EMC® NetWorker®

Version 9.0.x

Snapshot Management for NAS Devices Integration Guide

302-001-778

REV 05

EMC²

Copyright © 1990-2016 EMC Corporation. All rights reserved. Published in the USA.

Published June 2016

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com).

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

Figures 5

Tables 7

Preface 9

Chapter 1 Overview of NAS Snapshot Features 13

NetWorker snapshot management for NAS feature description 14
- NAS snapshot operations 14
- Types of NAS snapshot-based backups 15
- Types of NAS snapshot and clone recoveries 15
- NetWorker clone support 15
- Backup configuration methods 16
- Recovery interfaces 16
- Monitoring and reporting NAS snapshot operations 17
- Internationalization support 17

Components of the NAS snapshot network 17
- NAS devices 17
- NDMP environment 18
- NetWorker server 19
- NetWorker client 19
- NetWorker storage node 19
- Backup storage media 19

Licensing requirements 19

Example NAS snapshot environments 19
- Example of a snapshot and rollover to storage media 20
- Example of a snapshot from replication 21
- Examples of snapshot recovery 22

Chapter 2 Data Protection Policies 25

Introduction 26

Default data protection policies 26

Strategies for NAS snapshot backups 27
- Road map for configuring a new data protection policy 28
- Creating a policy 29
- Creating a workflow in a new policy 30
- Protection groups for NAS snapshot devices 32
- Supported actions in snapshot workflows 38
- Action in snapshot workflows 39
- Visual representation of NAS snapshot workflows 57

Chapter 3 Software Configuration 59

Backup group resource migration 60

Road map for NAS snapshot configuration 62

NetWorker with NAS configuration prerequisites 62
- NAS device prerequisites 63

Replication prerequisites 63
NetApp prerequisites 63
Storage node prerequisites 64
Configuring NDMP 64
Configuring a client resource with the wizard 64
Performing post Client Configuration Wizard steps 68
Configuring a NAS device client resource manually 68
Configuring the Application Information variables 69
Configuring preprocessing and postprocessing scripts 70

Chapter 4 Data Management and Recovery 71

Snapshot management 72
Snapshot reporting 72
Save set IDs and expiration policies 72
Browsing snapshot and clone save sets 72
Browsing and recovery on Windows hosts 73
NAS snapshot recovery support and limitations 73
Recovering data from a snapshot with the Recovery Wizard 73

Appendix A Application Information Variables 77

Using Application Information variables 78
Common Application Information variables 78

Appendix B Command-Line Operations for NAS Recovery 79

Using CLI commands for NetWorker operations 80
NAS snapshot commands 80
Using nsrsnapadmin operations 80
Example nsrsnapadmin operations 81
Querying with the mminfo command 83
Using nsrnassnap_recover operations 83

Appendix C Snapshot limitations 85

NAS snapshot support and limitation 86
Device-specific limitations for snapshot recovery 86

Glossary 91

FIGURES

1 NAS snapshot with rollover to storage media 20
2 Remote replication with snapshot and clone to storage 21
3 In-place recovery restores data to the original location on the source device 22
4 Out-of-place recovery restores data to a different location on the source device 23
5 Directed recovery restores data to the NetWorker client that runs the recovery 23
6 Platinum policy configuration 26
7 Gold policy configuration 27
8 Silver policy configuration 27
9 Bronze policy configuration 27
10 Data protection policy example 29
11 All possible workflow actions for a snapshot backup 40
12 Workflow path from a snapshot backup action 40
13 Workflow path from a discover action 40
14 Sample NAS snapshot workflow 57

TABLES

1 Revision history 9
2 Style conventions 11
3 NAS device support and limitations 17
4 Save set criteria 37
5 Schedule icons 42
6 Schedule icons 45
7 Backup type icons 47
8 Snapshot discovery icons 51
9 Snapshot generate icons 52
10 Schedule icons 54
11 Migration of Group attributes 60
12 Common Application Information variables 78
13 Commands and options that are supported in nsrsnapadmin interactive mode 80
14 Device limitations and support for snapshot management 86
15 Device support for recovery of save sets and individual files 88
16 NetApp support for types of local replication and platforms 89
17 NetApp C-Mode local replication and platforms 89
18 NetApp support for types of remote replication and platforms 90

Preface

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function correctly or does not function as described in this document.

Note

This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This document provides planning, practices, and configuration information for the use of the EMC NetWorker Snapshot Management for NAS devices features within an EMC NetWorker backup and storage management environment.

Audience

This document is intended for system administrators. Readers of this document must be familiar with the following tasks:

- Identifying the different hardware and software components that make up the NetWorker datazone.
- Following procedures to configure storage management operations.
- Following guidelines to locate problems and implement solutions.

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
05	June 29, 2016	Updated this document for EMC NetWorker 9.0.1. A new appendix for Limitations is added.
04	April 13, 2016	Updated the section "Data Protection Policies" chapter with the following changes: • Updated the section "Strategies for NAS snapshot backups", to revise the order in which you create the data protection policy resources. • Added the section " Default data protection policies".
03	January 25, 2016	Minor update to this document for EMC NetWorker 9.0.
02	December 14, 2015	Minor updates to this document for EMC NetWorker 9.0.

Table 1 Revision history (continued)

Revision	Date	Description
01	September 24, 2015	First release of this document for EMC NetWorker 9.0.

Related documentation

The NetWorker documentation set includes the following publications, available on EMC Online Support:

- *EMC NetWorker Online Software Compatibility Guide*
  Provides a list of client, server, and storage node operating systems supported by the EMC information protection software versions. You can access the Online Software Compatibility Guide on the EMC Online Support site at https://support.emc.com. From the Support by Product pages, search for NetWorker using "Find a Product", and then select the Install, License, and Configure link.
- *EMC NetWorker Administration Guide*
  Describes how to configure and maintain the NetWorker software.
- *EMC NetWorker Network Data Management Protocol (NDMP) User Guide*
  Describes how to use the NetWorker software to provide data protection for NDMP filers.
- *EMC NetWorker Cluster Integration Guide*
  Contains information related to configuring NetWorker software on cluster servers and clients.
- *EMC NetWorker Installation Guide*
  Provides information on how to install, uninstall, and update the NetWorker software for clients, storage nodes, and servers on all supported operating systems.
- *EMC NetWorker Updating from a Previous Release Guide*
  Describes how to update the NetWorker software from a previously installed release.
- *EMC NetWorker Release Notes*
  Contains information on new features and changes, fixed problems, known limitations, environment and system requirements for the latest NetWorker software release.
- *EMC NetWorker Command Reference Guide*
  Provides reference information for NetWorker commands and options.
- *EMC NetWorker Data Domain Boost Integration Guide*
  Provides planning and configuration information on the use of Data Domain devices for data deduplication backup and storage in a NetWorker environment.
- *EMC NetWorker Performance Optimization Planning Guide*
  Contains basic performance tuning information for NetWorker.
- *EMC NetWorker Server Disaster Recovery and Availability Best Practices Guide*
  Describes how to design and plan for a NetWorker disaster recovery. However, it does not provide detailed disaster recovery instructions. The Disaster Recovery section of the NetWorker Procedure Generator (NPG) provides step-by-step disaster recovery instructions.
- *EMC NetWorker Snapshot Management Integration Guide*
  Describes the ability to catalog and manage snapshot copies of production data that are created by using mirror technologies on EMC storage arrays.
- *EMC NetWorker Snapshot Management for NAS Devices Integration Guide*

Describes how to catalog and manage snapshot copies of production data that are created by using replication technologies on NAS devices.

- *EMC NetWorker VMware Integration Guide*
  Provides planning and configuration information on the use of VMware in a NetWorker environment.
- *EMC NetWorker Error Message Guide*
  Provides information on common NetWorker error messages.
- *EMC NetWorker Licensing Guide*
  Provides information about licensing NetWorker products and features.
- *EMC NetWorker REST API Getting Started Guide*
  Describes how to configure and use the NetWorker REST API to create programmatic interfaces to the NetWorker server.
- *EMC NetWorker REST API Reference Guide*
  Provides the NetWorker REST API specification used to create programmatic interfaces to the NetWorker server.
- EMC NetWorker Management Console Online Help
  Describes the day-to-day administration tasks performed in the NetWorker Management Console and the NetWorker Administration window. To view the online help, click **Help** in the main menu.
- EMC NetWorker User Online Help
  The NetWorker User program is the Windows client interface. Describes how to use the NetWorker User program which is the Windows client interface connect to a NetWorker server to back up, recover, archive, and retrieve files over a network.

Special notice conventions that are used in this document

EMC uses the following conventions for special notices:

NOTICE

Identifies content that warns of potential business or data loss.

Note

Contains information that is incidental, but not essential, to the topic.

Typographical conventions

EMC uses the following type style conventions in this document:

Table 2 Style conventions

Bold	Used for names of interface elements, such as names of buttons, fields, tab names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications that are referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, file names, prompts, and syntax • Commands and options
Monospace italic	Used for variables

Table 2 Style conventions (continued)

`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate non-essential information that is omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support

Go to EMC Online Support and click Service Center. Several options for contacting EMC Technical Support appear on the site. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Online communities

Go to EMC Community Network at https://community.emc.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all EMC products.

Your comments

Your suggestions help to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Overview of NAS Snapshot Features

This chapter includes the following topics:

- NetWorker snapshot management for NAS feature description 14
- Components of the NAS snapshot network 17
- Licensing requirements 19
- Example NAS snapshot environments 19

NetWorker snapshot management for NAS feature description

The EMC® NetWorker® 9.0 and later server software includes optional features to enable NetWorker snapshot management for network-attached storage (NAS), also called NSM for NAS. Supported NAS devices are EMC® Isilon®, EMC® VNX®, EMC® VNX2®, EMC® VNXe®3200, and NetApp.

A NAS device may also be called a NAS filer, NDMP data server, NDMP client, or a data mover.

Before you plan, configure, and administer the snapshot environment, become familiar with the concepts in this chapter. You will need an advanced working knowledge of the NAS devices that you will use with NetWorker snapshot management.

The *EMC NetWorker Hardware Compatibility Guide* provides details on NAS versions that NetWorker supports.

The *EMC NetWorker Release Notes* provides the latest details on NetWorker features, support, fixed problems, and known problems with workarounds.

NAS snapshot operations

A NAS device is a dedicated file server that provides primary data storage for application servers in a heterogeneous network environment. NAS devices are configured as clients of the NetWorker server, for example, by using the Client Configuration wizard, but you do not install NetWorker client software on a NAS device.

A NAS device presents stored data as file systems. Its snapshot and replication features are covered by NDMP licenses. NDMP enables the data transfer required between the primary NAS device storage and secondary storage on tape or VTL devices.

The amount of data that is stored on NAS devices can often be large and the backup times for tape and VTL devices can exceed the available backup window. By scheduling local point-in-time snapshot copies of the NAS data, NetWorker can use whatever time is required to clone the data to backup media independently of the normal backup windows.

NetWorker works with NAS devices to perform the following snapshot and replication operations:

- Create local snapshot save sets of the specified data on the NAS device.
- Replicate the specified snapshot data on a source NAS device to a different location on the same device or to a location on a different NAS device.
- Perform an immediate or a delayed clone backup of specified snapshot save sets to secondary storage by using NDMP.
- Apply retention policies to manage the lifecycles of the snapshot, replication, and clone save sets.
- Recover the specified data from snapshots and clones.

Discovery of non-NetWorker snapshots

NetWorker can discover snapshots on the NAS device that NetWorker did not create.

NetWorker can manage these snapshots as follows:

- NetWorker catalogs all discovered snapshots as snapshot save sets.
- NetWorker can clone, recover, and report details of discovered snapshots but cannot delete them.

- You can schedule discovery or perform discovery manually.

Types of NAS snapshot-based backups

The type of NAS snapshot-based backup that you configure depends on where you intend to create and store the snapshot data, as follows:

- Local snapshot backup
  - The NetWorker server creates a snapshot of the data on the NAS device and retains the snapshot on the NAS device. The NetWorker server catalogs the snapshot as a backup in the media database and can perform a recovery from the snapshot.
- Replicated snapshot backup
  - EMC Isilon SyncIQ—The NetWorker server starts data replication on the Isilon device. The device replicates the data to a local or remote Isilon device. NetWorker creates a snapshot of the replicated data and catalogs it as a backup. The NetWorker server can perform a clone to conventional storage from that snapshot.
  - NetApp SnapVault and SnapMirror—The NetWorker server starts a data replication on the NetApp device. The source device creates a snapshot on the same device and then sends information only about new, changed, or deleted data to the remote mirror NetApp device. For SnapMirror, NetWorker catalogs the remote mirror as a backup and can clone to conventional storage from the mirror. NetWorker clones the data from the source volume.

Example NAS snapshot environments on page 19 provides more details.

Types of NAS snapshot and clone recoveries

The types of recovery that you can perform for snapshot-based save sets depends on the location of the snapshot backup, and where you want to recover the data:

- Snapshot recovery—NetWorker mounts the snapshot volume, where you can browse the save sets and select the directories or the individual files to recover, from the snapshot volume. You can perform one of the following types of recoveries from the snapshot:
  - In-place—Recovers files and directories to the original locations on the NAS device.
  - Out-of-place—Recovers files and directories to a new location that you specify on the NAS device.
  - Directed recovery—Recovers files and directories to the NetWorker host that runs the recovery. You can configure the destination directory as an NFS or CIFS file share, which enables you to recover to a remote location. For example, another client or a NAS device.
- Recovery from a clone—Essentially the same as recovery from a backup. You perform a conventional NetWorker recovery from the backup storage media.

  Note

  You can perform a clone directed restore to a similar NAS box only.

NetWorker clone support

NetWorker uses cloning to copy snapshots to the following types of media:

- DD Boost, Advanced File Type Device (AFTD), Tape—You can clone any types of snapshots to these types of conventional media.
- DD ProtectPoint—You can clone VMAX3 SnapVX and RecoverPoint/XtremIO snapshots to a DD ProtectPoint device.

Note

DD ProtectPoint is not applicable for NAS.

Cloning supports full, incremental, and cumulative incremental cloning. Cloning permits restores to leverage traditional NetWorker restore methods.

NetWorker catalogs snapshots and clone copies in the media database as follows:

- For file system backups—NetWorker records the content of the snapshot in the client file index (CFI) only during a clone operation to conventional media.
- For application backups—NetWorker records the content of the backups (only the application files being protected) in the CFI for both snapshot and clone operations.

The *EMC NetWorker Administration Guide* provides details.

Note

NetWorker 8.2.x and earlier versions do not support the cloning of snapshot save sets.

Backup configuration methods

Use the Client Backup Configuration wizard or the **Client Properties** window in the NetWorker Administration interface to configure snapshot backups:

- Client Backup Configuration wizard—EMC recommends that you use the wizard to create and modify NAS snapshot configurations, because the wizard provides the correct sequence of steps and verifications. The wizard does not provide you with the ability to configure some special use directives and variables. After you use the wizard to create the client, you can modify the client resource to specify directives and variables.
- **Client Properties** window—A non-wizard manual method where you can modify most configurations for a NAS NDMP client. You cannot configure replication policies that are used for locally replicated and remotely replicated snapshots, which you must set in the wizard. You can configure uncommon directives or any special functions that are not supported by the wizard, such as the variables listed in Application Information Variables on page 77.

Recovery interfaces

You can use the following interfaces to recover snapshot-based data:

- The NetWorker Recovery Wizard is the recommended interface to use to recover data from snapshots and conventional storage media.
- The `nsrsnapadmin` command utility provides an interactive Command Line Interface (CLI) session for various snapshot-related operations, including recovery from a snapshot and recovery from conventional storage media.
- The `nsrnassnap_recover` command provides another CLI method to recover data from a snapshot.

The *EMC NetWorker Command Reference Guide* provides details of the NetWorker commands.

Monitoring and reporting NAS snapshot operations

NetWorker reporting features enable you to monitor NAS snapshot operations for each NetWorker client or NAS device, including snapshots that you did not create with NetWorker. NetWorker catalogs all snapshots as backup save sets. You can monitor the progress of the snapshot creation, mounting, deletion, and clone operations.

The NetWorker `nwnassnap.raw` log provides details of snapshot operations. Also, policy logs may provide more detailed information about the actions and workflows that have been run.

Internationalization support

NetWorker provides NAS snapshot operations with the standard NetWorker client support for non-ASCII international character sets.

Components of the NAS snapshot network

You can deploy various required and optional devices, hosts, and connectivity for NAS snapshot operations in a NetWorker datazone.

NAS devices

A NAS device is a dedicated file server that provides primary data storage that you can use for NDMP data operations. A NAS device may also be called an NDMP data server, datamover, NDMP client, or NAS filer. You must configure a NAS device as a client of the NetWorker server, but you do not install NetWorker client software on a NAS device.

All the supported NAS devices support directed recovery to the host that runs the recovery. You can recover to an NFS file share directory on that host, which enables recovery to a remote host or remote device.

Table 3 NAS device support and limitations

NAS device	Characteristics
EMC Isilon	• Supports snapshots with SnapshotIQ™, which requires OneFS® 7.02 or later. • Supports replications with SyncIQ®, which requires OneFS 7.1 or later. • Supports snapshots and replication at the directory level. • Supports in-place and out-of-place recovery of snapshot directories. • Supports directed recovery. • Does not support in-place or out-of-place recovery from a remotely replicated snapshot.
EMC VNX/VNX2	• Supports snapshots at the file system level. • The Client resource must specify the Control Station name. • Supports directed recovery. • Does not support in-place or out-of-place snapshot recovery. • Does not support replication.

