Symantec NetBackup™ Replication Director Solutions Guide

UNIX, Windows, Linux

Release 7.6

Symantec

Symantec NetBackup™ Replication Director Solutions Guide

Documentation version: 7.6

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introducing NetBackup Replication Director

This chapter includes the following topics:

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 Symantec 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. In NetBackup 7.6, the storage server is a NetApp DataFabric Manager 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.

Configuration overview for a NetBackup Replication Director environment

Table 1-1 describes the steps that are required to configure snapshots and snapshot replication.

These steps are also demonstrated in the following video:

http://www.symantec.com/connect/videos/netbackup-75-replication-director-configuration-demo

Table 1-1 Configuration tasks overview

Step	Description	Reference topic
1	Install or upgrade NetBackup software on the master server and media server(s).	See "Required licenses" on page 17.
2	Install and configure the OpenStorage partner.	See "About NetApp configuration for Replication Director" on page 24.
3	Run the Storage Server Configuration Wizard to configure the OpenStorage partner as a NetBackup storage server. For example, configure the DataFabric Manager server 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 54.

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 Symantec plug-in is installed by default with NetBackup. It uses the XML-based messaging SOAP protocol to query the disk array.

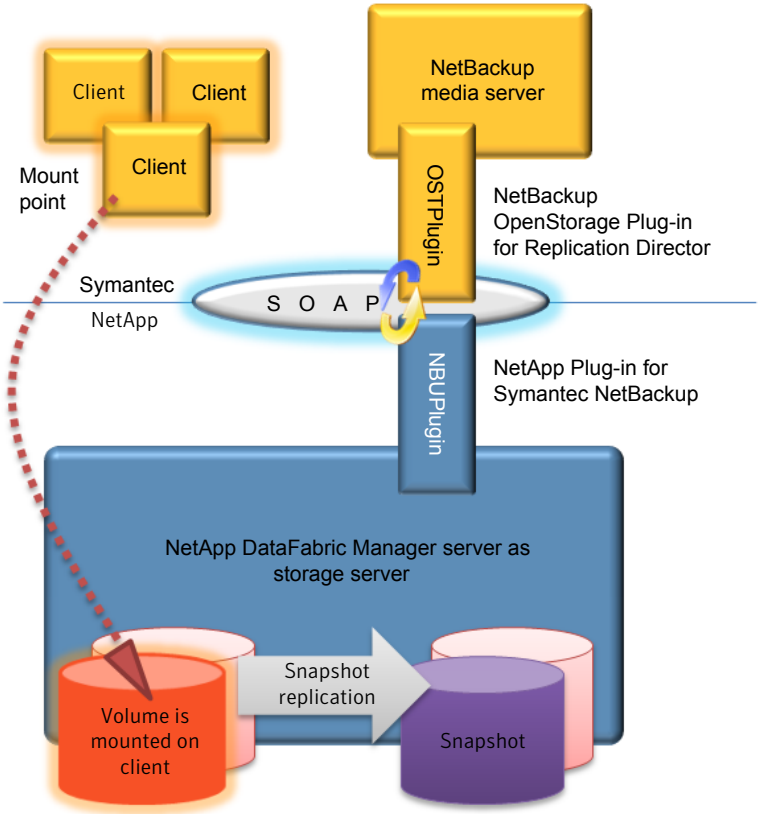
The OpenStorage partner also hosts a software plug-in that allows communication between NetBackup and the disk array. (See Figure 1-1.)

Table 1-2 lists the plug-ins used in NetBackup 7.6 by NetBackup and by the OpenStorage partners.

Table 1-2 Names of plug-ins used in Replication Director

Plug-in name	Installation location
OSTPlugin	Installed by default on NetBackup media servers and clients.
NetApp Plug-in for Symantec NetBackup	The plug-in is installed on the DataFabric Manager server in the following locations. ■ Windows: `C:\Program Files\NetApp\NBUPlugin` ■ UNIX: `/usr/NetApp/NBUPlugin` For installation instructions, see the *NetApp Plug-in for Symantec NetBackup Installation and Administration Guide*, available from the NetApp Support Site. **Note:** In NetBackup 7.6, the default communication between the two plug-ins is to use encryption. A change can be made to the NBUPlugin config file to disable encryption. The **Encryption** policy attribute has no impact on the encryption between the plug-ins. **Note:** By default, the NetApp Plug-in for Symantec NetBackup uses IPv4, however the system can be configured to use IPv6.

Figure 1-1 Communication between the OSTPlugin and the NetApp Plug-in for Symantec NetBackup



Chapter 2

Prerequisites for using Replication Director

This chapter includes the following topics:

Required licenses

The following NetBackup licenses are required to use Replication Director.

Table 2-1 NetBackup licenses required for Replication Director

NetBackup host	License
Master server	The NetBackup Replication Director option, which enables the following license key bits: Snapshot Client, OpenStorage Disk, and Replication Director.
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	A Symantec client license is required on clients for all non-NDMP backups.

The following NetApp licenses are required to use Replication Director.

Table 2-2 NetApp licenses required for Replication Director*

License	DataFabric Manager Server	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 for Symantec NetBackup Download from the NetApp Support Site. Earlier plug-in versions are supported, but they do not support new features. See "Compatibility between Replication Director and NetApp plug-ins" on page 22.	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 2-3 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 key 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 key on the SnapVault source and destination storage systems. Older platforms have separate SnapVault primary license keys for SnapVault primary (source) and secondary (designation) storage systems.

Table 2-3 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 key 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 key on the SnapMirror destination storage system.
FlexClone	Only for block data or indexing, restore, or tar backup of NAS data	Only indexing, restore, or tar backup of NAS data			Install the FlexClone license key on the secondary storage system that contains the SnapVault destination volumes. For the Primary-SnapVault-SnapMirror cascade (PVM) topology, install the license key on the SnapMirror destination. The FlexClone license is required on any controller that is used for indexing, restoring, or performing a streaming (tar) backup of NetApp block data.
CIFS	CIFS NAS data only (Windows)				Install the CIFS license key 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 key 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 license keys on both the source and the destination storage systems. See "About using NetApp SAN-connected storage with Replication Director" on page 27.

Table 2-3 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 key 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.

Required software

Install NetBackup 7.6 on all master servers, media servers, and NetBackup clients to be used with Replication Director.

See NetBackup Installation Guide.

The Symantec NetBackup Hardware Compatibility List (HCL) lists the platforms on which Replication Director is supported.

The following NetApp software is required to use Replication Director.

Table 2-4 NetApp software required for Replication Director

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

Table 2-4 NetApp software required for Replication Director *(continued)*

Configuration	Applies to DataFabric Manager Server?	Primary storage system	Secondary storage systems
NDMP Enable on all storage systems, including vFiler. Verify with the NetApp `ndmpd status` command.	No	Enable	Enable

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.

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

Compatibility between Replication Director and NetApp plug-ins

Replication Director in NetBackup 7.6 works with any version of the NetApp Plug-in for Symantec NetBackup. See Table 2-5 to determine the extent of the compatibility between the plug-ins.

Table 2-5 Version compatibility

NetBackup OSTPlugin version	NetApp NBUPlugin version	Compatibility
7.6	1.1	Full compatibility for all of NetBackup 7.6 Replication Director features.
7.6	1.0.1	Compatible; allows NetBackup 7.5 Replication Director features only.
7.5	1.0.1	Compatible; allows NetBackup 7.5 Replication Director features only.
7.5	1.1	Incompatible. Does not allow NetBackup 7.5 or 7.6 Replication Director features.

Note: You must upgrade the entire NetBackup environment to 7.6 before upgrading the NBUPlugin to 1.1. Upgrade all master servers, media servers, clients, and any host which communicates with the NBUPlugin.

Determining the NBUPlugin version

To determine the NBUPlugin version, look for the following version file on the DataFabric Manager server where the NBUPlugin is installed:

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

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

The contents of the file lists the product name, the build date, and the NBUPlugin version.

Upgrading the NBUPlugin

If upgrading the NetApp Plug-in for Symantec 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: `C:\Program Files\VERITAS\NetBackup\bin\admincmd>nbstlutil.exe stlilist -U`

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

Chapter 3

NetApp deployment

This chapter includes the following topics:

About NetApp configuration for Replication Director

The following table lists the general configuration steps necessary to set up NetApp storage for use with Replication Director. Each step is described in the NetApp Plug-in for Symantec NetBackup Installation and Administration Guide, found at the following NetApp website:

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

Additional documents and demonstrations provide supporting information:

- Replication Director tools for use with NetApp storage systems: http://www.symantec.com/docs/DOC5240
- A video demonstration: http://www.symantec.com/connect/videos/configuring-netapp-replication-director

- A step-by-step description of configuring NetApp storage using the NetApp Management Console:
  http://www.symantec.com/docs/HOWTO73062

Table 3-1 NetApp configuration tasks overview

Description	Reference topics
Install the NetApp Management Console.	See NetApp documentation. See "Configuring the port use between the DataFabric Manager server and NetBackup hosts" on page 43.
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. See "Required licenses" on page 17.
Install necessary licenses on NAS systems: ■ CIFS licenses ■ NFS licenses	See NetApp documentation. See "Required licenses" on page 17. See "Enabling Unicode and language settings on NetApp disk arrays" on page 27.
Install necessary licenses on SAN devices: ■ iSCSI licenses ■ Fibre Channel licenses	See NetApp documentation. See "Required licenses" on page 17. See "About using NetApp SAN-connected storage with Replication Director" on page 27. See "Configuring the primary NetApp device to use VSS with Replication Director" on page 36.

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

Description	Reference topics
Install the NetApp Plug-in for Symantec NetBackup (NBUPlugin).	Select either 8085 or 8086 as the communication port. The NBUPlugin uses port 8085 in HTTP mode or port 8086 in HTTPS to communicate with NetBackup. See "Configuring the port use between the DataFabric Manager server and NetBackup hosts" on page 43. After the NBUPlugin is installed, the **NetBackup** resource group is automatically added in the DataFabric Manager. The primary volumes that are configured on NetApp storage are exposed as primary snapshot logical storage units to the NBUPlugin. This lets NetBackup initiate and manage snapshots of the primary volumes. See NetApp documentation. See "Required licenses" on page 17. See "Compatibility between Replication Director and NetApp plug-ins" on page 22.
Configure IPv6 if necessary. By default, the NBUPlugin 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 45.
Add resource pools.	■ Configure resource pools in the DataFabric 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 DataFabric Manager. NetBackup can now access the resource pools as disk volumes during the NetBackup disk pool creation step. See NetApp documentation. See Symantec document HOWTO73062.

For information about the NetApp configurations that work with qualified third-party products and components, access the NetApp Interoperability Matrix Tool.

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_ucode` and `create_ucode` on all NetApp storage:

- `convert_ucode on`
  Forces the conversion of all directories to Unicode format.
- `create_ucode 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.

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.

See the following topics for iSCSI setup:

- See "Using SnapDrive for iSCSI setup on Windows" on page 28.
- See "iSCSI initiator configuration on Red Hat Enterprise Linux (RHEL)" on page 29.

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

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.

Using SnapDrive for iSCSI setup on Windows

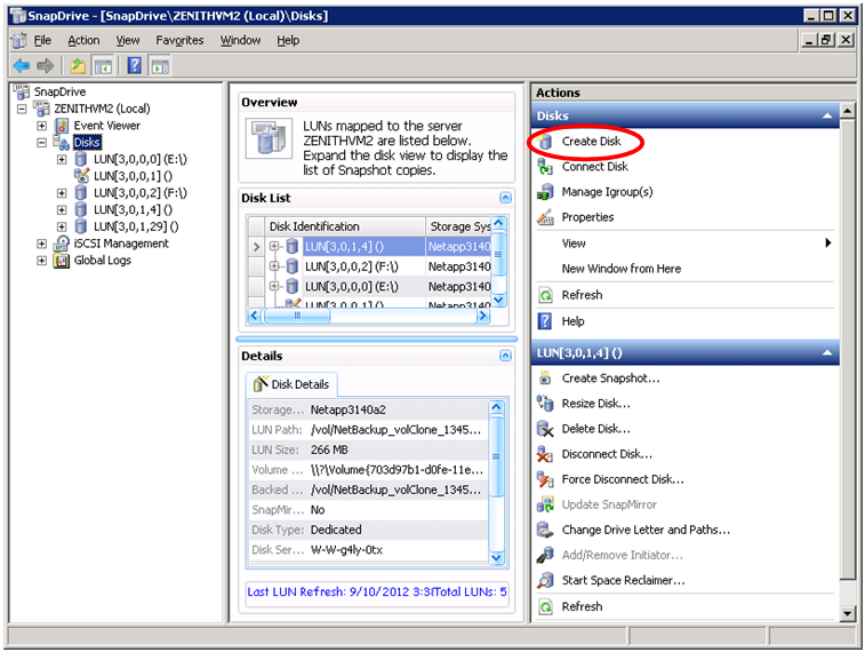
Use the NetApp SnapDrive software to simplify iSCSI setup on Windows hosts. See the following NetApp documentation for the most complete instructions. Instructions are listed here for ease of use.

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.



iSCSI initiator configuration on Red Hat Enterprise Linux (RHEL)

The following procedure describes iSCSI setup for Data ONTAP on Linux hosts. See the following NetApp documentation for the most complete instructions. Instructions are listed here for ease of use.

Data ONTAP 8.2 SAN Administration Guide For 7-Mode

Data ONTAP 8.2 SAN Configuration Guide For 7-Mode

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

To configure iSCSI on Linux

1 Install the `iscsi-initiator-utils` RPM package.

Use the following command to determine whether the package is installed. For example:

```
# rpm -qa | grep -i iscsi
iscsi-initiator-utils-6.2.0.872-6.el5

# rpm -qi iscsi-initiator-utils-6.2.0.872-6.el5
Name        : iscsi-initiator-utils        Relocations: (not relocatable)
Version     : 6.2.0.872                         Vendor: Red Hat, Inc.
Release     : 6.el5                      Build Date: Tue 09 Nov 2010 11:42:55 PM IST
Install Date: Wed 26 Oct 2011 01:19:25 AM IST      Build Host: hs20-bc2-5.build.redhat.com
Group       : System Environment/Daemons    Source RPM: iscsi-initiator-utils-6.2.0.872-6.el5.src.rpm
Size        : 2881111              License: GPL
Signature   : DSA/SHA1, Wed 08 Dec 2010 01:53:45 PM IST, Key ID 5326810137017186
Packager    : Red Hat, Inc. &lt;http://bugzilla.redhat.com/bugzilla&gt;
URL         : http://www.open-iscsi.org
Summary     : iSCSI daemon and utility programs
Description: The iscsi package provides the server daemon for the iSCSI protocol,
as well as the utility programs used to manage it. iSCSI is a protocol
for distributed disk access using SCSI commands sent over Internet
Protocol networks.
```

2 Configure the initiator. The iSCSI initiator is composed of two services: `iscsi` and `iscsid`.

Use `chkconfig` to allow the services to start at system start-up.

```
# chkconfig iscsi on
# chkconfig iscsid on
# chkconfig --list | grep iscsi
iscsi           0:off   1:off   2:on    3:on    4:on    5:on    6:off
iscsid          0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

After iSCSI is configured, start the service by using the `iscsi start` command:

```
# service iscsi start
iscsid is stopped
Starting iSCSI daemon:                                     [  OK  ]
                                                           [  OK  ]
Setting up iSCSI targets: iscsiadm: No records found!      [  OK  ]

# service iscsi start
iscsid (pid  14961) is running...
Setting up iSCSI targets: iscsiadm: No records found!      [  OK  ]
```

3 Find the name of the initiator server in the file `/etc/iscsi/initiatorname.iscsi`. In this example, the name of the server is *iqn*.

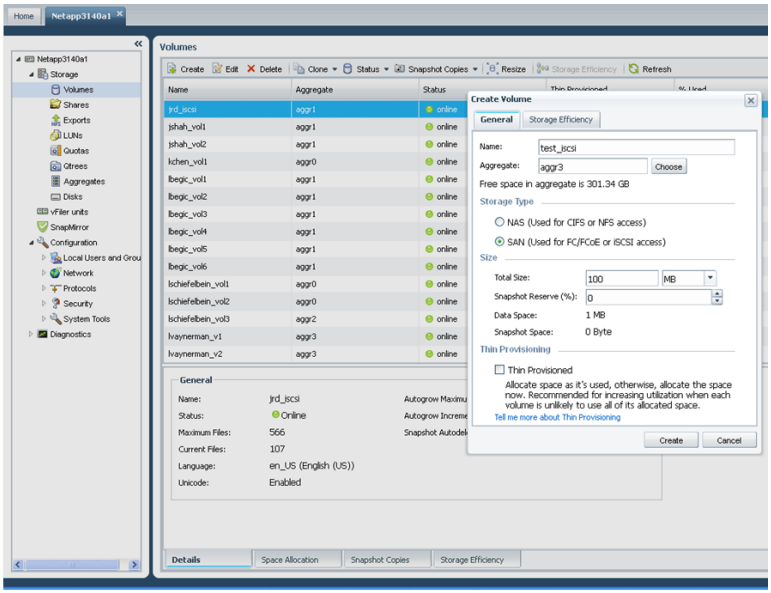
```
# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.1994-05.com.redhat:8e44f7dac2b
```

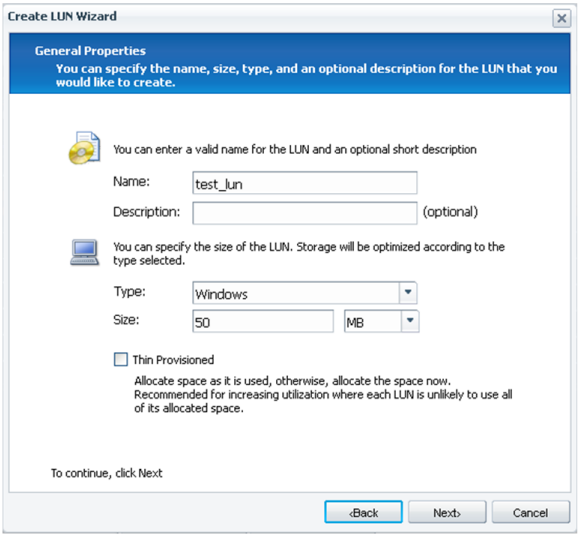
4 Create iSCSI LUNs on the storage system. Assign or map the LUNs to the RedHat system.

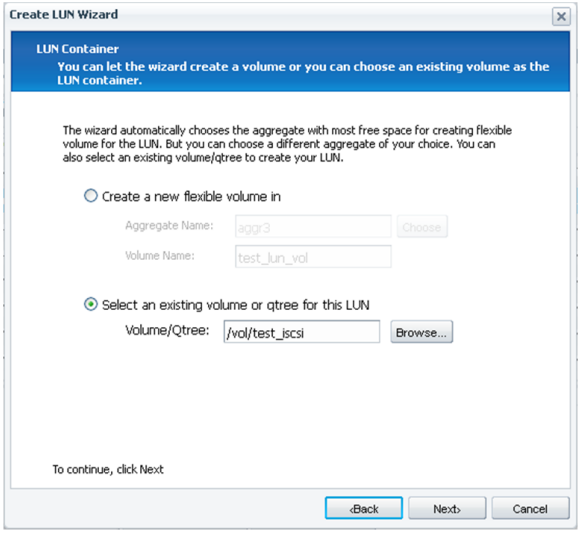
Create a volume on the NetApp volume. For example, `test_iscsi`.

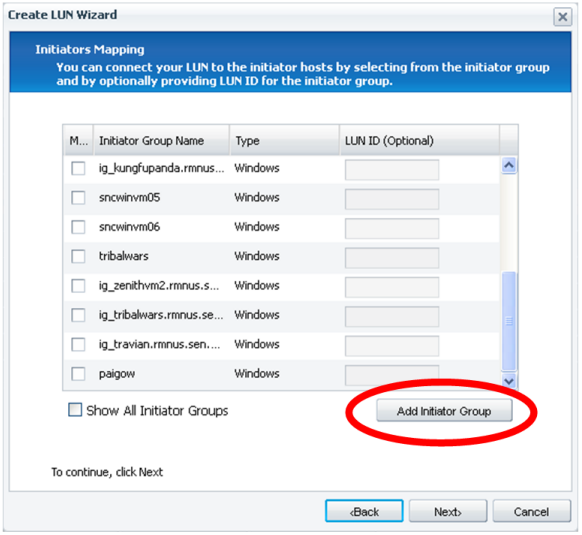
In the **Create Volume** dialog box, click **Create**.

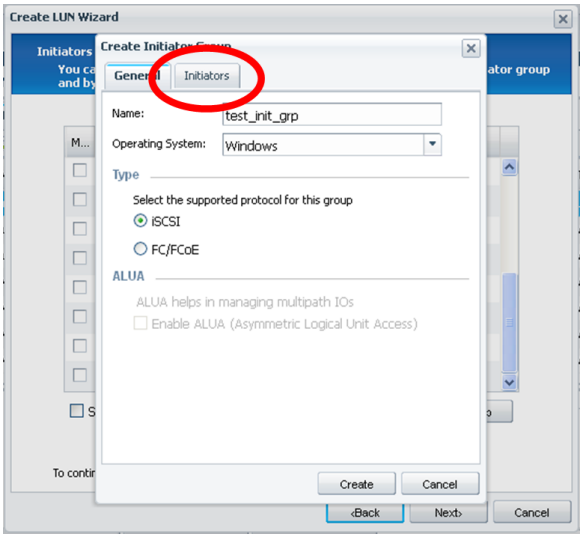
The LUN size should be less than 50% of the volume size.



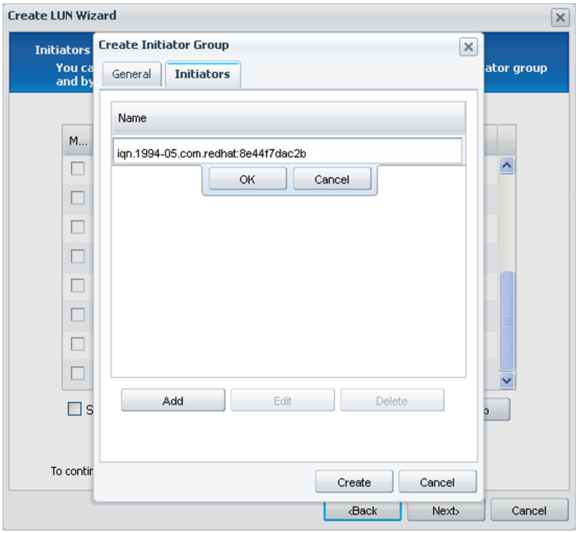

Create LUN Wizard
General Properties
You can specify the name, size, type, and an optional description for the LUN that you would like to create.
You can enter a valid name for the LUN and an optional short description
Name:
test_lun
Description:
(optional)
You can specify the size of the LUN. Storage will be optimized according to the type selected.
Type:
Windows
Size:
50
MB
Thin Provisioned
Allocate space as it is used, otherwise, allocate the space now. Recommended for increasing utilization where each LUN is unlikely to use all of its allocated space.
To continue, click Next
‹Back
Next›
Cancel


Create LUN Wizard
LUN Container
You can let the wizard create a volume or you can choose an existing volume as the LUN container.
The wizard automatically chooses the aggregate with most free space for creating flexible volume for the LUN. But you can choose a different aggregate of your choice. You can also select an existing volume/qtree to create your LUN.
Create a new flexible volume in
Aggregate Name:
aggr3
Choose
Volume Name:
test_lun_vol
Select an existing volume or qtree for this LUN
Volume/Qtree:
/vol/test_iscsi
Browse...
To continue, click Next
‹Back
Next›
Cancel





Enter the name of the initiator server from step 3. (The initiator name found in `/etc/iscsi/initiatorname.iscsi`.) In this example, the name is *iqn*.



Complete the wizard.

5 To discover the presented LUNs, run the `iscsiadm` command from the Linux server.

```
# iscsiadm -m discovery -t sendtargets -p 10.209.7.15
10.209.7.15:3260,1001 iqn.1992-08.com.netapp:sn.151754815
[fe80::2a0:98ff:fe27:c21c]:3260,1001 iqn.1992-08.com.netapp:sn.151754815
```

6 Restart the iSCSI initiator to make the new block device available to the operative system.

```
# service iscsi restart
```

Stopping iSCSI daemon:

```
iscsid is stopped                          [  OK  ]
Starting iSCSI daemon:                     [  OK  ]
                                           [  OK  ]
Setting up iSCSI targets: Logging in to [iface: default, target: iqn.1992-08.com.netapp:sn.151754815,
portal: fe80::2a0:98ff:fe27:c21c,3260]
Logging in to [iface: default, target: iqn.1992-08.com.netapp:sn.151754815, portal: 10.209.7.15,3260]
iscsiadm: Could not login to [iface: default, target: iqn.1992-08.com.netapp:sn.151754815,
portal: fe80::2a0:98ff:fe27:c21c,3260].
iscsiadm: initiator reported error (4 - encountered connection failure)
Login to [iface: default, target: iqn.1992-08.com.netapp:sn.151754815,
portal: 10.209.7.15,3260] successful.
                                           [  OK  ]
```

Use the `lsscsi` command to check that the new disk is available.

