Replication Director
 adding OpenStorage credentials 24
 checklist 12, 122
 configuration demonstration video 122
 creating storage lifecycle policies for 52
 Replication operation 59
 use of Index From Snapshot operation in SLP 63

Replication operation 59

resource pools 121, 134

restoring

- about restoring an array-based snapshot 96
- enabling multiple media servers 20
- files and folders from an array-based snapshot 97
- from an array-based snapshot 104
- OpenStorage partner NetApp 102
- Point-in-time rollback 157, 177

retention types for SLP operations

- Expire after copy 72
- Fixed 73
- Maximum snapshot limit 73
- Mirror 75
- Target 75

RMAN

- scripts 152

rollback restores

- OpenStorage partner NetApp 102
- Point-in-time rollback 102, 104, 157, 177

S

Simplified File Restore 61, 102

See also OpsCenter Operational Restore

SLP Parameters host properties 52

SnapDrive 128–129

snapdupe 68

See also Backup From Snapshot operation

SnapMirror 126, 134

- license for Clustered Data ONTAP 136

SnapRestore 134

- license for Clustered Data ONTAP 136

Snapshot operation type 55

Snapshot Type parameter 79, 84, 154, 159

snapshots

- about restoring an array-based snapshot 96
- backup policy 84
- cataloging 61, 64
- job 56
- storage unit groups for 47
- storage units 46

SnapVault 126, 134

- license for Clustered Data ONTAP 136

SQL Server databases 164, 172

status codes

- 156 (snapshot error encountered) 86
- 4206 (Authentication error occurred) 14, 87
- 83 (media open error) 130

storage lifecycle policies

- and synthetic backups 73

storage lifecycle policies *(continued)*

- best practices document 52
- cataloging snapshots 61, 64
- operations 52
 - windows 56, 60, 63, 69, 71
- reporting 112
- retention types 71

storage servers

- updating to reflect plug-in partner updates 23, 31, 33

storage unit groups

- create for snapshots 47
- reporting 112

storage units

- configuring for replication 45
- reporting 112

Storage Virtual Machine (SVM) 133

- configuring 134
- in backup policies 140

storage virtual machines (SVM) 178

synthetic backups

- multiple copy backups method 73

T

tar-formatted backup 51–52, 59, 68, 70, 118, 125, 175

Target retention type 75

topologies

- unsupported 118
- using bpstsinfo to view 40–41

TPCommandTimeout 131

tpconfig command line utility 130

U

Unicode, enabling on NetApp storage 132

updating the OpenStorage plug-in 23

UTF-8 132

V

versions, determining NetApp NBUPlugin 113

vFilers 126

video configuration demonstration 122

VMware

- policy for Clustered Data ONTAP 147
- support 164

volume GUID 129

volume language setting 132

- volume-level rollback restore
 - OpenStorage partner NetApp 102
- VOLUME_EXCLUDE_LIST 91
- Vservers 66, 178
- VSS 84

W

- widelinks 133
- Windows 2003 128
- Windows 2008 128
- Windows Volume Shadow Services (VSS) 84
- windows, for storage lifecycle policy operation 56, 60, 63, 69, 71