Table 3 NAS device support and limitations (continued)

NAS device	Characteristics
EMC VNXe	• Requires Unisphere Management client (uemcli) on the NetWorker server. • Supports snapshots at the file system level. • The Client resource must specify the Control Station name. • Supports directed recovery. • Does not support in-place or out-of-place snapshot recovery. • Does not support replication.
NetApp	• Requires operating system libraries from the NetApp Manageability SDK, available from NetApp. • Supports snapshots using 7-mode and cluster mode, and requires OnTAP 8.0 or later. **Note** The *EMC NetWorker Online Software Compatibility Guide* provides details about Data ONTAP Version NetApp Cluster-Mode support. • Supports SnapMirror for local and remote replication of snapshots in c-mode and 7-mode. • Supports SnapVault for local and remote replication of snapshots in 7-mode. • Supports SnapVault for remote replication only of snapshots in C-mode. **Note** SnapVault for local replication is NOT supported for snapshots in C-mode. • Supports Cluster Aware Backup (CAB) for affinity awareness of volumes and tape devices. • Supports in-place and out-of-place recovery of snapshot files but not directories or save sets (except if the save set is a single file), and only to the same volume as the source. • Supports directed recovery. • NetApp on Linux systems does not support a temporary mount point for snapshot browse and recover, but must use an existing, manually configured NFS mount point. • For SnapMirror in-place or out-of-place, recovery is not supported for local and remotely replicated snapshots.

NDMP environment

NetWorker software uses NDMP functionality to enable access to storage in a heterogeneous network environment. NDMP uses TCP/IP to control the movement of the data, and specifies various device drivers to store the data on devices.

NetWorker server

The NetWorker server manages the NAS devices and the configuration settings that are required to create the snapshots and perform the clone and the recovery operations. It is the Data Management Agent (DMA).

NetWorker client

NAS devices do not run NetWorker client software. However, to do remote replication, you must also have a client resource for the remote target NAS device, and you must create a NetWorker Client resource for the device, if you want to perform backup, clone, or indexing actions. The Client resource specifies the snapshot replication target and provides credentials to the NetWorker server for replication, cloning, and recovery operations. To do remote replication, you must also have a client resource for the remote target NAS device.

NetWorker storage node

The NetWorker storage node hosts and manages the devices for cloning to secondary storage media, such as tape or VTL devices. The storage node is the NDMP tape server.

If you plan to use NAS devices only to create and recover snapshots without cloning to secondary storage, then the use of a storage node is optional.

Backup storage media

NetWorker uses NDMP services to clone NAS snapshot save sets to tape or VTL storage media. During cloning, NetWorker catalogs the clone save set files in its client file index.

Licensing requirements

NAS snapshot and replication features are covered by NDMP licenses.

The *EMC NetWorker Licensing Guide* and an EMC sales representative can provide details about licensing for NSM.

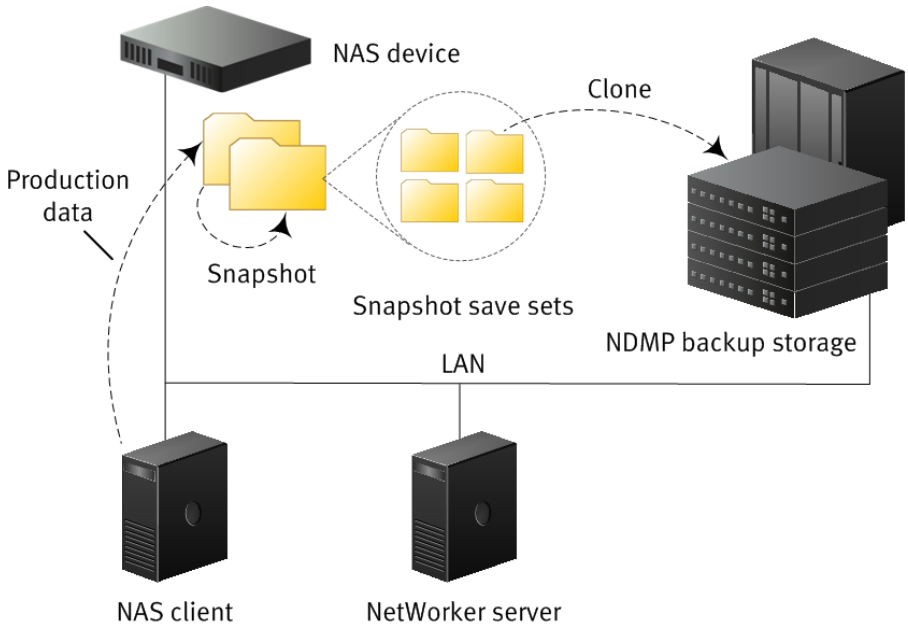
Example NAS snapshot environments

Plan the NAS environment to manage replication and snapshot operations efficiently as illustrated by the following examples.

Example of a snapshot and rollover to storage media

The following figure and description illustrates the data flow in a typical environment for a local snapshot backup of NAS client data with optional rollover to an NDMP storage device.

Figure 1 NAS snapshot with rollover to storage media

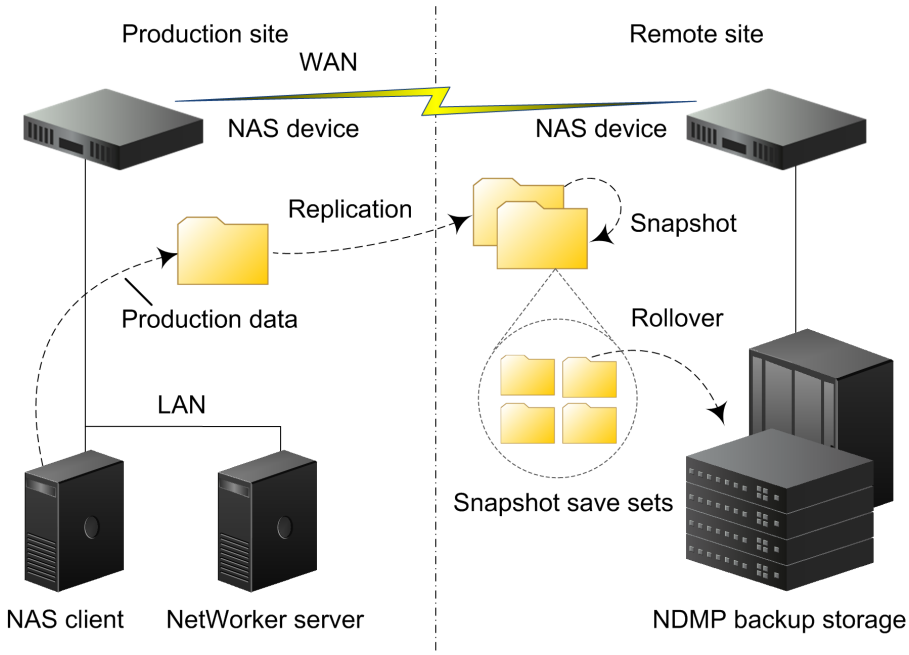


1. A NAS client writes its production data to primary storage on a NAS device.
2. At a specified time, the NetWorker server instructs the NAS device to use its proprietary operations to create a snapshot (replication) of production file systems, as specified in the NetWorker Client resource for the device.
   The NetWorker server catalogs the snapshot as a backup save set from which recoveries can be made.
3. The NetWorker workflow may also include a clone action. In that case, the NetWorker server instructs the NAS device to clone the snapshot save set to secondary storage such as an NDMP tape or VTL device.
4. The NetWorker server manages both the snapshot save set and any secondary backup save set according to the options that are configured in the Data Protection Policy.
5. The NAS device retains the snapshot until it expires or until a NetWorker operator deletes it.

Example of a snapshot from replication

The following figure and description illustrates the data flow for a snapshot of remotely replicated NAS client data with optional clone to NDMP storage media.

Figure 2 Remote replication with snapshot and clone to storage



1. A NAS client writes its production data to primary storage on a NAS device.
2. At a specified time, the NetWorker server instructs the NAS device to create a remote replication/snapshot of production file systems. The NAS device uses its proprietary operations to create the replication on the remote NAS device.
   - For EMC Isilon devices, the production file systems to replicate are specified by the NetWorker Client resource for the device.
   - For NetApp devices, the device creates a local full PIT snapshot of the production data on the same device, and then updates the Local and Remote NetApp mirror device with any new, changed, or deleted data.
3. Based on the schedule of the Data Protection Policy for the remote NAS device, the NetWorker server instructs the device to use its proprietary operations to create a snapshot/replication of the replicated file systems. The NetWorker server catalogs the remote snapshot as a backup save set from which recoveries can be made.
4. The NetWorker data Protection policy may also include a clone action. In that case, the NetWorker server instructs the remote NAS device to clone the snapshot save set to secondary storage such as a NDMP tape or VTL device.
5. The NetWorker server manages both the remote snapshot save set and any secondary backup save set according to the retention options and other options configured in the Data Protection Policy.
6. The NAS device retains the snapshot until it expires or until a NetWorker operator deletes it.

Examples of snapshot recovery

The following description of process and figures illustrate the data flow for recovery of directories or files from a snapshot save set:

1. Select the snapshot volume that contains the data that you want to recover. NetWorker mounts the snapshot volume.
2. Browse for the files, file systems, or volumes that you want to recover.
3. Specify where to recover the data on the NAS device host or on a NetWorker host.
   - In-place recovery—Recover to the original location on the NAS device.
   - Out-of-place recovery—Recover to a different location on the NAS device.
   - Directed recovery—Recover to a directory on the NetWorker client host that is running the recovery. The recovery directory may be a local directory or a locally mounted CIFS or NFS remote file system.
4. NetWorker copies the data from the snapshot volume to the specified location.

Figure 3 In-place recovery restores data to the original location on the source device

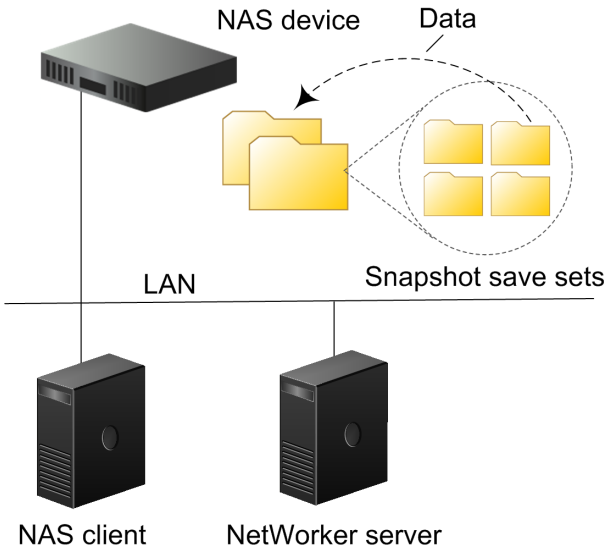


Figure 4 Out-of-place recovery restores data to a different location on the source device

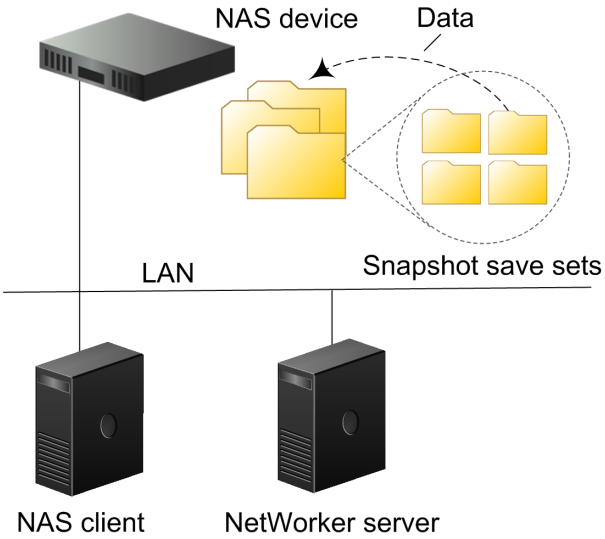
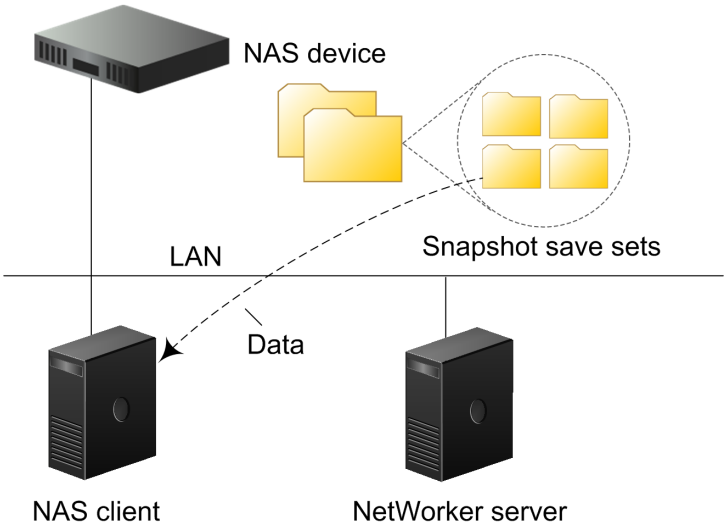


Figure 5 Directed recovery restores data to the NetWorker client that runs the recovery



CHAPTER 2

Data Protection Policies

This chapter includes the following topics:

- Introduction 26
- Default data protection policies 26
- Strategies for NAS snapshot backups 27

Introduction

You can protect your data on NAS devices in two ways:

- Using the NDMP protocol.
- Using snapshot management technology.

NDMP follows the traditional backup strategy.

For a detailed overview about creating, editing, and deleting groups and policies, refer to the Data Protection Policies chapter in the *EMC NetWorker Administration Guide*.

Default data protection policies

NetWorker provides you with preconfigured data protection polices resources that you can use immediately to protect your environment, modify to suit your environment, or use an example to create new resource configurations. To use these policy resources, you must add clients to the appropriate group resource.

Each protection policy provides an example of the EMC best practices that you should follow when you design your data protection solution:

- Separate file system backups from application database backups, to provide ease of access at recovery time.
- Stagger the start times for file system backup from the application database backups, to prevent disk contention on the target hosts.

The default data protection policy resources mimic the requirements of a service provider, with different policies to that are designed to provide protection based on service level agreements.

Platinum policy

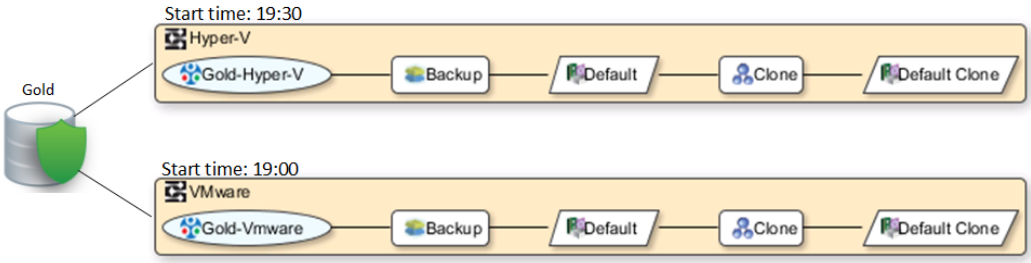
The Platinum policy provides you with an example of a data protection policy for an environment that contains EMC storage arrays or appliances and requires backup data redundancy. The policy contains one workflow with two actions, a snapshot backup action, followed by a clone action.

Figure 6 Platinum policy configuration

Gold policy

The Gold policy provides an example of a data protection policy for an environment that contains virtual machines and requires backup data redundancy. The policy contains two workflows, one to protect Hyper-V hosts and one to protect VMware hosts. Each workflow contains a backup action followed by a clone action.

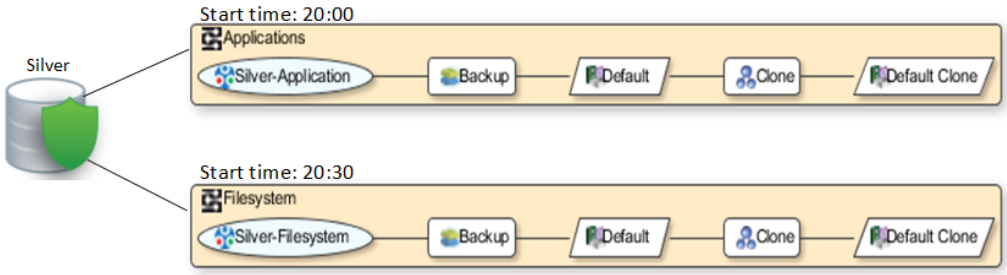
Figure 7 Gold policy configuration



Silver policy

The Silver policy provides an example of a data protection policy for an environment that contains non-virtualized machines and requires backup data redundancy. The policy contains two workflows, one to protect hosts file systems and one to protect database applications. Each workflow contains a backup action followed by a clone action.

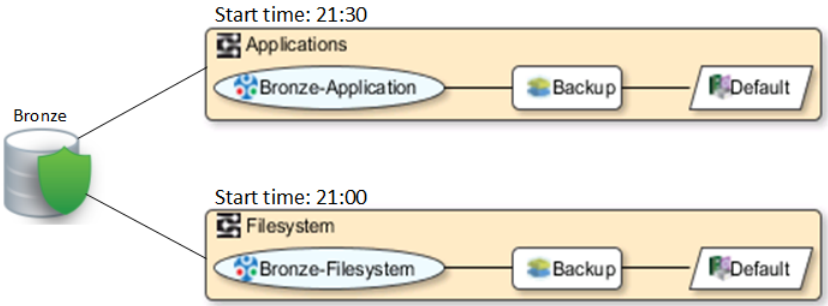
Figure 8 Silver policy configuration



Bronze policy

The Bronze policy provides an example of a data protection policy for an environment that contains non-virtualized machines. The policy contains two workflows, one to protect hosts file systems and one to protect database applications. Each workflow contains a backup action.