```
# lsscsi

[0:0:0:0]    disk    VMware   Virtual disk     1.0   /dev/sda
[0:0:1:0]    disk    VMware   Virtual disk     1.0   /dev/sdb
[1:0:0:0]    mediumx STK      L700-vtl         5400  -
[2:0:0:0]    tape    QUANTUM  SDLT600          5400  /dev/st0
[2:0:0:1]    tape    QUANTUM  SDLT600          5400  /dev/st1
[4:0:0:1]    disk    NETAPP   LUN              7360  /dev/sdc
[4:0:0:2]    disk    NETAPP   LUN              7360  /dev/sdd
[4:0:0:3]    disk    NETAPP   LUN              7360  /dev/sde
```

At this point the iSCSI configuration is done. The new LUNs will be available through a system reboot as long as the iscsi service is enabled. Create a filesystem on the device. For example:

```
mkfs -t ext3 /dev/sdc
```

Mount the available LUNS using the `mount` command. For example:

```
mount  /dev/sdc  /data1
```

Configuring the primary NetApp device to use VSS with Replication Director

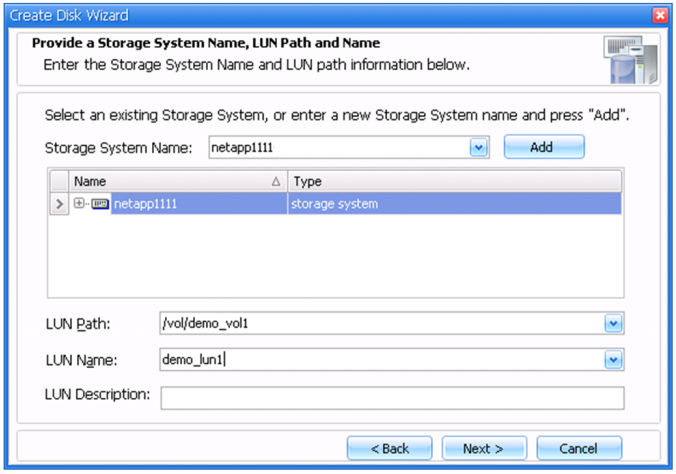
For SAN (block) device support on Windows hosts, the primary NetApp disk array must be configured to use Windows Volume Shadow Services (VSS) with Replication Director.

The primary NetApp device can be configured using the SnapDrive application or without using the application. See the NetApp documentation for the most complete instructions. Procedures are listed here for ease of use.

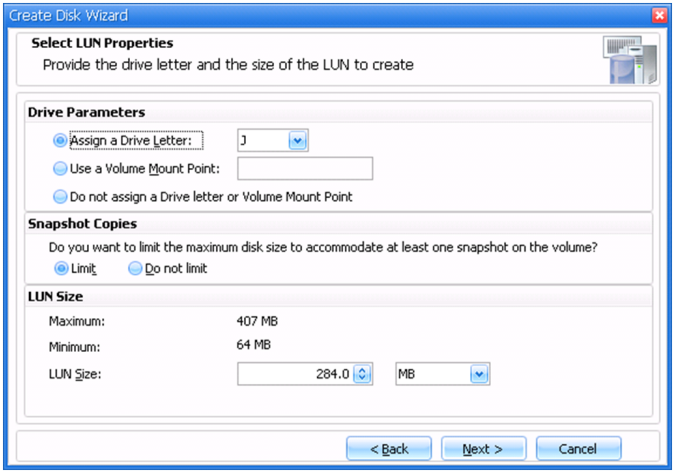
Note: After configuration, make sure that the `NOSNAPDIR` option is set to off for the storage system. If it is not, the Windows Event Viewer displays a SnapDrive entry urging you to turn it off.

To configure the primary NetApp device with the SnapDrive application

1. Create the volume or the qtree on the disk array.
2. Install the SnapDrive application on the host.
3. In the NetApp **SnapDrive** console, select the **Create disk** action to start the **Create Disk Wizard**.
4. Enter the name of the disk array as the **Storage System Name**. The wizard then lists all of the volume paths that are available on the array.

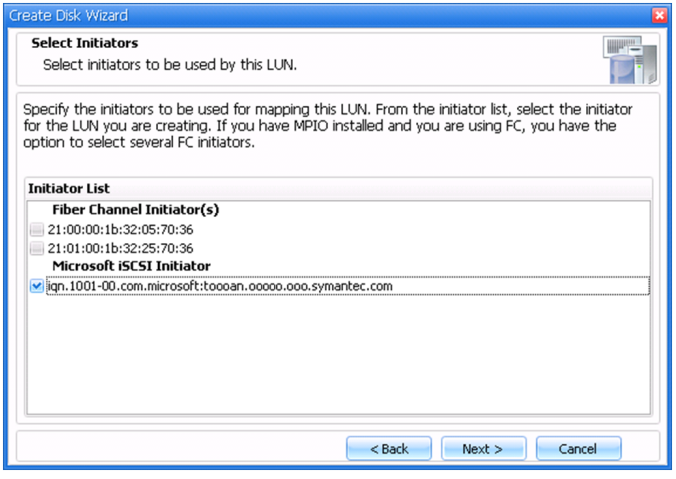


5 In the **LUN Path** drop-down menu, select the volume path where you want to create the LUN. Enter the **LUN Name** and click **Next**.



6 In the **Select LUN Properties** panel, select the drive letter and the LUN size that needs to be created.

7 In the **Select Initiators** panel, select the initiator.



8 Complete the remaining panels of the **Create Disk Wizard**.

To configure the primary NetApp device without using the SnapDrive application

1. Create the volume or the qtree on the disk array.
2. Create the LUN on the volume or the qtree.
3. To connect devices through the Fibre Channel, create the SAN zoning between the disk array and the client.
4. To connect devices through iSCSI, enable the iSCSI initiator on the client.
5. Create an initiator group on the disk array with the port WWN or the iSCSI initiator name of the client.
6. Map the LUN to this new initiator.
7. Rescan the devices on the host.
8. Create the file system on the LUN through **Disk Management**.

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.

Supported NetApp topologies

Table 3-2 describes the NetApp topologies that Replication Director supports. All begin with a snapshot of the data on the primary volume.

Table 3-2 Supported NetApp snapshot replication topologies

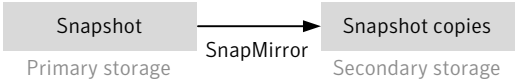
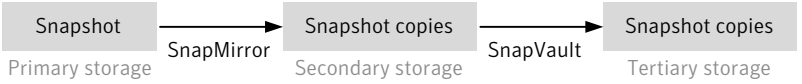
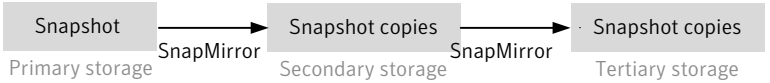
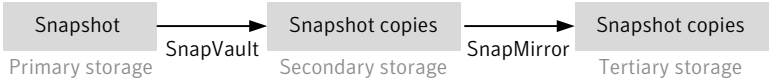
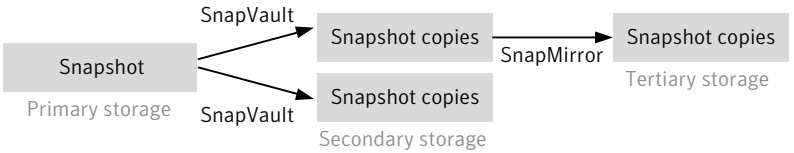
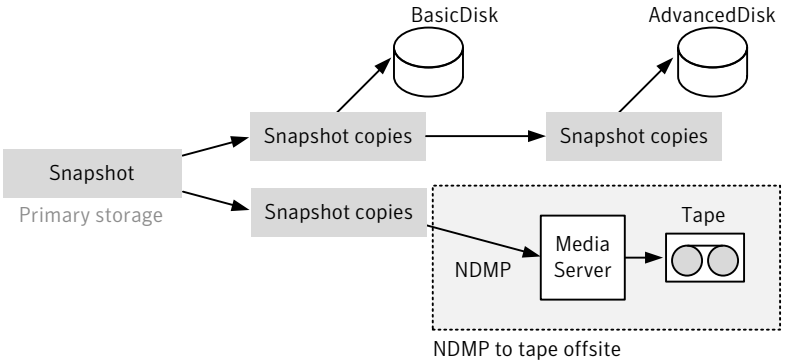
Representation	Description
	The snapshot can be replicated using SnapVault.
	The snapshot can be replicated using SnapMirror.
	The snapshot can be replicated using SnapMirror, and then replicated again using SnapVault.
	The snapshot can be replicated using SnapMirror, and then replicated again using SnapMirror.
	The snapshot can be replicated using SnapVault, and then replicated again using SnapMirror.
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.)

Table 3-2 Supported NetApp snapshot replication topologies *(continued)*

Representation	Description
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 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 3-3 lists the topologies that are not supported in this release.

Table 3-3 Unsupported snapshot replication topologies

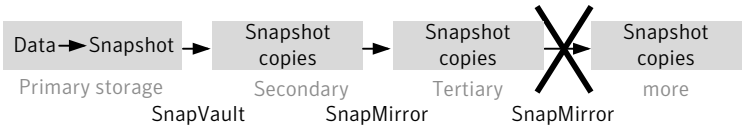
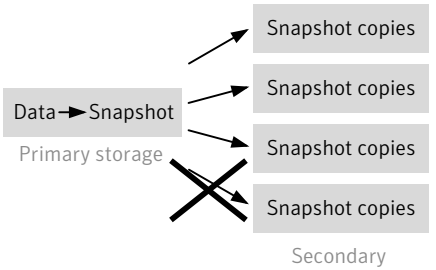
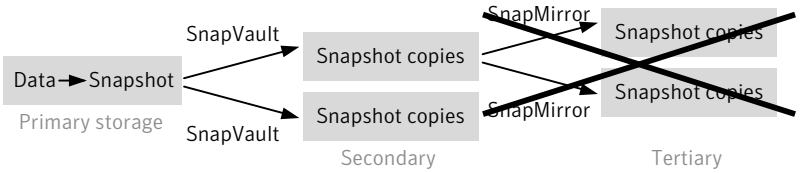
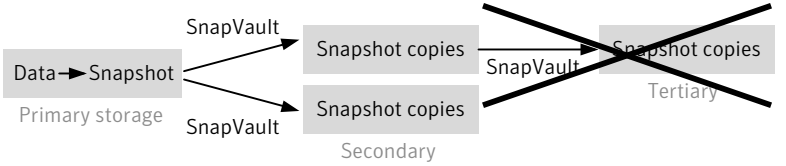
Example of an unsupported configuration	Description
One example of an unsupported configuration: 	The snapshot can be replicated in succession, or cascaded, no more than two times.

Table 3-3 Unsupported snapshot replication topologies *(continued)*

Example of an unsupported configuration	Description
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: Mixed aggregate replications are not qualified or tested with Replication Director in NetBackup 7.6. For example, from a 32-bit aggregate to a 64-bit aggregate and vice versa.

If the DataFabric Manager root or administrator password has changed

If the root or the administrator password for the DataFabric Manager server 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.

Configuring the port use between the DataFabric Manager server and NetBackup hosts

NetBackup communicates with the DataFabric Manager server through SOAP plug-ins: the OSTPlugin on master servers, media servers, and clients, and the NetApp Plug-in for Symantec NetBackup (NBUPlugin) on DataFabric Manager servers.

In order for the plug-ins to communicate, the client (NetBackup) needs to know on which port the DataFabric Manager server listens. The web service that the NBUPlugin 1.1 implements, listens on port 8086 (for `Https`) by default. (In NetBackup 7.5 the NBUPlugin listened on port 8085 (for `Http`) by default.)

During an upgrade from NetBackup 7.5 to NetBackup 7.6, the user is not prompted for the port change from 8085 to 8086 because NetBackup changes it automatically. NetBackup 7.6 assumes 8086, but falls back to port 8085 if necessary.

Note: Earlier versions of the NBUPlugin offer limited capability.

See "Compatibility between Replication Director and NetApp plug-ins" on page 22.

During the NBUPlugin installation, the administrator is asked on which port the NBUPlugin should listen. Certain firewall considerations on the DataFabric Manager server may require that the default port be changed upon installation to allow communication between the plug-ins.

However, if the default port was not changed during NBUPlugin installation and the firewall settings on the DataFabric Manager server do not allow access to port 8086 (for `Https`), the following procedure describes the necessary steps to change the port after installation

To change the port that the NetApp NBUPlugin and the NetBackup OSTPlugin use for SOAP communication

1. Locate the following file on DataFabric Manager server that runs the NBUPlugin:

   On Windows: *Install_path*\Program Files\NetApp\NBUPlugin\NBUPlugin.cfg

   On UNIX: /usr/NetApp/NBUPlugin/config/NBUPlugin.cfg

2. Locate the following setting within NBUPlugin.cfg:

   The default port for NBUPlugin 1.1:

   ```
   [NBUPlugin:https_port]

   Value=8086
   ```

   The default port for NBUPlugin 1.0.1:

   ```
   [NBUPlugin:port]

   Value=8085
   ```

3. Change the port value from the default port to another port that accommodates the firewall. For example, 8090:

   For NBUPlugin 1.1, enter:

   ```
   [NBUPlugin:https_port]

   Value=8090
   ```

   For NBUPlugin 1.0.1, enter:

   ```
   [NBUPlugin:port]

   Value=8090
   ```

   Save and close the file.

4. Shut down, then restart the NBUPlugin after changing the port number.

   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
   ```

5 On every NetBackup host that communicates with this DataFabric Manager server, create a file named `soapwrapper.conf` in the following location:

On Windows: *`Install_path`*`\Program Files\VERITAS\Netbackup\bin\ost-plugins\soapwrapper.conf`

On UNIX: `/usr/openv/lib/ost-plugins/soapwrapper.conf`

6 Add a line with the following syntax to each `soapwrapper.conf` file:

`OC_host_ie_storage_servername` `= http://`*`OC_host_ie_storage_servername`*`:`*`Desired_port`*

Where:

- *OC_host_ie_storage_servername* is the name of the DataFabric Manager server.
- *Desired_port* is the desired port (and not the default). This port number should match the port that was entered in step 3.

For example, if the storage server name is *OCserver1* and the desired port is 8090:

```
OCserver1 = http://OCserver1.yourdomain.com:8090
```

7 Create a `soapwrapper.conf` file that includes this line on every NetBackup host that communicates with this DataFabric Manager server. That means every master server, media server, client, and alternate client that is included in a policy or in a storage lifecycle policy for Replication Director

In the environments that contain multiple storage servers that do not use the default port, use one `soapwrapper.conf` file on each NetBackup host. In the file, list each storage server and the non-default port for each.

Importing existing NetApp relationships for NetBackup control

NetApp offers an import tool to migrate DataFabric Manager server 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 DataFabric Manager server 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 Symantec NetBackup Installation and Administration Guide*, available from the NetApp Support Site.

Chapter 4

NetBackup configuration

This chapter includes the following topics:

NetBackup configuration for Replication Director

NetBackup configuration is performed by the NetBackup administrator, as described in Table 4-1.

Table 4-1 NetBackup configuration tasks overview

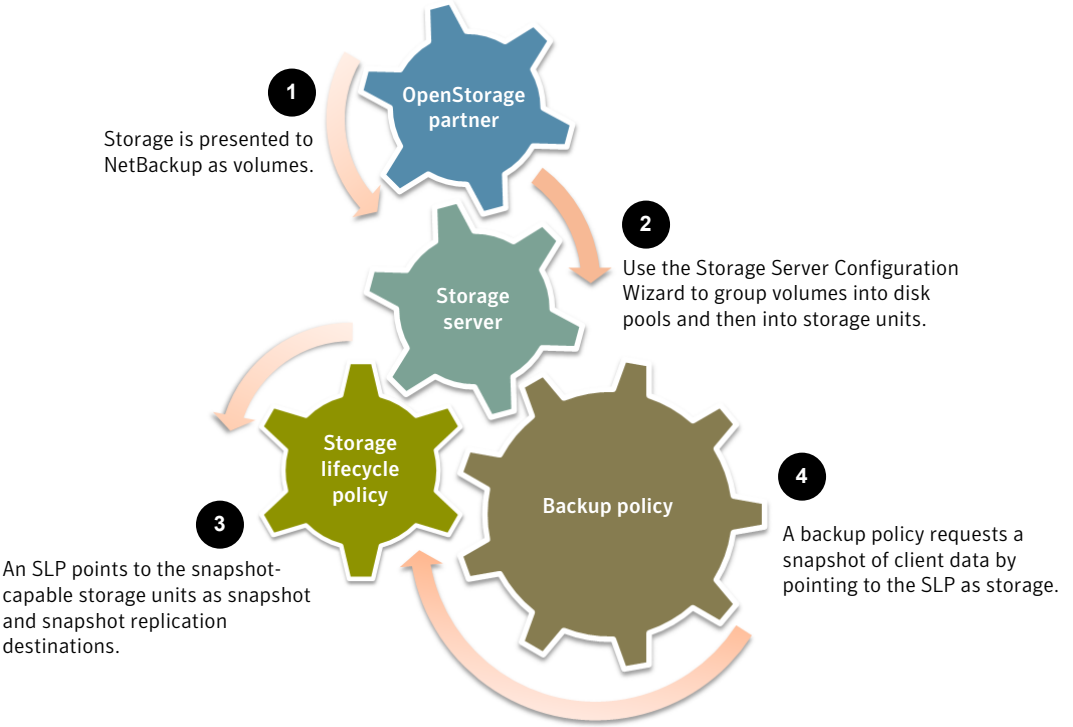
Step	Description	Reference topic
1	Install or upgrade NetBackup software on the master server and media server(s).	See "Required software" on page 21.
2	Run the Storage Server Configuration Wizard to configure the OpenStorage partner as a NetBackup storage server. This wizard also configures the following: ■ 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 54.
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 72.
4	Create a storage unit for any operation that will produce duplications (non-snapshot copies).	See "Creating a storage unit" on page 91.

Table 4-1 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 118.
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 use Replication Director to protect NAS volumes" on page 140. See "Configuring an NDMP policy to protect a NAS host using NDMP with Replication Director" on page 128. See "About Oracle support for Replication Director" on page 147. See "About virtual machines and Replication Director" on page 158.

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 4-1 How NetBackup uses OpenStorage partner storage



Chapter 5

Advanced configuration topics

This chapter includes the following topics:

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 77.

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:

`-storage_server storage_server`	The name of the disk appliance.
`-stype server_type`	The storage vendor provides the string that identifies the server type.
`-media_server media_server`	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.

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 5-1.

Table 5-1 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.

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 this, 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.

Chapter 6

Configuring a NetBackup storage server for Replication Director

This chapter includes the following topics:

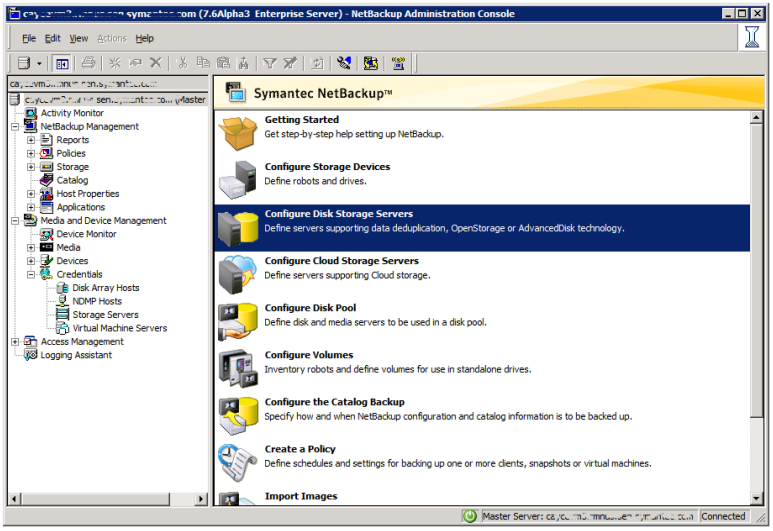
Creating a NetBackup storage server for snapshot replication

A NetBackup storage server is a NetBackup entity that has exclusive access to manage snapshots on the volumes of an OpenStorage partner. In NetBackup 7.6, Replication Director can use a NetApp DataFabric Manager server.

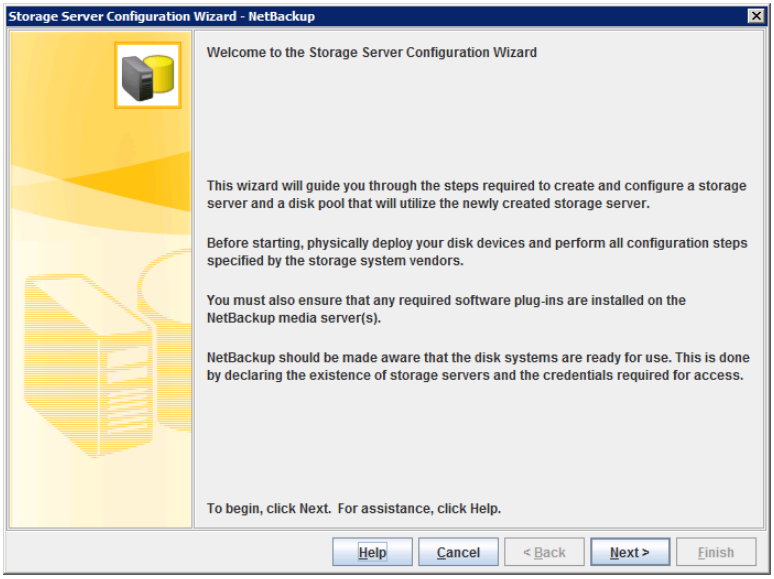
- One NetBackup domain can support multiple DataFabric Manager servers.
- Five master servers can communicate efficiently with one NBUPlugin on a DataFabric Manager server. The DataFabric Manager server determines the number of concurrent jobs that it can run from any number of media servers.

To create a storage server

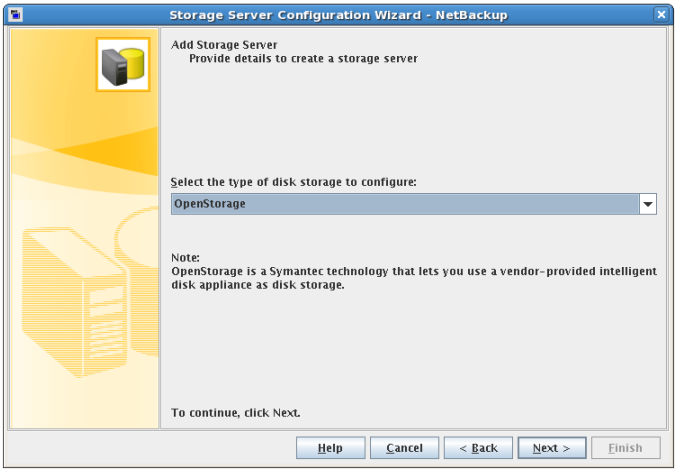
1. Before launching the **Storage Server Configuration Wizard** wizard, make sure that the OpenStorage partner has the necessary software installed and is online. The volumes of the disk array must also be configured.
2. To create a storage server, click **Configure Disk Storage Servers** in the **NetBackup Administration Console** main window.



3 Before continuing, make sure that all necessary disk storage devices are configured in the environment and that the vendor plug-in is installed



4 Select **OpenStorage** as the disk storage type to be configured in this wizard. Click **Next**.



5 Configure the details of the storage server.

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. If not, snapshot replication may fail.

Enter the exact name of the storage server, whether a fully-qualified name or a short name. This name is the name of the OnCommand server (the DataFabric Manager server).

Use the `bpstsinfo` command, located in the following directory, to verify the exact storage server name:

- Windows: *`Install_path`*`\NetBackup\bin\admincmd\`
- UNIX: `/usr/openv/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 DataFabric Manager server is *DFMServer*, enter the following command:

```
bpstsinfo -serverinfo -storage_server DFMServer -stype
Network_NTAP
```

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

Storage server type

Select the type of storage server to create. Select **NetApp OnCommand server** (DataFabric Manager server) 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/openv/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.

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. The user must have administrator or root privileges on the DataFabric Manager server.
  For NetApp, the credentials are used to log on to the DataFabric Manager server.
  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.

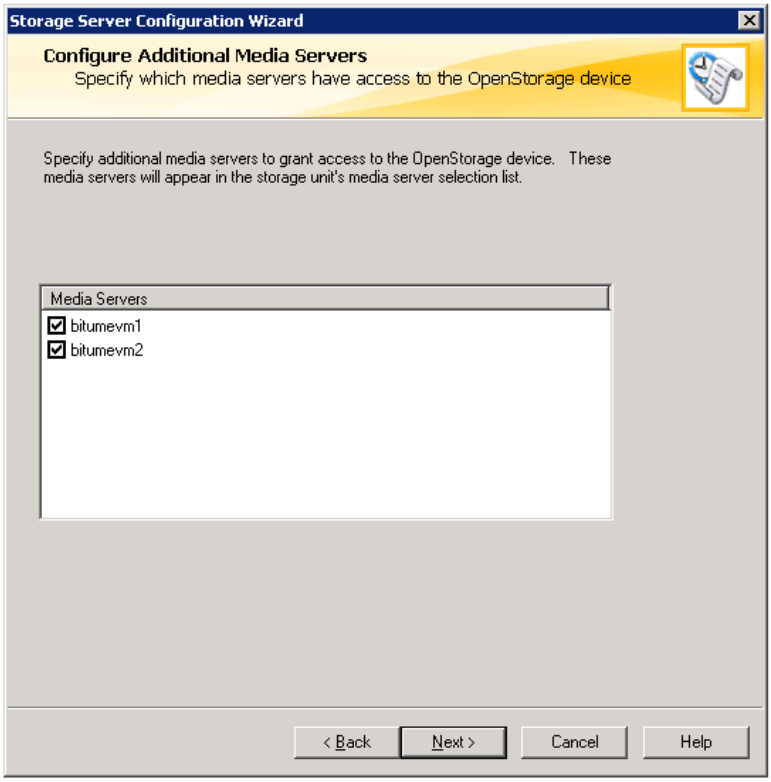
See "Adding the storage server credentials to a NetBackup server" on page 67.

Click **Next**.

6 The **Configure Additional Media Servers** 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 5).



7 The wizard displays a summary panel that lists the configuration information that you've entered. Click **Next**.

8 The wizard displays a panel that contains the creation status of the storage server. Click **Next**.

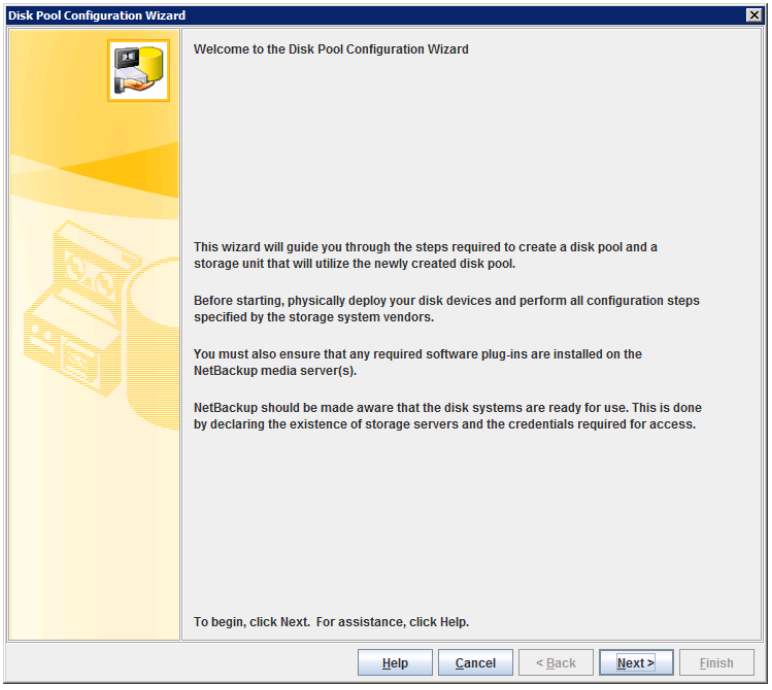
9 The wizard declares that the storage server was successfully created. Click **Next** to launch the **Disk Pool Configuration Wizard**. A disk pool is necessary for snapshots and snapshot replication.