Figure 9 Bronze policy configuration



Strategies for NAS snapshot backups

Multiple data protection policy strategies are available to help you optimize the way that snapshots are performed and backed up.

When you protect NAS devices by using snapshot technology, there are four actions that you can perform on the NAS data:

- Create a snapshot backup.
- Discover snapshots on the NAS device that were created independent of NetWorker:
  - Add newly discovered snapshots to the media database on the NetWorker server.
  - Remove previously discovered snapshots from the media database when the snapshots are no longer available on the NSA device.
- Update client file index entries with information about:
  - Snapshots that are created by NetWorker.
  - Snapshots created independent of NetWorker.
- Clone a snapshot.

Road map for configuring a new data protection policy

Procedure

1. Create a policy.

   When you create a policy, you specify the name and notification settings for the policy.

2. Within the policy, create a workflow for each data type.

   For example, create one workflow to protect file system data and one workflow to protect application data. When you create a workflow, you specify the name of the workflow, the time to start the workflow, notification settings for the workflow, and the protection group to which the workflow applies.

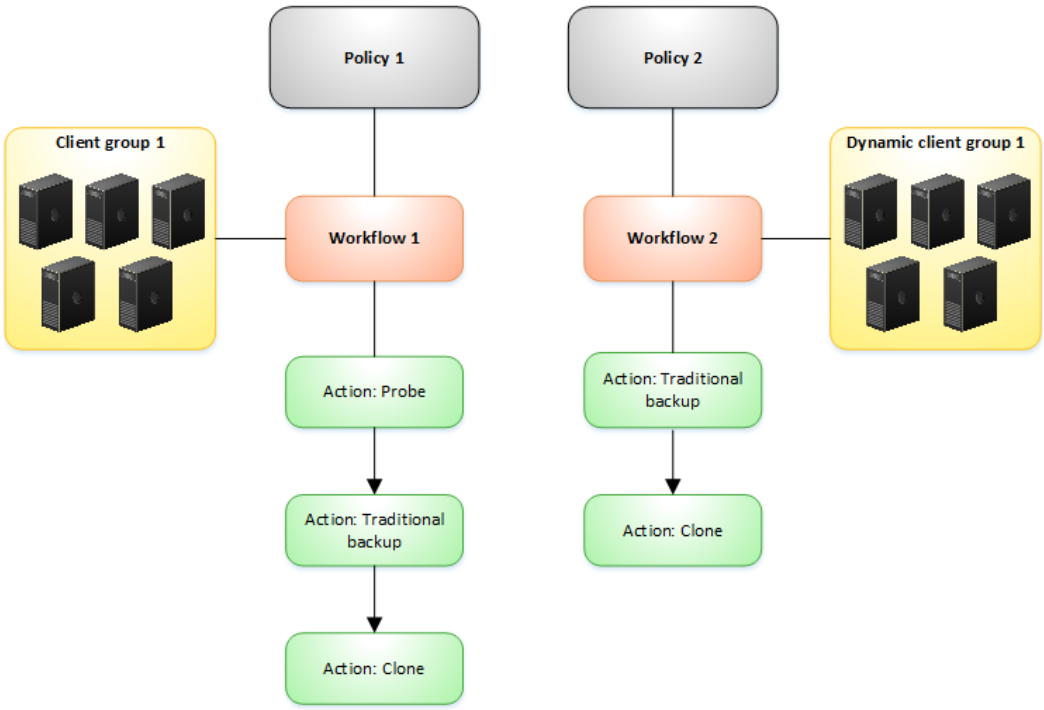
3. Create a protection group.

   The type of group that you create depends on the types of clients and data that you want to protect. The actions that appear for a group depend on the group type.

4. Create one or more actions for the workflow.
5. To define the backup data that you want to protect, configure Client resources, and then assign the client resources to a protection group.

The following figure illustrates a policy with two different workflows. Workflow 1 performs a probe and then a backup of the Client resources in Client group 1, and then clones the save sets from the backups. Workflow 2 performs a backup of the Client resources in Dynamic client group 1, and then clones the save sets from the backups.

Figure 10 Data protection policy example



Creating a policy

Procedure

1. On the **Administration** window, click **Protection**.
2. In the expanded left pane, right-click **Policies**, and then select **New**.

   The **Create Policy** dialog box appears.
3. On the **General** tab, in the **Name** field type a name for the policy.

   The maximum number of characters for the policy name is 128.

   Note

   After you create a policy, the **Name** attribute is read-only.
4. In the **Comment** box, type a description for the policy.
5. From the **Send Notifications** list, select whether to send notifications for the policy:
   - To avoid sending notifications, select **Never**.
   - To send notifications with information about each successful and failed workflow and action after all the actions in the policy complete, select **On Completion**.
   - To send a notification with information about each failed workflow and action after all the actions in the policy complete, select **On Failure**.

6. In the **Send notification** attribute when you select the **On Completion** or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` action to write the notifications to a log file or configure an email notification.

   The default notification action is to log the information to the `policy_notifications.log` file. The `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows, by default. You can use the `smtpmail` application on Windows or the default mailer program on Linux to send email messages.

   For example:

   - To log notifications to a file named `policy_notifications.log`, type the following command:

     ```
     nsrlog -f policy_notifications.log
     ```

   - On Linux, to send a notification email, type the following command:

     ```
     mail -s subject recipient
     ```

   - On Windows, to send a notification email, type the following command:

     ```
     smtpmail -s subject -h mailserver recipient1@mailserver
     recipient2@mailserver...
     ```

     where:

     - ***-s subject***—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the `smtpmail` program assumes that the message contains a correctly formatted email header and nothing is added.
     - ***-h mailserver***—Specifies the hostname of the mail server to use to relay the SMTP email message.
     - *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

7. To specify the Restricted Data Zone (RDZ) for the policy, select the **Restricted Data Zones** tab, and then select the RDZ from the list.
8. Click **OK**.

After you finish

Create the workflows and actions for the policy.

Creating a workflow in a new policy

A policy must contain one or more workflows.

Procedure

1. In the left pane of the **Protection** window, expand **Policies**, and then select the policy that you created.
2. In the right pane of the **Protection** window, select **Create a new workflow**.
3. In the **Name** field, type the name of the workflow.

   The maximum number of characters for the name of the group is 64.

4. In the **Comment** box, type a description for the workflow. The maximum number of characters for the **Comment** field is 128.
5. From the **Send Notifications** list, select how to send notifications for the workflow:
   - To use the notification configuration that is defined in the policy resource to determine when to send the notification, select **Set at policy level**.
   - To send notifications with information about each successful and failed workflow and action, after all the actions in the workflow complete, select **On Completion**.
   - To send notifications with information about each failed workflow and action, after all the actions in the workflow complete, select **On Failure**.
6. In the **Send notification** attribute when you select the **On Completion** or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` action to write the notifications to a log file or configure an email notification.

   The default notification action is to log the information to the `policy_notifications.log` file. The `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows, by default. You can use the `smtpmail` application on Windows or the default mailer program on Linux to send email messages.

   For example:

   - To log notifications to a file named `policy_notifications.log`, type the following command:

     ```
     nsrlog -f policy_notifications.log
     ```

   - On Linux, to send a notification email, type the following command:

     ```
     mail -s subject recipient
     ```

   - On Windows, type the following command:

     ```
     smtpmail -s subject -h mailserver recipient1@mailserver
     recipient2@mailserver...
     ```

     where:

     - **`-s subject`**—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the `smtpmail` program assumes that the message contains a correctly formatted email header and nothing is added.
     - **`-h mailserver`**—Specifies the hostname of the mail server to use to relay the SMTP email message.
     - *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

7. In the **Running** group box, define when and how often the workflow runs.
   a. To ensure that the actions contained in the workflow run when the policy or workflow is started, in the **Enabled** box, leave the option selected. To prevent the actions in the workflow from running when the policy or workflow that contains the action is started, clear this option.
   b. To ensure that the workflow starts at the time that is specified in the **Start time** attribute, on the days that are defined in the action resource, in the **AutoStart**

Enabled box, leave the option selected. To prevent the workflow from running at the time that is specified in the **Start time** attribute, clear this option.

c. To define the time to start the actions in the workflow, in the **Start Time** attribute, use the spin boxes.

   The default value is 9:00 P.M.

d. To define how frequently to repeat the actions that are defined in the workflow over a 24 hour period, In the **Interval** attribute, use the spin boxes.

   The default value is 24 hours, or once a day. When you select a value that is less than 24 hours, the **Interval End** attribute appears. To define the last time to start a workflow in a defined interval period, use the spin boxes .

e. To define the duration of time in which NetWorker can manually or automatically restart a failed or canceled workflow, in the **Restart Window** attribute, use the spin boxes.

   If the restart window has elapsed, NetWorker considers the restart as a new run of the workflow. NetWorker calculates the restart window from the start of the last incomplete workflow. The default value is 24 hours.

For example, when you set the **Start Time** to 7:00 PM, the **Interval** to 1 hour, and the **Interval end time** to 11:00 P.M., then the workflow automatically starts every hour beginning at 7:00 P.M. and the last start time is 11:00 PM.

8. To create the workflow, click **OK**.

After you finish

Create the actions that will occur in the workflow, and then assign a group to the workflow. If a workflow does not contain a group, a policy does not perform any actions.

Protection groups for NAS snapshot devices

Create protection groups for NAS devices that support snapshot technology.

The type of protection group that you create to protect snapshot data depends on the data operation that you want to perform:

- Basic client group—Defines a static list of Client resources to back up.
- Dynamic client group—Specifies a dynamic list of Client resources to back up. A dynamic client group automatically generates a list of Client resources that use client tag which matches the client tag that is specified for the group.
- NAS device group—Use this group to define a static list of NAS devices on which you want to perform discovery operations, to detect NAS snapshots and backups that were created or deleted independent of NetWorker. The discovery operation will create entries in the media database for the new backups and remove media database entries for deleted backups.
- Save set ID List—Use this group to generate a static list of NAS snapshot backup save sets in the media database. Use this list to perform one of the following operations:
  - Create client file index entries for the save sets.
  - Clone the save sets.
- Save Set Query—Use this group to generate a dynamic list of NAS snapshot backup save sets in the media database, based on matching criteria. Criteria that you can define in a query group includes:
  - Date and time range for the save set.

- Backup level of the save set.
- Client resource that is associated with a save set.
- Policy, workflow, group, or action that is used to generate the save set.

Note

A NAS environment does not support the use of the Query by Pool or the Number of clone copies criteria to generate a dynamic list of NAS snapshot backup save sets.

Use a query group to generate a save set list to perform one of the following operations:

- Create client file index entries for the save sets.
- Clone the save sets.

Note

For query groups that include NAS devices you cannot specify a volume. If you use this query to do a clone, the clone will fail.

Create multiple protection groups to perform different types of snapshot backups or discovery for different devices, or to perform snapshot backups or discovery on different schedules. For example:

- Create one basic client group for a workflow that performs a snapshot backup of NAS devices.
- Create one NAS device group for a workflow that performs discovery, and then a query group to generate a list of save sets for a workflow that generates index data for the snapshot save sets at a different time.

Creating a client group

Basic client groups define a static list of Client resources for a traditional backup, check connectivity, or probe action.

Before you begin

Create the Client resources for the data to include in a protection group.

Procedure

1. In the **Administration** window, click **Protection**.
2. In the expanded left pane, right-click **Groups**, and then select **New**.

   The **Create Group** dialog box appears, starting with the **General** tab.
3. In the **Name** attribute, type a name for the group.

   The maximum number of characters for the group name is 64.

   Note

   After you create a group, the **Name** attribute is read-only.
4. From the **Group Type** list, leave the default selection of **Clients**.
5. In the **Comment** field, type a description of the group.
6. Select the workflow in which to assign the group from the **Policy-Workflow** list.

Note

You can also assign the group to a workflow when you create or edit a workflow.

7. (Optional) On the **Restricted Datazones** tab, to specify the Restricted Datazone (RDZ) for the group, select the RDZ from the list.
8. Click **OK**.

After you finish

Create Client resources. The Client Configuration wizard and **General** tab on the **Client Properties** dialog box properties page provide you with the ability to assign clients to a protection group.

Creating a dynamic client group

Dynamic client groups prevent you from having to edit group settings when you add Client resources to the NetWorker datazone. You can configure a dynamic group to include all the clients on the NetWorker server or you can configure the dynamic group to perform a query that generates a list of clients that is based on a matching tag value. A tag is a string attribute that you define in a Client resource. When an action starts in a workflow that is a member of a tagged dynamic protection group, the policy engine dynamically generates a list of Client resources that match the tag attribute value.

Use dynamic client groups to specify a dynamic list of Client resources for a traditional backup, probe, check connectivity, or server backup action.

Procedure

1. In the **Administration** window, click **Protection**.
2. In the expanded left pane, right-click **Groups**, and then select **New**.

   The **Create Group** dialog box appears, starting with the **General** tab.
3. In the **Name** attribute, type a name for the group.

   The maximum number of characters for the group name is 64.

   Note

   After you create a group, the **Name** attribute is read-only.
4. From the **Group Type** list, select **Dynamic Clients**.
5. In the **Comment** field, type a description of the group.
6. Select the workflow in which to assign the group from the **Policy-Workflow** list.

   Note

   You can also assign the group to a workflow when you create or edit a workflow.
7. (Optional) On the **Restricted Datazones** tab, to specify the Restricted Datazone (RDZ) for the group, select the RDZ from the list.
8. Click **OK**.

After you finish

Create Client resources. The Client Configuration wizard and **General** tab on the **Client Properties** dialog box properties page provide you with the ability to assign clients to a protection group and define one or more tags.

Creating a NAS device group

A NAS device group defines a list of NAS devices for discovery.

Procedure

1. In the **Administration** window, click **Protection**.
2. In the expanded left pane, right-click **Groups**, and then select **New**.

   The **Create Group** dialog box appears, starting with the **General** tab.
3. In the **Name** attribute, type a name for the group.

   The maximum number of characters for the group name is 64.

   Note

   After you create a group, the **Name** attribute is read-only.

4. From the **Group Type** list, select **NAS Device**.
5. In the **Comment** field, type a description of the group.
6. Select the workflow in which to assign the group from the **Policy-Workflow** list.

   Note

   You can also assign the group to a workflow when you create or edit a workflow.

7. Click **Add**.

   The **Add NAS Device - Current Selection** dialog box appears.
8. Select or create a NAS device resource.

Method	Steps
Select a NAS device resource	a. Next to the resource in the **Add NAS Device - Current Selection** dialog box, select the checkbox . b. Click **Add**.
Create a NAS device resource	a. In the **Add NAS Device - Current Selection** dialog box, click **New**. The **Create NSR NAS Device** dialog box appears. b. In the **Name** and **Comment** boxes, on the **General** tab, type the name and a comment about the device. c. Select the **Snapshot Management** tab. d. To access data on the client instance of the NAS device, for example, to create, delete, or share snapshots, in the **NAS management user** and **NAS management password** boxes, type a username and password for the user authorized. Each instance can have a different user. You may need to provide a Management Name or address, for example, for a VNX Control Station name, if it differs from the NAS device name itself. e. In the **NAS device management name** box, type the hostname or IP address of the NAS device.

Method	Steps
	f. Next to the resource in the **Add NAS Device - Current Selection** dialog box, select the checkbox. g. Click **Add**.

9. (Optional) Remove one or more NAS devices from the group:
   a. In the **Create Group** dialog box, click **Remove**.

      The **Remove NAS Device - Current Selection** dialog box appears.
   b. Next to the devices, select the checkbox.
   c. Click **Remove**.
10. (Optional) On the **Restricted Datazones** tab, to specify the Restricted Datazone (RDZ) for the group, select the RDZ from the list.
11. Click **OK**.

Creating a save set group

A save set group defines a static list of save sets for cloning or for snapshot index generation.

Before you begin

Determine the save set ID or clone ID (ssid/clonid) of the save sets for the group by using the **Administration** › **Media** user interface or the `mminfo` command.

Procedure

1. In the **Administration** window, click **Protection**.
2. In the expanded left pane, right-click **Groups**, and then select **New**.

   The **Create Group** dialog box appears, starting with the **General** tab.
3. In the **Name** box, type a name for the group.
4. From the **Group Type** list, select **Save Set ID List**.
5. In the **Comment** box, type a description of the group.
6. (Optional) To associate the group with a workflow, from the **Workflow (Policy)** list, select the workflow .

   You can also assign the group to a workflow when you create or edit a workflow.
7. In the **Clone specific save sets (save set ID/clone ID)** box, type the save set ID/clone ID (ssid/clonid) identifiers.

   To specify multiple entries, type each value on a separate line.
8. To specify the Restricted Data Zone (RDZ) for the group, select the **Restricted Data Zones** tab, and then select the RDZ from the list.
9. Click **OK**.

Creating a query group

A query group defines a list of save sets for cloning or snapshot index generation, based on a list of save set criteria.

Procedure

1. In the **Administration** window, click **Protection**.
2. In the expanded left pane, right-click **Groups**, and then select **New**.

   The **Create Group** dialog box appears, starting with the **General** tab.
3. In the **Name** box, type a name for the group.
4. From the **Group Type** list, select **Save Set Query**.
5. In the **Comment** box, type a description of the group.
6. (Optional) To associate the group with a workflow, from the **Workflow (Policy)** list, select the workflow.

   You can also assign the group to a workflow when you create or edit a workflow.
7. Specify one or more of the save set criteria in the following table.

   Note

   When you specify more than one save set criteria, the list of save sets only includes save sets that match all the specified criteria.