Note: If the **Disk Pool Configuration Wizard** does not launch automatically, click **Configure Disk Pool** in the **NetBackup Administration Console** to start the wizard manually.

---

10 In the **Disk Pool Configuration Wizard** welcome panel, click **Next**.

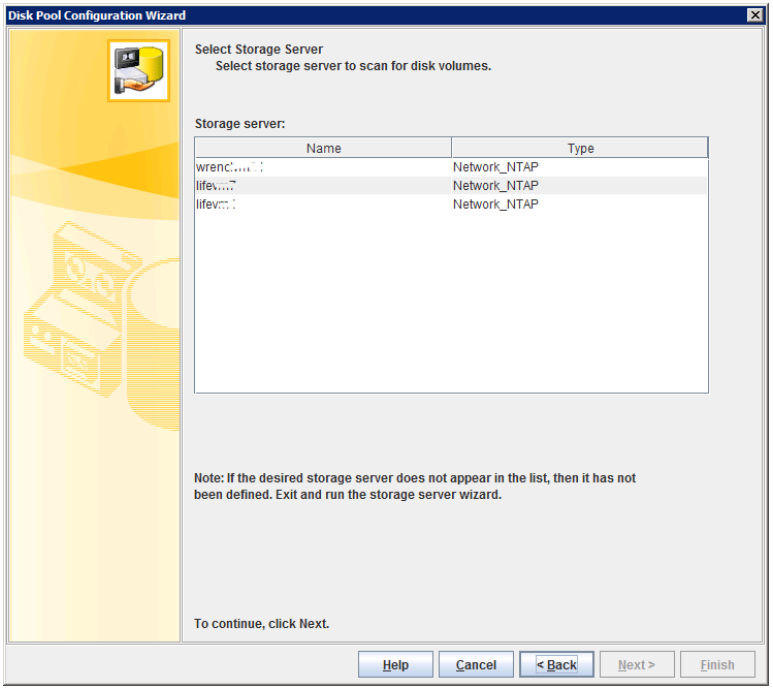
Again you are asked whether all necessary disk storage devices are configured in the environment and the vendor plug-ins necessary for Replication Director are installed.



11 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

To configure a disk pool for NetApp, select **OpenStorage (Network_NTAP)**.

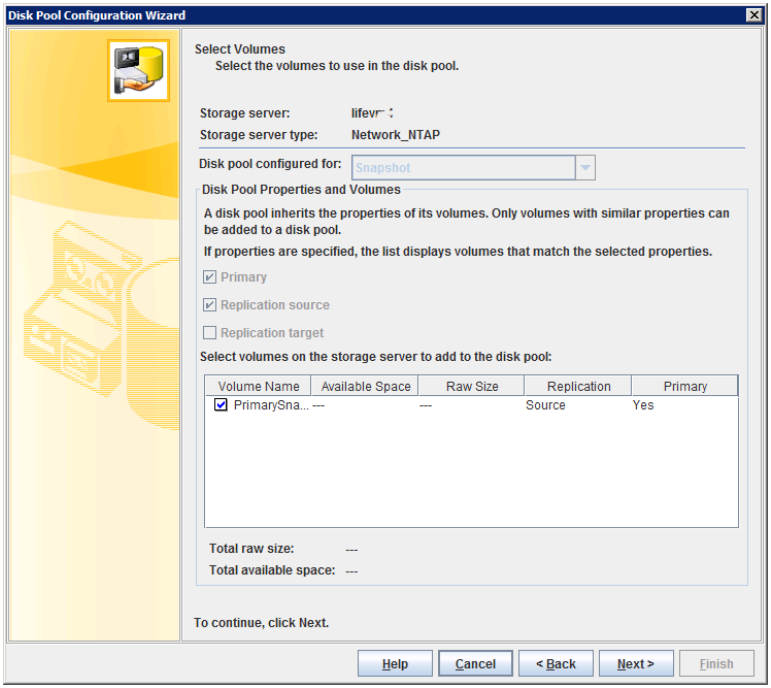
12 On the **Select Storage Server** panel, select the storage server that was created earlier in the wizard. Click **Next**.



13 The **Select 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.



Regarding disk pools for DataFabric Manager storage servers:

- For DataFabric Manager storage servers, the total sizes on the primary volume always display as 0 bytes, as indicated by a dash.
- When the NBUPlugin is installed on the DataFabric Manager server, a NetBackup group is automatically created on the DataFabric Manager server. On the DataFabric Manager server, 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.

14 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**.

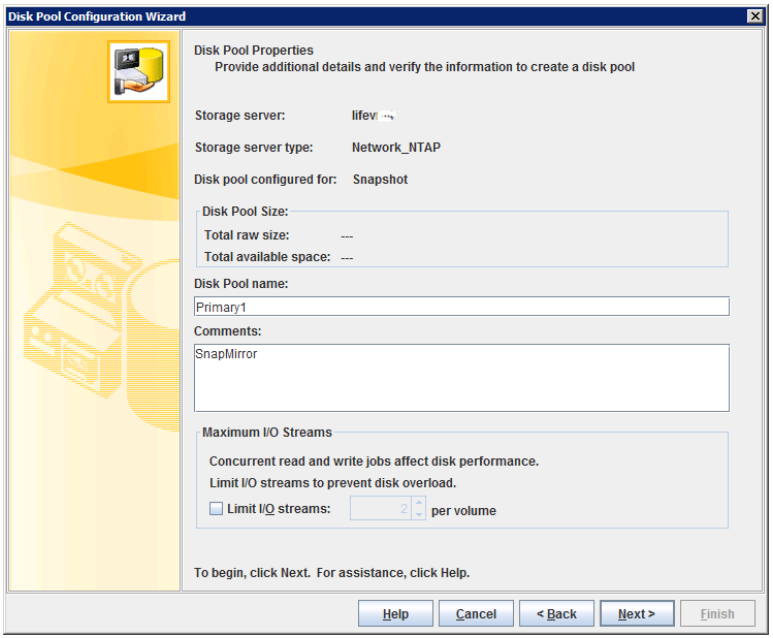
15 In the **Additional Disk Pool Information** panel, name the disk pool and add any comments you want to make regarding the disk pool.

See "NetBackup naming conventions" on page 67.

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 DataFabric Manager storage servers, the sizes on the primary volume always display as 0 bytes, as indicated by a dash.

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**.

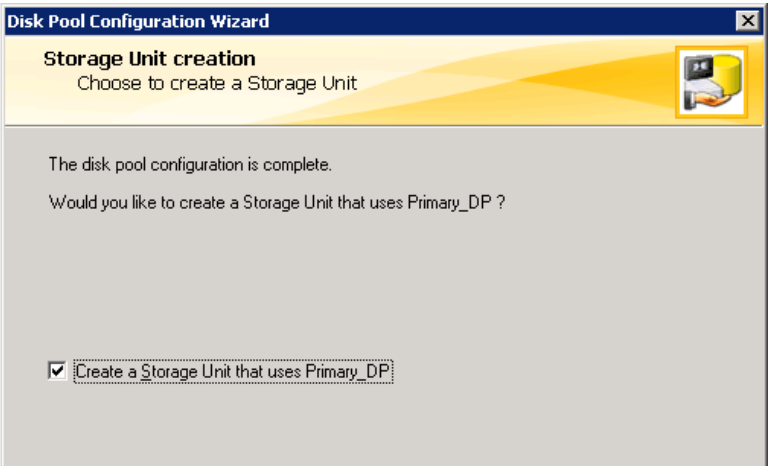


16 The disk pool summary panel displays the storage server configuration up to this point. Click **Next** to configure the disk pool.

17 The wizard announces the successful creation of the disk pool. Click **Next**.

18 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 snapshots.

Select **Create a storage unit that uses *New disk pool name*** and click **Next**.



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

See "NetBackup naming conventions" on page 67.

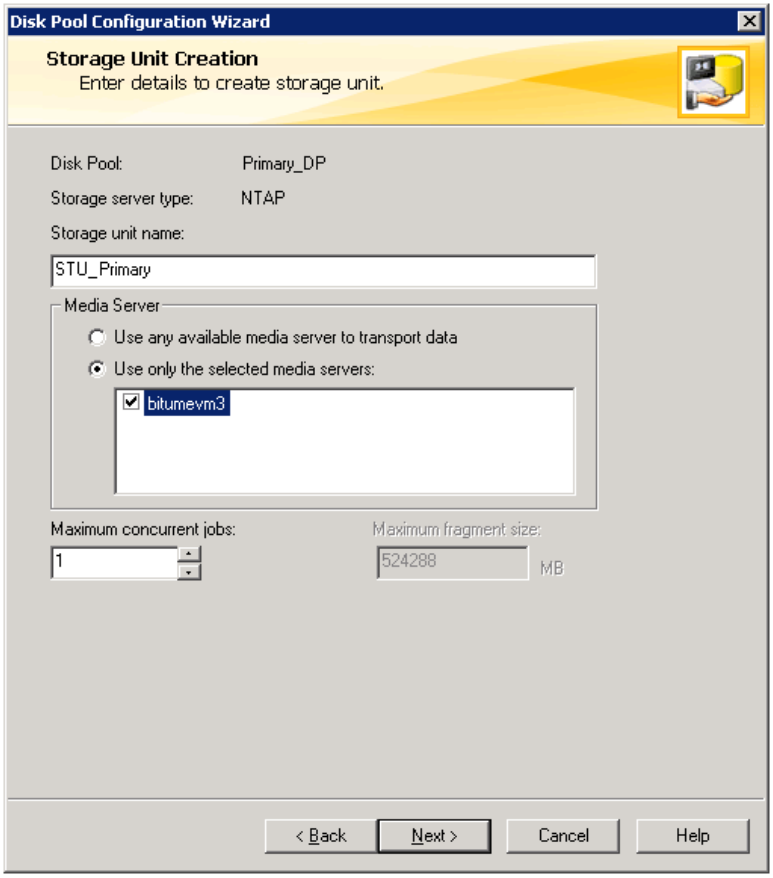
Select the media server(s) that can use the storage unit.

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.

See "Adding the storage server credentials to a NetBackup server" on page 67.

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.

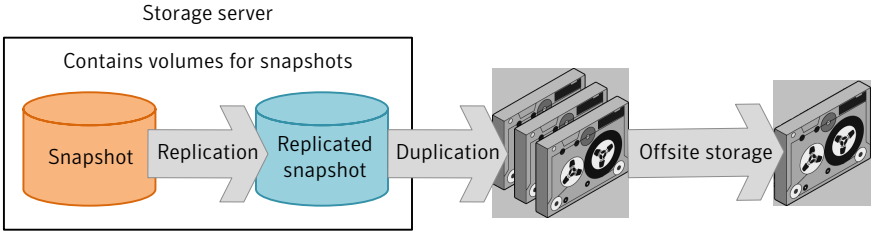


20 Click **Next**. The final wizard panel displays, announcing that the wizard has been completed.

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.



NetBackup controls the data throughout its lifecycle

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

See "Creating disk pools for snapshot replication" on page 72.

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**.

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.

Chapter 7

Configuring disk pools for snapshot and replication

This chapter includes the following topics:

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 and 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 72.

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 101.
- 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 102.

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 96.

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 (S*n*) to the disk pool you use for snapshot creation. Then, add the target volumes (T*n*) 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 SnapMirror relationship is not defined at the volume layer, then the **Mirror** property does not appear in the wizard panel for selection.

Table 7-1 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 7-1 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 be 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.

Run the **Disk Pool Configuration Wizard** after running the `bpstsinfo` command. The output from the command is necessary 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 the device" on page 84.

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. For example, to configure an OpenStorage disk pool for NetApp, select **OpenStorage (Network_NTAP)**.
4. On the **Select Storage Server** panel, select the storage server. Click **Next**.

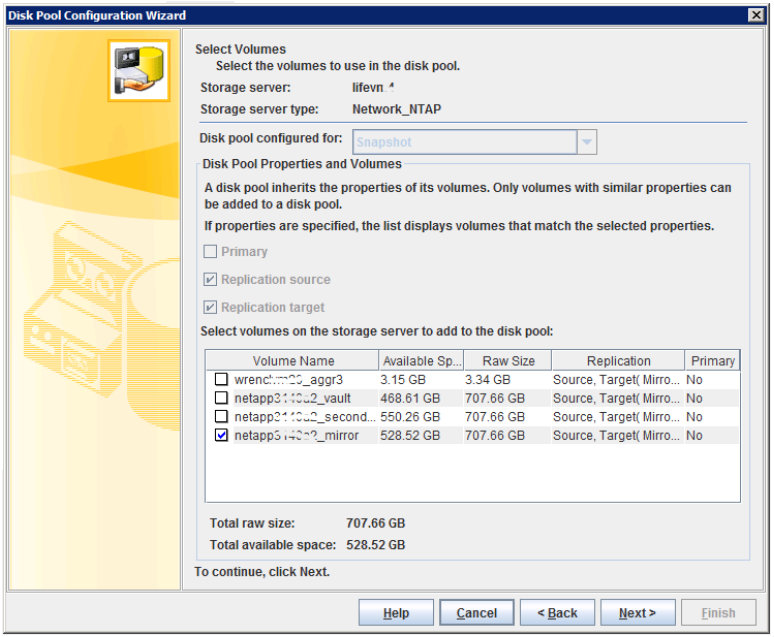
5 The **Select Volumes** panel presents all of the volumes that have been configured in the storage of the OpenStorage partner by the storage administrator.

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.

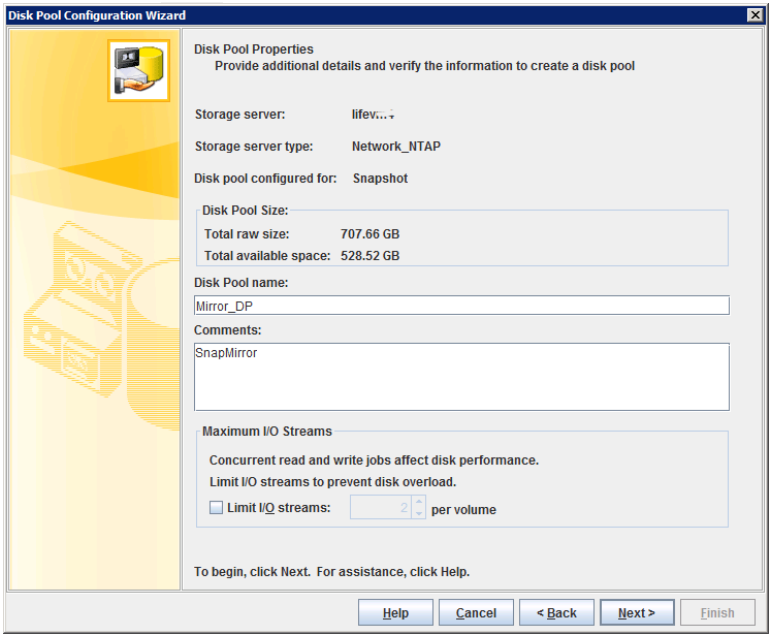
Note: When the NBUPlugin is installed on the DataFabric Manager server, a NetBackup group is automatically created on that server. On the DataFabric Manager server, use the NetApp Management Console to add resource pools to the NetBackup group so that the resource pools are exposed to NetBackup. If the NetBackup group contains no resource pools, no LSUs display in the disk pool configuration wizard.

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 67.

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 *Mirror_DP*** and 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.

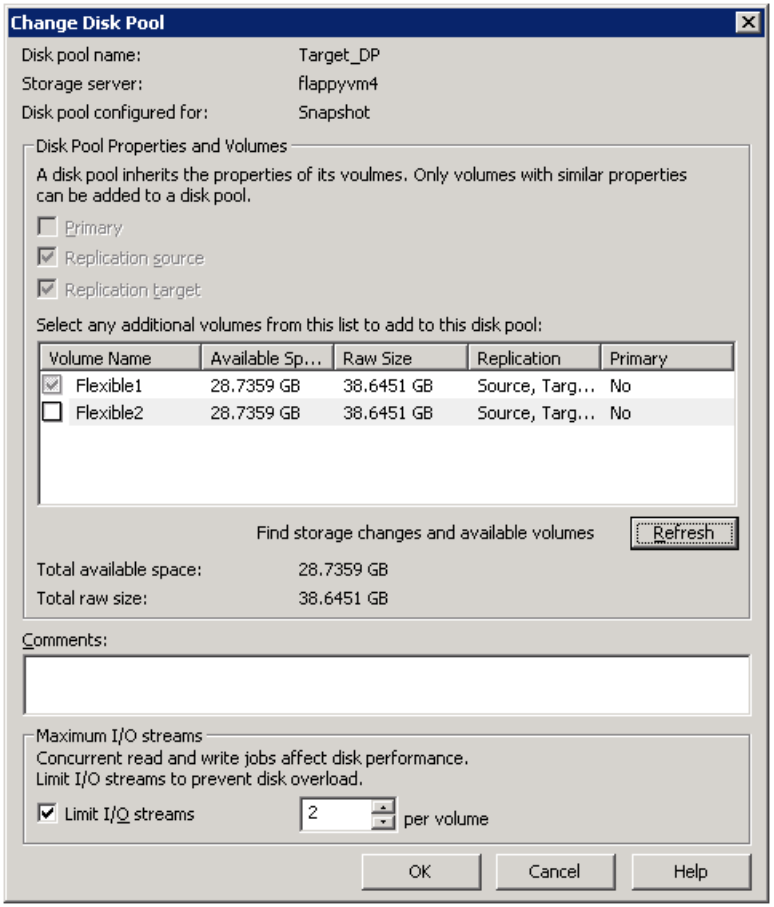
Note: If an OpenStorage partner updates the plug-in on a disk-array, update the NetBackup storage server and the disk pools to reflect the new functionality of the plug-in.

See "Updating an OpenStorage storage server to reflect plug-in updates" on page 50.

See "Updating an OpenStorage disk pool to reflect plug-in updates" on page 77.

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.



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 78.

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

  See the following descriptions of the options that require arguments:

`-changedp disk_pool_name`	The name of the disk pool.
`-stype server_type`	The storage vendor provides the string that identifies the server type.
`-setattribute attribute`	The *attribute* 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

Symantec 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 7-2 describes the possible outcomes and describes how to resolve them.

Table 7-2 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 7-2 Refresh outcomes *(continued)*

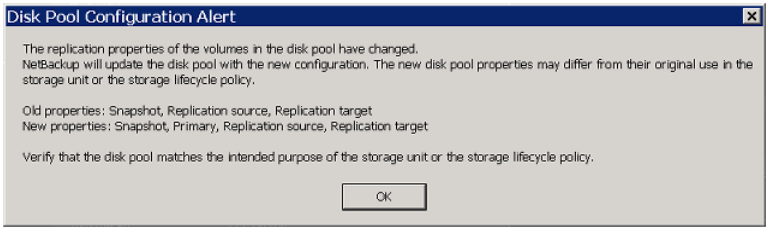
Outcome	Description
The replication properties of all of the volumes changed, but they are still consistent.	A **Disk Pool Configuration Alert** pop-up box notifies you that the properties of all of the volumes in the disk pool changed, but they are all the same (homogeneous).  You must click **OK** 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 7-2 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.  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 7-2 Refresh outcomes *(continued)*

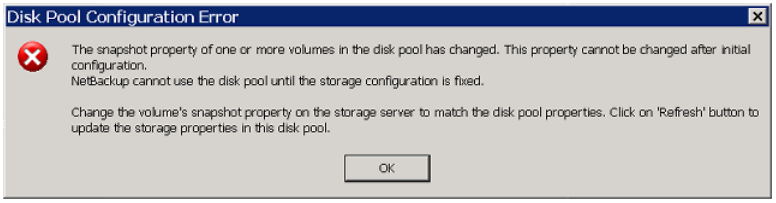
Outcome	Description
The snapshot properties changed.	A **Disk Pool Configuration Error** pop-up box notifies you that the snapshot properties of some of the volumes in the disk pool changed.  You must click **OK** in the alert box. In the **Change Disk Pool** dialog box, the properties of the disk pool 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 7-2 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 `bpstsinfo -lsuinfo` command to discover the current topology. Compare the new topology to the previous topology. See "Using bpstsinfo to view the replication topology of the device" on page 84. 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 7-2 Refresh outcomes *(continued)*

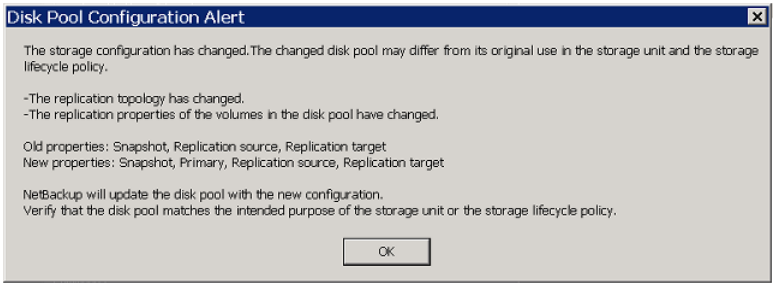
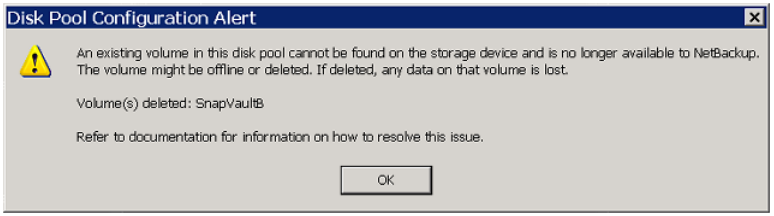
Outcome	Description
The replication topology changed and the replication properties of the volumes in the disk pool changed.	A **Disk Pool Configuration Alert** pop-up box notifies you that the replication topology changed and all of the replication properties of all of the volumes in the disk pool changed. 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 `bpstsinfo -lsuinfo` command to discover the current topology. Compare the new topology to the previous topology. See "Using bpstsinfo to view the replication topology of the device" on page 84. 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 7-2 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 `bpimmedia` command or the Images on Disk report to display the images on the specific volume. ■ Expire the images on the volume. ■ Use the `nbdevconfig` command to set the volume state to DOWN so NetBackup does not try to use it.