Table 4 Save set criteria

Criteria	Description
Date and time range	Specify the start date and time range for the save sets. To specify the current date and time as the end date for the range, select **Up to now**. To specify a different date and time as the end date for the range, select **Up to**, and then select the date and time from the lists.
Backup level	In the **Filter save sets by level** section, next to the backup level for the save set, select the checkbox: • **full** • **cumulative incr** • **logs** • **incremental** • **manual**
Limit the number of clones	Specify the number for the limit in the **Limit number of clones** list. The clone limit is the maximum number of clone instances that can be created for the save set. **Note** The default is set to 0, and cannot be changed for NAS or Block.

Table 4 Save set criteria (continued)

Criteria	Description
Client	Next to one or more client resources that are associated with the save set in the **Client** list, select the checkbox.
Policy	Next to the policy used to generate the save set in the **Policy** list, select the checkbox.
Workflow	Next to the workflow used to generate the save set in the **Workflow** list, select the checkbox.
Action	Next to the action used to generate the save set in the **Action** list, select the checkbox.
Group	Next to the group associated with the save set in the **Group** list, select the checkbox.
Pools	Next to the media pool on which the save set is stored in the **Pools** list, select the checkbox. **Note** You cannot select Pools for NAS.
Name	In the **Filter save sets by name** box, specify the name of the save set. **Note** You cannot use wildcards to specify the save set name.

If you specify multiple criteria, the save set must match all the criteria to belong to the group.

8. To specify the Restricted Data Zone (RDZ) for the group, select the **Restricted Data Zones** tab, and then select the RDZ from the list.
9. Click **OK**.

Supported actions in snapshot workflows

Snapshot workflow supports the following actions types.

Probe

A probe action runs a user-defined script on a NetWorker client before the start of a backup. A user-defined script is any program that passes a return code. If the return code is 0 (zero), then a client backup is required. If the return code is 1, then a client backup is not required.

Only a backup action can follow a probe action.

Check connectivity

A check connectivity action tests connectivity between clients and the NetWorker server before a probe or backup action occurs. If the connectivity test fails, then the backup does not occur on the client.

Snapshot backup
A snapshot backup action performs a snapshot on a supported NAS device, backs up the snapshot, and then generates a save set entry for the snapshot backup in the NetWorker media database.

Note

A snapshot backup does not generate an entry for the snapshot backup in the client file index. To index a snapshot backup, use the generate index action after the snapshot backup action.

Discover
A discover action discovers snapshots on a NAS device that the current NetWorker server did not create. NetWorker then creates save set entries for the discovered snapshots on a NAS client in the media database.

The discover action also compares the save sets in the media database for the NAS client against the actual snapshots that are stored on the client. If the media database entry does not have a corresponding snapshot on the NAS client, then the media database entry is removed.

Note

A discover action does not generate entries for the discovered snapshots in the client file indexes. To index a discovered snapshot, use the generate index action after the discover action.

Generate index
A generate index action creates entries in the client file indexes for snapshot backups and discovered snapshots.

You can configure a generate index action to occur automatically in a workflow after a snapshot backup or discover action. Alternatively, you can configure a generate index action to occur separately for a group of save sets.

Clone
A clone action creates a copy of one or more save sets. Cloning allows for secure offsite storage, transfer of data from one location to another, and verification of backups.

You can configure a clone action to occur after a backup in a single workflow, or simultaneously with a backup action in a single workflow. You can also use save set and query groups to define a specific list of save sets to clone, in a separate workflow.

Action in snapshot workflows

Workflows enable you to chain together multiple actions and run them sequentially or concurrently.

You can perform a snapshot or you can use the discover action to discover snapshots on the NAS device that the current NetWorker server did not create, and create save set entries in the NetWorker media database for the snapshots.

Neither the snapshot backup action nor the discover action create entries for snapshots in the client file indexes. Use a generate index action to create snapshot entries in the client file indexes. You can configure the generate index action to occur automatically after the snapshot backup action or the discover action as part of a single workflow. To index the snapshot at a different time than the snapshot backup or discovery, create a separate workflow with the generate index action.

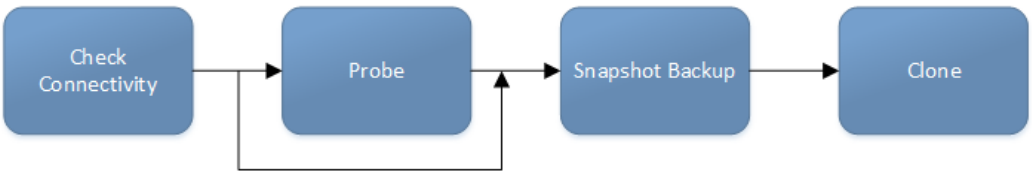
The *EMC NetWorker Snapshot Management for NAS Devices Integration Guide* provides details on backing up NAS devices with NetWorker.

The following sections provide details on supported actions that can follow the lead action and other actions in a workflow.

All possible workflow actions for a snapshot backup

The following figure illustrates the possible workflow actions that are associated with a snapshot backup.

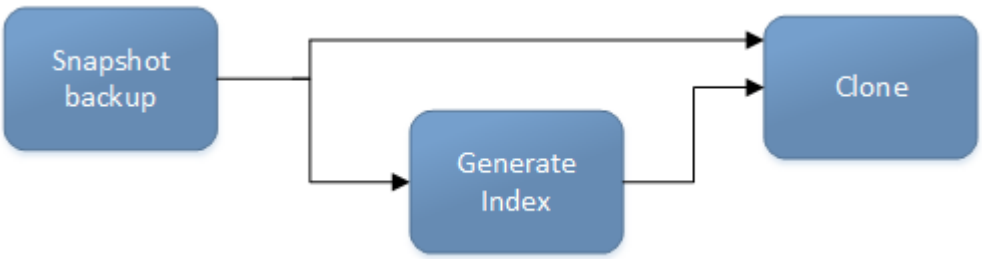
Figure 11 All possible workflow actions for a snapshot backup



Workflow path from a snapshot backup action

You can perform a generate index action (to generate an index of the snapshot) or a clone action after a snapshot backup action.

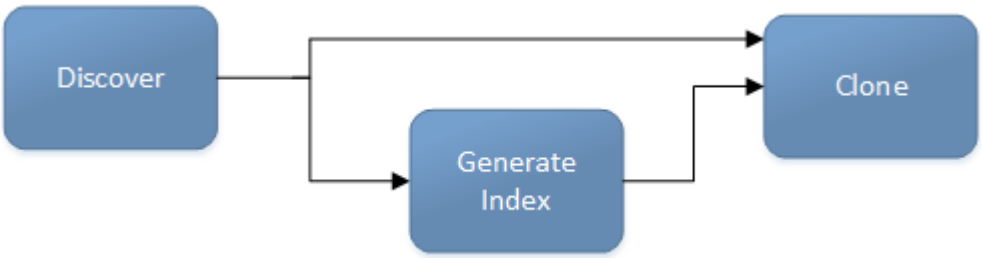
Figure 12 Workflow path from a snapshot backup action



Workflow path from a snapshot discover action

When you perform snapshot discovery, the discover action must be the first action in the workflow. You can optionally include a generate index or clone action concurrently with or after the discovery.

Figure 13 Workflow path from a discover action



Creating a probe action

A probe action runs a user-defined script on a NetWorker client before the start of a backup. A user-defined script is any program that passes a return code. If the return code

is 0 (zero), then a client backup is required. If the return code is 1, then a client backup is not required.

Before you begin

- Create the Probe resource script on the clients that use the probe. Create a client Probe resource on the NetWorker server, and then associate the client Probe resource with the Client resource on the NetWorker server.
- Create the policy and workflow that contain the action.
- (Optional) Create a check connectivity action to precede the probe action in the workflow. A check connectivity action is the only supported action that can precede a probe action in a workflow.

Procedure

1. In the expanded left pane, select the workflow, and then perform one of the following tasks in the right pane to start the Policy Action wizard:
   - If this is the first action in the workflow, select **Create a new action**.
   - If the workflow has other actions, right-click an empty area of the **Actions** pane, and then select **New**.

   The **Specify the Action Information** page appears.
2. In the **Name** field, type the name of the action.

   The maximum number of characters for the action name is 64.
3. In the **Comment** field, type a description for the action.
4. To ensure that the action runs when the policy or workflow that contains the action is started, in the **Enabled** box, select the option. To prevent the action from running when the policy or workflow that contains the action is started, clear this option.

   Note

   When you clear the **Enabled** option, any action that occurs after a disabled action will not start, even if the succeeding options are enabled.

5. From the **Action Type** list, select **Probe**.
6. When you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is grayed out.
7. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, select the action that should precede this action from the **Previous** box.
   - If the action should run concurrently with an action, select the concurrent action from the **Previous** box, and then select the **Concurrent** checkbox.
8. Select whether to use a weekly or monthly schedule for the action:
   - To specify a schedule for each day of the week, select **Weekly by day**.
   - To specify a schedule for each day of the month, select **Monthly by day**.
9. Click the icon on each day to specify whether to probe the client.

   The following table provides details on the icons.

Table 5 Schedule icons

Icon	Label	Description
	Execute	Perform the probe on this day.
	Skip	Do not perform a probe on this day.

To perform a probe every day, select **Execute** from the list, and then click **Make All**.

10. Click **Next**.

    The **Specify the Probe Options** page appears.

11. Choose whether to start the subsequent backup action only after all probes succeed by selecting or clearing the **Start backup only after all probes succeed** checkbox.

    - To start the backup only if all the probes associated with Client resources in the assigned group succeed, select the checkbox.
    - To start the backup if any one of the probes are associated with a Client resource in the assigned group succeed, clear the checkbox.

12. Click **Next**.

    The **Specify the Advanced Options** page appears.

13. In the **Retries** box, specify the number of times that NetWorker should retry a failed probe or backup action, before NetWorker considers the action as failed. When the **Retries** value is 0, NetWorker will not retry a failed backup or probe action.

    Note

    The **Retries** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types. When you specify a value for this option in other actions, NetWorker ignores the values.

14. In the **Retry Delay** field, specify a delay in seconds to wait before retrying a failed backup or probe action. When the **Retry Delay** value is 0, NetWorker retries the failed backup or probe action immediately.

    Note

    The **Retry Delay** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types. When you specify a value for this option in other actions, NetWorker ignores the values.

15. In the **Inactivity Timeout** field, specify the maximum number of minutes that a job run by an action is allowed to fail to communicate back to the server.

    If the job fails to respond within the timeout value, the server considers the job a failure. If a job fails, NetWorker retries the job immediately. This ensures that no time is lost due to failures.

    Increase the timeout value if a backup consistently aborts due to inactivity. Inactivity timeouts may occur for backups of large save sets, backups of save sets with large sparse files, and incremental backups of many small static files.

Note

The **Inactivity Timeout** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types. When you specify a value for this option in other actions, NetWorker ignores the values.

16. In the **Parallelism** field, specify the maximum number of concurrent operations for the action.

    Note

    The **Parallelism** value should not exceed 25.

17. From the **Failure Impact** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action** .

      Note

      The **Abort action** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types.

    - To abort the entire workflow if there is a failure with one of the jobs in the action, select **Abort workflow**.

    Note

    If any of the actions fail in the workflow, the workflow status does not appear as interrupted or cancelled. NetWorker reports the workflow status as failed.

18. Leave the default selections for the Notification group box. NetWorker does not support notifications for probe actions and ignores the values that are defined in the attributes.
19. From the **Soft Limit** list, specify the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no limit.
20. From the **Hard Limit** list, specify the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no limit.
21. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To change the month on which to schedule the override, use the navigation buttons and the month list box. To change the year, use the spin boxes. You can set an override in the following ways:

    - Select the day in the calendar, which changes the action task for the specific day.
    - Use the action task list to select the task, then perform one of the following steps:
      - To define an override that occurs on a specific day of the week, every week, select **Specified day**, then use the drop downs. Click **Add Rules based override**.
      - To perform the action task on the last day of the calendar month, select **Last day of the month**. Click **Add Rules based override**.
      - In the **Override** field, type an override.

Note

To remove an override, delete the entry from the **Override** field.

22. Click **Next**.

    The **Action Configuration Summary** page appears.

23. Review the settings that you specified for the action, and then click **Configure**.

Creating a check connectivity action

A check connectivity action tests connectivity between clients and the NetWorker server, usually before another action such as a backup occurs.

Before you begin

Create the policy and workflow that contain the action. The check connectivity action should be the first action in the workflow.

Procedure

1. In the expanded left pane, select the workflow, and then perform one of the following tasks in the right pane to start the Policy Action wizard:
   - If this is the first action in the workflow, select **Create a new action**.
   - If the workflow has other actions, right-click an empty area of the **Actions** pane, and then select **New**.

   The **Specify the Action Information** page appears.

2. In the **Name** field, type the name of the action.

   The maximum number of characters for the action name is 64.

3. In the **Comment** field, type a description for the action.
4. To ensure that the action runs when the policy or workflow that contains the action is started, in the **Enabled** box, select the option. To prevent the action from running when the policy or workflow that contains the action is started, clear this option.

   Note

   When you clear the **Enabled** option, any action that occurs after a disabled action will not start, even if the succeeding options are enabled.

5. From the **Action Type** list, select **Check Connectivity**.
6. When you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is grayed out.
7. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, select the action that should precede this action from the **Previous** box.
   - If the action should run concurrently with an action, select the concurrent action from the **Previous** box, and then select the **Concurrent** checkbox.
8. Select whether to use a weekly or monthly schedule for the action:
   - To specify a schedule for each day of the week, select **Weekly by day**.
   - To specify a schedule for each day of the month, select **Monthly by day**.
9. Click the icon on each day to specify whether to check connectivity with the client.

   The following table provides details on the icons.

Table 6 Schedule icons

Icon	Label	Description
	Execute	Check connectivity on this day.
	Skip	Do not check connectivity on this day.

To check connectivity every day, select **Execute** from the list, and then click **Make All**.

10. Click **Next**.

    The **Specify the Connectivity Options** page appears.

11. Select the success criteria for the action:
    - To specify that the connectivity check is successful only if successful connectivity is achieved with all clients in the assigned group, select the **Succeed only after all clients succeed** checkbox.
    - To specify that the connectivity check is successful if connectivity is achieved with one or more clients in the assigned group, clear the checkbox.

12. Click **Next**.

    The **Specify the Advanced Options** page appears.

13. (Optional) Configure advanced options and schedule overrides.

    Note

    Although the **Retries**, **Retry Delay**, **Inactivity Timeout**, or the **Send Notification** options appear, the Check Connectivity action does not support these options and ignores the values.

14. In the **Parallelism** field, specify the maximum number of concurrent operations for the action.

15. From the **Failure Impact** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action** .

      Note

      The **Abort action** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types.

    - To abort the entire workflow if there is a failure with one of the jobs in the action, select **Abort workflow**.

    Note

    If any of the actions fail in the workflow, the workflow status does not appear as interrupted or cancelled. NetWorker reports the workflow status as failed.

16. From the **Soft Limit** list, specify the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no limit.

17. From the **Hard Limit** list, specify the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no limit.
18. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To change the month on which to schedule the override, use the navigation buttons and the month list box. To change the year, use the spin boxes. You can set an override in the following ways:

    - Select the day in the calendar, which changes the action task for the specific day.
    - Use the action task list to select the task, then perform one of the following steps:
      - To define an override that occurs on a specific day of the week, every week, select **Specified day**, then use the drop downs. Click **Add Rules based override**.
      - To perform the action task on the last day of the calendar month, select **Last day of the month**. Click **Add Rules based override**.
      - In the **Override** field, type an override.

        Note

        To remove an override, delete the entry from the **Override** field.
19. Click **Next**.

    The **Action Configuration Summary** page appears.
20. Review the settings that you specified for the action, and then click **Configure**.

After you finish

(Optional) Create one of the following actions to automatically occur after the check connectivity action:

- Probe
- Traditional backup

  Note

  This option is not available for NAS snapshot backups.
- Snapshot backup

Creating a snapshot backup action

A snapshot backup action performs a snapshot on a supported storage device, and then generates a save set entry for the snapshot-based backup in the NetWorker media database.

Before you begin

- Create the policy and workflow that contain the action.
- (Optional) Create actions to precede the snapshot backup action. Supported actions that can precede a snapshot backup include:
  - Probe
  - Check connectivity

Procedure

1. In the expanded left pane, select the workflow, and then perform one of the following tasks in the right pane to start the Policy Action wizard:

- If this is the first action in the workflow, select **Create a new action**.
- If the workflow has other actions, right-click an empty area of the **Actions** pane, and then select **New**.

The **Specify the Action Information** page appears.

2. From the **Action Type** list, select **Backup**.
3. From the secondary action list, select **Snapshot**.
4. When you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is grayed out.
5. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, select the action that should precede this action from the **Previous** box.
   - If the action should run concurrently with an action, select the concurrent action from the **Previous** box, and then select the **Concurrent** checkbox.
6. Select whether to use a weekly or monthly schedule for the action:
   - To specify a schedule for each day of the week, select **Weekly by day**.
   - To specify a schedule for each day of the month, select **Monthly by day**.
7. Click the icon on each day to specify the type of backup to perform.

   The following table provides details on the backup type that each icon represents.

Table 7 Backup type icons

Icon	Label	Description
	Full	Perform a full backup on this day. Full backups include all files, regardless of whether the files changed.
	Incr	Perform an incremental backup on this day. Incremental backups include files that have changed since the last backup of any type (full or incremental).
	Cumulative Incr	Perform a cumulative incremental backup. Cumulative incremental backups include files that have changed since the last full backup.
	Logs Only	Perform a backup of only database transaction logs. **Note** This is not applicable for NAS.
	Synthetic Full	Perform a synthetic backup on this day. A synthetic full backup includes all data that changed since the last full backup and subsequent incrementals to create a synthetic full backup. **Note** Synthetic Full backups are not supported.
	Skip	Do not perform a backup on this day.