Using bpstsinfo to view the replication topology of the 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/openv/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, `Network_NTAP`.
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 )
   .
   .
   .
```

Chapter 8

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

This chapter includes the following topics:

Creating storage units for snapshots and snapshot replication

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 67.

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*)**.

For example, select **OpenStorage (Network_NTAP)** for NetApp.

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 67.

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 a storage unit

A storage unit is a label that NetBackup associates with physical storage. The label can identify a robot, a path to a volume, or a 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**.

For more information about the storage unit settings, see the online Help or the NetBackup Administrator's Guide, Volume I.

To create a storage unit

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 67.

4 Select the **Storage unit type**. The selection specifies the type of storage that the storage unit uses: **Media Manager**, **Disk**, or **NDMP**.

5 For disk storage units:

- Select a disk type from the **Disk type** drop-down menu.
  The **Disk type** identifies the type of storage unit destination:

AdvancedDisk storage unit	The destination is a disk pool.
BasicDisk storage unit	The destination is a path to a volume on a host.
Cloud Storage storage unit	The destination is a disk pool of the type that includes a ***VendorName*** string. ***VendorName*** can be the name of a cloud storage provider. Possible values include **Amazon**, **AT&T**, **Nirvanix**, and **Rackspace**. These values also can contain a **_crypt** suffix (for example, **Amazon_crypt**). The **_crypt** suffix indicates encrypted storage.
NDMP storage	The destination is an NDMP host. The NDMP protocol is used to perform backups and recoveries.
OpenStorage storage unit	The destination is a disk pool of the type that includes a ***VendorName*** string. The vendor supplies the ***StorageName*** string. To configure snapshots and snapshot replication with Replication Director, select **OpenStorage (*storage type*)**. For example, select **OpenStorage (Network_NTAP)** for NetApp.
PureDisk storage unit	The destination is a disk pool. See the NetBackup Deduplication Guide.

- Select a media server in the **Media server** drop-down menu. The selection indicates that the media server has permission to write to the storage unit.
- **Absolute pathname to directory** or **Absolute pathname to volume setting**.
  Specifies the absolute path to a file system or a volume available for backups to disk.
- **Maximum concurrent jobs**
  Specifies the maximum number of jobs that NetBackup can send to a disk storage unit at one time.
- **Reduce fragment size**
  Adjust the fragment size to specify the largest fragment size that NetBackup can create to store backups.

- **High water mark**
  This setting applies to BasicDisk and disk pools. This value is a threshold that, when reached, causes NetBackup to consider the disk full and begin actions to reduce the data on the volume.
- **Low water mark**
  This setting has no effect unless backups are written through a storage lifecycle policy, using the capacity-managed retention type.
- **Enable block sharing**
  Allows the sharing of data blocks that have not changed from one backup to the next.
- **Enable Temporary staging area**
  Allows this storage unit to be used as a temporary staging area for basic disk staging.

6 For Media Manager storage units, data is written to tape robots and stand-alone tape drives:

- Select a storage device from the **Storage Device** drop-down menu.
- Select a media server in the **Media server** drop-down menu. The selection indicates that the media server has permission to write to the storage unit.
- **Maximum concurrent write drives**
  Specifies the number of tape drives that NetBackup can use at one time for jobs to this storage unit.
- **Enable multiplexing**
  Allows multiple backups to multiplex onto a single drive in a storage unit.
- **Reduce fragment size**
  Adjust the fragment size to specify the largest fragment size that NetBackup can create to store backups.

7 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 67.
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**

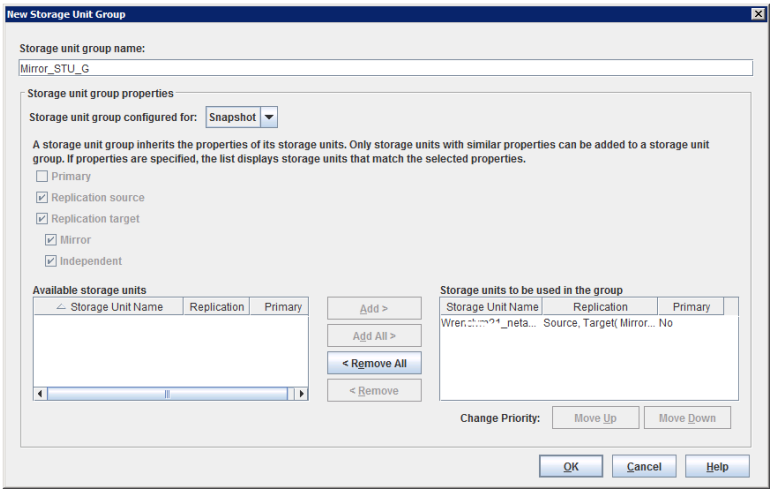
Optionally, enable **Independent** to display the storage units that can act as either a **Mirror** replication target (SnapMirror) or a non-mirror replication target (SnapVault).

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**.
- On Windows:
  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.
- On UNIX:
  To change the priority of a storage unit, select the storage unit and click **Increase Priority** or **Decrease Priority**. 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 8-1 Snapshot storage unit group configuration dialog box



Chapter 9

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

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 9-1 describes the four types of operations that are required in this example replication scenario.

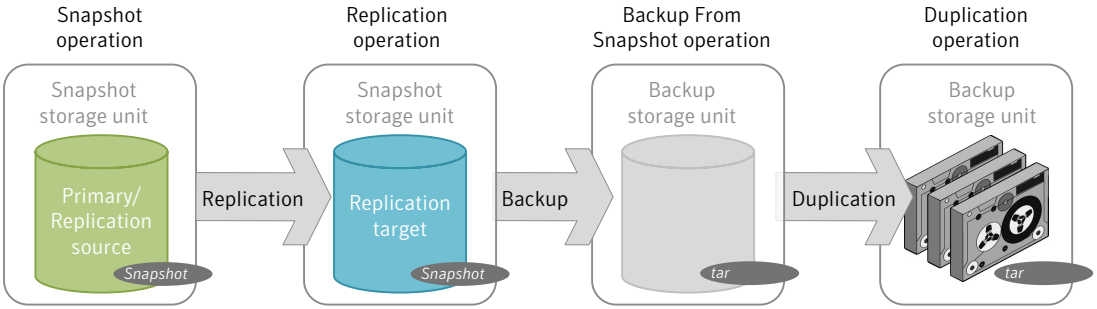


Table 9-1 Example of a storage lifecycle policy configured for snapshots and snapshot replication

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 9-1 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, 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 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.

See "About configuring a backup policy for Replication Director" on page 125.

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.symantec.com/docs/TECH208536

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 99.
■ See "Replication operation in an SLP" on page 103.

- See “Index From Snapshot operation in an SLP” on page 105.
- **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 109.
- See “Duplication operation in an SLP” on page 111.
- **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. Since this guide concentrates on snapshots, 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 a client volume. 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 9-1 Snapshot operation in the New Storage Operation dialog box

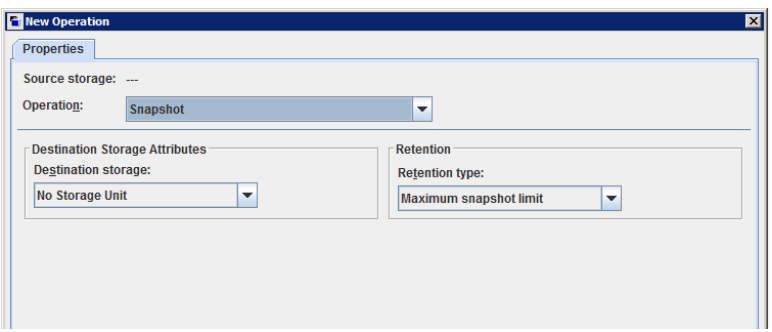


Table 9-2 Snapshot operation characteristics

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 101. ■ See "Primary + Replication source snapshot storage unit" on page 101. ■ See "Replication source + Replication target snapshot storage unit" on page 102. ■ See "Replication target snapshot storage unit" on page 102. ■ See "Replication source + Replication target + Mirror snapshot storage unit" on page 103. ■ See "Replication source + Replication target + Mirror snapshot storage unit" on page 103. 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 118.
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 "Window tab of the Storage Operation dialog box" on page 120.

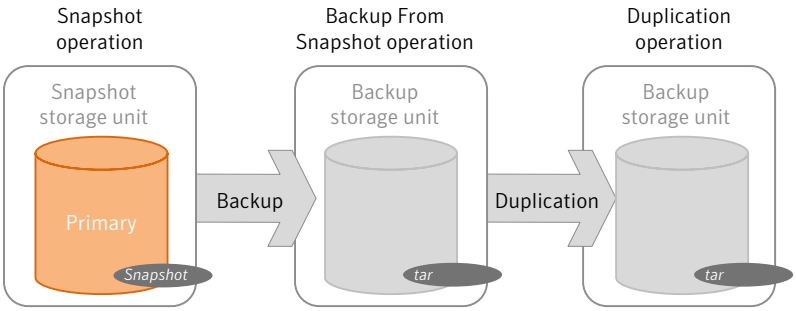
See "About configuring storage lifecycle policies for snapshots and snapshot replication" on page 96.

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 9-2 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 9-2 SLP that contains a Snapshot operation, a Backup From Snapshot operation, and a Duplication operation



An SLP that contains only one **Snapshot** operation cannot perform replication for the following reasons:

- The primary-only operation does not have the source property set so that it can act as a source for replication.
- The SLP does not contain a **Replication target** for a replica.

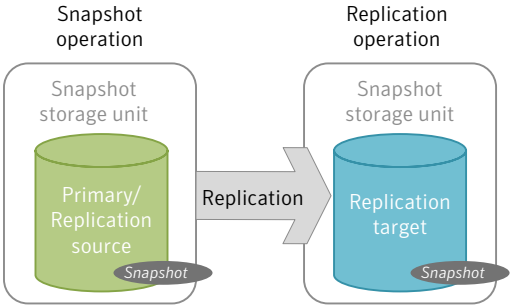
Primary + Replication source snapshot storage unit

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 9-3 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 9-3 SLP that contains a Snapshot operation and a Replication operation

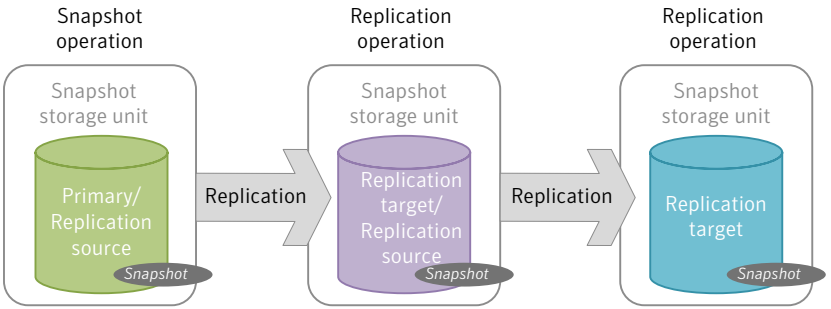


Replication source + Replication target snapshot storage unit

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 9-4 SLP that contains a Snapshot operation and two Replication operations

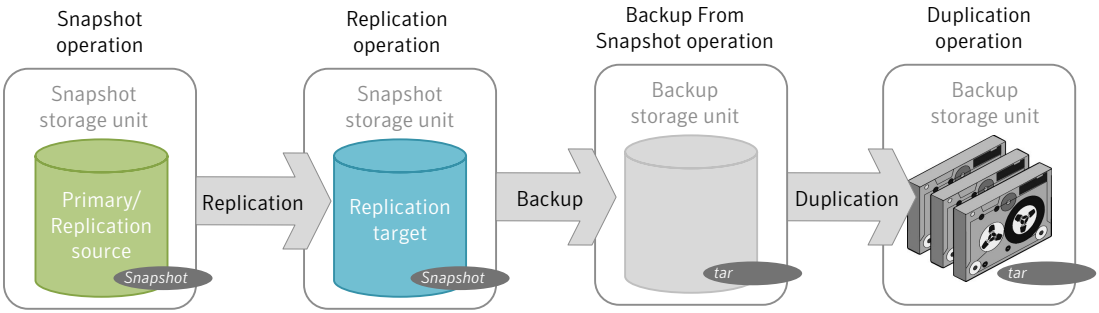


Replication target snapshot storage unit

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 9-5 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 9-6. See "About NetBackup Replication Director" on page 12.
- NetBackup Auto Image Replication to replicate a backup, as shown in Figure 9-7.

Figure 9-6 Replication operation following a Snapshot operation

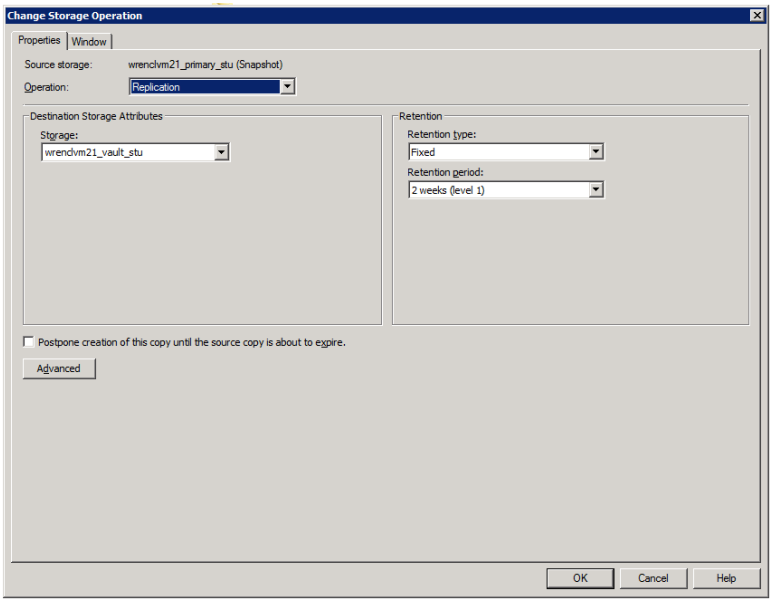


Figure 9-7 Replication operation following a Backup operation

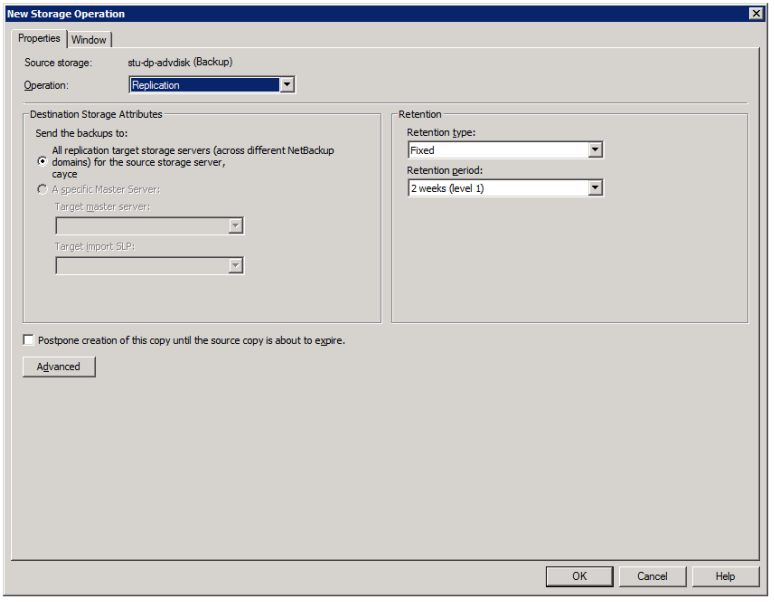


Table 9-3 Replication operation characteristics

Characteristic	Description
Storage unit selection	Under **Destination storage attributes**: ■ For Replication Director, select the **Storage** that is configured to contain replicated snapshots. ■ For Auto Image Replication, choose to either: ■ Replicate the backup to storage servers in all target NetBackup domains. ■ Replicate the backup to a specific master server in a specific domain.
Child of	Click on the appropriate operation when adding a **Replication** operation. A **Replication** operation can be the child of any of the following operations: ■ **Snapshot** operation for NetBackup Replication Director to replicate a snapshot. ■ Another **Replication** operation. ■ **Backup** operation for NetBackup Auto Image Replication. See "Creating a storage lifecycle policy for snapshots and snapshot replication" on page 118.
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 109.
Job type	A **Replication** operation generates a **Replication** job in the **Activity Monitor**.
Window	The only SLP window that a **Replication** operation can use is the **Default_24x7_Window**. See "Window tab of the Storage Operation dialog box" on page 120.

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 `.f` file in the NetBackup catalog for each snapshot. The presence of an image .f file assists the user when a file needs to be restored from the snapshot, as described in Table 9-4.

The **Backup From Snapshot** operation also creates an image .f 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 9-4 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 .f 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 a .f 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 .f file must be present in the NetBackup catalog.

Table 9-5 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.

Table 9-5 Index From Snapshot operation characteristics *(continued)*

Characteristic	Description
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 118.
Source for	While an **Index From Snapshot** operation cannot be the source for any operation, a **Replication** operation can follow it.
Hierarchy notes	The **Index From Snapshot** operation can consume system resources and requires that each snapshot be mounted to create the .f file. See "Determining where and when the Index From Snapshot operation occurs" on page 108.
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. See "Window tab of the Storage Operation dialog box" on page 120.

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** and **MS-Windows** backup policy types support the use of storage lifecycle policies that contain the **Index From Snapshot** operation.
  The **Index From Snapshot** operation is not supported for any policy that uses NDMP. (For example, an **NDMP** policy, or a **Standard** or **MS-Windows** policy with NDMP **Data Mover** enabled.)
- The **Index From Snapshot** operation can run from a full or an incremental schedule. The file entries that are added to the `.f` 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 `.f` file.
- The **Index From Snapshot** operation differs from other operations in that it does not create a copy of a snapshot or backup. Even though this operation does not create a copy, the existence of the operation in the SLP counts toward the number indicated by the **Maximum backup copies**. The **Maximum backup copies** property in the **Global Attributes** host properties specifies the total number of backup copies that can exist in the NetBackup catalog.

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.
  See "Window tab of the Storage Operation dialog box" on page 120.
- 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 `.f` 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 `.f` 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 9-8 shows an SLP with a valid configuration.
    Figure 9-9 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 9-8 Example 1 of a valid placement of the Index From Snapshot operation

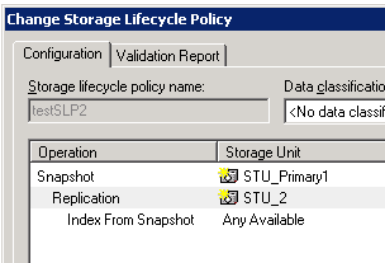
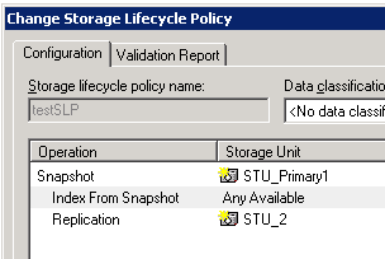


Figure 9-9 Example 2 of a valid placement of the Index From Snapshot operation



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 9-10 Backup From Snapshot operation in the New Storage Operation dialog box

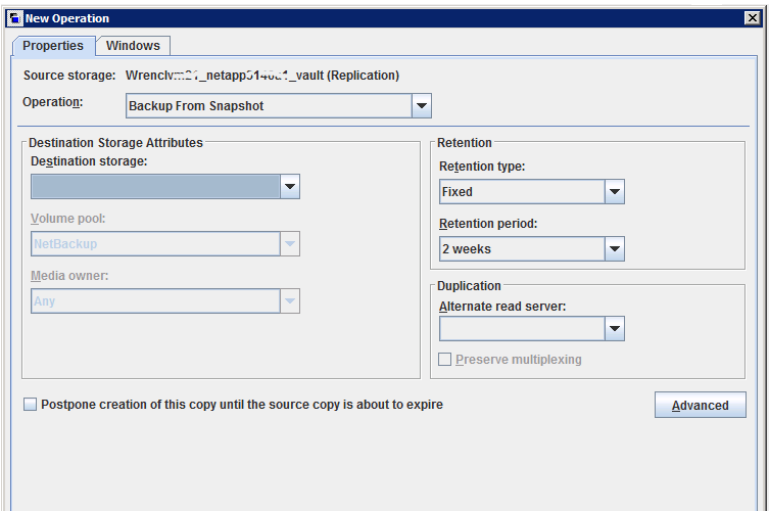


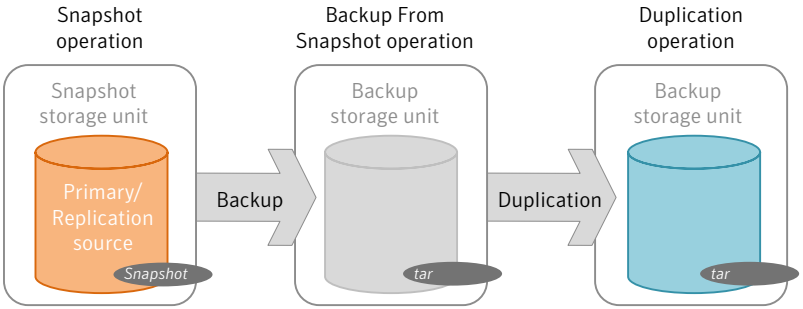
Table 9-6 Backup From Snapshot operation characteristics

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.
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 118.
Source for	A **Backup From Snapshot** operation can be the source for a **Duplication** operation. (See Figure 9-11.)
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:** If the SLP is to be used by an **NDMP** policy (or a **Standard** or **MS-Windows** policy with NDMP **Data Mover** enabled) the SLP may contain only one **Backup From Snapshot**.

Table 9-6 Backup From Snapshot operation characteristics *(continued)*

Characteristic	Description
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 and the Duplication Manager. The Duplication Manager decides when to run the backup job, which may be outside of the backup window as defined 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. See "Window tab of the Storage Operation dialog box" on page 120.

Figure 9-11 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 103.

Figure 9-12 Duplication operation in the New Storage Operation dialog box

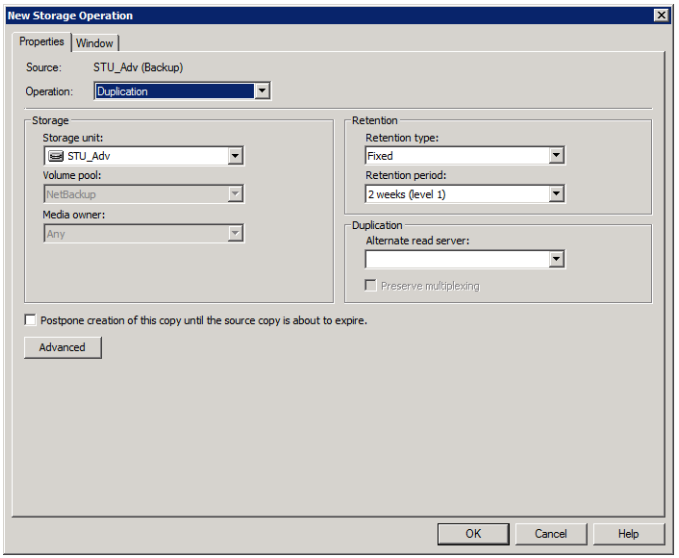


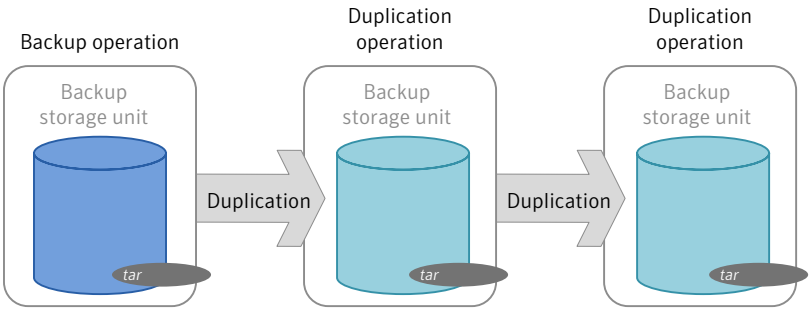
Table 9-7 Duplication operation characteristics

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.
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 118.
Source for	A **Duplication** operation can be the source for a **Duplication** operation. (See Figure 9-13.)
Hierarchy notes	When a **Duplication** operation appears in an SLP, it cannot be the first operation.

Table 9-7 Duplication operation characteristics *(continued)*

Characteristic	Description
Job type	A **Duplication** operation generates a **Duplication** job in the **Activity Monitor**.
Window	An SLP window can be created for a **Duplication** operation. See "Window tab of the Storage Operation dialog box" on page 120.

Figure 9-13 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 9-8 describes which retention types are valid selections for the various operations.

Table 9-8 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

Table 9-8 Operation and retention type configurations *(continued)*

Retention type	Backup operation	Snapshot operation	Replication operation	Backup From Snapshot operation	Duplication operation
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.

Mixing retention types

Symantec does not recommend allowing capacity-managed images and fixed-retention images to be written to the same volume in a disk storage unit. The volume may fill with fixed-retention images and not allow the space management logic to operate as expected.

Keep in mind the following points when configuring SLP operations or selecting the storage location for a policy:

- All SLPs that write to a volume in a disk storage unit should write images of the same retention type: fixed or capacity-managed.
- Do not write images both to a volume in a disk storage unit within an SLP and to the same volume (by the storage unit) directly from a policy.
- Mark all disk storage units that are used with SLPs as **On demand only**.

- Check any storage unit groups to make sure that fixed and capacity-managed images cannot be written to the same volume in a disk storage unit.

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.

Symantec 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.

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

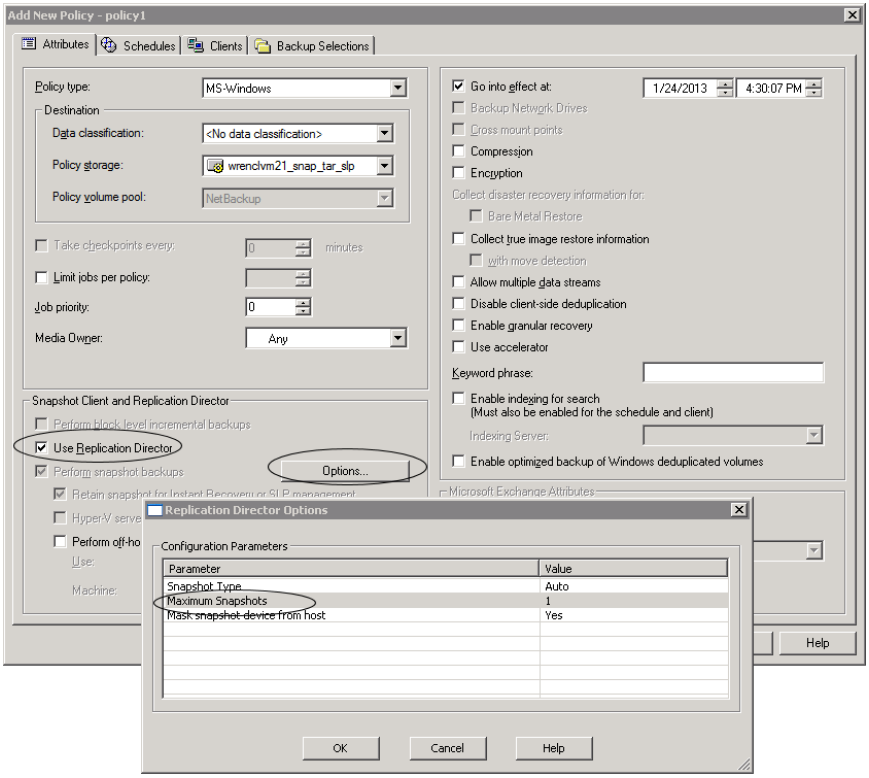
The **Maximum snapshot limit** determines the maximum number of snapshots that can be stored for a particular policy and client pair.

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 9-14 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 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.

Creating a storage lifecycle policy for snapshots and snapshot replication

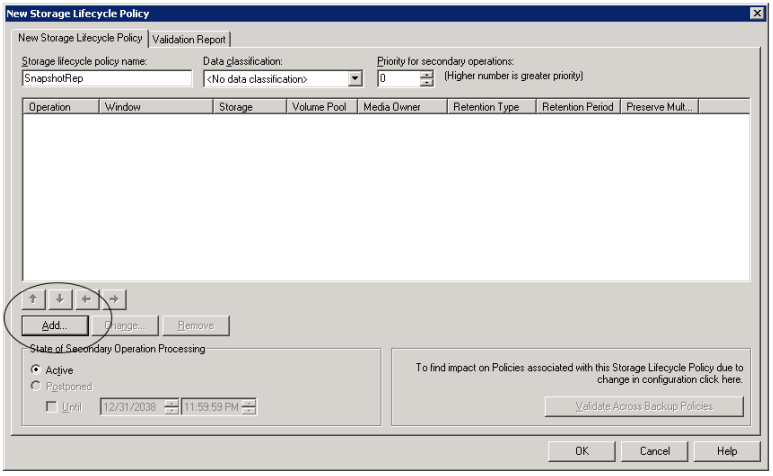
Use the following procedure to configure a storage lifecycle policy that creates snapshots and snapshot replications with Replication Director. Only those options that are necessary to configure an SLP for Replication Director are listed.

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 > New Storage Lifecycle Policy** (Windows) or **Actions > New > Storage Lifecycle Policy** (UNIX).
3. In the **New Storage Lifecycle Policy** dialog box, enter a **Storage lifecycle policy name**.

   See "NetBackup naming conventions" on page 67.

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 103.
- A **Backup From Snapshot** operation.
  See "Backup From Snapshot operation in an SLP" on page 109.
- An **Index From Snapshot** operation.
  See "Index From Snapshot operation in an SLP" on page 105.

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 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.

See "Window tab of the Storage Operation dialog box" on page 120.

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.

Window tab of the Storage Operation dialog box

The **Window** tab appears for secondary operations in a storage lifecycle policy.

Creating a window for a secondary operation is optional. However, creating a window can better define when the job for the operation can run. In this way, the job from a secondary operation does not interfere with jobs of a higher priority, such as backup jobs. Without a window defined, the job for an operation can run at any time, on any day.

Figure 9-15 Window tab for secondary operations in a storage lifecycle policy

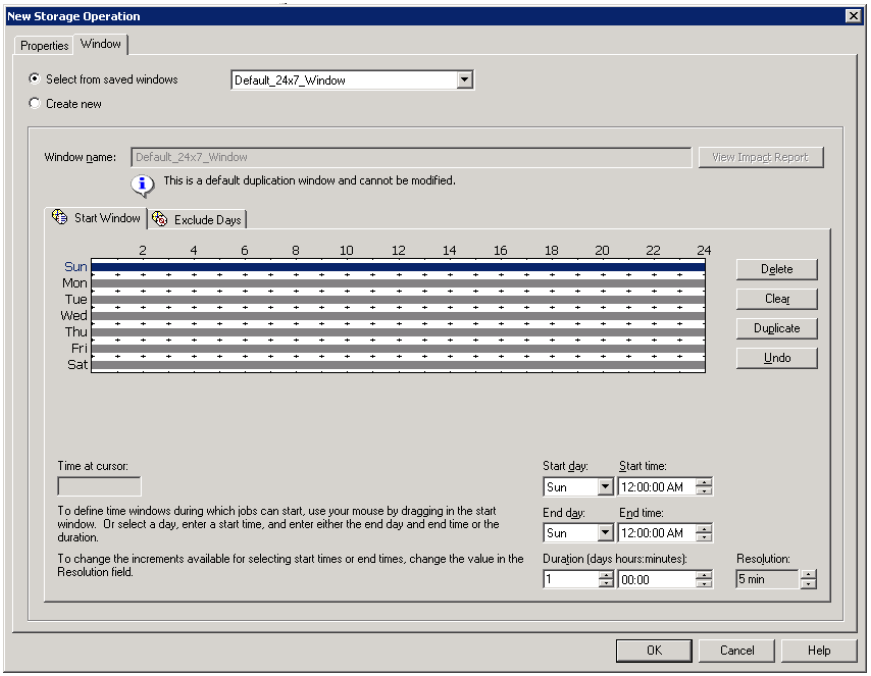


Table 9-9 Window tab of the Storage Operation dialog box

Setting	Description
Select from saved windows	You can either assign an existing window to the operation or create a new window for the operation. To use an existing window, select this option and then select a window from the drop-down menu.
Create new	Select this option to create a new window for this operation to use.
Window name	Enter a name for the new window.
View Impact Report button	This button generates an Impact Report which lists the names of the storage lifecycle policies that currently use the window. The Impact Report also lists the operation that uses the window, and the source and destination storage for the operation.

Table 9-9 Window tab of the Storage Operation dialog box *(continued)*

Setting	Description
Start Window tab	The **Start Window** grid is grayed out and cannot be modified if the **Default_24x7_Window** is selected. The **Start Window** grid is active if a saved window is selected or when a new window is created. If the **Start Window** grid is changed for a saved window, click the **View Impact Report** button to display information about other operations in other SLPs that use the window. See "Creating a new window for a storage lifecycle policy operation" on page 122.
Exclude Days tab	Use the **Exclude Days** tab to exclude specific dates from a window. See "Excluding days from a window for a storage lifecycle policy operation" on page 123.

Creating a new window for a storage lifecycle policy operation

To create a new window for SLP operations

1. In the **Window** tab, enable **Create new**.
2. Select the **Start Window** tab.
3. The days of the week appear along the left side of the grid. The time of day appears along the top of the grid in 24-hour time. The **Time at cursor** field specifies the day and time that corresponds to the current position of the cursor.

   To change the increments available for selecting start times or end times, change the value in the **Resolution** field.
4. Indicate the opening and closing times of the window for each day. The following lists several methods to do so:

   - Drag the cursor along the Start Window grid on each day you want the window to open and close. (Available only in the **NetBackup Administration Console** on Windows.)

     To move a window of time, click and drag the time bar to a new position.
   - Use the drop-down menus to select a **Start day** and an **End day**. Then select a **Start time** and an **End time**.
   - Use the drop-down menu to select a **Start day** and the **Duration** of the window for that day in hours and minutes. Adjust the **Start time** for your environment.

To create multiple time windows do one of the following:

To add windows on successive days	■ With the cursor over the chosen start time, press and hold the **Shift** Key. ■ Click and drag the cursor to the time when you want to the time window to close. ■ Continue holding the **Shift** Key, and drag the cursor down to the last day of the week you want to include. Duplicates of the time window appear for successive days.
To copy windows	■ Create one window. ■ Click **Duplicate**. The window is duplicated to any days without existing schedules. Duplication stops when it reaches a day that already contains a window. ■ On days that you do not want the time window to be open, select the window and click **Delete** .

5 Use the buttons under the Start Window grid to do the following:

To change the start time or end time	■ Adjust the **Start time** or **End time**. ■ Click and drag the end of the time window bar to a new position.
To delete a time window	Select a time window and click **Delete**.
To delete all the time windows	Click **Clear**.
To erase the last action	Click **Undo**.

6 Click **OK** to save the window and the operation.

Excluding days from a window for a storage lifecycle policy operation

Use the **Exclude Days** tab to exclude specific days from a window. If a day is excluded from a window, jobs do not run on that day. The tab displays a calendar of three consecutive months. Use the lists at the top of the calendar to change the first month or year displayed.

To exclude a day from the storage lifecycle policy window

1 In the **Window** tab, select the name of an existing window from the drop-down menu.

2 Select the **Exclude Days** tab.

3 Use one or more methods to indicate the days to exclude:

- Select the day(s) on the 3-month calendar that you want to exclude. Use the drop-down lists at the top of the calendar to change the months or year.
- To indicate **Recurring Week Days**:
  - Click **Select All** to select all of the days in every month for every year.
  - Click **Deselect All** to remove all existing selections.
  - Check a box in the matrix to select a specific day to exclude for every month.
  - Click the column head of a day of the week to exclude that day every month.
  - Click the **1st**, **2nd**, **3rd**, **4th**, or **Last** row label to exclude that week every month.
- To indicate **Recurring Days of the Month**:
  - Click **Select All** to select all of the days in every month.
  - Click **Deselect All** to remove all existing selections.
  - Check a box in the matrix to select that day to exclude each month.
  - Click **Last Day** to exclude the last day of every month.
- To indicate **Specific Dates**:
  - Click **New**. Enter the month, day, and year in the **Date Selection** dialog box. Click **OK**.
    The date appears in the **Specific Dates** list.
  - To delete a date, select the date in the list. Click **Delete**.

4 Add additional dates as necessary, then click **OK** to save the window and the operation.

Chapter 10

Configuring backup policies for snapshots and snapshot replication

This chapter includes the following topics:

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 126.

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 use Replication Director to protect NAS volumes" on page 140.
  Configure policies that use Replication Director to create snapshots of NAS volumes.
- See "Configuring a Standard or MS-Windows policy to use Replication Director to protect SAN-connected devices" on page 144.
  Configure policies that use Replication Director to create snapshots of SAN (block) devices.
- See "About Oracle support for Replication Director" on page 147.
  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 158.
  Configure policies to protect virtual machines in a Replication Director environment.

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 10-1 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 using NDMP with Replication Director" on page 128. ■ **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 Replication Director" on page 132.	**Standard** or **MS-Windows** (Do not enable NDMP **Data Mover**.)

Table 10-1 Comparison of NDMP or non-NDMP policy types *(continued)*

Functionality	NDMP	Non-NDMP
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.
Mount snapshot for indexing*	No: Indexing of NDMP snapshots is not supported in 7.6. That is, the **Index From Snapshot** operation is not supported with NDMP policies.	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 105.

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.

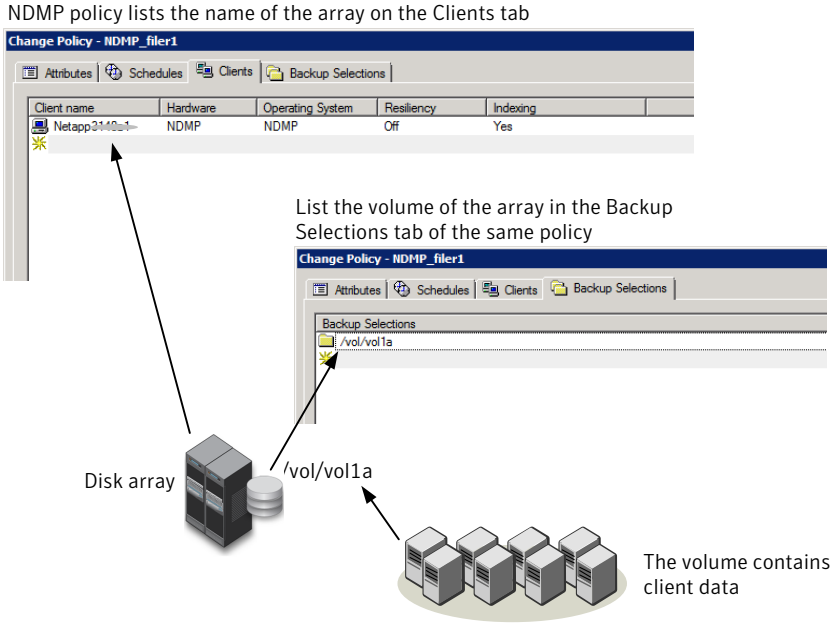
- Only one NDMP backup of a snapshot per `backupid` is allowed.
- The **Index From Snapshot** operation is not supported for any policy that uses NDMP. (For example, an **NDMP** policy, or a **Standard** or **MS-Windows** policy with NDMP **Data Mover** enabled.)
  See "Index From Snapshot operation in an SLP" on page 105.

Configuring an NDMP policy to protect a NAS host using NDMP with Replication Director

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 10-1 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.

Figure 10-1 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.

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.

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 136.
   - Make sure that NDMP is enabled on the NetApp storage by using the `ndmpd status` command.
   - On the DataFabric Manager server, make sure that the NDMP Status is **Up** and that the NDMP Credentials are **Good**.
2. In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Policies**.
3. On the **Actions** menu, click **New > New Policy**.
4. 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 67.
5. 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 118.
   - **Use Replication Director**: Enable **Use Replication Director** to automatically select other options that Replication Director requires. These include the following **Perform off-host backup** options:
     - To use **Data Mover**.
     - To use **NDMP** as the **Machine** selection.
   - **Options** button

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.
- **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 Instant Recovery 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.

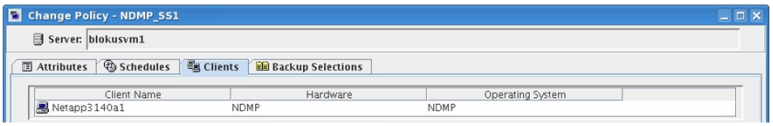
See "Maximum snapshot limit retention type for SLP operations" on page 116.

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

6 Select the **Schedules** tab and configure the schedules as you would for any other policy.

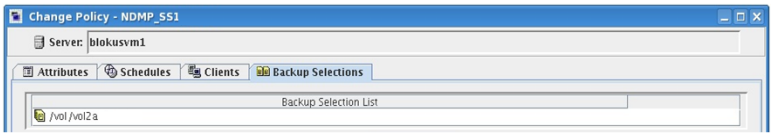
7 Select the **Clients** tab. Specify the name of the disk array (the NAS host). (It may be helpful to refer to Figure 10-1.)

The following figure shows the name of a NetApp storage system in the **Clients** tab:



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

The following figure shows the **Backup Selections** tab and the volume that is to be backed up:



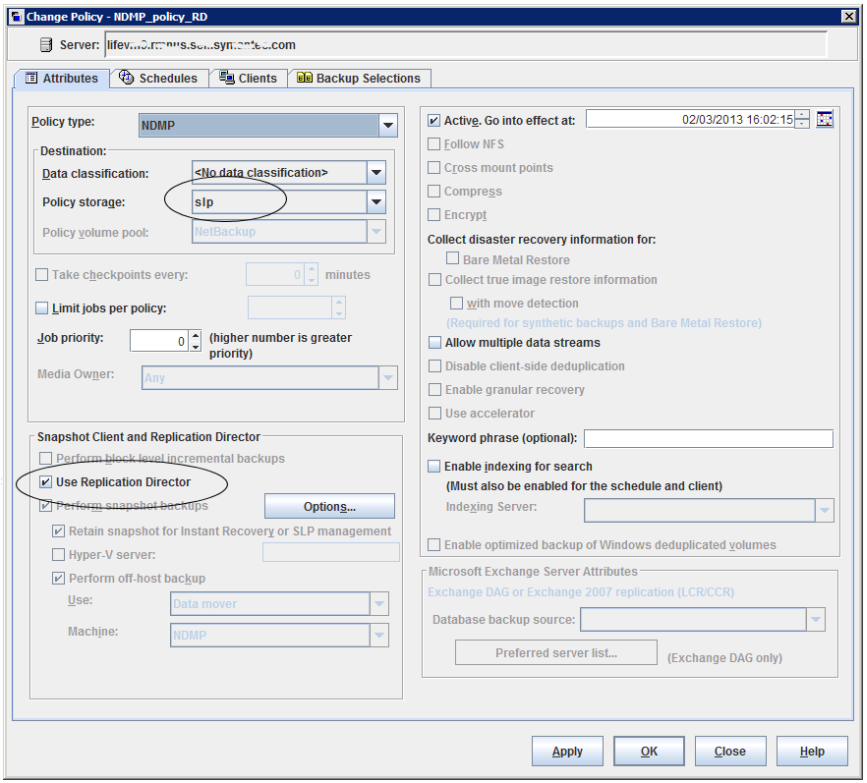
Note: Backup selections for both SAN devices and NAS volumes are not supported in a single backup policy.

9 When the policy configuration is complete, click **OK**.

10 NetBackup checks the policy to ensure that it can run successfully. Select **Complete** to perform the most comprehensive policy validation. The errors that it may discover now can help to avoid troubleshooting problems later.

If the validation finds no problems, the policy saves and closes.

Figure 10-2 NDMP policy configuration to back up a NAS host



Configuring a Standard or MS-Windows policy to protect clients using NDMP with Replication Director

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

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

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.

To create a Standard or MS-Windows 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 136.
- Make sure that NDMP is enabled on the NetApp storage by using the `ndmpd status` command.
- On the DataFabric Manager server, make sure that the NDMP Status is **Up** and that the NDMP Credentials are **Good**.

2 In the **NetBackup Administration Console**, in the left pane, expand **NetBackup Management > Policies**.

3 On the **Actions** menu, click **New > New Policy**.

4 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 67.

5 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 118.
- **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.
- **Options** button
  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.
- **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 Instant Recovery 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.

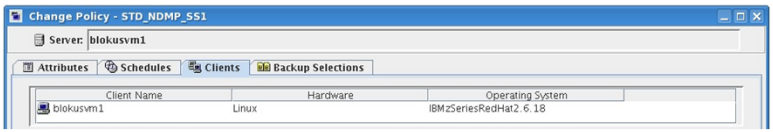
See "Maximum snapshot limit retention type for SLP operations" on page 116.

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

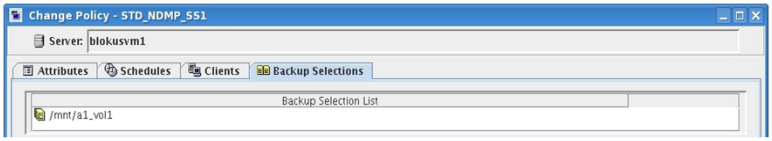
6 Select the **Schedules** tab and configure the schedules as you would for any other policy.

7 Select the **Clients** tab. Specify the clients to be backed up.

The following figure shows the name of one Linux client:



8 Select the **Backup Selections** tab to specify the files and directories to be backed up on each client.



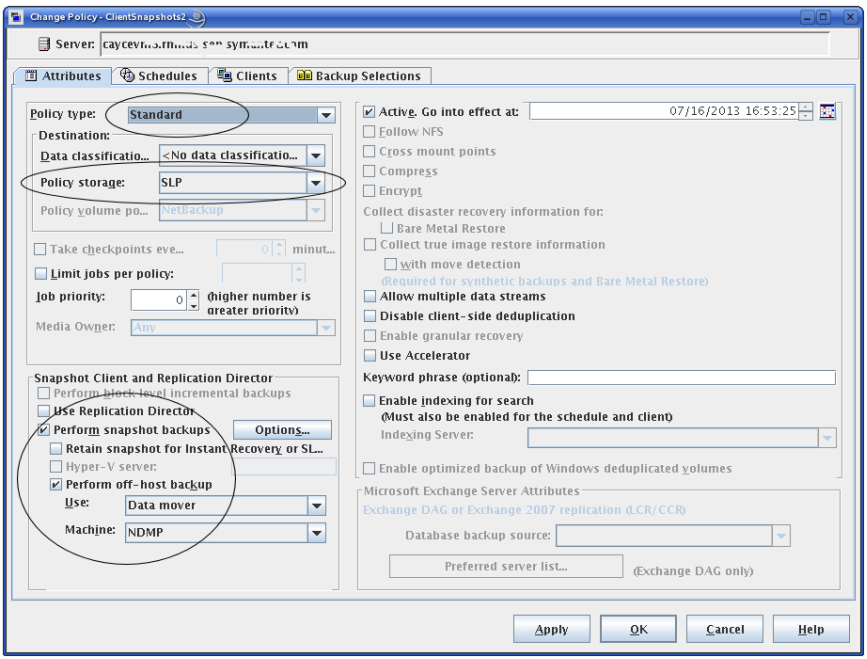
Note: Backup selections for both SAN devices and NAS volumes are not supported in a single backup policy.

9 When the policy configuration is complete, click **OK**.

10 NetBackup checks the policy to ensure that it can run successfully. Select **Complete** to perform the most comprehensive policy validation. The errors that it may discover now can help to avoid troubleshooting problems later.

If the validation finds no problems, the policy saves and closes.

Figure 10-3 Standard policy configuration to use NDMP to back up clients



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.

   The NDMP host name is case-sensitive. The name must match the name that is entered here whenever this host name is used. For example, enter this name exactly when you configure tape drives and storage units for this host.)

   Note: If 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 refer 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.

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 Symantec Support website:
  http://www.symantec.com/docs/TECH31885
- **Password** and **Confirm Password**: Enter the password for this user.
  To add a NetApp vFiler as an NDMP host, the encrypted vFiler password is required.
  To retrieve the encrypted password, log on to the vFiler and run the following command:
  `ndmp password user`
  The following example shows the command and response to retrieve the encrypted password for the `root` user:
  ```
  ndmp password root
  password hFlNXOXjpHpNXXOG
  ```

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. More information about wildcard characters is available:

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, Symantec recommends that you use storage lifecycle policies (SLPs) to control backups on the secondary filer.

- 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, Symantec 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.

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 for Replication Director 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 parameter.

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.

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 136.

Configuring a Standard or MS-Windows policy to use Replication Director to protect NAS volumes

The following procedure describes how to create a policy that uses Replication Director to protect NAS volumes.

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.

To create a Standard or MS-Windows policy to use Replication Director for NAS

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 67.
4. 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 118.
- **Use Replication Director**: Enable **Use Replication Director** to automatically select other options that Replication Director requires.
- **Options** button
  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.
- **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 Instant Recovery 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 116.

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 and configure the schedules as you would for any other policy.

6 Select the **Clients** tab and specify the local mount point on the production client. The client needs to run the same NetBackup version as the master server.

Make sure that the client can reach the storage server of the OpenStorage partner and the data volume to be backed up. For example, the client must be able to contact the volumes of the NetApp DataFabric Manager server.

To test the connectivity, run the `ping` command from the client for the storage server. It must be reachable from the client using the DNS name.