To perform the same type of backup on each day, select the backup type from the list and click **Make All**.

Note

The schedule for a snapshot backup or discovery defines the days of the week or month on which to perform the snapshot backup or discovery. For a snapshot backup action, the schedule also defines the level of backup to perform on each day. This level also applies to the clone action, if created.

8. Click **Next**.

   The **Snapshot Options** page appears.

9. From the **Destination Storage Node** list box, select the storage node with the devices on which to store the backup data.
10. From the **Destination Pool** list box, select the media pool in which to store the backup data.
11. From the **Retention** list box, specify the amount of time to retain the backup data.

    After the retention period expires, the save set is removed from the media database and the snapshot is deleted.

12. From the **Minimum Retention Time** list box, specify the minimum amount of time to retain the backup data.

    When the minimum retention time passes, a snapshot action that is in progress can remove the snapshot from the storage device to ensure that there is sufficient disk space for the new snapshot.

13. Click **Next**.

    The **Specify the Advanced Options** page appears.

14. In the **Retries** box, specify the number of times that NetWorker should retry a failed probe or backup action, before NetWorker considers the action as failed. When the **Retries** value is 0, NetWorker will not retry a failed backup or probe action.

    Note

    The **Retries** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types. When you specify a value for this option in other actions, NetWorker ignores the values.

15. In the **Retry Delay** field, specify a delay in seconds to wait before retrying a failed backup or probe action. When the **Retry Delay** value is 0, NetWorker retries the failed backup or probe action immediately.

    Note

    The **Retry Delay** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types. When you specify a value for this option in other actions, NetWorker ignores the values.

16. In the **Inactivity Timeout** field, specify the maximum number of minutes that a job run by an action is allowed to fail to communicate back to the server.

    If the job fails to respond within the timeout value, the server considers the job a failure. If a job fails, NetWorker retries the job immediately. This ensures that no time is lost due to failures.

Increase the timeout value if a backup consistently aborts due to inactivity. Inactivity timeouts may occur for backups of large save sets, backups of save sets with large sparse files, and incremental backups of many small static files.

Note

The **Inactivity Timeout** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types. When you specify a value for this option in other actions, NetWorker ignores the values.

17. In the **Parallelism** field, specify the maximum number of concurrent operations for the action.

    Note

    The **Parallelism** value should not exceed 25.

18. From the **Failure Impact** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action** .

      Note

      The **Abort action** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types.

    - To abort the entire workflow if there is a failure with one of the jobs in the action, select **Abort workflow**.

    Note

    If any of the actions fail in the workflow, the workflow status does not appear as interrupted or cancelled. NetWorker reports the workflow status as failed.

19. From the **Send Notifications** list box, select whether to send notifications for the action:
    - Select **Set at policy level** to use the notification configuration that is defined in the Policy resource to send the notification.
    - Select **On Completion** to send a notification on completion of the action.
    - Select **On Failure** to send a notification only if the action fails to complete.

20. In the **Send notification** attribute when you select the **On Completion** or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` action to write the notifications to a log file or configure an email notification.

    The default notification action is to log the information to the `policy_notifications.log` file. The `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows, by default. You can use the `smtpmail` application on Windows or the default mailer program on Linux to send email messages.

    For example:

- To log notifications to a file named `policy_notifications.log`, type the following command:

  ```
  nsrlog -f policy_notifications.log
  ```

- On Linux, to send a notification email, type the following command:

  ```
  mail -s subject recipient
  ```

- On Window, to send a notification email, type the following command: `smtpmail -s subject -h mailserver recipient1@mailserver recipient2@mailserver...`
  where:
  - **-s *subject***—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the `smtpmail` program assumes that the message contains a correctly formatted email header and nothing is added.
  - **-h *mailserver***—Specifies the hostname of the mail server to use to relay the SMTP email message.
  - *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

21. From the **Soft Limit** list, specify the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no limit.
22. From the **Hard Limit** list, specify the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no limit.
23. Click **Next**.

    The **Action Configuration Summary** page appears.
24. Review the settings that you specified for the action, and then click **Configure**.

Creating a discover action

A discover action discovers snapshots on a NAS device that the current NetWorker server did not create. NetWorker then creates save set entries for the discovered snapshots on a NAS client in the media database. The discover action also compares the save sets in the media database for the NAS client against the actual snapshots stored on the client. If the media database entry does not have a corresponding snapshot on the NAS client, then the media database entry is removed.

Before you begin

Create the policy and workflow that contain the action. Ensure that the group assigned to the workflow contains only NAS devices. The discover action should be the first action in the workflow.

Procedure

1. In the expanded left pane, select the workflow, and then perform one of the following tasks in the right pane to start the Policy Action wizard:
   - If this is the first action in the workflow, select **Create a new action**.
   - If the workflow has other actions, right-click an empty area of the **Actions** pane, and then select **New**.

   The **Specify the Action Information** page appears.
2. From the **Action Type** list, select **Discover**.

3. When you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is grayed out.
4. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, select the action that should precede this action from the **Previous** box.
   - If the action should run concurrently with an action, select the concurrent action from the **Previous** box, and then select the **Concurrent** checkbox.
5. Select whether to use a weekly or monthly schedule for the action:
   - To specify a schedule for each day of the week, select **Weekly by day**.
   - To specify a schedule for each day of the month, select **Monthly by day**.
6. Click the icon on each day to specify whether to perform snapshot discovery.

   The following table provides details on the icons.

   Table 8 Snapshot discovery icons

Icon	Label	Description
	Execute	Perform snapshot discovery on this day.
	Skip	Do not perform snapshot discovery on this day.

   To perform snapshot discovery every day, select **Execute** from the list and click **Make All**.

7. Click **Next**.

   The **Discover Options** page appears.
8. From the **Discover Type** list, select the NAS snapshot data to discover.
9. Click **Next**.

   The **Specify the Advanced Options** page appears.

After you finish

(Optional) Create a generate index action to create entries in the client file indexes for the snapshot save sets, or a clone action to automatically clone the save sets after the discover action.

Creating a generate index action

A generate index action creates client file indexes of existing NAS snapshots.

Before you begin

- Create the policy and workflow that contains the action.
- (Optional) Create actions to precede the generate index action in the workflow. Supported actions that can precede a generate index action include:
  - Discover
  - Snapshot backup

Note

This point is only optional if you are using a saveset ID group. If you are using a NAS Device group, or Client group, one of these two actions must be used for the index action.

Procedure

1. In the expanded left pane, select the workflow, and then perform one of the following tasks in the right pane to start the Policy Action wizard:
   - If this is the first action in the workflow, select **Create a new action**.
   - If the workflow has other actions, right-click an empty area of the **Actions** pane, and then select **New**.

   The **Specify the Action Information** page appears.
2. From the **Action Type** list, select **Generate Index**.
3. When you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is grayed out.
4. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, select the action that should precede this action from the **Previous** box.
   - If the action should run concurrently with an action, select the concurrent action from the **Previous** box, and then select the **Concurrent** checkbox.
5. Select whether to use a weekly or monthly schedule for the action:
   - To specify a schedule for each day of the week, select **Weekly by day**.
   - To specify a schedule for each day of the month, select **Monthly by day**.
6. Click the icon on each day to specify whether to perform snapshot index generation.

   The following table provides details on the icons.

   Table 9 Snapshot generate icons

Icon	Label	Description
	Execute	Perform snapshot index generation on this day.
	Skip	Do not perform snapshot index generation on this day.

   To perform snapshot index generation every day, select **Execute** from the list and click **Make All**.

7. Click **Next**.

   The **Index Options** page appears.
8. From the **Type of saveset to be indexed** list, select the NAS snapshot to index.
9. Click **Next**.

   The **Specify the Advanced Options** page appears.

After you finish

(Optional) Create a clone action to automatically clone the data after the generate index action. A clone action is the only supported action after a generate index action in a workflow.

Creating a clone action

A clone action creates a copy of one or more save sets. Cloning allows for secure offsite storage, the transfer of data from one location to another, and the verification of backups.

Procedure

1. In the expanded left pane, select the workflow, and then perform one of the following tasks in the right pane to start the Policy Action wizard:
   - If this is the first action in the workflow, select **Create a new action**.
   - If the workflow has other actions, right-click an empty area of the **Actions** pane, and then select **New**.

   The **Specify the Action Information** page appears.
2. In the **Name** field, type the name of the action.

   The maximum number of characters for the action name is 64.
3. In the **Comment** field, type a description for the action.
4. To ensure that the action runs when the policy or workflow that contains the action is started, in the **Enabled** box, select the option. To prevent the action from running when the policy or workflow that contains the action is started, clear this option.

   Note

   When you clear the **Enabled** option, any action that occurs after a disabled action will not start, even if the succeeding options are enabled.
5. From the **Action Type** list, select **Clone**.
6. When you create the action as part of the workflow configuration, the workflow appears automatically in the **Workflow** box and the box is grayed out.
7. Specify the order of the action in relation to other actions in the workflow:
   - If the action is part of a sequence of actions in a workflow path, select the action that should precede this action from the **Previous** box.
   - If the action should run concurrently with an action, select the concurrent action from the **Previous** box, and then select the **Concurrent** checkbox.
8. Select whether to use a weekly or monthly schedule for the action:
   - To specify a schedule for each day of the week, select **Weekly by day**.
   - To specify a schedule for each day of the month, select **Monthly by day**.
9. Click the icon on each day to specify whether to perform cloning.

   The following table provides details on the icons.

Table 10 Schedule icons

Icon	Label	Description
	Execute	Perform cloning on this day.
	Skip	Do not perform cloning on this day.

To perform cloning every day, select **Execute** from the list and click **Make All**.

10. Click **Next**.

    The **Specify the Clone Options** page appears.

11. In the **Data Movement** group box, define the volumes and devices to which NetWorker sends the clone data.

    a. From the **Destination Storage Node** list, select the storage node with the devices on which to store the cloned save sets.

    b. In the **Delete source save sets after clone completes**, select the option to instruct NetWorker to remove the source save set information from the client file index, and to mark the save set as recyclable in the media database during a Server expiration maintenance action. Clear this option to allow the source save sets to expire based on the defined retention time.

    c. From the **Destination Pool** list, select the target media pool for the cloned save sets.

    Note

    When you clone SnapVX snapshots or ProtectPoint snapshots, you can clone to media devices, for example Data Domain or to a ProtectPoint device. If you select a pool that contains ProtectPoint devices and media devices, then NetWorker clones the SnapVX and ProtectPoint save sets to the ProtectPoint devices. This is not applicable for NAS devices.

    d. From the **Retention** list, specify the amount of time to retain the cloned save sets.

    After the retention period expires, the save sets are marked as recyclable during an expiration server maintenance task.

12. In the **Filters** group box, define the criteria that NetWorker uses to create the list of eligible save sets to clone. The eligible save sets must match the requirements that are defined in each filter. NetWorker provides the following filter options:

    a. Time filter—Use the **Time** section to define the time range in which NetWorker should inspect, when searching for eligible save sets to clone in the media database. Use the spin boxes to specify the start of the time range and the end of the time range. The **Time** filter list includes three options, which define how NetWorker determines save set eligibility, based on the time criteria:

    - **Do Not Filter**—NetWorker inspects the save sets in the media database to create a clone save set list that meets the filter criteria.
    - **Accept**—The clone save set list includes save sets whose save time is within the time range that is specified by the spin boxes and meet all the other defined filter criteria.

- **Reject**—The clone save set list does not include save sets whose save time is within the time range that is specified by the spin boxes and meet all the other defined filter criteria.

b. Save Set filter—Use the **Save Set** section to instruct NetWorker to include or exclude ProtectPoint and Snapshot save sets, when searching for eligible save sets to clone in the media database. The **Save Set** filter list includes three options, which define how NetWorker determines save set eligibility, based on the save set criteria:

- **Do Not Filter**—NetWorker inspects the save sets in the media database to create a clone save set list that meets the filter criteria.
- **Accept**—The clone save set list includes eligible ProtectPoint or Snapshot save sets, when you also enable the ProtectPoint or Snapshot checkboxes.
- **Reject**—The clone save set list does not include eligible ProtectPoint and Snapshot save sets when you also enable the ProtectPoint and Snapshot checkboxes.

c. Clients filter—Use the **Client** section to define a list of clients to include or exclude, when NetWorker searches for eligible save sets to clone in the media database. The **Client** list includes three options, which define how NetWorker determines save set eligibility, based on the client criteria:

- **Do Not Filter**—NetWorker inspects save sets that are associated with the clients in the media database, to create a clone save set list that meets the filter criteria.
- **Accept**—The clone save set list includes eligible save sets for the selected clients.
- **Reject**—The clone save set list does not include eligible save sets for the selected clients.

d. Levels filter—Use the **Levels** section to define a list of backup levels to include or exclude, when NetWorker searches for eligible save sets to clone in the media database. The **Levels** filter list includes three options, which define how NetWorker determines save set eligibility, based on the level criteria:

- **Do Not Filter**—NetWorker inspects save sets regardless of level in the media database, to create a clone save set list that meets all the filter criteria.
- **Accept**—The clone save set list includes eligible save sets with the selected backup levels.
- **Reject**—The clone save set list does not include eligible save sets with the selected backup levels.

13. Click **Next**.

    The **Specify the Advanced Options** page appears.

14. Configure advanced options, including notifications and schedule overrides.

    Note

    Although the **Retries**, **Retry Delay**, or the **Inactivity Timeout** options appear, the clone action does not support these options and ignores the values.

15. In the **Parallelism** field, specify the maximum number of concurrent operations for the action.

Note

The **Parallelism** value should not exceed 25.

16. From the **Failure Impact** list, specify what to do when a job fails:
    - To continue the workflow when there are job failures, select **Continue**.
    - To abort the current action if there is a failure with one of the jobs, but continue with subsequent actions in the workflow, select **Abort action** .

      Note

      The **Abort action** option only applies to probe actions, and the backup actions for the Traditional and Snapshot action types.
    - To abort the entire workflow if there is a failure with one of the jobs in the action, select **Abort workflow**.

Note

If any of the actions fail in the workflow, the workflow status does not appear as interrupted or cancelled. NetWorker reports the workflow status as failed.

17. From the **Send Notifications** list box, select whether to send notifications for the action:
    - Select **Set at policy level** to use the notification configuration that is defined in the Policy resource to send the notification.
    - Select **On Completion** to send a notification on completion of the action.
    - Select **On Failure** to send a notification only if the action fails to complete.
18. In the **Send notification** attribute when you select the **On Completion** or **On failure** option, the **Command** box appears. Use this box to configure how NetWorker sends the notifications. You can use the `nsrlog` action to write the notifications to a log file or configure an email notification.

    The default notification action is to log the information to the `policy_notifications.log` file. The `policy_notifications.log` file is located in the `/nsr/logs` directory on Linux and the `C:\Program Files\EMC NetWorker\nsr\logs` folder on Windows, by default. You can use the `smtpmail` application on Windows or the default mailer program on Linux to send email messages.

    For example:
    - To log notifications to a file named `policy_notifications.log`, type the following command:

      ```
      nsrlog -f policy_notifications.log
      ```
    - On Linux, to send a notification email, type the following command:

      ```
      mail -s subject recipient
      ```
    - On Window, to send a notification email, type the following command:

      ```
      smtpmail -s subject -h mailserver recipient1@mailserver
      recipient2@mailserver...
      ```

where:

- **-s *subject***—Includes a standard email header with the message and specifies the subject text for that header. Without this option, the `smtpmail` program assumes that the message contains a correctly formatted email header and nothing is added.
- **-h *mailserver***—Specifies the hostname of the mail server to use to relay the SMTP email message.
- *recipient1@mailserver*—Is the email address of the recipient of the notification. Multiple email recipients are separated by a space.

19. From the **Soft Limit** list, specify the amount of time after the action starts to stop the initiation of new activities. The default value of 0 (zero) indicates no limit.
20. From the **Hard Limit** list, specify the amount of time after the action starts to begin terminating activities. The default value of 0 (zero) indicates no limit.
21. (Optional) Configure overrides for the task that is scheduled on a specific day.

    To change the month on which to schedule the override, use the navigation buttons and the month list box. To change the year, use the spin boxes. You can set an override in the following ways:

    - Select the day in the calendar, which changes the action task for the specific day.
    - Use the action task list to select the task, then perform one of the following steps:
      - To define an override that occurs on a specific day of the week, every week, select **Specified day**, then use the drop downs. Click **Add Rules based override**.
      - To perform the action task on the last day of the calendar month, select **Last day of the month**. Click **Add Rules based override**.
      - In the **Override** field, type an override.

        Note

        To remove an override, delete the entry from the **Override** field.

22. Click **Next**.

    The **Action Configuration Summary** page appears.
23. Review the settings that you specified for the action, and then click **Configure**.

After you finish

(Optional) Create a clone action to automatically clone the save sets again after this clone action. Another clone action is the only supported action after a clone action in a workflow.

Visual representation of NAS snapshot workflows

When you create actions for a workflow, a map provides a visual representation of the actions in the second right pane of the **Protection** window of the **Administration** interface.

Figure 14 Sample NAS snapshot workflow

The oval icon at the beginning of the visual representation specifies the group to which the workflow applies, the rounded rectangle icons identify actions, and the parallelogram icons identify the destination pool for the action.