```
ping storage_server_dnsname
```

Also, make sure that the data volume from the storage system is properly mounted on the client.

To test, run the `mount` command or use the `df -k` command on the 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.

---

7 Select the **Backup Selections** tab to indicate the client data to be backed up.

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.

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

- 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.
- Use the `nosharecache` option to mount qtrees that are under the same volume. For example:

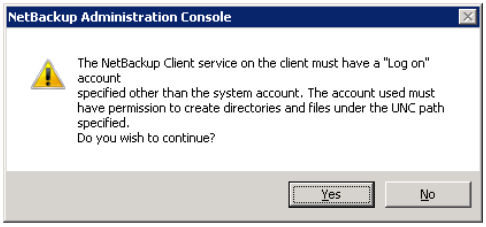
  ```
  mount -o vers=3,nosharecache filer:/vol/volume1/qtree1 /mnt1
  ```

- 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 Symantec NetBackup (NBUPlugin) 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`

8 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 53.



9 When the policy configuration is complete, click **OK**.

10 NetBackup checks the policy to ensure that it can run successfully. Select **Complete** to perform the most comprehensive policy validation. The errors that it may discover now can help to avoid troubleshooting problems later.

If the validation finds no problems, the policy saves and closes.

Configuring a Standard or MS-Windows policy to use Replication Director to protect SAN-connected devices

The following procedure describes how to create a policy that uses Replication Director for SAN (block) device support.

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

See "Configuring the primary NetApp device to use VSS with Replication Director" on page 36.

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.

To create a Standard or MS-Windows policy for SAN-connected devices to use 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**.

   Do not use the **Policy Configuration Wizard** to configure a policy for Replication Director.

   See "NetBackup naming conventions" on page 67.
4. 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 118.
   - **Use Replication Director**: Enable **Use Replication Director** to automatically select other options that Replication Director requires.
   - **Options** button
     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. By default, **Differential** is selected for this snapshot.
- **Differential**: If selected, NetBackup instructs the VSS vendor hardware provider to create a shadow copy using a differential or copy-on-write implementation. If the VSS vendor hardware provider that is installed on the system doesn't support the requested attributes, snapshot creation fails with an error VSS_E_VOLUME_NOT_SUPPORTED.
- **Plex**: If selected, NetBackup instructs the VSS vendor hardware provider to create a shadow copy using a plex implementation. If the VSS vendor hardware provider that is installed on the system doesn't support the requested attributes, snapshot creation fails with an error VSS_E_VOLUME_NOT_SUPPORTED.
- **Clone**: **Clone** is not supported for Windows SAN devices. If selected, the policy validation and snapshot creation fail with status code 4201 (incorrect configuration for snapshot).

  Note: NetApp disk arrays do not support **Clone**.

Maximum Snapshots

Sets the maximum number of Instant Recovery 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 116.

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 and configure the schedules as you would for any other policy.

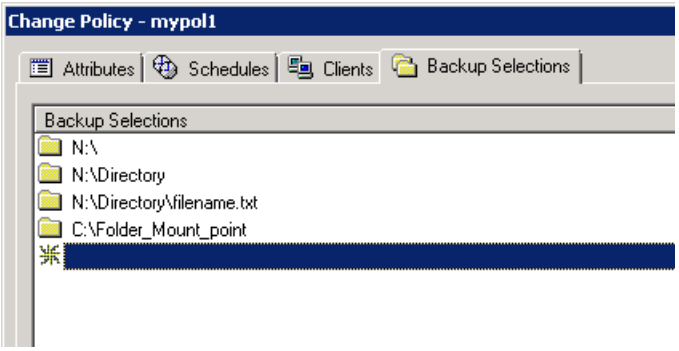
6 Select the **Clients** tab and specify the client.

7 Select the **Backup Selections** tab to 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.

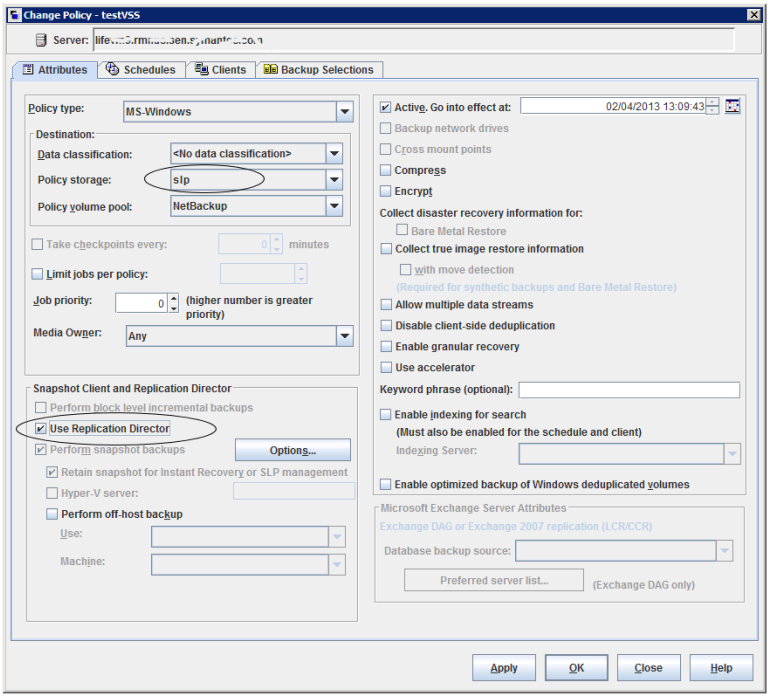
---

8 When the policy configuration is complete, click **OK**.

9 NetBackup checks the policy to ensure that it can run successfully. Select **Complete** to perform the most comprehensive policy validation. The errors that it may discover now can help to avoid troubleshooting problems later.

If the validation finds no problems, the policy saves and closes.

Figure 10-4 MS-Windows policy configuration to use VSS with Replication Director



About Oracle support for Replication Director

In NetBackup 7.6, 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 148.
- Create a script- or template-based Oracle policy.
  See "Configuring a script- or template-based Oracle policy" on page 153.

Table 10-2 describes the differences between the two methods:

Table 10-2 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 67.

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 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

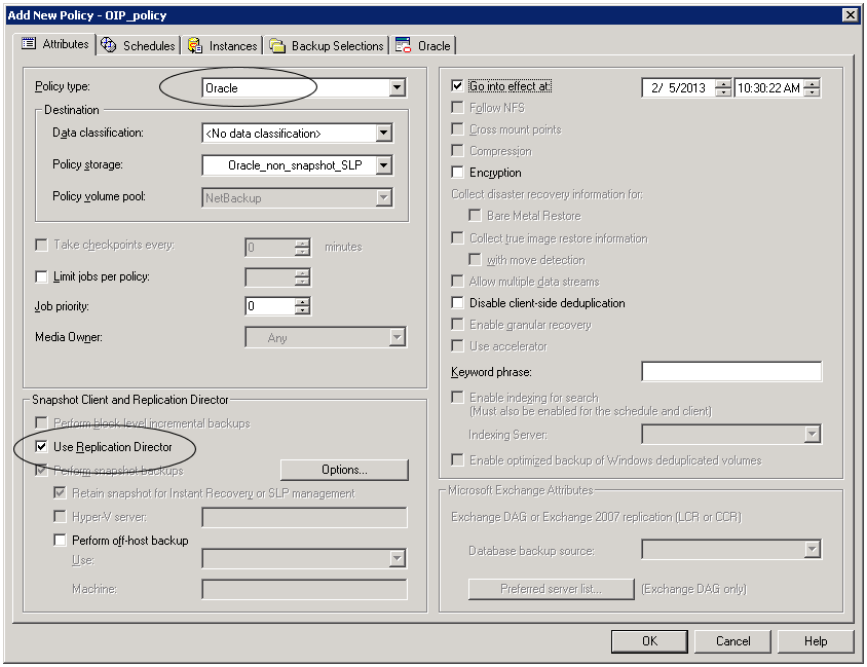
Sets the maximum number of Instant Recovery snapshots to be retained at one time.

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 116.

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



5 Select the **Schedules** tab. Create one schedule:

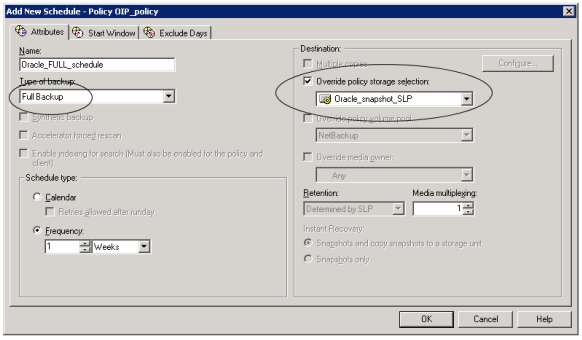
- **Type of backup**: Select **Full Backup**. The **Full Backup** is used for both the snapshot (proxy) part of the database and the non-snapshot (stream-based) part of the Oracle database.
  The Oracle Intelligent Policy does not support the snapshot of an **Archived Redo Log Backup**. To take a snapshot of the archived redo logs, use the script- or template-based Oracle policy method.

  Note: Unless creating Block Level Incremental (BLI) backups, always select **Full Backup** to create snapshots of the Oracle database.

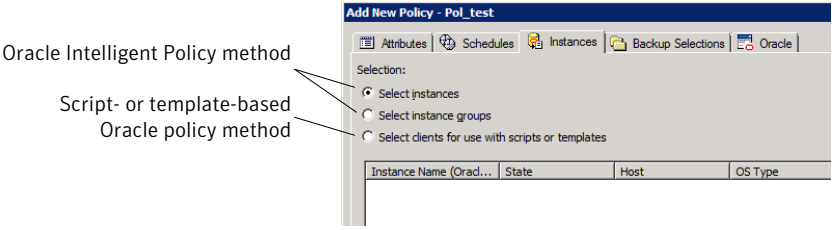
- **Override policy storage selection**: Enable and select the SLP that is configured for snapshot replication. (A snapshot SLP is one in which the first operation is a snapshot operation.) This option must be enabled so that the schedule storage overrides the policy storage with a snapshot SLP.
- **Retention**: The retention for the streamed data is based on the non-snapshot SLP that was indicated as the **Policy storage** in Step 4.

- The non-snapshot SLP specified on the policy storage in Step 4 determines the retention for the streamed data.
- The snapshot SLP that is specified as the schedule storage (**Override policy storage selection**) determines the retention for the snapshot data.

Click **OK** to save the schedule.



6 Select the **Instances** 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 **Select instances** or **Select 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.

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 datafiles 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 67.

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.

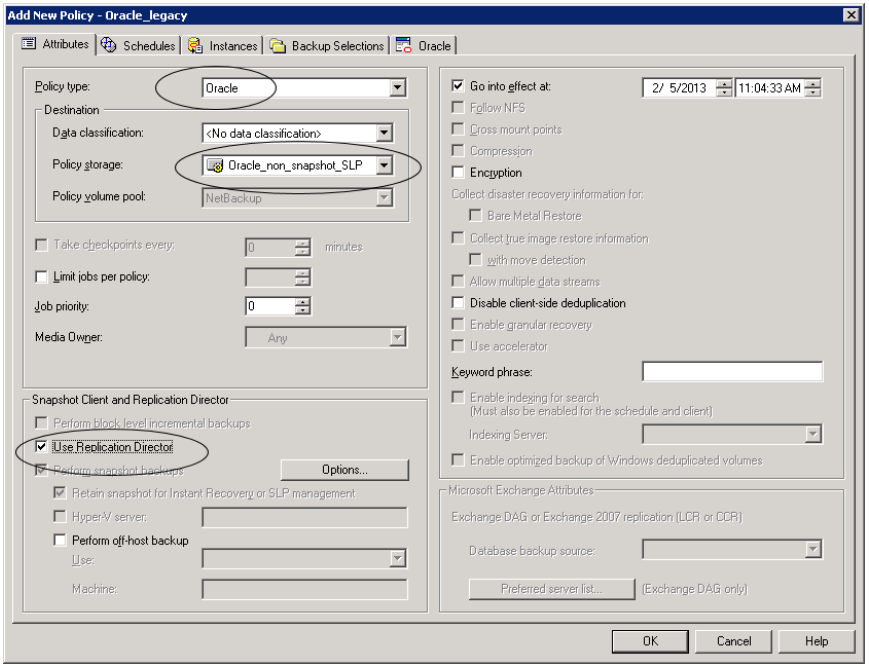
Maximum Snapshots Sets the maximum number of Instant Recovery snapshots to be retained at one time.

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.

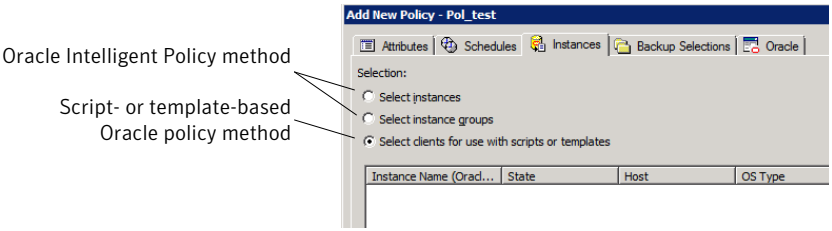
When the maximum is reached, snapshot rotation occurs: The next snapshot causes the oldest to be deleted.

See "Maximum snapshot limit retention type for SLP operations" on page 116.

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



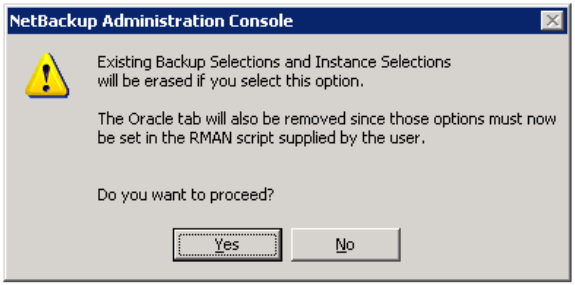
5 Select the **Instances** tab and specify the instances to back up. Select **Select clients for use with scripts and templates**. If either of the other two are selected, the Oracle Intelligent Policy is used and the scripts are created automatically.



After selecting the **Select clients for use with scripts and templates** option, a message appears that describes the effect of this choice:

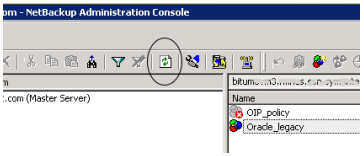
- Existing selections (if any) for this policy are erased.
- The **Oracle** tab is removed from this policy.
- Another effect is that the **Selections** tab turns into the **Clients** tab.

Click **Yes** to continue Oracle policy configuration.



6 Click **Yes** to save and close the entire policy.

7 In the **NetBackup Administration Console**, select the policy and click the refresh button in the toolbar.



8 Re-open the policy and select the **Schedules** tab.

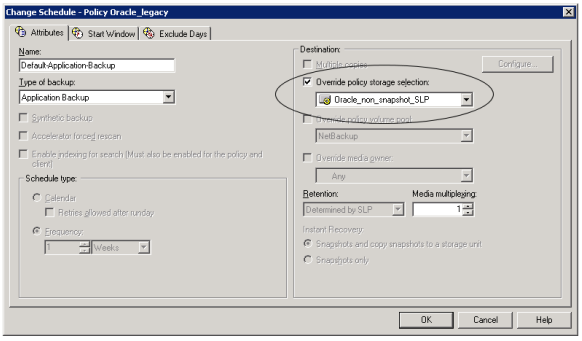
Modify the **Default-Application-Backup** schedule:

- **Override policy storage selection**: Enable and select a non-snapshot storage unit or a non-snapshot SLP. This is most likely the storage unit that

is specified on the **Attributes** tab. Indicating it here makes the selection explicit.

- **Retention**: The policy or SLP indicates the retention for the backup:
  - When the storage is an SLP, the SLP determines the retention and no selection is possible here.
  - When the storage is not an SLP, the schedule determines the retention and a selection is possible here.

Click **OK** to save the schedule.

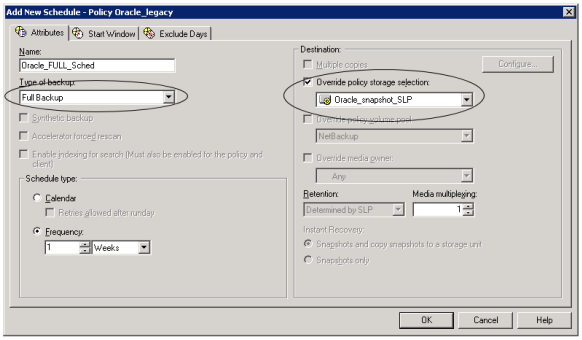


Create one **Full Backup** schedule:

- Name the schedule.
- **Type of backup**: Select **Full Backup**.

  Note: Unless creating Block Level Incremental (BLI) backups, always select **Full Backup** to create snapshots of the Oracle database.

- **Override policy storage selection**: Enable and select the SLP that is configured for snapshot replication.
- **Retention**: The SLP indicates the retention for the backup.



9 Configure the schedule in the **Start Window** tab and the **Exclude Days** tab.

Click **OK** to save and close the schedule.

10 Select the **Clients** tab. By default, the **Select 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**.

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 10-3 describes the scenarios for virtual machine protection with Replication Director.

Table 10-3 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).
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 *NetBackup for VMware Guide*. ■ 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 53.

  More information is available on all the procedures for configuring a NetBackup environment that uses Replication Director:
  See "Configuration overview for a NetBackup Replication Director environment" on page 14.

The following table lists the additional steps that are required for Replication Director and virtual machines.

Table 10-4 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 *NetBackup for VMware Guide*.
2	Add the VMware backup host to your NetBackup configuration.	See the topic on adding the VMware backup host to NetBackup, in the *NetBackup for VMware Guide*.
3	Configure NetBackup access credentials for the VMware vCenter server or ESX server.	See the topic on adding NetBackup credentials for VMware, in the *NetBackup for VMware Guide*.
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 162.

Notes on Replication Director for virtual machines

Note the following about Replication Director for virtual machines:

- For supported vCenter versions and datastores and other support details, see the following Symantec tech note:
  Support for NetBackup 7.x in virtual environments
- 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 storage server (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.

- When restoring from Replication Director backups, note the following:
  - If you select more than one image in the BAR 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 BAR and OpsCenter interfaces 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 165.

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 67.
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:

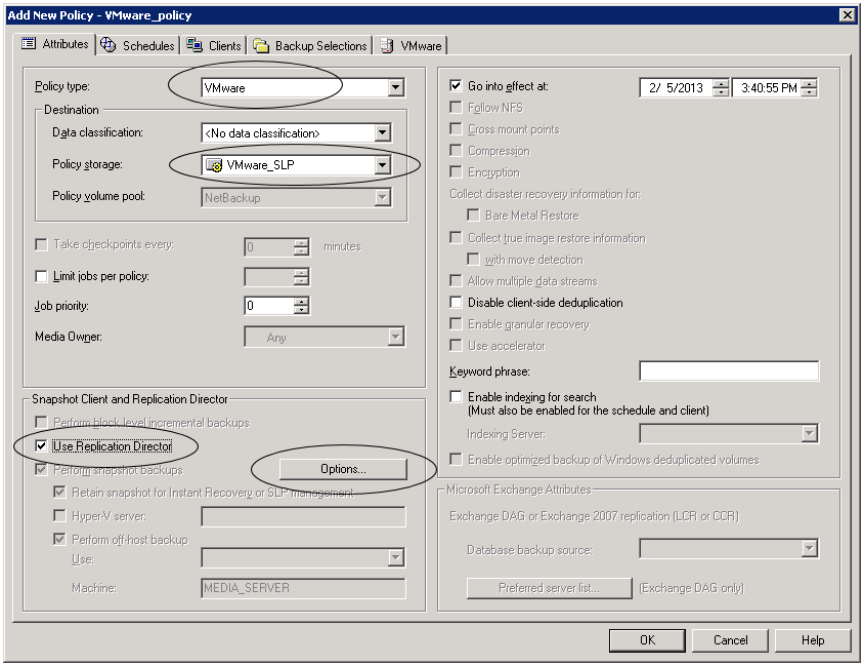
  Maximum Snapshots parameter
  Sets the maximum number of Instant Recovery snapshots to be retained at one time. When the maximum is reached, snapshot rotation occurs: The next snapshot causes the oldest to be deleted.

  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, Symantec 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 file**s are disabled.
    - The **Appliclation 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 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 list

  The 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, Symantec 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 10-5 describes the **Activity Monitor** jobs that appear in each configuration: with the **Application Consistent Snapshot** option enabled or disabled.

Table 10-5 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.

Chapter 11

Restoring from a snapshot

This chapter includes the following topics:

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 96.

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 170. ■ The NetBackup `bprestore` command. See the *NetBackup Commands Reference Guide*. ■ The Symantec OpsCenter interface. See "Using OpsCenter to restore from array-based snapshots" on page 175.
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 176. See "Restoring (rolling back) from an array-based snapshot" on page 177. **Note:** The NetBackup 7.6 release 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 clients that use multiple NICs, and if using NetApp storage, see the following topic:

See "How to configure a multi-NIC environment" on page 51.

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.

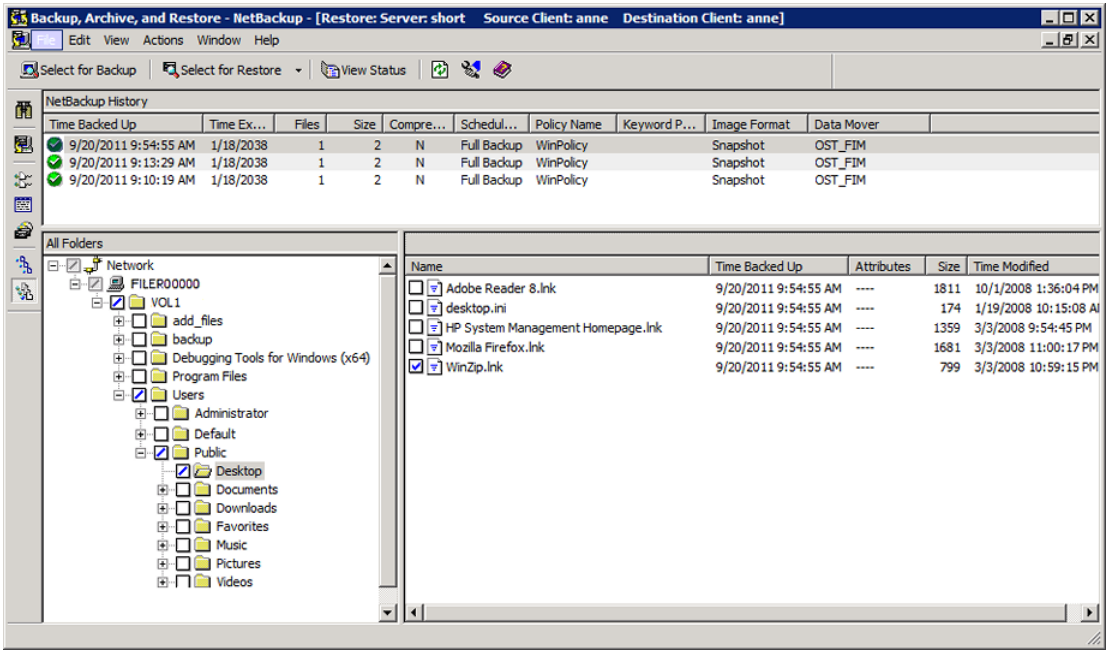
See "About restores from array-based snapshots" on page 168.

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:

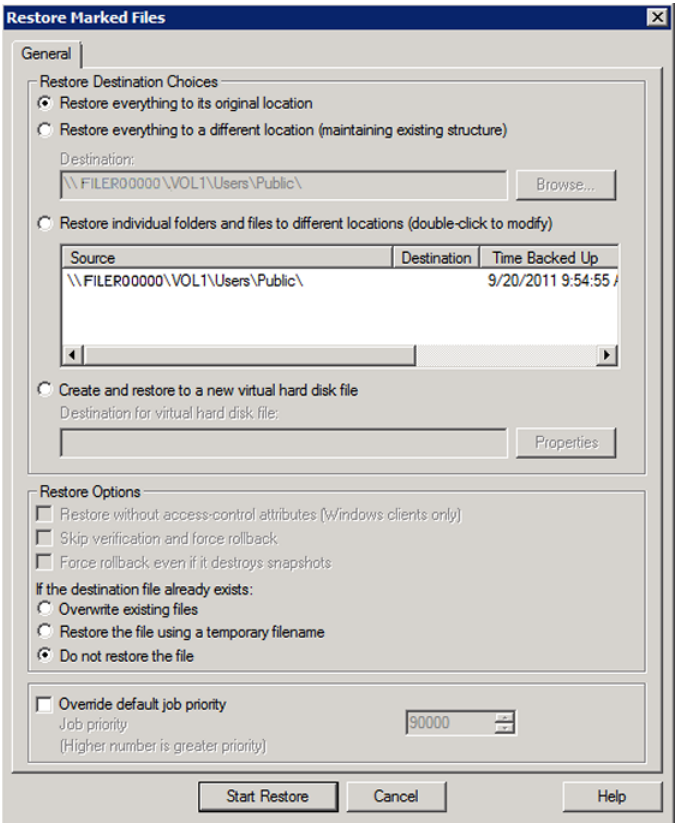
Windows	In the **NetBackup History** pane, select the snapshot to restore. The snapshot appears in the **All Folders** pane.
UNIX	Open the **Date Range** or the **Backup History** to select a snapshot to restore. Select a snapshot from the list and click **OK**. The snapshot contents appear in the **Directory 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 on a Windows computer:



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.

Use default progress log filename

By default, progress log messages are written to the following location on the UNIX client:

```
/usr/openv/netbackup/logs/user_ops/loginID/logs
```

To change the location and the name of the progress log file for this backup, take the following actions:

- Click this check box to remove the check mark.
- In the **Progress log filename** field, enter a new path and file name.

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

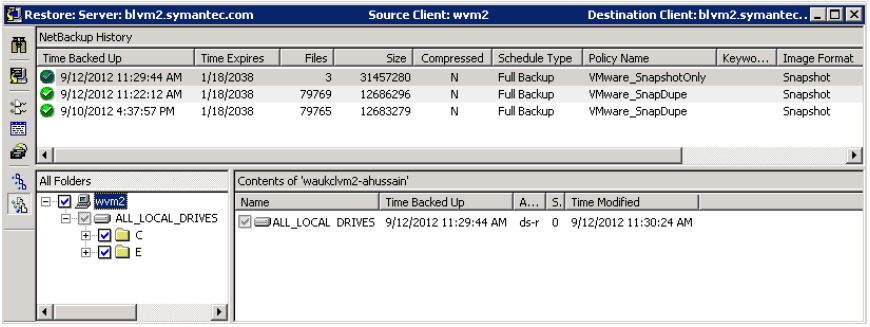
Note: When you browse files to restore, the Backup, Archive, and Restore interface displays the files and folders from the primary backup copy. A storage lifecycle policy however can create several images or copies from one job. To restore files from a different copy, set that copy as the primary. See 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*.

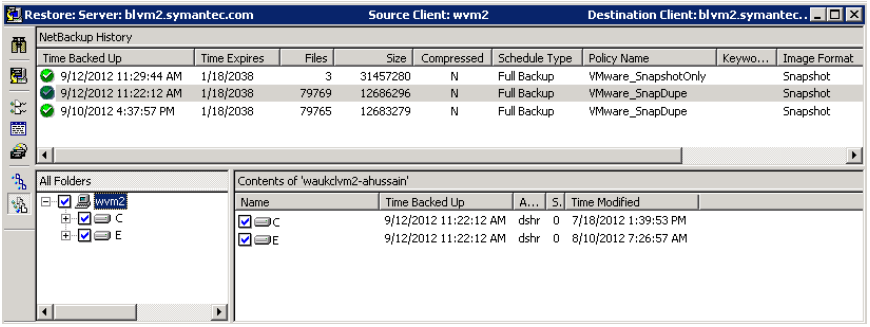
Note the following when restoring files from Replication Director snapshots:

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.

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 105.

For more information about Operational Restore using OpsCenter, see the Symantec 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 get deleted from the storage system.

Table 11-1 describes the interaction between the various factors.

Table 11-1 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 11-1 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.

In NetBackup 7.6, point-in-time rollback restores are supported 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 168.

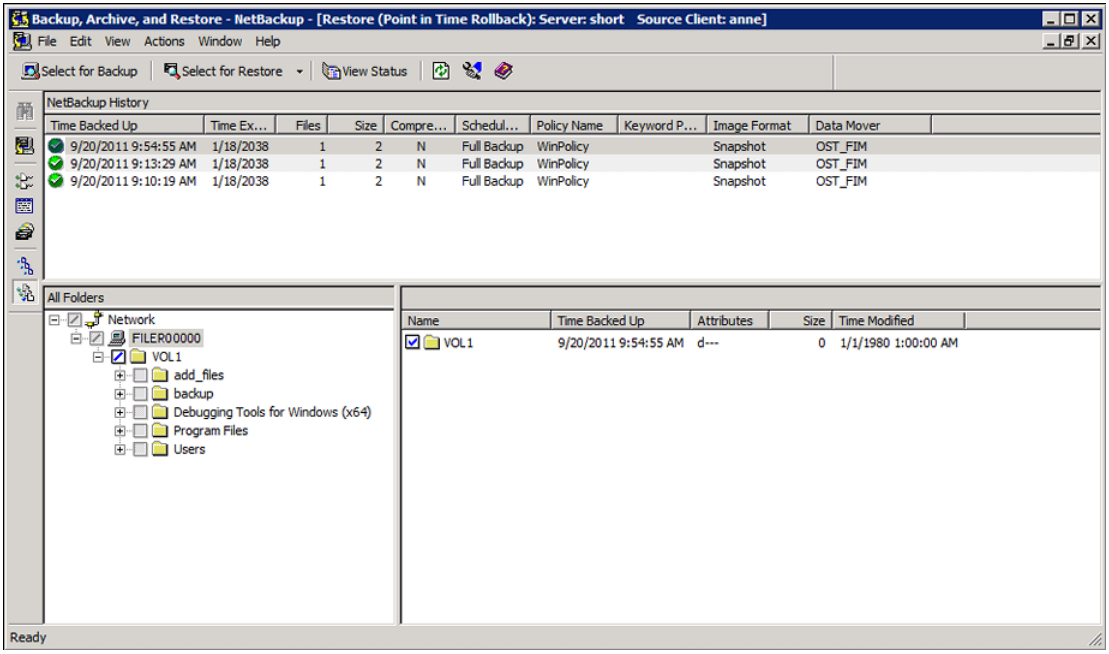
See "How NetApp performs a volume-level rollback restore" on page 176.

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.

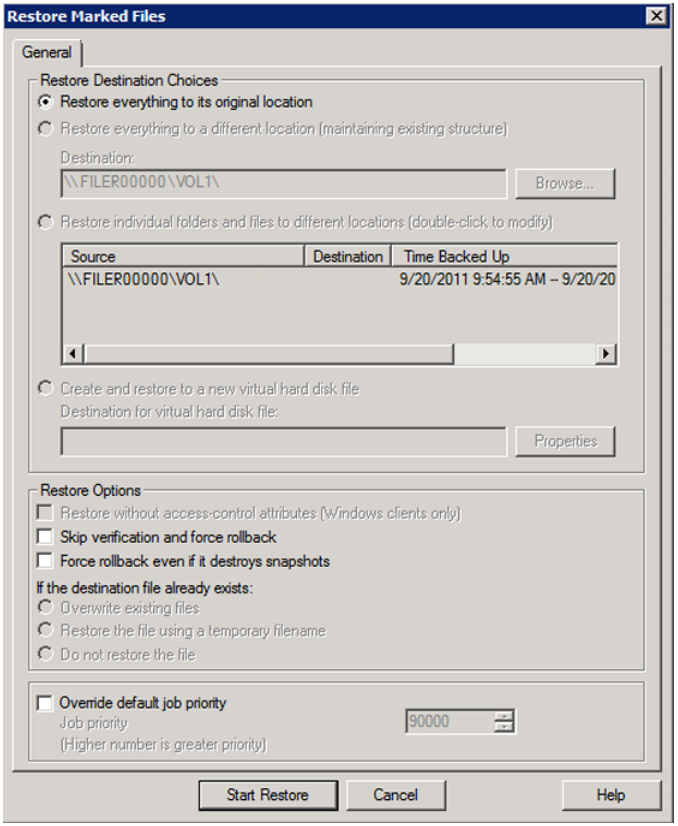
4 Begin the restore, as follows:

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 176.

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.

Use default progress log file name

UNIX systems only.

By default, progress log messages are written to the following location on the UNIX client:

`/usr/openv/netbackup/logs/user_ops/`*`loginID`*`/logs`

To change the location and the name of the progress log file for this restore, do the following:

- Click this check box to remove the check mark.
- In the **Progress log filename** field, enter a new path and file name.

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.

Chapter 12

OpsCenter reporting

This chapter includes the following topics:

Symantec OpsCenter reporting

Use Symantec 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.

Symantec 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):

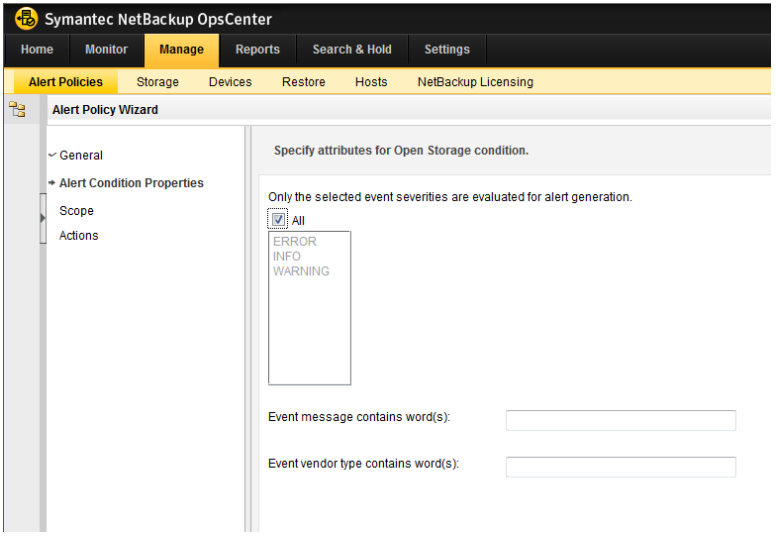
- The storage server can generate threshold or **Volume Almost Full** alarms.

- 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.

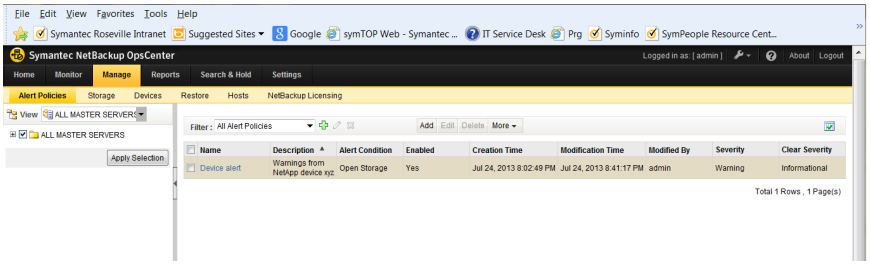
Figure 12-1 Attribute selection for OpenStorage device alerts



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 Symantec OpsCenter Administrator's Guide for information about configuring alerts.

Figure 12-2 OpsCenter device alert example



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 (Figure 12-3) 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 (Figure 12-4) 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.

Figure 12-3 Disk Pool General tab

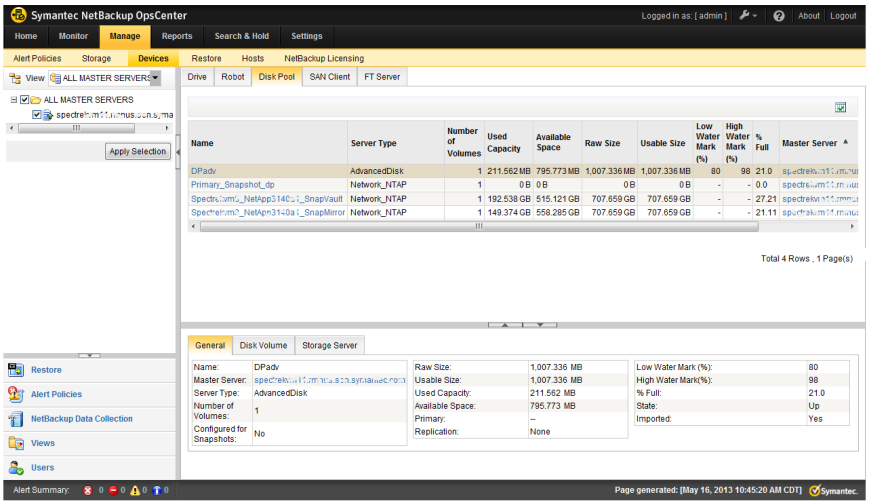
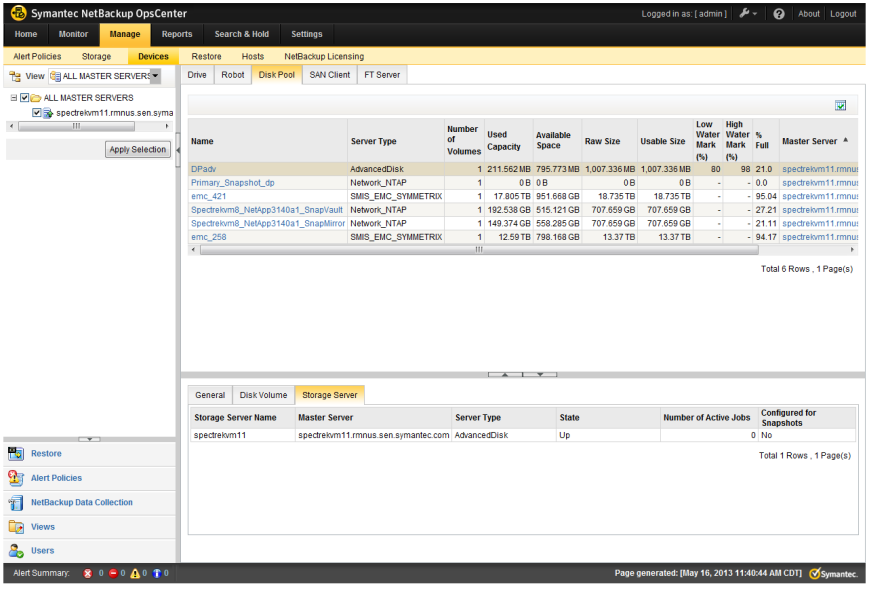


Figure 12-4 Disk Pool Storage Server tab



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 (Figure 12-5) 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.

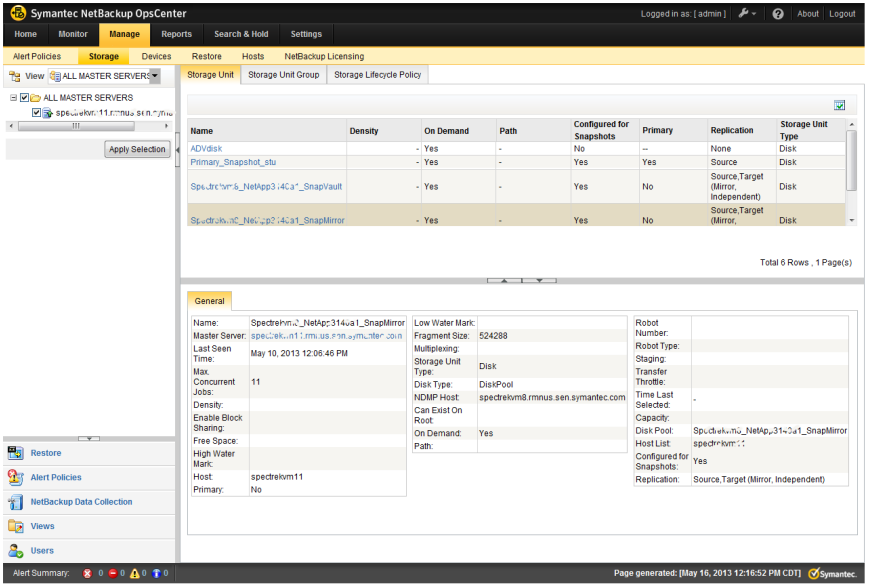
Storage Lifecycle Policy tab

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.

Figure 12-5 Storage Unit General tab



Chapter 13

Terminology

This chapter includes the following topics:

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 or snapshot images of the data. ■ The process of creating a new backup (tar) image of the client's data. ■ The process of creating a snapshot of the client's data.
Copy	An instance of a NetBackup image which can stand alone; it can be read or deleted without affecting any other copy.
Data movement	A copy operation as performed by a third-party copy device or NetBackup media server.
Data mover	The mechanism that is used to move data from storage on the production client to backup storage. Or, to duplicate, the data mover moves 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).
Device	A general term for any of the following: LUN, logical volume, appliance, or disk array.

Table 13-1 Replication terms *(continued)*

Term	Definition
Disk array	A disk array which exposes LUNs (block device) or network shares (file system) to a host server over SAN, NFS, CIFS, or iSCSI protocols.
Domain	See NetBackup domain.
Duplication	NetBackup creates a copy by using a media server to move the data or by using the optimized duplication method.
Instant recovery	Sometimes called Persistent Frozen Image (PFI).
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 Symantec NetBackup	Also referred to as the NBUPlugin, this plug-in communicates with the OSTPlugin, using the XML-based messaging SOAP protocol to query the DataFabric Manager server. The *NetApp Plug-in for Symantec NetBackup Installation and Administration Guide* is available from the NetApp Support Site.

Table 13-1 Replication terms *(continued)*

Term	Definition
NetBackup domain	A NetBackup installation with one master server and one or more media servers and clients. A single NetBackup domain may span more than one site or location. That is, the media servers and clients of a single NetBackup master server may not all be at same site where the master server resides.
NetBackup OpenStorage Plug-in for Replication Director	Also referred to as the OSTPlugin, this plug-in from NetBackup communicates with the NBUPlugin, using the XML-based messaging SOAP protocol to query the DataFabric Manager server.
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 bit-by-bit block copy of the snapshot.
Replication	The process of replicating a snapshot onto a separate disk array using NetBackup Replication Director.
Replication Director	A Symantec NetBackup product that is used to manage snapshot replication as a disaster recovery solution.
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.

Table 13-1 Replication terms *(continued)*

Term	Definition
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 Disk Array.
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.
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.

Chapter 14

Troubleshooting

This chapter includes the following topics:

Tools to troubleshoot Replication Director problems

The following Symantec document contains checklists to help with Replication Director configuration. It also contains scripts to download that verify that the correct software and licenses have been installed as well as scripts for troubleshooting various issues.

http://www.symantec.com/docs/DOC5240

Use NetBackup policy validation to discover errors

After an administrator configures a backup policy to use Replication Director, NetBackup validates the policy before it can be saved and closed. Policy validation helps ensure that the policy can run successfully.

If you encounter problems running Replication Director jobs, reopen the backup policy that is failing. In the open policy, click **OK**. In the **Validate Policy** dialog box, select **Complete** to validate the policy again.

NetBackup can expose the problems that may have occurred since the policy was created. For example, policy validation can inform you that the storage space isn't adequate to contain all of the data that you want to back up. Or that the storage server is offline or that the network connection is not working.

Logging for Replication Director

The following topics concern various aspects of logging for Replication Director.

Configuring the logging level in the NetBackup Administration Console

To view the information that is related to snapshots and snapshot replication, increase the verbose level of the logs to generate more detailed logs.

To configure the logging level in the NetBackup Administration Console

1. Make sure that the `bpfis` directory has been created for logging. (See Configuring logging for the OST_FIM.)
2. In the **NetBackup Administration Console**, select **NetBackup Management > Host Properties > Master Servers**.
3. Double-click on the master server name. In the **Master Server Properties** dialog box, select **Logging**.
4. Select **5** in the **Global logging level** drop-down menu for maximum logging.

   Note: To configure logging for OST_FIM, the logging level must be set to `9` using the command line. Additional configuration is also required.

   Configuring logging for the OST_FIM
5. Click **OK** to save the setting.

Also check the logs of the OpenStorage partner for more information.

Configuring logging for the OST_FIM

The bpfis directory is not present by default and must be created. To create the directory, run the mklogdir command, found in the following locations:

- On Windows: *install_path*\NetBackup\Logs
- On UNIX: /usr/openv/netbackup/logs

The bpfis directory contains both the bpfis log and the OSTPlugin logs for OpenStorage partners. After mklogdir is run, the bpfis directory appears in the following locations:

- On Windows: *install_path*\NetBackup\logs\bpfis
- On UNIX: /usr/openv/netbackup/logs/bpfis

By default, log entries for the OST_FIM do not appear in the bpfis directory. Perform the following steps to log information about OST_FIM.

To configure logging for the OST_FIM

1. The ostfi.conf file must appear in the following location:

   - On Windows:
     C:\Program Files\Common Files\Symantec Shared\VxFI\ostfi.conf
   - On UNIX:
     /usr/openv/lib/vxfi/configfiles/ostfi.conf
     If the configfiles directory is not present, create it.

   If the ostfi.conf file is not present, create it and add the following contents:

```
[DEBUG_TRACE_INFO]
"TRACERUNTIMEUPDATE"=dword:00000000
"TRACEFILE"="ostfi.log"
"TRACESTDOUT"=dword:00000000
"TRACEDIR"="/usr/openv/netbackup/logs/bpfis/"
"TRACELEVEL"=dword:00000009
```

If the `ostfi.conf` file is present, make sure that the `TRACELEVEL` is set to `00000009`.

2 Use the command line to change the logging level to 9. Information about the OST_FIM is not logged when the **Global logging level** is set to **5** in the **NetBackup Administration Console**.

First use the `bpgetconfig` command to obtain a list of configuration entries. Then use `bpsetconfig` to change the entries as needed.

For example:

```
echo VERBOSE=9 | bpsetconfig
```

For information about `bpgetconfig` and `bpsetconfig`, see the NetBackup Commands Reference Guide.

When the OST_FIM is configured to generate logs, the information appears in the `ostfi.log` log directory in addition to the `bpfis` log.

Configuring logging for VSS on Windows

Check the VSS-related event logs in the Microsoft Windows Event Viewer to help determine the failures that are related to VSS

To generate logs in a specified file in the registry for the Windows Volume Shadow Services (VSS), use the following Microsoft Windows procedure:

http://msdn.microsoft.com/en-us/library/windows/desktop/dd765233(v=vs.85).aspx#using_vsstrace

Configuring logging for NetBackup VSS providers

The `vss.conf` file must appear in the following location:

- On Windows:
  `C:\Program Files\Common Files\Symantec Shared\VxFI\vss.conf`
- On UNIX:
  `/usr/openv/lib/vxfi/configfiles/vss.conf`
  If the `configfiles` directory is not present, create it.

If the `vss.conf` file is not present, create it and change the `TRACELEVEL` in the following file to `6`.

The logs will be available in the following directory: `VXFI_ROOT\logs`.

Throttling Replication Director operations with NetBackup

NetBackup offers several methods to control or to throttle Replication Director operations:

- Adjust the Disk pool Limit I/O streams setting
- Change how snapshot jobs are batched
- Change the asyncWaitSnap interval
- Control the number of I/O snapshot streams

Adjust the Disk pool Limit I/O streams setting

The **Limit I/O streams** setting appears in the **New** or **Change Disk Pool** dialog box. The setting controls the number of NetBackup jobs that can use a disk pool concurrently.

By default, the **Limit I/O streams** check box is clear (not enabled), so there is no limit to the jobs that use a disk pool concurrently. Note that the **Limit I/O streams** setting must be expressed in increments of two because a single replication job requires two I/O resources.

For example, consider a situation in which the **Limit I/O streams** is set to *4* for the disk pool that contains the *PrimarySnapshot* LSU. This means that two concurrent replication jobs can be active in NetBackup, assuming that no batching is occurring. If a third replication job starts, it is queued until one of the first two replication jobs is complete. The NetBackup Job Manager queues the third job until one of the two running jobs is complete.

Batching can cause many replications to occur within a single NetBackup job. For this reason, another setting may be required in tandem with **Limit I/O streams**, as described here:

Change how snapshot jobs are batched

Change the **Maximum images per snapshot replication job** property within the **Storage Lifecycle Parameters** host properties. This property applies only to the snapshot replication jobs that are batched together. By default, the value is 50 images.

Batching combines replications for multiple backup IDs (spanning policies and clients) whenever:

- The source and the target storage units are the same.
- The replication types are the same (mirror or non-mirror).

- The copy numbers are the same.

The scalability issue this can cause is that the NetBackup media manager can send a large number of nearly simultaneous snapshot replication requests to the NetApp Plug-in for Symantec NetBackup which can overwhelm either the plug-in or the DataFabric Manager server.

This parameter can control how many NetBackup backup IDs can be batched together into a single replication job.

Based on the previous example of setting the disk pool **Limit I/O streams** limit, change the **Maximum size per snapshot replication** parameter in the **Storage Lifecycle Parameters** host properties.

- Disk pool **Limit I/O streams** is set to *4* for the disk pool containing the *PrimarySnapshot* LSU.
- Change the **Maximum size per snapshot replication** parameter to 10:
- Suppose that a duplication session starts and 25 backup IDs are pending replication for copy number 2.
  - Two replication jobs start, each for replicating 10 BIDs.
  - The Job Manager queues a third job: A replication job (for the remaining 5 BIDs). The job waits until one of the first two jobs completes.

For additional information about the **Storage Lifecycle Parameters** host properties, see the NetBackup Administrator's Guide, Volume I or the online Help.

Change the asyncWaitSnap interval

The `bpdm` touchfile contains a value for the `asyncWaitSnap` interval. During a batched replication job, `bpdm` calls `asyncWait` on all snapshots for all BIDs in succession. It then sleeps for a timeout value that is specified by the vendor as a return value to the `asyncWaitSnap` API before it makes another round of wait calls.

Because of the timeout, it can take up to 60 seconds for NetBackup to discover that a replication has completed. To increase job throughput at the expense of the DataFabric Manager server load, this timeout value can be adjusted by creating the following file:

- On Windows:

  Install_path\netbackup\db\config\RPL_ASYNC_WAIT_SLEEP
- On UNIX:

  /usr/openv/netabackup/db/config/RPL_ASYNC_WAIT_SLEEP

The file should contain one line with a number that represents the number of seconds to use for this interval. The default value for the NetApp Plug-in forSymantec NetBackup is 60 seconds.

The setting takes effect the next time `bpdm` starts as part of a replication job.

The following example entry in the `bpdm` log indicates the current `asyncWait` sleep interval:

```
14:21:03.856 [26524] <2> prm_set_config: Using 10 for async wait
sleep value
```

Control the number of I/O snapshot streams

By default a snapshot creation job consumes one I/O stream on the primary disk pool. You can make a change so that snapshot creation consumes zero I/O resources:

Add the following entry to the `bp.conf` file:

```
REQUEST_STU_RESOURCE_FOR_SNAPSHOT_JOBS = NO
```

Then, restart services.

A snapshot replication job consumes two (2) I/O streams on the source disk pool and zero (0) on the target.

Standard policy restore error (2800)

The following table describes the restore problems that can result in status code 2800 and possible solutions for the error:

`Standard policy restore error (2800).`

Table 14-1 Solutions for the problems that can cause status code 2800

Problem or cause	Solution
The administrator attempts to restore a backup to its original location. However, the NetApp volume fails with status code 2800. The progress log displays the message: `No space left on device.`	The NetApp volume on which the snapshot resides must have enough free space for the restore to succeed. Even if the **Overwrite existing files** option is selected, the free space must equal more than the original backup size. The size requirement exists because the data blocks that correspond to the old file cannot be deleted while the snapshot refers to them. Use the `aggr show_space` command on the storage system to display the breakup of used space in the aggregate.
The restore fails with a `permission denied` error while copying files to the primary volume.	The time on the NetBackup servers, the DataFabric Manager server, and the storage system must be synchronized or have a difference of less than 5 minutes.

Table 14-1 Solutions for the problems that can cause status code 2800 *(continued)*

Problem or cause	Solution
The restore from a snapshot fails with status code 2800. The progress log displays the message: `no files matched in the given data range`	The restore fails if you select a different path other than what is listed in the **Backup Selections** tab of the policy. For example, `vol6` and `vol7` are volumes mounted on `/mnt/vol6` and `/mnt/vol7` respectively. These mount points are specified in the **Backup Selections** tab. During a restore, if you select only `/mnt`, (the parent directory of the path that is listed in the **Backup Selections** tab), the restore fails with status code 2800. To successfully restore from the snapshot copy, select the original path that is listed in the **Backup Selections** tab. In this example, specify `/mnt/vol6` and `/mnt/vol7` or the subdirectory or file. For more information on restoring snapshots, see the NetBackup Snapshot Client Administrator's Guide.

Snapshot-based backups and restores fail if the backup selection that is listed in the NetBackup policy contains any spaces either in the mount points or mount devices.	■ No spaces in mount points
	Block device example:
	`/dev/dg/vol` is mounted on `/mnt point`
	NFS example:
	`Filer:/vol/datavol` is mounted on `/nfs mnt`
	■ No spaces in mount devices
	Block device example:
	`/dev/dg/vol data` is mounted on `/mntpoint`
	NFS example:
	`Filer:/vol/data vol` is mounted on `/nfsmnt`

Status 156 errors

The following situations can cause status code 156:

Table 14-2 Solutions for the problems that can cause status code 156

Problem or cause	Solution
Alternate client backups and restores fail for a Windows client when logged into the NetBackup Client Service as the **Local system account** instead of as the Administrator account.	To perform alternate client backups and restores for a Windows client, log into the NetBackup Client Service as the Administrator account, not as the **Local system account**. If the **Local system account** is selected, the backup fails with status code 156. See "Configuring the NetBackup Client Service" on page 53.

A live browse restore from the mirror copy fails.	Before creating any snapshots, perform the following on the volume on which the NFS or CIFS share is created:
	
	■ Create the volume. Then, use the NetApp `vol` command options to enable the following:
	  ■ Set `convert_ucode on`
	  ■ Set `create_ucode on`
	■ Begin to use the volume using CIFS or NFS to create snapshots.

Multiple snapshot jobs that were started at a high frequency fail with code 156 or 1541.	Regarding snapshot the jobs that end with status code 156 or 1541 or other error. These errors may occur in the following situation: An administrator manually (or by using a script), starts multiple snapshot jobs at a high frequency. (For example, one snapshot job every 5 seconds.) At the same time, multiple rotation processes begin. The processes operate on the same catalog information, which includes information about existing snapshots. Because the processes work on the same information at the same time, a problem of inconsistency can occur. Some of the processes delete the snapshots and update the catalog while other processes continue to refer to the obsolete information. The result is that the snapshot jobs can end with status codes 156 (snapshot error encountered), 1541 (snapshot creation failed), or other unpredictable errors. This behavior does not occur for scheduled snapshot jobs, as NetBackup controls the job execution.
Snapshot jobs fail with code 156 for the backup selections that contain dynamic disks.	If using Veritas Storage Foundation for Windows for disk groups, dynamic volumes are not supported: ■ Volume Shadow Copy Service (VSS) does not allow a dynamic volume snapshot to be imported on the same host. ■ VSS does not allow the importing of two snapshot devices of the same source dynamic volumes. Replication Director cannot support the replication of dynamic volumes, since it is impossible to import snapshots and replicate snapshots onto same client.

Policy and storage lifecycle policy issues

The following tables describe various causes for policy and storage lifecycle policy configuration and validation failures and possible solutions:

Table 14-3 Policy issues

Problem or cause	Solution
The volume is not visible in the Operations Manager. That means that the DataFabric Manager server is not aware of the volume that was created on the filer.	Enable the SSH on filer. Restart the DataFabric Manager server or refresh the connection. The volume should be visible in Operations Manager on the DataFabric Manager server.
The filer and the DataFabric Manager server are in different domains.	Make sure the `/etc/hosts` file on both the filer and the DataFabric Manager server have entries for one another. Or, install the filer in the same domain.
The host credentials that are required to access a CIFS share are not set for the NetBackup Client Service (`bpcd`).	Set the credentials that are required to access a CIFS share in the NetBackup Client Service and restart the service.
The SLP that contains **Backup From Snapshot** or **Index From Snapshot** operations fails with status code 130. The backup policy that uses the SLP contains multiple backup selections that include a mix of native multi-pathing and `vxdmp`. Veritas Dynamic Multi-Pathing (DMP) supports Veritas Volume Manager (VxVM) volumes on DMP metadevices, and Veritas File System (VxFS) file systems on those volumes.)	Do not use two types of multi-pathing software on the same device. http://www.symantec.com/docs/TECH75913
An NDMP policy that is configured for Replication Director fails.	Check to see if a schedule for the NDMP policy has the **Override policy storage selection** option enabled. If the override is an SLP that contains an **Index From Snapshot** operation, the **Index From Snapshot** operation is not supported in the NDMP policies that are configured for Replication Director. The SLP validation process does not detect the unsupported configuration because it does not check whether the **Override policy storage selection** option is enabled in the policy schedules. See "Index From Snapshot operation in an SLP" on page 105.

Table 14-4 Policy and SLP validation issues

Problem or cause	Solution
Storage lifecycle policy validation cannot be completed because the request times out.	SLPs that contain replication operations can take more than 60 seconds to validate. If the connectivity between NetBackup and the NetApp DataFabric Manager server exceeds 60 seconds, the SLP may not validate. To increase the timeout to account for the latency in connectivity, perform one of the following tasks, depending on which **NetBackup Administration Console** is used: ■ For the **NetBackup Administration Console** on Windows: Increase the **GUI connect timeout**. To access the timeout option, select **View > Options**. Then select the **Administration Console** tab. Increase the **GUI connect timeout** value. ■ For the **NetBackup-Java Administration Console** or the **Java Windows Administration Console**: Increase the timeout value in the following files: On Windows: The `setconf.bat` file (*`Install_path`*`\java\setconf.bat`). On UNIX: The `NBJAVA_CORBA_DEFAULT_TIMEOUT` option in the `nbj.conf` configuration file (`/usr/openv/java/nbj.conf`).
Policy validation fails with status code 14 (file write failed).	Policy validation fails with status code 14 if the storage server name is 232 characters or longer.
Policy validation fails for a policy to back up a Windows client. The `bpfis` log on the NetBackup client contains status code 71 (none of the files in the file list exist).	The NetBackup Client Service is using the Local System Account. For Windows clients accessing a CIFS share on a NetApp storage system using a UNC path, the account used to run the NetBackup Client Service must be a non-system account After adding the correct credentials to access the CIFS share, restart the NetBackup Client Service on the client. See "Configuring the NetBackup Client Service" on page 53.
Policy validation fails with status code 223 (an invalid entry was encountered).	Make sure the data volume on the filer to back up is mounted on the client that is listed in the NetBackup policy.
Policy validation fails due to a problem with a specified volume.	Make sure that a volume or qtree in the backup selection of the policy is not offline. Also note that snapshot, indexing, and backup jobs remain in an active state if a volume or qtree in the backup selection is offline.
When using NetApp storage, policy validation can take a very long time to complete in some situations.	When the first replication job in an SLP is in progress, then any concurrent validation or snapshot jobs for the same policy wait until the replication job completes. This situation can arise in the case of large volumes where the base replication can take a significant amount of time to complete.

Table 14-4 Policy and SLP validation issues *(continued)*

Problem or cause	Solution
Policy validation fails when SAN-connected storage is used.	If either a Fibre Channel or an iSCSI license is installed on a storage system, make sure that the service is running. Policy validation fails if the license for either is present on the storage system and the service is not running.

Snapshot issues

The following table describes various causes for snapshot failures and possible solutions:

Table 14-5 Snapshot issues

Problem or cause	Solution
Snapshot creation fails if the maximum snapshot limit is reached and no catalog image is marked as SLP-complete. In this case, rotation of snapshot fails.	The SLP is marked as complete sometime after the job completes. By default, NetBackup processes SLP images every five minutes. This interval is configurable in the **SLP Parameters** host properties in the NetBackup Administration Console.
Snapshots and snapshot replications fail. The Windows Event Viewer displays the following SnapDrive entry in the Event log: `NOSNAPDIR option is currently turned ON in storage system 'system_name', Please turn this to OFF for snap shot creation to succeed`	Use the following command to turn the `NOSNAPDIR` option off for the storage system: `vol options vol_name nosnapdir off`
Delays in snapshot processing on Windows for SAN devices.	Only one shadow copy can be created, imported, or deleted at a time. The VSS snapshot-related operation can fail when multiple VSS operations are performed simultaneously. The Windows VSS API requestor is responsible for serializing the shadow copy operations. (The serialization can be observed by using Windows VShadow or DiskShadow utilities.) Two registry keys can facilitate the serialization for NetBackup clients. Table 14-6 describes the details of the keys and the settings that allow for serialized and quicker snapshots.

Table 14-5 Snapshot issues *(continued)*

Problem or cause	Solution
Snapshot jobs may fail for a Windows client with status code 4200 (Operation failed: Unable to acquire snapshot lock).	If a job fails to take a VSS operation lock within the timeout that the `VssOperationMutexLockTimeout` key specifies, the snapshot job fails. The VSS Mutex Lock Timeout error returns NetBackup status code 4200. The VSS operation on each client is serialized. If multiple snapshot creation jobs are triggered on a Windows client, all of the jobs are serialized. Each job waits for a VSS lock and if the lock does not happen by the specified time, the job fails. Increase the length of the timeout by increasing the value for `VssOperationMutexLockTimeout`. (For instructions, see Table 14-6.) The default value for `VssOperationMutexLockTimeout` is 3600000 microseconds (1 hour). **Note:** If the key is not available in the registry, create a new key.
Snapshot jobs fail for NDMP policies with status code 252 (Topology validation failed).	This can occur if one of the volumes that is specified in the policy's backup selection is removed during policy validation or during the snapshot job. The failure applies to a backup selection specified explicitly or as part of the NDMP `ALL_FILESYSTEM` directive. In this situation, the following error message appears during policy validation: `Snapshot [Storage unit: Primary_STU; Index: 1]: Network_NTAP:DFM_Server_Name : FilerHost given is (Filer_Name) but volume (Volume_Name) is found on host (invalid/Filer_Name) [vendor code=2060061]` The policy validation or snapshot job will be successful when retried.

Table 14-5 Snapshot issues *(continued)*

Problem or cause	Solution
Snapshots fail for a policy of type **MS-Windows**, yet the policy passes policy validation. The policy uses Volume Shadow Copy Service (VSS) with Replication Director and the storage lifecycle policy contains only snapshots in a SAN topology.	The vendor has the responsibility to provide certain policy validation checks. In this situation, where the policy is of type **MS-Windows**, NetBackup tries to validate the policy through the VSS framework. However, the VSS framework cannot provide the necessary validation. For example, NetBackup policy validation cannot detect whether mandatory licenses for snapshot and replication operations (such as SnapRestore) are available or not on NetApp arrays.
Snapshot creation fails when using a NetApp disk array.	Check that the Import_snap_by_name capability is available on the storage server. Add the Import_snap_by_name capability to the MWS configuration file.
NetApp error messages display the following resync failure: No common snapshot to use as the base for resynchronization.	The resync failure occurred because a point-in-time rollback restore was performed to a snapshot before the P-M-V (Primary-SnapMirror-SnapVault) relationship was established. The SnapVault destination on the storage system does not have the snapshot to which the restore was performed on the primary storage, so the SnapVault resync failed In this situation, perform the following actions based on one of the topology types: ■ For the topology type PMV (Primary-SnapMirror-SnapVault): In the OnCommand interface, change the protection policy to PM (Primary-SnapMirror) and re-run the job from NetBackup. ■ For either topology type PV (Primary-SnapVault) or PVM (Primary-SnapVault-SnapMirror): In the OnCommand interface, change the protection policy to Primary (a NetBackup backup only) and re-run the job from NetBackup.
Problems running snapshot jobs using a NetApp disk array.	NetApp recommends that the administrator does not cancel snapshot jobs that are running.

Table 14-5 Snapshot issues *(continued)*

Problem or cause	Solution

Snapshot creation fails when using a NetApp disk array.
 	
The NetBackup_create_import_*timestamp* dataset may have been deleted.
 	
Check the log of the NetApp Plug-in for Symantec NetBackup for a message that includes the following information:
 	
`Import snap failed.`
 	
For example:
 	
`0 IMGINFO :-245482608 98 0 154918 2011/10/17 10:49:18 Import snap failed There is no dataset named '2718'. : 22255`
	To clear the failure, 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`

Snapshots fail with status code 20 (Invalid Command Parameter). A NetApp volume is deleted and then recreated with the same name. However, the same case was not used for the recreated volume.	The names of volumes are case-sensitive. If a volume is deleted and then recreated, the name of the new volume must be identical, with letters in the same case. For example, if volume *abc_vol* is deleted, do not recreate it as *Abc_Vol*. Similarly, policy validation and snapshot creation can fail if two volumes have the same name but in different cases. The cause is that different object IDs reference the same DataFabric Manager server, which is case-insensitive.
Snapshot jobs can take a very long time to complete for **MS-Windows** backup polices when using a SAN-connected NetApp disk array.	Traffic on the NetApp Management Console can significantly delay the SnapDrive snapshot commands. Block the data traffic on the Management Console and route the snapshot replication traffic over the 10 GB interface instead. Use the following command to make the 10 GB interface the preferred interface for NDMP on the storage system: `options interface.blocked.mgmt_data_traffic on` `options ndmpd.preferred_interface` *`interface_name`*

Table 14-5 Snapshot issues *(continued)*

Problem or cause	Solution
Snapshot jobs fail with status 4209 (Snapshot metadata or statefiles cannot be created) when using NetApp disk array.	NetApp storage does not support NetBackup backup selections that contain special characters such as the at sign (@), the asterisk (*), the number sign (#), and the ampersand (&). Unsupported characters are also listed in the NetApp Plug-in for Symantec NetBackup Installation and Administration Guide.

Table 14-6 Registry keys and settings to facilitate snapshot serialization

Key name	Possible values	Default type	Comment
`HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Config\VSS_SERIALISE_OPERATIONS`	`0` or `1`	`1`	`0`: Disable VSS snapshot operation serialization. `1`: Enable VSS snapshot operation serialization. By default, the serialization of VSS snapshot creation is enabled.
`HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Config\VssOperationMutexLockTimeout`	An integer value.	`3600000`	The timeout is indicated in microseconds.

Import issues

The following table describes various causes for import failures and possible solutions.

Table 14-7 Import issues

Problem or cause	Solution
The snapshot import failed. The NetApp Plug-in for Symantec NetBackup failed to export the snapshot volume.	Perform the following steps on the source volume: ■ Create the volume and enable `convert_ucode on` and `create_ucode on` using `vol` options commands. ■ Begin to use the volume using CIFS or NFS and create snapshots.

Table 14-7 Import issues *(continued)*

Problem or cause	Solution

When using NetApp storage:
The iSCSI management session is not visible in the SnapDrive window.
	`cd C:\Windows\system32\wbem`
	`mofcomp iscsidsc.mof`
	`mofcomp iscsiprf.mof`
	`mofcomp iscsihba.mof`
	Restart the SnapDrive service.
	Refresh the storage, SnapDrive, and local server.

When using NetApp storage: The snapshot import fails for iSCSI devices.	If Fibre Channel is attached to the host, NetBackup expects the LUN to arrive on Fibre Channel. If the zoning is not in place, the device does not arrive on the host and the import fails. Have the Fibre Channel zoning between the disk array and the host if a Fibre Channel card is used.
When using NetApp storage: The snapshot or replica import fails for NetApp SAN devices.	The device is not visible on the mount host. The `bpfis` log reports: `UDID NOT FOUND` ■ For Fibre Channel devices: Check that zoning is available between the disk array and the mount host. ■ For iSCSI devices: Establish an iSCSI session between the mount host and the disk array.
The replica import fails on Windows.	Multiple paths may exist for the same target devices. Install multipathing software on the host.

Avoiding problems importing snapshots on a RHEL client using the Device Mapper Multipathing solution

Snapshot imports may fail on a Red Hat Enterprise Linux client using the Device Mapper Multipathing solution. This is due to a failure to mount the snapshot.

The following are example `bpfis` log entries that are typical of this problem:

```
04:36:23.230 [15246] <2> onlfi_vfms_logf: INF - snapshot services:
gfspfi:Sun Mar 17 2013 04:36:23.230503 <Thread id - 1>
GFSP::importTreeNode - command [/bin/mount -o ro "/dev/sde1"
"/tmp/_vrts_frzn_img__oracle_iscsi_13872_2"] failed with message
'mount: /dev/sde1 already mounted or
/tmp/_vrts_frzn_img__oracle_iscsi_13872_2 busy
```

```
04:36:23.231 [15246] <2> onlfi_vfms_logf: INF - snapshot services:
hpevafi: Caught unhandled execution pipe exception
VFI_EXEC_PIPE_CMD_FAILED at /bin/mount -o ro "/dev/sde1"
"/tmp/_vrts_frzn_img__oracle_iscsi_13872_2", ../gfsp_plugin.cpp,
1,415
```

The problem can occur if either of the following are set incorrectly:

- The device `features` setting for Device Mapper is set as follows in the `/etc/multipath.conf` file.

  ```
  1 queue_if_no_path
  ```

  When set in this way, the I/O for a process that tries to access the device hangs until the device comes up. The setting also creates stale device node entries in the device mapper when the device has been unmapped from the host or deleted completely.

  To avoid this problem, use the following `features` setting in the `multipath.conf` file:

  ```
  no_path_retry number
  ```

  Where *number* indicates the number of I/O access retries permitted on the device until it times out.

- The `features "1 queue_if_no_path"` option is set as a compiled-in default for the vendor device.

  For the device vendor, set the following parameters in the `multipath.conf`:

  ```
  features "0 queue_if_no_path"
  no_path_retry 15
  ```

Refer to the following Device Mapper Multipathing documentation for detailed information about `queue_if_no_path` feature issues and solutions:

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/5/html/DM_Multipath/queueifnopath_issues.html

Cleaning up snapshot devices after leak from import

A backup policy (**MS-Windows** type) that uses Replication Director VSS snapshots for SAN devices on Windows may fail due to an import failure. While the snapshot operation on the storage device is successful, the import fails, causing the job to fail. However, the snapshot being taken on the storage device causes a storage device leak.

In this situation, the **Activity Monitor** displays the job failure with one of the following NetBackup status codes:

- 4201: Incorrect snapshot method selected or snapshot method configured incorrectly.
- 58: Cannot connect to the client machine.

The import failure may occur if the alternate client services are not accessible in the event of an offhost backup or a VSS failure. If this is the case, the `bpfis` log on the primary client contains the following message:

```
In case of snapshot creation using vendor VSS hardware provider,
snapshot devices may get leaked due to incomplete import operation.
VSS framework does not allow to delete un-imported snapshot. The
leaked snapshot devices can be recovered using Microsoft Vshadow
utility. Please use the xml file [xml file location] created on
client [primary client name]  to import and delete the snapshot
manually using Vshadow utility on alternate client
[alternate client name]. Please refer event viewer and Hardware
VSS provider logs for more details. Delete the file manually
after cleanup.
```

Use the following procedure to clean up the snapshot devices after the leak:

To clean up leaked snapshot devices

1. Use the Microsoft Windows Vshadow utility to manually import and delete the unimported snapshot. In case of offhost backup, copy the xml file from the primary client to the alternate client.
2. Use the xml file to import the snapshot:

```
C:\>vshadow.exe -i=
C:\Program Files\Veritas\NetBackup\temp\
bpfis.fim.rtpqe07.12345.1.0.xml

VSHADOW.EXE 3.0 - Volume Shadow Copy sample client.
Copyright (C) 2005 Microsoft Corporation. All rights reserved.

(Option: Import shadow copy set from file
'C:\Program Files\Veritas\NetBackup\temp\
bpfis.fim.rtpqe07.12345.1.0.xml')
Reading the file C:\Program Files\Veritas\NetBackup\temp\
bpfis.fim.rtpqe07.12345.1.0.xml'
...
- Setting the VSS context to: 0xffffffff
Importing the transportable snapshot set...
(Waiting for the asynchronous operation to finish...)
Shadow copy set successfully imported.
```

3. Use the snapshot ID from the xml file to delete the snapshot.

   The following is an example of the snapshot ID content from the xml file:

```
<SNAPSHOT_DESCRIPTION snapshotId=
"566a7cb3-4ca4-4a8b-b8b0-707911a5e234"
C:\>vshadow.exe -ds={566a7cb3-4ca4-4a8b-b8b0-707911a5e234}

VSHADOW.EXE 3.0 - Volume Shadow Copy sample client.
Copyright (C) 2005 Microsoft Corporation. All rights reserved.

(Option: Delete a shadow copy)
- Setting the VSS context to: 0xffffffff
- Deleting shadow copy {566a7cb3-4ca4-4a8b-b8b0-707911a5e234} ...
```

Replication issues

The following table describes various causes for replication failures and possible solutions:

Table 14-8 Replication issues

Problem or cause	Solution
The DataFabric Manager server licenses are not installed.	Install all of the licenses on the DataFabric Manager server for Operations Manager, Provisioning Manager, and Protection Manager.
Entries for backup volumes exist in the DataFabric Manager server which have been deleted from filer.	Delete the stale entries from the DataFabric Manager server using the NetApp OnCommand System Manager.
SnapVault and SnapMirror options are not configured to access the vault and mirror from the target filer.	Configure the SnapVault and SnapMirror options on the source filer to access the vault and mirror from the target filer.

Incorrect DataFabric Manager server configuration.	Run the following command on the DataFabric Manager server.
	`$ dfm option list pmUseSDUCompatibleSnapshotNames`
	`Option Value`
	`------------------------------ ------------------------------`
	`pmUseSDUCompatibleSnapshotNames Yes`
	By default, the output value should be `Yes`. If the output is `No`, run the following command to correctly set it:
	`$ dfm option set pmUseSDUCompatibleSnapshotNames=yes`

Duplication issues

The following table describes various causes for duplication of backup (tar) image failures and possible solutions:

Table 14-9 Duplication issues

Problem or cause	Solution
The credentials that are required to access a CIFS share are not set for the NetBackup Client Service (`bpcd`).	Set the credentials that are required to access a CIFS share in the NetBackup Client Service and restart the service.

Table 14-9 Duplication issues *(continued)*

Problem or cause	Solution
A space [ ] appears in one of the backup selections.	Rename the backup selection, omitting the space. Policy validation can discover invalid entries in the **Backup Selections** list. See "Use NetBackup policy validation to discover errors" on page 194.

Restore issues

The following table describes problems and possible solutions for restore issues.

Table 14-10 Restore issues

Problem or cause	Solution
Unable to browse to client data that resides on a CIFS share on NetApp storage. Browse produces the following error in the **Backup, Archive, and Restore** client interface: **Permission denied by client during rcmd**.	Run the NetBackup Client Service on the NetBackup client or alternate client with a non-system account that has credentials to enable access to the CIFS share on the NetApp storage. If the NetApp appliance is not running with valid credentials to the CIFS share, NetBackup fails to access the content of the snapshot and returns an error. After adding the correct credentials, restart the NetBackup Client Service on the client or alternate client. See "Configuring the NetBackup Client Service" on page 53.
The alternate client cannot browse the contents of a snapshot share when using the **Backup, Archive, and Restore** client interface.	In the NetBackup backup policy, check how the path of the backup selection is configured. The storage system must resolve on both the primary client and the alternate client for the alternate client to access the snapshot share. If the configuration is not the same, the export may succeed but the alternate client cannot access the share of the snapshot.

Table 14-10 Restore issues *(continued)*

Problem or cause	Solution
On a Windows-based client, a live browse operation, a **Backup From Snapshot** operation, or an **Index From Snapshot** fails. ■ The **Backup, Archive, and Restore** client interface displays no content. ■ The **Backup From Snapshot** or **Index From Snapshot** operation fails with status code 71 (none of the files in the file list exist) ■ The following error appears on the NetApp console when accessing the share from Windows Explorer: `Unable to acquire filer credentials: (0x96c73a25) Filer and domain time differ by more than 5 minutes.`	The time on the Windows domain controller and the filer must be synchronized or have a difference of less than 5 minutes. If the difference is greater than 5 minutes, the filer does not give the Windows client CIFS share access, resulting in error on the filer console. Use the date command to set the time on the NetApp storage.
Unable to browse the snapshot contents for restore even after the snapshot job was done successfully.	Check the **Backup Selections** tab of the backup policy to make sure that different storage stacks are not protected by a single policy. Specifying multiple volumes of different storage stacks in a single policy is not supported.
Unable to browse the snapshot contents for restore when the policy has multistreaming enabled.	A catalog image is created for every possible client and path combination in a snapshot policy. An image is created, even if a client does not contain the specified path. Note that in the **Backup, Archive, and Restore** interface, the user is presented with all images, even if no files were backed up. During a restore, if the user selects an image that contains no files, NetBackup displays a *No files found* message.
Unable to browse to the snapshot for an alternate client restore. Also, a **Backup From Snapshot** operation fails with status code 4213.	To successfully perform an alternate client restore from a snapshot, the Veritas Volume Manager (VxVM) versions must be the same on both the client and the alternate client. The different versions of VxVM can also cause a **Backup From Snapshot** operation to fail with status code 4213. Upgrade the NetBackup clients to the same version of VxVM.

Table 14-10 Restore issues *(continued)*

Problem or cause	Solution
Unable to browse incremental backup images exclusively from **Backup from Snapshot** jobs.	Check the master server host properties for this master server. Open the **Servers** host properties and select the **Media Servers** tab. The name of the media server should also appear on the **Additional servers** tab. If it does not, add the media server name to this tab. After the backup policy runs again, the user will see the differential incremental and cumulative incremental files in the **Backup, Archive, and Restore** interface.
Restores or **Backup From Snapshot** operations do not work properly. Back up and restore problems exist if the operating system that is used is RHEL 5.3 with kernel version 2.6.18-128.el5. Specifically, a problem exists with `kobject_add`.	NetBackup 7.6 does not support this kernel version. A request for a kernel fix has been opened with RHEL.
Point-in-time rollback restores that have the force option enabled fail.	If using Data ONTAP 8.1.1 or 8.1.2, the length of the path to any file that is backed up should not exceed 528 characters. If the path exceeds 528 characters, point-in-time rollback restores that have the force option enabled fail. Instead of a point-in-time rollback restore, perform a normal restore.
Browse of snapshots from **Backup, Archive, and Restore** client interface fails.	Browse problems can arise if the exported LUN uses Fibre Channel for the mounted volume and the volume is protected with iSCSI. This can occur in the case where a NetBackup client is configured for both Fibre Channel and iSCSI.

Assorted issues

The following table describes various problems and possible solutions:

Table 14-11 Assorted troubleshooting issues

Problem or cause	Solution
Problems with policy validation, snapshot creation, and duplication.	The NetApp Plug-in for Symantec NetBackup may not be installed properly. ■ Perform complete policy validation on the backup policy that is causing problems. See "Use NetBackup policy validation to discover errors" on page 194. ■ Check the installation logs of the NetApp Plug-in for Symantec NetBackup for errors and warnings. The log should contain no errors. Generally, if licenses are not installed on the DataFabric Manager server, the plug-in has not been installed properly. Before installing the plug-in, install the required licenses on the DataFabric Manager server. The install logs are available in the following location: *NBUPlugin_INSTALL_PATH*\NBUPlugin_install.log ■ Make sure that the three plug-in processes are running: nadapter_32, processmanager, and commnmanager. Check the following directory: NBUPlugin_INSTALL_PATH/processmanager status ■ Check the plug-in logs available in the following file: *NBUPlugin_INSTALL_PATH*\trace\NBUPlugin*.log
Job fails with PFI rotation error 13.	Some operations may take longer to complete due to network connectivity, causing jobs to time out and fail. Consider increasing the REQUEST_DELIVERY_TIMEOUT configuration option from the default of 300 (5 minutes) to 900 (15 minutes). For example: REQUEST_DELIVERY_TIMEOUT = 900 This option does not appear in the **NetBackup Administration Console** host properties. See the NetBackup Commands Reference Guide for information about using the bpgetconfig and the bpsetconfig commands to change the configuration option in the bp.conf file (UNIX) or the registry (Windows).
The NetBackup logs display messages regarding the inability to connect to the storage server.	Restarting the NetApp Plug-in for Symantec NetBackup can cause this issue. Restart the NetBackup services.
Expiration of catalog image fails.	A space [ ] appears in one of the backup selections. Rename the backup selection.

Table 14-11 Assorted troubleshooting issues *(continued)*

Problem or cause	Solution
An **Index From Snapshot** job fails with status code 4213 where the client is Windows 2003.	For Windows 2003 clients only, the Fibre Channel Information Tool (fcinfo) must be installed on the system. Verify that the Fibre Channel Information Tool (fcinfo), is installed on the system. See the following link for more information: http://www.microsoft.com/en-us/download/details.aspx?id=17530
An **Index From Snapshot** job fails with status code 4213 or 13 (upon retry).	Stale disk groups on an off-host client can cause an **Index From Snapshot** job to fail. The stale devices can be caused when part of an earlier import job failed and the deport did not conduct a proper cleanup of the devices. Delete stale disk groups on the off-host client and retry the job.
A **Backup From Snapshot** job or an **Index From Snapshot** job fails with status code 55 (permission denied by client during rcmd). The `bpcd` log on the NetBackup client contains exit status 55.	The NetBackup Client Service on the NetBackup client or alternate client must have valid credentials to access the CIFS share on the NetApp storage system. For Windows clients accessing a CIFS share on a NetApp storage system, the account used to run the NetBackup Client Service must be a non-system account After adding the correct credentials to access the CIFS share, restart the NetBackup Client Service on the client. See "Configuring the NetBackup Client Service" on page 53.
Backup From Snapshot or **Index From Snapshot** jobs fail with status code 4213 for replica copies. The `bpfis` import job fails with status code 4213 and the devices are not visible or available online.	■ Check that the SAN zoning has completed between the disk arrays and the client. ■ For NetApp iSCSI devices, establish an iSCSI session between the client and the disk arrays on which the replica is created. **Note:** For iSCSI to support block devices, make sure that no HBA cards are attached to the host. If NDMP is used, it must be enabled on both the primary and the secondary filers. The following error displays in the `bpfis` logs when snapshot import fails with error 4213 due to an iSCSI establishment error: *For host with HBA card, verify correct zoning and mapping exist between host and target array. For host without HBA card, verify iSCSI session is established between host and target array.*
Backup From Snapshot or **Index From Snapshot** jobs fail with status code 4213.	If using a GNOME system configuration, check to see if automount is enabled. Disable automount and reboot the server.

Table 14-11 Assorted troubleshooting issues *(continued)*

Problem or cause	Solution
When configuring a disk pool for a NetApp DataFabric Manager server, no LSUs display for selection in the Disk Pool Configuration Wizard.	The default NetBackup group on the DataFabric Manager server does not contain any resource pools. When the NBUPlugin is installed on the DataFabric Manager server, a NetBackup group is automatically created on the DataFabric Manager server. On the OnCommand server, 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 contains no resource pools, no LSUs display in the Disk Pool Configuration Wizard.
A **Backup From Snapshot** job or a snapshot import fails with status code 4213 (Snapshot import failed) when using LUNs.	If the Windows version in use is any other version than Windows 2003 or Windows 2008 R2, the state of the snapshot device cannot be detected properly. Make sure that the Windows version is Windows 2003 or Windows 2008 R2.
A **Backup From Snapshot** is partially successful where the policy contains multiple clients.	The **Backup From Snapshot** may be partially successful for a client where all of the backup selections are not present on that client. This is expected behavior.
In a clustered environment, jobs fail with status code 41 (network connection timed out) when a failover occurs.	If the master server timeout is less than the client timeout (**Client connect timeout** setting), jobs can fail with status code 41. Increase the client timeout on the master server. The client timeout is configured in the **NetBackup Administration Console** in the **Timeouts** host properties. The default **Client connect timeout** is 300 seconds.

Table 14-11 Assorted troubleshooting issues *(continued)*

Problem or cause	Solution

Using Veritas Volume Manager (VxVM), snapshots and snapshot replication imports fail with status code 4213.
 	
The bpfis logs display the following error:
 	
`14:50:32.562 [14800] <2> onlfi_vfms_logf: INF - snapshot services: vxvmfi:Fri Aug 2 2013`
 	
`14:50:32.562832 <Thread id - 1> Warning - failed with message='VxVM vxdisk`
 	
`ERROR V-5-1-16007 Data Corruption Protection Activated - User Corrective Action Needed`
	This issue indicates that the Veritas Dynamic Multi-Pathing (DMP) device contains multiple device registrations for the indicated Major/Minor numbers with conflicting serial numbers.
	
	For detailed information about solving this problem, see the following Symantec document:
	
	http://www.symantec.com/docs/TECH128862

Index

M

N

O

P

Q

R

S

T

U

V

W