You can work directly in the visual representation of a workflow to perform the following tasks:

- Adjust the display of the visual representation by right-clicking and selecting one of the following options:
  - **Zoom In**—Use to increase the size of the visual representation.
  - **Zoom Out**—Use to decrease the size of the visual representation.
  - **Zoom Area**—Use to limit the display to a single section of the visual representation.
  - **Fit Content**—Use to fit the visual representation to the window area.
  - **Reset**—Use to reset the visual representation to the default settings.
  - **Overview**—To view a separate dialog box with a high-level view of the visual representation and a legend of the icons.
- View and edit the properties for the group, action, or destination pool by right-clicking the icon for the item and selecting **Properties**.
- Create a group, action, or destination pool by right-clicking the icon for the item and selecting **New**.

CHAPTER 3

Software Configuration

This chapter includes the following topics:

- Backup group resource migration 60
- Road map for NAS snapshot configuration 62
- NetWorker with NAS configuration prerequisites 62
- Configuring a client resource with the wizard 64
- Configuring a NAS device client resource manually 68
- Configuring the Application Information variables 69
- Configuring preprocessing and postprocessing scripts 70

Backup group resource migration

During the migration process, NetWorker creates resources to replace each Group resource, and then migrates configuration attributes from the 8.2.x and earlier resources to the new NetWorker 9.0.1 resources.

Resource migration for group resources when Snapshot is enabled

This section summarizes the Group attribute values that migrate to 9.0.1 resources attributes, when the group is Snapshot enabled.

Table 11 Migration of Group attributes

9.0.1 Resource type	9.0.1 Resource name	Migration process overview Attribute values that are migrated from Group resource	Attribute values that are migrated from Group resource
Policy	Backup	One policy resource that is called Backup appears and contains all migrated information for all NetWorker group resources that backup files ystem and NMM data.	Not applicable
Protection Group	Name of the Group resource	One Protection Group resource appears for each migrated Group resource. Each Protection Group contains the same client resources that were associated with the pre-9.0.1 group resource.	Comment
Workflow	Name of the Group resource	One Workflow resource appears for each migrated Group resource. Each Workflow resource is associated with the Protection Group resource that was created for the migrated Group resource.	• Autostart • Start Time • Next Start • Interval • Restart Window • End Time attribute value is set to Start Time+(Interval*(n-1)) When the Probe backup group attribute was enabled, the following values are also migrated: • Probe Interval—To the Interval attribute • Probe Start Time—To the Start Time attribute • Probe End Time—To the End Time attribute

Table 11 Migration of Group attributes (continued)

9.0.1 Resource type	9.0.1 Resource name	Migration process overview Attribute values that are migrated from Group resource	Attribute values that are migrated from Group resource
Probe	Probe	The Probe action resource appears when the Probe based group attribute was enabled in the pre-9.0.1 migrated group.	Not applicable
Action—Snapshot backup	Backup	The Snapshot Backup action appears for a Group resource that has the Snapshot attribute enabled.	• Parallelism • Retries • Retry delay • Success Threshold • Option attributes: ▪ No save, Verbose, Estimate, Verify Synthetic Full, Revert to full when Synthetic Full fails • Schedule • Schedule Time • Retention policy • Inactivity Timeout • Soft Runtime Limit—To Soft Limit • Hard Runtime Limit—To Hard Limit • File Inactivity Threshold—To Inactivity Threshold • File Inactivity Alert Threshold—To Inactivity Alert Threshold • Min expiration = (1440/(backups per day/retain count))-10 • If Retain snapshot=0, then Backup snapshots attribute is set to ALL
Action—Clone	Clone	The Clone action resource appears when the Clone attribute was enabled in the Group resource.	Clone Pool—To the Destination Pool attribute

Note

The *EMC NetWorker Updating from a Previous Release Guide* provides details about resources that are migrated during the update process.

Considerations about migration

1. A clone action is created for every backup action. The clone action moves snapshot data to media.
2. A NetWorker 8.2.x and earlier snapshot policy resource that was configured for **Every nth snapshot** value is not migrated to NetWorker 9.0.1.
3. A NetWorker 8.2.x and earlier snapshot policy resource that was configured for **nth snapshot** is not migrated to NetWorker 9.0.1, and a clone action is not created.

   For example, a NetWorker 8.2.2 snapshot policy of 6-6-Week-3 which resolves to take 6 snapshots, retain 6, expire snapshots every week, and backup the first and third snapshot. The last value **Backup Snapshots** or **3** will not be migrated. Instead, a clone action is created to backup every snapshot.
4. Each backup action under snapshot policy is followed by a clone action. Clone actions have filtering options. Check whether filtering meets the backup requirements of snapshot management.

Road map for NAS snapshot configuration

Plan the NAS snapshot configuration by using a high-level road map that outlines the sequence of configuration tasks that you must perform.

Procedure

1. Ensure that you meet the configuration prerequisites.

   NetWorker with NAS configuration prerequisites on page 62 provides details.
2. Configure the snapshot and the clone operations by using the Data Protection Action Wizard or the CLI.

   The following topics provide details:

   - Configuring a client resource with the wizard on page 64
   - Configuring a NAS device client resource manually on page 68
3. Configure any necessary Application Information variables.

   Configuring the Application Information variables on page 69 provides details.
4. Configure any necessary preprocessing or postprocessing scripts.

   Configuring preprocessing and postprocessing scripts on page 70 provides details.
5. Test the configuration.

NetWorker with NAS configuration prerequisites

Verify the basic compatibility of all systems that are used for NetWorker operations. Components of the NAS snapshot network on page 17 provides details.

The following sections describe the prerequisites for the hosts that are involved in NetWorker operations.

NAS device prerequisites

Ensure that the NAS device is installed with the prerequisite software for snapshot and clone operations:

- EMC Isilon—None required.
- EMC VNX or VNX2—None required.
- EMC VNXe—VNXe Unisphere CLI, available at https://support.emc.com.
- NetApp—NetApp Manageability SDK, available from NetApp.
  - On Microsoft Windows systems, which are installed in a directory in the system-level PATH variable.
    For example, `C:\Program Files\EMC Networker\nsr\bin`
  - On Linux systems, which are installed in the `/usr/lib64` directory.
  - On NetApp, ensure `options.httpd.admin.enable` is set to ON.
  - (Optional) for HTTPS access on NetApp, `options.httpd.admin.ssl.enable` may be set to ON.

Ensure that you have synchronized the system times on the NAS devices and the NetWorker server. If not synchronized within 10 seconds, the snapshot and replication operations can cause problems or fail. The recommended method is to use a common Network Time Protocol (NTP) server to obtain system time. This method prevents time drift.

The support matrix for the NAS device that you use, available from EMC Online Support, provides requirement details on systems and software.

Replication prerequisites

Ensure the following prerequisites for replication operations:

- For remotely replicated directories, ensure the remote system has a client resource set up on the NetWorker server.
- Ensure you have correctly configured the replication policy on the NAS device before you create the Client resource for the NAS device.
- Ensure you have configured the replication policy to create a snapshot when the replication operation completes.

The NAS device documentation provides details.

NetApp prerequisites

For SnapVault and SnapMirror replication operations, ensure that the following prerequisites are met:

- The source and destination volumes or Qtrees must exist before you configure a replication. The volumes may be on the same or on separate NetApp devices on the same or on separate servers that may be NetApp virtual machines or Vserver, and both volumes must be in an online state.
- The source volume must be read-writable and the destination volume must be a data protection type.
- Configure SnapVault and SnapMirror replication policies on the NetApp devices.

- Validate the replication configuration by performing an initial replication operation. This makes the replication policies available as selections in the NetWorker client wizard.

The NetApp documentation provides details.

Note

Qtree-Qtree remote replication is not supported.

Storage node prerequisites

If you plan to clone the snapshot save sets to conventional storage media, then a NetWorker storage node is required for recovery operations.

Ensure the following prerequisites:

- NetWorker storage node software is installed.
- NDMP backup storage devices are configured on the storage node for the clone operations.

Configuring NDMP

If you plan to clone the snapshot save sets to conventional storage media, then complete the NDMP configuration on the NAS client system. The *EMC NetWorker Network Data Management Protocol (NDMP) User Guide* provides information about NDMP configuration.

Note

The *Isilon OneFS Administration Guide* provides updates and details about Isilon commands. You can also perform this configuration through the Isilon OneFS Storage Administration user interface.

Procedure

1. Use `ssh` to connect to a node in the cluster.
2. Use the `isi` command to create the NDMP username and password:

   ```
   isi ndmp user create username password
   ```

3. Use the `isi` command to enable NDMP:

   ```
   isi services ndmpd enable
   ```

4. Use the `isi` command to enable NDMP settings:

   ```
   isi ndmp settings set --name dma --value emc
   ```

Configuring a client resource with the wizard

NMC configures NAS devices as NetWorker clients. NDMP enables NAS devices to mimic NetWorker clients for configuration purposes without NetWorker client software installed. The wizard is the recommended configuration method.

Procedure

1. Ensure the necessary prerequisites.

   NetWorker with NAS configuration prerequisites on page 62 provides details.

2. Run NMC.
3. ,In the **Enterprise** view, browse tree, right-click the NetWorker server that will manage the snapshots, and then select **Launch Application**.
4. You can access the client wizard to create a NAS device from two areas:
   - The **Protection** view
   - The **Devices** view
5. In the **Protection** view, launch the client wizard (NMC configures NAS devices as NetWorker clients):
   - To create a NAS device configuration, right-click **Client** in the navigation tree, and then select **New Client Wizard.**
   - To modify a configuration, right-click an existing NAS device in the Client table, and then select **Modify Client Wizard** or **Modify Client Properties**.
6. In the wizard, complete the **Specify the Client Information** page:
   a. In the **Client Name** field, type an associated hostname.

      Note

      For Isilon, use a non-aggregated (nonteamed) network connection to one of the Isilon cluster nodes that has a fixed IP address. Do not use the SmartConnect hostname.

   b. In the **Client Type** field, select **NAS-Device**.
   c. Click **Next**.
7. Complete the **Specify Credentials for the NAS device** page:
   a. For the user authorized to access data on this client instance of the NAS device, for example, to create, delete, or share snapshots, in the **Management Credentials** fields, type a **User Name** and **Password**. Each instance can have a different user. You may need to provide a management name or address, for example, for a VNX Control Station name if it differs from the NAS device name.
   b. for the user authorized to perform NDMP operations on the NAS device, such as browsing the file system during configuration, in the **NDMP Credentials** fields, type a **User Name** and **Password**.
   c. If a Microsoft Windows client will access the snapshot data, complete the **File Server Credentials**. These fields are ignored by other operating system types. Type a **User Name** and **Password** for the user authorized to mount and access the snapshot data on a Windows recovery host for this instance of the NAS device. Each instance can have a different user.
   d. Click **Next**.
8. Complete the **Verify the NAS Device Information** page:
   a. Review the **Vendor Information** details.
   b. If you are configuring snapshot clones to NDMP devices, complete the **NDMP Clone Information** details. Available values are those supported by the client's NDMP configuration. The *EMC NetWorker Administration Guide* provides details:

      Specify the **NDMP backup type**.

NAS device	Supported backup types
EMC VNX	• tar • dump—The best backup type for this device. It traverses a file tree in mixed width first and depth-first order. • vbb—Use the volume-based backup type to back up the entire volume at the block level, more efficient than traditional file-based backups. Used to back up the entire volume at the block level rather than at a file level, but does not support DDAR, TBB, and Three Party backups. • ts—Tape silvering.
EMC Isilon	• tar • dump
NetApp	• dump—An inode-based backup that traverses a file tree in directory first and file-based order.

Review the **App Info** options that the wizard has selected for the NAS device. You can disable options, as required.

In the **Advanced App Info** field, you may specify additional NAS-specific variables that are supported by the client's NDMP configuration, one per line. For example, for an Isilon or NetApp remote replication backup, specify NDMP_MNT_HOST=*remote host*. Common Application Information variables on page 78 and Configuring the Application Information variables on page 69 provides more information.

c. Click **Next**.

9. Complete the **Select the File System Objects** page for NAS devices that do not support file browsing:

   a. Type a list of absolute pathnames of file systems, directories, and individual files to include in the snapshot save set. List each item on a separate line.

   b. Click **Next**.

Note

For a NetApp Cluster Mode, specify the file system as `/vol/volumename`.

10. Complete the **Specify Snapshot Location** page.

    a. Specify a local or remote location for the snapshot. The available snapshot locations depend on the replication policies that the storage administrator has configured on the NAS device. The available locations for replication are those capable of replicating all the save set paths that were specified earlier in the wizard.

       - **Local snapshot**—The device will not replicate the selected data and NetWorker will create a snapshot of the original data.
       - **Locally replicated snapshot**—The device will replicate the selected data to a different location on the same device and NetWorker will create a snapshot from the replicated data.

- **Remotely replicated snapshot**—The device will replicate the selected data to a location on a different NAS device and NetWorker will create a snapshot from the replicated data.

For example, if you have defined the following replication policies on a NAS Isilon device.

NAS policy name	Local system	Local path	Remote system	Replicated path
Local1	System_A	`/ifs/home/folders`	Not applicable	`/ifs/localrep`
Remote1	System_A	`/ifs/home/folders`	System_B	`/ifs/remoterep/1`
Remote2	System_A	`/ifs/home`	System_B	`/ifs/remoterep/2`

Then the following snapshot location paths will use the corresponding NAS replication policies.

Snapshot save set location	NAS policies
`/ifs`	none
`/ifs/foo`	none
`/ifs/home`	Remote2
`/ifs/home/folders`	Local1, Remote1, Remote2
`/ifs/home/folders/bar`	Local1, Remote1, Remote2

Note

For NetApp devices, if the snapshot destination volume is written to, the destination becomes the new source volume and the relationship switches.

b. Click **Next**.

11. Complete the **Backup Configuration Summary** page:

    a. Review the attributes and values that are listed in the summary.

    To modify a setting, click **Back** or click the link in the steps panel.

    b. To accept and create the configuration, click **Create**.

12. Complete the **Client Configuration Results** page:

    a. Ensure that the backup configuration successfully completes.

    b. Click **Finish**.

After you finish

The Data Protection Policies chapter describes how to schedule a snapshot backup and clone of the data. Common Application Information variables on page 78 provides more information.

Performing post Client Configuration Wizard steps

After the Client Configuration Wizard creates the NAS client, modify the properties of the new NAS client.

Procedure

1. On the **Administrator** window, from the navigation pane, select **Clients**.
2. Right-click the client that you just created, and then select **Modify Client Properties**.
3. On the **Globals (2 of 2)** tab, in the **Remote Access** field, specify the remote access credentials for the NetWorker Server as follows:
   - For a Windows NetWorker server—system@*networker-server-name*
   - For a UNIX NetWorker server—root@*networker-server-name*

   where *networker-server-name* is the hostname of the NetWorker server.
4. Click **OK**.

Configuring a NAS device client resource manually

In some situations, you may need to configure a NAS device manually instead of using the NMC Client Configuration Wizard. For NetWorker purposes NAS devices are configured as NetWorker clients.

NAS devices are configured as NetWorker clients. You can manually modify a NAS device by using the NMC property windows. This method enables you to configure special directives or available options that the wizard interface does not support, such as Application Information Variables on page 77.

You cannot configure replication policies, which are required for locally replicated and remotely replicated snapshots. Configure these policies with the wizard.

The *EMC NetWorker Administration Guide* provides additional Client resource details that are not specific to NAS device configuration.

Procedure

1. Ensure the necessary prerequisites.

   NetWorker with NAS configuration prerequisites on page 62 provides details.
2. Run NMC, and in the NMC **Enterprise** view, browse tree, right-click the NetWorker server that manages the snapshots, and then select **Launch Application**.
3. In the NetWorker server's **Protection** view, right-click the NAS device in the **Clients** table, and then select **Modify Client Properties**.
4. On the **General** tab, in the **Save set** field, type or browse, and then select all the file systems, directories, or individual files that you want to include in the snapshot. List each item on a separate line.
5. On the **Apps & Modules** tab, ensure the following settings:
   a. If you plan to clone the snapshot, provide NDMP credentials in the **Remote User** and **Password** fields.
   b. Select the **NAS device** checkbox.
   c. Select the **NDMP** checkbox.

d. In the **Application information** field, type any optional NDMP variables that you want to use in the clone.

Note

NetApp configurations must specify the NSR_MOUNTPOINT_NAME variable to enable data recovery from NetApp replications. Also, for Isilon and NetApp add NDMP_MNT_HOST. For example, NDMP_MNT_HOST=*remote system name*.

Variables must be uppercase. NetWorker does not validate the variables. Application Information Variables on page 77 and Configuring the Application Information variables on page 69 provides details.

6. On the **Snapshot Management** tab, ensure the following settings:
   a. In the **Management credentials** attribute, type the name and password for the user authorized to access data, for example, to create, delete, or share data for this instance of the NAS device. Each instance can have a different user.
   b. In the **NAS device management name** field, type the fully qualified domain name (FQDN), required by some devices that use a special address for data management. For example, the VNX or VNXe Control Station address, which is different than the NAS file server address.
   c. If a Microsoft Windows client accesses the snapshot data, complete the **NAS file access user** fields. These fields are ignored by other operating system types. For the user authorized to mount and access the snapshot data on a Windows recovery host for this instance of the NAS device, type a **User Name** and **Password**. Each instance can have a different user.
7. When you have completed the NAS device configuration, click **OK**.
8. To verify the configurations, in NMC, right-click the NAS device in the **Clients** table, and then select **Check Snapshot Configuration**. The verification can take some time. A pop-up message lists detected problems. Verification assumes that sufficient resources are available for the snapshot and the clone operations and does not guarantee success.

Configuring the Application Information variables

Special Application Information variables provide specific control of snapshot processes. The Client Configuration Wizard cannot configure these variables. Manually configure these variables in the NetWorker Client resource for the NAS device by using the NetWorker property windows. Application Information Variables on page 77 provides details.

Note

For NetApp recovery operations, configure the NSR_MOUNTPOINT_NAME variable.

For SnapMirror and SnapVault the NDMP clone application variables must be set to N as follows:

DIRECT=*N*

UPDATE=*N*

Configuring preprocessing and postprocessing scripts

You can run user-defined preprocessing and postprocessing scripts from the application client. You can run these scripts only for file system backups.

Use preprocessing scripts and postprocessing scripts for operations such as application quiescing, shutdown, or startup. The scripts can produce output such as log files, but the scripts must return an exit status of 0, which means that the script did not fail and the backup can run. Any other exit code for a preprocessing script causes the backup to fail.

Note

EMC Technical Support does not support user-defined scripts.

Procedure

1. Provide the script files with the following security:
   - On Microsoft Windows systems, provide the script files with security that grants full control only to the local SYSTEM, local Administrators, or Backup Operators groups. Otherwise, the scripts do not run.

     To set this security in Windows Explorer, right-click the script file, select **Properties**, and click **Advanced** on the **Security** tab of the **Properties** window.
   - On UNIX systems, the root user must own the script files. The scripts can set only owner access permissions, and the scripts must at least have run access. Otherwise, the scripts do not run. Also, the parent directory of the scripts must have at least owner run permissions, and must not have write permissions for the group and world.
2. To add, modify, or run the resident scripts, place the scripts in a directory where a user must have administrator/root privileges. Otherwise, any backups that use the scripts fail.

   On Microsoft Windows systems, NetWorker searches for relative pathnames in the `NetWorker_install_path/bin` directory.
3. Include the pathnames of user-defined scripts in the **Application Information** attribute of the property window of the application Client resource by using the following variables:

   NSR_PRE_SNAPSHOT_SCRIPT=*pre-mirror_split-script_path*
   NSR_POST_SNAPSHOT_SCRIPT=*post-mirror_split-script_path*
4. After a backup completes, verify the log files that are generated in the `/nsr/logs` (UNIX) directory on the application client host. The log file name is in the form of *script_name*`_LOGFILE.txt`. The script output appears in the log file.

CHAPTER 4

Data Management and Recovery

This chapter includes the following topics:

- Snapshot management 72
- NAS snapshot recovery support and limitations 73
- Recovering data from a snapshot with the Recovery Wizard 73

Snapshot management

The chapter describes the management and the recovery operations for NAS device file system data only.

The NMC Recovery Wizard and the NetWorker CLI commands provide features that enable you to browse, delete, change snapshot expiration, and recover snapshot data.

Snapshot reporting

You can use NMC Reports to create individual reports of NAS snapshot, replicate, and clone activities.

The *EMC NetWorker Administration Guide* provides details.

Procedure

1. In NMC, select the **Reports** view.
2. In the **Snapshot Statistics** folder, select a summary report or a statement report to view. The **Configure** tab for the selected report type appears in the right panel.
3. In the **Configure** tab, customize the items that you want to include in the report. Select the item parameters. Click the **Remove (‹)**, **Remove All (‹‹)**, or **Add All (››)** buttons as required. If you do not specify **Save Time** values, the report displays all the available data. The **View Report** tab shows the resultant report.

Save set IDs and expiration policies

When NetWorker creates a snapshot, it generates a separate save set ID for each snapshot object that is specified in the Client resource.

For example, a single physical snapshot can create save sets for `/home/folders/user1` and `/home/folders/user2` if they both reside on the same NAS device. Each save set will have a separate save set ID, even if both save sets belong to the same client and both reside on the same NAS device.

During cloning to conventional storage media, NetWorker assigns a different save set ID to each cloned snapshot object. Each save set has an independent expiration policy, and when one save set expires, you can still use the other save set to perform a recovery.

The retention time of the backup action that created the save set determines the expiration of a snapshot save set. However, you can change the expiration period of a snapshot save set and the change does not affect the browse or expiration periods of an associated clone.

Browsing snapshot and clone save sets

The NetWorker client file index records only the save sets that it clones to conventional storage media. Because NetWorker indexes clones, you can browse the save set files in NMC.

The NetWorker media database contains entries for snapshot save sets. However, unlike clones, NetWorker does not catalog the snapshot save sets in the client file index. To browse snapshot save sets, you must use the NMC Recovery Wizard or the `nsrsnapadmin` command utility. NetWorker will mount the snapshot file system on the mount host, which enables you to browse and select files to recover.

Browsing and recovery on Windows hosts

When performing file-by-file browsing, or performing a directed recovery from the NAS device to a Microsoft Windows host, NetWorker connects to the NAS device by using the File Server credentials in the Client resource for the NAS device.

Microsoft Windows cannot connect to the NAS device by using different credentials than a previously established file service connection. NetWorker does not use the credentials that a previously established file service connection has used.

NAS snapshot recovery support and limitations

The following support and limitations apply to NAS snapshot recovery operations:

- A NAS snapshot recovery supports the following user interfaces:
  - NMC Recovery Wizard GUI
  - `nsrsnapadmin` command utility
  - `nsrnassnap_recover` command for NAS devices
- You can recover individual files or complete file systems from snapshot save sets.
- You cannot combine individual files from multiple save sets in a single recovery session.
- You can recover data from snapshots that NetWorker has cloned to conventional storage media as you would for any conventional NetWorker backup.
- You can recover data from NAS discovered snapshots that NetWorker has cloned to conventional storage media, as you would for any conventional NetWorker backup.

Note

NAS snapshot support and limitation on page 86 provides more information on NAS file system limitations.

Recovering data from a snapshot with the Recovery Wizard

You can use the NMC Recovery Wizard to recover file system data from a snapshot that is stored on a supported NAS device.

Procedure

1. Run NMC, and in the **Enterprise** view, select the NetWorker server name, and then select **Enterprise** › **Launch Application**.
2. In the NetWorker server **Recover** view, select **Recover** › **New Recover** to launch the Recovery Wizard.
3. Complete the **Select the Recovery Hosts** page:
   a. In the **Source Host** field, specify the NAS device that was the original source for the snapshot files or directories you want to recover.
   b. In the **Destination Host** field, specify where you want to recover the snapshot files and directories:
      - **Recover to the same host**—The wizard later prompts you to recover to a location on the source NAS device.

- **Select a destination host**—The wizard later prompts you to direct the recovery to a location on the NetWorker host that is running the recovery.

Note

For recovery on a Microsoft Windows host, the NAS device must be configured with the **File Server Credentials** fields (wizard method) or the **NAS file access user** fields (manual method). Configuring the NAS device manually on page 68 provides details for the manual method.

c. In the **Available Recover Types** field, select **NAS Snapshots** or **Filesystem (NDMP)**.

d. Click **Next**.

4. Complete the **Select a NAS Snapshot** page. You can recover the entire snapshot save set or you can recover individual directories and individual files from the snapshot save set:

a. In the **NAS Snapshots** table, select the snapshot to recover from, based on the snapshot time and save set volumes.

b. In **Select save set**, select a single save set volume to mount and recover from.

Note

You can select only one save set for this operation. Each additional save set volume requires a separate pass through the wizard.

c. In **Recover mode**, select from the following options:

- **Browse and recover save set**—When you click **Next**, the wizard mounts the snapshot volume for the save set and open the **Select Data to Recover** page. The mount operation can take some time.
- **Recover full save set**—When you click **Next**, the wizard goes directly to the **Select the Recovery Options** page.
- **Create temporary mount point for access**—If you want to use an existing mount point for volume access, clear this checkbox. You can set the mount point by using the NSR_MOUNTPOINT_NAME variable. Using application information variables on page 78 provides details.

Note

Ensure that this setting is not selected for NetApp NAS devices on Linux operating systems, which cannot use a temporary mount point. Use an existing mount point.

d. Click **Next**. The resultant wizard step depends on the selections.

5. If you selected the **Browse and recover save set** option, complete the **Select Data to Recover** page, otherwise, skip this step:

a. Specify the items to recover in the browse tree or type the full path of a location. Mark which directories or files the wizard will recover in the table.

Note

The wizard does not list expired save sets. You can recover expired save sets manually by using the `nsrsnapadmin` command utility with the `R` command option or the `nsrnassnap_recover` command. Using nsrsnapadmin for NetWorker operations on page 80 and the *EMC NetWorker Command Reference Guide* provide details.

b. Click **Next**.

6. Complete the **Select the Recovery Options** page.

   a. In the **File Path for Recovery** field, select, browse, or type a location where the wizard will restore the recovered files:

      - **Original path**:
        - In-place recovery—Restore to the original location on the NAS device.
      - **New destination path**:
        - Out-of-place recovery—Restore to a different location on the NAS device.
        - Directed recovery—Restore to a location on the NetWorker host that is running the recovery. A directed recovery may specify a location that is configured as a CIFS or NFS file share, which directs the recovery to a remote location.

      Note

      In-place and out-of place recovery on the NAS device is not available for the following devices and conditions:

      - VNX, VNX2, and VNXe devices.
      - Isilon devices for a remotely replicated snapshot.
      - NetApp recovery of an entire directory or save set. You may recover one or more files, provided the files do not make up the entire contents of a directory.

      Examples of snapshot recovery on page 22 illustrates the recovery options.

   b. In the **Duplicate file options** field, specify how the wizard resolves conflicts in file names or directory names:

      - **Rename the recovered file**—The wizard recovers the file or directory with a new name that NetWorker automatically generates. This option is available for directed recoveries only.
      - **Do not recover the file**—The wizard does not recover the file or directory, but skip it.
      - **Overwrite the existing file**—The wizard replaces the file content or the directory content.
      - **Fail the recover**—The wizard does not recover any further files or directories. This option is not available for directed recoveries.

      Note

      For NetApp devices, select an option, otherwise the recovery fails.

c. To specify further options, select **Advanced Options** and specify the attributes.

Note

For a Remote Replication recovery, specify `-R` in the extra recovery options.

d. Click **Next**.

7. Complete the **Perform the Recover** page:

a. In the **Recovery Name** field, type a name for the recovery.

b. In the **Recovery Start Time** field, specify the following attributes:

- **Start recovery now** is the only option that snapshot recovery supports.
- In **Specify a hard stop time**, you can specify a time limit that stops an incomplete recovery process.

c. In the **Recovery Resource Persistence** field, select the retain or delete option for this recovery resource:

- **Persist this resource until deleted by user**
- **Automatically remove this resource based on jobs database retention**

d. Review the **Summary** of the recovery and make any necessary corrections by going to the previous pages in the wizard.

e. Click **Run Recover**.

The wizard performs the recovery. The *EMC NetWorker Administration Guide* provides more details on the NMC Recovery Wizard.

APPENDIX A

Application Information Variables

This appendix includes the following topic:

- Using Application Information variables 78

Using Application Information variables

As part of the manual configuration of a NAS device, some NetWorker configurations require the use of special variables that provide specific control of snapshot processes.

To implement these controls, type the variables and their values in the Application Information attribute of the Client resource for the NAS device.

Configuring the Client resource manually for the NAS device on page 68 provides the manual configuration procedure that can include Application Information variables.

Common Application Information variables

The following table lists Application Information variables that are common to the NAS devices that NetWorker supports.

Table 12 Common Application Information variables

Common variable	Definition
NASDeviceType	Specifies the snapshot provider. Usually not required due to device type discovery. Valid values are Isilon, NetApp, VNX, and VNXe. If you do not specify a value, NSM tries each of these values in order.
NSR_DEBUG_LEVEL	Specifies the verbosity of error message logs. Valid values are 0 to 9. The default value is 0.
NSR_MOUNTPOINT_NAME	This variable is mandatory to restore from NetApp replications. Specifies the name of the mount point to use when NetWorker needs to mount a snapshot on a client.
NSR_POST_SNAPSHOT_SCRIPT	Specifies the pathname of the postprocessing command script. There is no default value.
NSR_PRE_SNAPSHOT_SCRIPT	Specifies the pathname of the preprocessing command script. There is no default value.
NSR_PS_RECOVER_FILE_OPT=(N/R/Y)	Specifies options to handle duplicate file behavior on recover. Options are: • N (skip, do not overwrite) • R (rename) • Y (overwrite)
NSR_USE_EXISTING_MOUNTPOINT	Specifies use of an existing mount point instead of creating a temporary mount point. Not available for NetApp on Linux. The default value is No.
NDMP_MNT_HOST	Specifies the name of the remote host when you configure remote replication backups on Isilon or NetApp filers.

APPENDIX B

Command-Line Operations for NAS Recovery

This appendix includes the following topics:

- Using CLI commands for NetWorker operations 80
- Using nsrsnapadmin operations 80
- Querying with the mminfo command 83
- Using nsrnassnap_recover operations 83

Using CLI commands for NetWorker operations

This appendix provides a summary of CLI commands and examples for NetWorker operations.

The *EMC NetWorker Command Reference Guide* and NetWorker man pages provide details on the commands.

NAS snapshot commands

You can use the following commands for managing NetWorker NAS snapshots:

- `nsrnassnap`
- `nsrnassnap_discover`
- `nsrnassnap_recover`
- `nsrnassnap_save`
- `nsrnassnapck`
- `nsrnassnap_index`

The NetWorker man pages and the *EMC NetWorker Command Reference Guide* provide details.

Using nsrsnapadmin operations

You can run the `nsrsnapadmin` command utility in interactive mode to query, recover, delete, and expire file system snapshot save sets.

Note

The `nsrsnapadmin` interactive commands support only snapshots of file systems. The commands do not support the snapshots of application data, such as NMDA or NMSAP data.

To start interactive mode, type `nsrsnapadmin` at the CLI prompt. When you receive an input prompt, you can type a specific command and its available options to perform the NetWorker options that are listed in the following table.

Table 13 Commands and options that are supported in nsrsnapadmin interactive mode

NSM operation	Command and available options
Display snapshot save sets	`p` [-s *nsr_server*] [-c *client*] [-v] [*path* | -S *ssid*]
Delete a snapshot save set	`d` [-s *nsr_server*] [-c *client*] [-v] [-a] [-y] -S *ssid* [or -S "*ssid ssid* ..."]
Perform a save set recovery	`R` [-s *nsr_server*] [-c *client*] [-M *mount_host*] [-v] -S *ssid* [-t *destination*] [-T *recover_host*] -m *path* [-A attr=*val*]
Perform a file-by-file browsing and recovery	`r` [-s *nsr_server*] [-c *client*] [-M *mount_host*] [-T *recover_host*] -S *ssid* [-A attr=*val*]

Table 13 Commands and options that are supported in nsrsnapadmin interactive mode (continued)

NSM operation	Command and available options
Reset the expiration time for a snapshot save set	`e` *time* [-s *nsr_server*] [-c *client*] [-v] -S *ssid* [or -S "*ssid ssid* ..."]
Exit the program	`q` or `quit`

where:

- *nsr_server* is the hostname of the NetWorker server.
- *client* is the name of the NAS device.
- *mount_host* is the hostname of the mount host.
- -v is for verbose logging.

The *EMC NetWorker Command Reference Guide* and NetWorker man pages provide details.

Example nsrsnapadmin operations

After you start the `nsrsnapadmin` utility in interactive mode, you can type a specific command and its options at the input prompt to perform an NSM operation. The following sections provide examples of the commands and options that are used for specific NSM operations.

Querying snapshot save sets

When you type the `p` command and its options at the `nsrsnapadmin` prompt, the program queries the NetWorker server for snapshot save sets for the client. The program lists specific properties of the snapshot save sets, such as the creation time and the date of each snapshot. For example:

`p -s server -c client [-v] path`

where:

- *server* is the hostname of the NetWorker server.
- *client* is the hostname of the NAS device.
- *path* is the pathname of a particular snapshot save set. Type the pathname to query a single save set only. Otherwise, the output message lists all the save sets.

A message similar to the following appears:

```
nsrsnapadmin> p -c isilon-1.myorg.com
  ssid = 643255862  savetime="4/16/2014 11:05:02 AM"
(1397660702)   expiretime="4/17/2015 9:41:59 AM"
(1429278119)   ssname=/ifs/data
```

File-by-file browsing and recovery

When you type the `r` command and its options at the `nsrsnapadmin` prompt, the program lists the file system as it existed at the time of the snapshot backup. Options enable you to browse, select, and recover the elements of the file system. For example:

```
r -s server -c client -M mount_host -T recover_host -S ssid
```

where *client* is the name of the NAS device.

Deleting a snapshot save set

Deleting a snapshot save set is similar to deleting a standard NetWorker save set. The `nsrsnapadmin` command deletes the physical snapshot from the NAS device and deletes all save sets that refer to that physical snapshot from the media database.

For example:

```
nsrsnapadmin -d -s server -c client -S ssid
```

where:

- *server* is the hostname of the NetWorker server.
- *client* is the name of the NAS device.
- *ssid* is the snapshot save set ID.

You can also use the `nsrnassnapck` command to delete a snapshot.

Modifying retention periods of a snapshot save set

To modify the expiration date of a snapshot, type the `e` command at the `nsrsnapadmin` prompt. For example:

```
e time -s server -c client -S ssid
```

where:

- *time* is the date and time when the snapshot save set will expire.
  Acceptable date and time formats are as follows:
  - mm/dd[/yy]
  - month_name dd[/yy]
  - hh[:mm[:ss]] [meridian] [zone]
  - hhmm [meridian] [zone]
- *server* is the hostname of the NetWorker server.
- *client* is the hostname of the NAS device.
- *ssid* is the ID of the snapshot save set you want to modify.

A message similar to the following appears:

```
Resetting expire time for ssid : 4090300235
```

The message indicates that you have successfully changed the expiration time.

Note

- If you omit the year, the year defaults to the current year.
- If you omit the meridian, NetWorker uses a 24-hour clock.
- If you omit the time zone (for example, GMT), NetWorker uses the current time zone.
- If you specify a date mm/dd/yy as in -e 09/04/13, the time defaults to 00:00:00. NetWorker changes the snapshot save set browse and retention times to 09/04/13 00:00:00.
  If you specify a time hh:mm:ss as in -e 20:00:00, the date defaults to the system time, for example, 09/03/13. NetWorker changes the snapshot save set browse and retention times to 09/03/13 20:00:00.

Querying with the mminfo command

Another way to query a client's snapshot save sets is with the `mminfo` command. The `-q snap` option lists all snapshot save sets for a particular client. It is also possible to query for snapshots in two other ways:

- **`mminfo -qsnap -r "queries specification"`** (Sample query specification: **`-r "ssid, savetime, name"`**) Also, **`mminfo -c <client name> -r "<query specification>"`**
- **`-ot`** or **`-on`** can also be added to display in time based order or alphabetical order based on the save set name.

To list the snapshot save sets for a client, type the following at the command prompt:

```
mminfo -s server -S -a -q "client=clientname,snap"
```

where:

- *server* is the hostname of the NetWorker server.
- *clientname* is the hostname of the NAS device.
  Example output:

```
mminfo -a -q"client=isilon-1.emc.com,snap" -r "ssid,savetime,name”
ssid        date   name
4259966917 1/29/2014 /ifs
643255862  4/16/2014 /ifs/data
609701430  4/16/2014 /ifs/data/folders
1700220469  1/6/2013 /ifs/data/folders/anne
2736137348  3/4/2014 /ifs/data/linux
576146998   5/7/2012 /ifs/data/amsr_jr
1633111605  2/5/2014 /ifs/localtgt/2
777473590  3/28/2014 /ifs/localtgt/2
```

The *EMC NetWorker Command Reference Guide* and NetWorker man pages provide details on the `mminfo` command.

Using nsrnassnap_recover operations

You can use the `nsrnassnap_recover` command to recover save set files and directories.

When specifying the file or directory to recover, directories must end with a slash character (/).

For example:

Single file:

```
nsrnassnap_recover -S file123 -s nas456.lss.cor.com -c
file789.lss.cor.com -d d:\recover\7777 -A NSR_PS_FILE_RECOVER_OPT=Y -A
NSR_DIRECTED_RECOVER_HOST=file1133 -G9 /vol/jjr4/test1.xml
```

Entire directory tree:

```
nsrnassnap_recover -S file123 -s nas456.lss.cor.com -c
file789.lss.cor.com -d d:\recover\7777 -A NSR_PS_FILE_RECOVER_OPT=Y -A
NSR_DIRECTED_RECOVER_HOST=file1133 -G9 /vol/jjr4/
```

The recovery options for the `-A NSR_PS_FILE_RECOVER_OPT=(Y/N/R)` command are as follows:

- Y = Overwrite the file or directory
- N = Skip the file or directory
- R = Rename the file or directory

Note

For NetApp devices, a recovery option must be specified, otherwise the recovery fails. For Isilon and NetApp devices, specify **-R** remote hostname option to recover from a remote replication backup.

APPENDIX C

Snapshot limitations

This appendix includes the following topics:

- NAS snapshot support and limitation 86
- Device-specific limitations for snapshot recovery 86

NAS snapshot support and limitation

For backup and recovery operations the following limitations apply:

- LINUX systems must use NFS exports.
- Microsoft Windows systems must use CIFS exports.

Note

On Windows systems, a file share connection cannot exist between the Windows system running the recovery and the NAS device with the stored data.

Device-specific limitations for snapshot recovery

The following tables list the snapshot recovery limitations and the support specific to each of the supported NAS devices. Restore from clone copies is supported on all supported platforms.

Table 14 Device limitations and support for snapshot management

NAS device	Limitation
Isilon	• Remote replication does not support in-place recoveries and out-of-place recoveries. • Renaming the data is supported only for directed recovery. • Directed recoveries overwrite an existing file. **Note** You must add *NDMP_MNT_HOST=remote device* to the application variables before a save, for a NDMP recovery to be successful. **Note** For Isilon and NetApp remote replication NDMP recoveries, you must enter the – R with the source filer specified in the extra recovery options.
VNX/ VNX2	• In-place recoveries and out-of-place recoveries are not supported. • Renaming the data is supported only for directed recovery. • Directed recoveries overwrite an existing file.
VNXe	• In-place recoveries and out-of-place recoveries are not supported. • Renaming the data is supported only for directed recovery. • Recovery of NFS volumes on Windows systems is not supported. • Recovery of CIFS volumes on Linux systems is not supported. • Directed recoveries overwrite an existing file.
NetApp	• In-place recoveries and out-of-place recoveries restore selected files only. NetApp does not restore directory structures.

Table 14 Device limitations and support for snapshot management (continued)

NAS device	Limitation

	• To enable selected file-by-file (FBF) recovery from snapshot replications, you must specify the NSR_MOUNTPOINT_NAME variable.
	-A NSR_MOUNTPOINT_NAME=*source_volume*
	Using application information variables on page 78 provides details.
	• If a recovered file exists at the recovery destination then you must specify an overwrite option:
	▪ For NMC Recovery Wizard recovery, select an overwrite option.
	▪ For CLI recovery, when you issue the recover command, you must specify an overwrite option in the `nsrsnapadmin` prompt, for example:
	-A NSR_PS_FILE_RECOVER_OPT=Y
	Windows example:
	`nsrsnapadmin> r -S 3895199998 -T 10.13.999.99`
	`Current working directory is /vol/win_bang/`
	`snaprecover> add NetWorkerEXT.XML.old`
	`1 file(s) marked for recovery`
	`snaprecover> recover -A NSR_PS_FILE_RECOVER_OPT=Y`
	• On Linux operating systems, NetApp devices cannot use a temporary mount point for in-place or out-of-place recovery:
	▪ Ensure the NSR_MOUNTPOINT_NAME variable is set.
	▪ For NMC Recovery Wizard recovery, in the **Browse and recover save set** step, ensure that **Create temporary mount point for access** is not selected.
	▪ For CLI recovery, when you issue the recover command, in the `nsrsnapadmin` prompt, you must specify that you will use the existing mount point.
	-A NSR_USE_EXISTING_MOUNTPOINT=Yes
	Linux example:
	`nsrsnapadmin> r -S 4046199999 -A`
	`NSR_USE_EXISTING_MOUNTPOINT=yes`
	`-A NSR_MOUNTPOINT_NAME=/vol/arnab -T 10.13.999.99`
	`Current working directory is /vol/arnab/`
	`snaprecover> cd dir1`
	`snaprecover> add file1`
	`1 file(s) marked for recovery`
	`snaprecover> recover -A NSR_PS_FILE_RECOVER_OPT=Y`
	• On Linux systems, renaming the recovery data is not supported for in-place or out-of-place recoveries. Renaming the data is supported only for directed recovery.

Table 14 Device limitations and support for snapshot management (continued)

NAS device	Limitation
	Note You must add NDMP_MNT_HOST=*‹remote device›* to the application variables before a save, for a NDMP recovery to be successful. For NDMP recovery using a NetApp Cluster Mode system, in the Recovery Configuration wizard, on the **Select the Recovery Options** window, select the **New destination path** option. You must specify: ***/vserver name/volume name***. If you are using the command line option using the CLI, specify: ***-m /vserver name/volume name***. Only for remotely replicated NDMP recoveries, the `-R` command is required. For example: **`nsrndmp_recover -c <client name>-s <server> -m /<Vserver name>/<volume name> -S <ssid> -R <source vserver>`** **Note** For Isilon and NetApp remote replication NDMP recoveries, type **`-R`** with the source filer specified in the extra recovery options.

Table 15 Device support for recovery of save sets and individual files

Recovery from snapshot	Isilon	Isilon local replication	Isilon remote replication	NetApp	VNX	VNX2	VNXe
Directed recovery of save set	Yes	Yes	Yes	Not applicable	Yes	Yes	Yes
In-place recovery of save set	Yes	Yes	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Out-of-place recovery of save set	Yes	Yes	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Directed recovery of individual files	Yes	Yes	Yes	Yes	Yes	Yes	Yes
In-place recovery of individual files	Yes	Yes	Not applicable	Yes	Not applicable	Not applicable	Not applicable
Out-of-place recovery of individual files	Yes	Yes	Not applicable	Yes	Not applicable	Not applicable	Not applicable

Table 16 NetApp support for types of local replication and platforms

Local replication 7-mode	SnapVault (Windows)	SnapMirror (Windows)	SnapVault (Linux)	SnapMirror (Linux)
Backup	Yes	Yes	Yes	Yes
PIT restore from CLI				
FBF directed restore	Yes	Yes	Yes	Yes
FBF in-place restore	Yes	No	Yes	No
FBF out-of-place restore	Yes	No	Yes	No
PIT restore from GUI				
FBF directed restore	Yes	Yes	Yes	Yes
FBF in-place restore	Yes	No	Yes	No
FBF out-of-place restore	Yes	No	Yes	No
PIT restore from clone copy				
In-place restore from clone copy	Yes	Yes	Yes	Yes

Note

For C-mode local replication clones, enable **Node Scope Mode** on the Netapp filer.

Table 17 NetApp C-Mode local replication and platforms

Local replication C-mode	SnapVault (Windows)	SnapMirror (Windows)	SnapVault (Linux)	SnapMirror (Linux)
Backup	No	Yes	No	Yes
PIT restore from CLI				
FBF directed restore	No	No	No	No
FBF in-place restore	No	No	No	No
FBF out-of-place restore	No	Yes	No	Yes
PIT restore from GUI				
FBF directed restore	No	No	No	No
FBF in-place restore	No	No	No	No
FBF out-of-place restore	No	Yes	No	Yes
PIT restore from clone copy				
In-place restore from clone copy	No	Yes	No	Yes

Table 18 NetApp support for types of remote replication and platforms

Remote replication NetApp	SnapVault (Windows)	SnapMirror (Windows)	SnapVault (Linux)	SnapMirror (Linux)
Backup	Yes	Yes	Yes	Yes
PIT restore from CLI				
FBF directed restore	Yes	Yes	Yes	Yes
FBF in-place restore	Yes	Not applicable	Yes	Not applicable
FBF out-of-place restore	Yes	Not applicable	Yes	Not applicable
PIT restore from GUI				
FBF directed restore	Yes	Yes	Yes	Yes
FBF in-place restore	Yes	Not applicable	Yes	Not applicable
FBF out-of-place restore	Yes	Not applicable	Yes	Not applicable
PIT restore from clone copy				
In-place restore from clone copy	Yes	Yes	Yes	Yes

GLOSSARY

This glossary contains the definitions of terms used in this guide.

B

backup

1. Duplicate of database or application data, or an entire computer system, stored separately from the original, which can be used to recover the original if it is lost or damaged.
2. Operation that saves data to a volume for use as a backup.

backup volume A volume used to store backup data. NetWorker backup data cannot be stored on an archive volume or a clone volume.

browse policy NetWorker policy that specifies the period of time during which backup entries are retained in the client file index. Backups listed in the index are browsable and readily accessible for recovery.

C

client Host on a network, such as a computer, workstation, or application server whose data can be backed up and restored with the backup server software.

client file index Database maintained by the NetWorker server that tracks every database object, file, or file system backed up. The NetWorker server maintains a single index file for each client computer. The tracking information is purged from the index after the browse time of each backup expires.

client-initiated backup See manual backup.

Client resource NetWorker server resource that identifies the save sets to be backed up on a client. The Client resource also specifies information about the backup, such as the schedule, browse policy, and retention policy for the save sets.

clone

1. Duplicate copy of backed-up data, which is indexed and tracked by the NetWorker server. Single save sets or entire volumes can be cloned.
2. Type of mirror that is specific to a storage array.

cluster Group of linked virtual or physical hosts, each of which is identified as a node, with shared storage that work together and represent themselves as a single host.

consistent State of a data set that fully matches an application's active view of the data at any point in time.

Console server See NetWorker Management Console (NMC).

D

datazone Group of clients, storage devices, and storage nodes that are administered by a NetWorker server.

device
1. Storage folder or storage unit that can contain a backup volume. A device can be a tape device, optical drive, autochanger, or disk connected to the server or storage node.
2. General term that refers to storage hardware.
3. Access path to the physical drive, when dynamic drive sharing (DDS) is enabled.

F

file index See client file index .

file system
1. Software interface used to save, retrieve, and manage files on storage media by providing directory structures, data transfer methods, and file association.
2. Entire set of all files.
3. Method of storing files.

G

group One or more client computers that are configured to perform a backup together, according to a single designated schedule or set of conditions.

H

host Computer on a network.

hostname Name or address of a physical or virtual host computer that is connected to a network.

L

live backup See rollover-only backup

logical unit (LUN) Logical storage space on a storage array that is addressed by SCSI or Fibre Channel protocols. Multiple LUNs can be used to represent a storage volume.

logical volume manager (LVM) Software that controls disk resources by mapping data between a logical view of storage space and the actual physical disks.

M

manual backup Backup that a user performs from the client, also known as an unscheduled, on-demand, or ad hoc backup.

media Physical storage, such as a disk file system or magnetic tape, to which backup data is written. **See** volume.

media database Database that contains indexed entries of storage volume location and the life cycle status of all data and volumes managed by the NetWorker server.

mirror
1. Exact duplicate of data or another object, such as a disk.
2. To write duplicate data to more than one device.

mount To make a volume physically available for use, such as the placement of a removable disk volume or tape into a drive for reading or writing.

mount host Host in a network that is used to mount storage array snapshot volumes to perform snapshot restore and rollover operations.

N

network attached storage (NAS) Disk array or storage device (NAS filer) that connects directly to the messaging network or LAN interfaces and uses the common communication protocols of TCP/IP or NDMP.

Network Data Management Protocol (NDMP) Software component that uses TCP/IP standards to specify how heterogeneous network components communicate for the purposes of backup, recovery, and transfer of data between storage systems.

NetWorker Management Console (NMC) Software program that is used to manage NetWorker servers and clients. The NMC server also provides reporting and monitoring capabilities for all NetWorker processes.

NetWorker server Computer on a network that runs the NetWorker server software, contains the online indexes, and provides backup and restore services to the clients and storage nodes on the same network.

NetWorker Snapshot Management (NSM) EMC technology that provides point-in-time snapshot copies of data. NetWorker software backs up data from the snapshot. This allows applications to continue to write data during the backup operation, and ensures that open files are not omitted.

P

point-in-time copy (PIT copy) Fully usable copy of a defined collection of data, such as a consistent file system, database, or volume that contains an image of the data as it appeared at a specific point in time. A PIT copy is also called a snapshot or shadow copy.

policy Set of defined rules for client backups that can be applied to multiple groups. Groups have dataset, schedule, browse, and retention policies.

pool
1. NetWorker sorting feature that assigns specific backup data to be stored on specified media volumes.
2. Collection of NetWorker backup volumes to which specific data has been backed up.

Q

quiesce State in which all writes to a disk are stopped and the file system cache is flushed. Quiescing the database prior to creating the snapshot provides a transactionally consistent image that can be remounted.

R

recover To restore data files from backup storage to a client and apply transaction (redo) logs to the data to make it consistent with a given point-in-time.

resource Software component whose configurable attributes define the operational properties of the NetWorker server or its clients. Clients, devices, schedules, groups, and policies are all NetWorker resources.

restore To retrieve individual data files from backup media and copy the files to a client without applying transaction logs.

retention policy NetWorker setting that determines the minimum period of time that backup data is retained on a storage volume and available for recovery. After this time is exceeded, the data is eligible to be overwritten.

rollback restore Process by which a snapshot is restored to its source location by using the capability of the storage array. A rollback restore destroys existing data on the source location.

rollover Backup of a snapshot to conventional storage media, such as disk or tape. Previously known as a live backup.

rollover-only backup Rollover whereupon the snapshot copy is deleted. Previously known as a serverless backup, live backup, or nonpersistent backup.

S

save set

1. Group of tiles or a file system copied to storage media by a backup or snapshot rollover operation.
2. NetWorker media database record for a specific backup or rollover.

save set ID (ssid) Internal identification number assigned to a save set.

scheduled backup Type of backup that is configured to start automatically at a specified time for a group of one or more NetWorker clients. A scheduled backup generates a bootstrap save set.

snapshot Point-in-time, read-only copy of specific data files, volumes, or file systems on an application host. Operations on the application host are momentarily suspended while the snapshot is created on a proxy host. Also called a PiT copy, image, or shadow copy.

snapshot backup Snapshot created on a storage array as a backup. Previously called instant backup.

snapshot mount host See mount host.

snapshot policy Sets of rules that control the life cycle of snapshots. These rule specify the frequency of snapshot creation, how long snapshots are retained, and which snapshots will be backed up to conventional storage media.

snapshot restore Restore from a snapshot backup. Previously called instant restore.

snapshot save set Group of files or other data included in a single snapshot. Previously called a snapset.

source LUN LUN on the application host, whose production data can be copied by snapshot.

specific point-in-time (SPIT) copy RecoverPoint term for PIT copy. **See** point-in-time copy (PIT copy).

storage array Integrated collection of subsystem disks, controllers, bus adapters, and software that provides storage services to one or more hosts.

storage node Computer that manages physically attached storage devices or libraries, whose backup operations are administered from the controlling NetWorker server. Typically a “remote” storage node that resides on a host other than the NetWorker server.

T

target client NetWorker client on which data is to be restored This may be the same as the original source client from which the data was backed up, or it may be a different client.

V

volume

1. Unit of physical storage medium, such as a disk or magnetic tape, to which backup data is written.
2. Identifiable unit of data storage that may reside on one or more computer disks.

volume group Logical group that contains sets of disks, as configured by a volume manager.